IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 2 (February. 2019), ||S (III) || PP 64-71

A Secure Off-line Micro-payment For an E-commerce System

Dr K.Shirisha, S.Sravanya
Sreenidhi Institute of Science and Technology, Hyderabad.
Corresponding Author: Dr K.Shirisha

Abstract- The wider reach of the internet and it's easy to use has promoted online shopping in India develop at a rapid pace and is existing to grow exponentially. Credit and debit cards' data are largely used by the transacting customer for online payments. The personal and secure data of these cards are at risk of losing its confidentiality and privacy due to the number of reasons. Primarily, the adversary would steal the information by targeting the Point of Sale(POS) system after installing and executing the malware software. At times, a network connection remains unavailable due to network service disruption. The data breaches that take place are mainly in the online mode of payment, thereby leading to insecure online payment. This paper describes a secure off-line micro-payment solution for an e-commerce system that is able to withstand the point of sale data breaches. A thorough analysis of its architecture, components and security properties is provided. This solution addresses the shortcomings observed in the current practices of online payments, thereby offering flexibility and security and provide secure fully off-line micro-payment.

Keywords: Offline Payment, the point of sale tractions, coin element, identity element.

Date of Submission: 15-02-2019 Date of acceptance: 04-03-2019

I. INTRODUCTION

Over the last decade, due to the growing speed of the internet where people used to buy and sell their products online. The adoption of technology is enabling the e-commerce sector to be more reachable and efficient. Stealing payment card data has become an everyday crime that gives quick monetary gains. The main of the goal of an attacker is to steal the data stored on the magnetic stripe of payment cards to create clones. There several routes that an attacker tries to steal the data, by gaining access to a database where payment card information is stored or by targetting the point-of-sale system where the customer store the personal data at retailer first. The points of sale (POS) systems are connected to a network to contact to an external server that is required to authenticate the customer transaction. The larger business organizations are interested to tie their point of sale with the other back-end systems which may connect the point of sale system to their own internal networks. These internal networks are used to reduce costs and to improve performance. However, such an online solution is not very efficient, because the remote communication over the network may be delayed in the transaction process due to lack of network coverage or temporary network service disruption.

II. LITERATURE SURVEY

Vanesa Daza and Robert Di Pietro [1] introduced a micropayment system in which all the parties that are involved can be off-line. It completely depends upon the local data for performing the operations that are requested. The system uses digital credit, i.e. prepaid coins that can be spent only once. It requires scratch card that can be inserted into any device which can read SD cards and no other special hardware is required. Digital credits that are used in this model are digital version of real cash and are linked to cardholder only. Unique to other payment solutions that depend upon the hardware which is temper proof, FORCE presumes that the chips built upon PUF's only can utilize the tamper evidence feature provided by the PUFs themselves. Depending upon the data obfuscation it provided weak prevention strategy.

Ronald L. Rivest, Adi Shamir [2], proposed two simple micropayment methods, pay word and micro mint. Payword is a credit based scheme that used to minimize communication with the third parties. It does not require the merchant to interact with the third parties for each payment transaction.

The merchant needs to clear the payment once a day. MicroMint is a debt-based scheme which makes use of coin element, the third party produces the coins and sell it to the user. Then the user uses these coins to pay for the merchant for the payment transaction. Larger payments will not be processed using these schemes. High investment is required to generate the coins.

Sergio Martins and Yang Yang[3], introduced a bitcoins. Bitcoin is a digital currency that is based on coins and coin ownership verification. In which online payments of digital currency are done from one person to another without the involvement of third-party institutions. A computer network system supervises the bit coin

payments, approves and records the transactions. When bit coin payment is made, an instruction regarding payment is sent to the network. In the network, the computers validate the instruction and inform it to other computers. Payment then gets updated in one of the block and added to the bit coin block chain file on all the systems in the network.

Miyazaki and Sakurai have analyzed the attacks that will occur inside the e-cash system from unauthorized user based on existing system. He has taken a security measures such as audit and logging techniques to identify double spending in the e-cash system. This system follows Chaum-Fiat-Naor (CNF) paradigm to identify double spending of electronic cash, where customer can spend e-cash only once without interacting with the bank. In these they have explained about transaction of electronic cash securely in offline with certain secure measures to inside attacks that occur from the unauthorized persons,

III. CLASSIFICATION OF POS BREACHES

The widely used context of an e-commerce establishment is shown in the Fig.1. Network setup for the PoS Systems. Point of sale (POS) systems is not very secure, because they are connected to a network and exposed the location. Point of sale (POS) stores important data and these data is being handled from remote server, a typical situation for corporate environments that executes software package management solutions. Some standards established by Industry-established standards such as the PCI Data Security Standards (DSS) are used to set up and ensure that the systems that handle important data to remain safe from unauthorized, but it only have one weakness that the network is infiltrate.

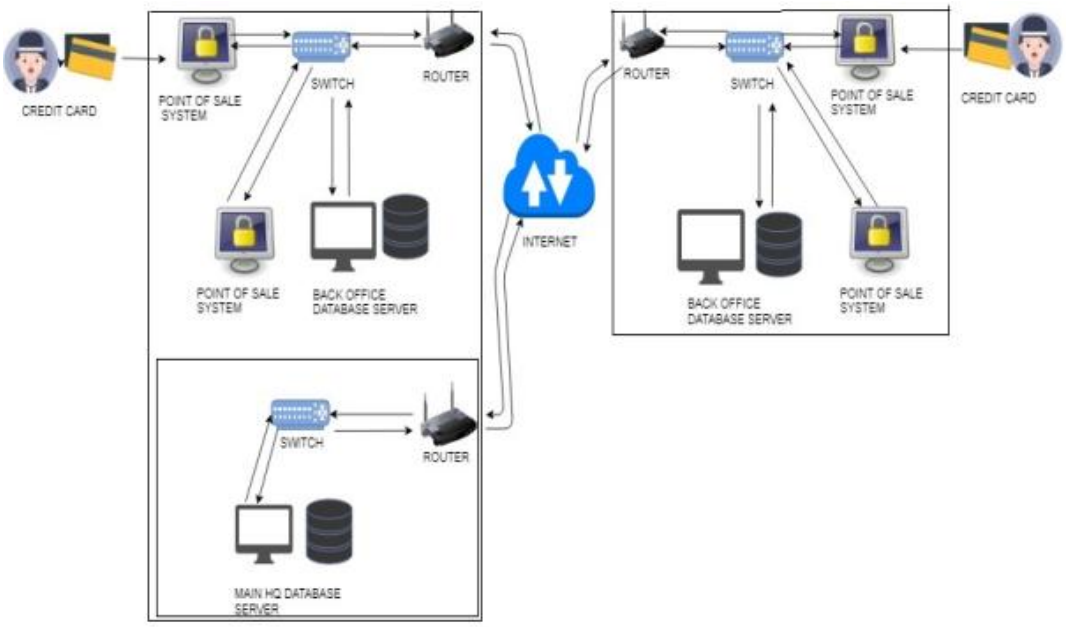


Figure 1 Network setup for POS System

3.1 POS System breaches

Infiltration: An attacker can gain to access to the network by looking at defaults in the external systems by using SQL injection on a web location. Another way the attacker can attack is by sending a spear-phishing email (contain a malicious attachment that will install onto the victim's computer).

Network Traversal or propagation: An attacker must gain access to an associated network. Then they must traverse the network, ultimately to reach the point of sale systems and approach them.. Attackers make use of different techniques to reach the network in order to point out the point of sale systems. They may obtain administrative-level credentials and also get a control of a domain controller that allow complete access to all the computers in the network. So that they can reach the cardholder data environment.

Aggregation: Once gaining access to the CDE, then the attacker can install malicious software in the POS systems, to reach and use the customer information.

Data Exfiltration: All the point of sale system requires some external network connection from which attacker steal the data and these data can be sent to an internal back office waiting for the attacker to be back.

3.2 POS Device Breaches

In an electronic payment system, the POS device plays an important role. The point of sale system is protected by an employee during their executing time so that the reaching to POS device and installing malware

into it is difficult for an attacker though still very do able. To reach the POS system, the attacker takes a discontented employee or a well-disguised attacker. Attackers can also use the advantage of "self-service" terminals and POS system locations that are not as closely examined as other stations.

IV. THREATS AND ATTACKS

The attacker aimed at threatening customer sensitive data by injecting malicious software and changes the messages being transferred between the user and the merchant. Attacker will try to steal user information by aiming the point of sale system. In addition, there are most relevant attacks that take place at the PoS system are:

Denial-of-Service (DOS): It is an attack in which attacker tries to temporarily disrupt the network services of the host which is connected to the internet to make network resources unavailable to the user.

Structured Query Language Injection: It is an attack where an attacker inserts a malicious Sql code that is attached to an application to the backend database. Then these malicious data forces it reveal the information.

Skimmers: Skimmers are devices that fraudulently collect customer card information when the card is used at the point of sale system. The user card device which is inserted into point of sale system is displacing with the duplicate device to get user card information.

RAM Scrapers: It is malware that scans the memory of digital devices, particularly point-of-sale systems to collect customer sensitive information. Then, they usually encrypt the stolen data and place it somewhere on the POS device network still they are exfiltrated.

Offline authentication: It is an attack, where an attacker utilizes the denial of service attack that forces the point of sale system to be offline. So, the payment card data at the PoS system is being processed locally by allowing an attacker to easily collect required data.

Sniffing: An attacker examine the network traffic to intercept the data being transferred. An attacker can read the data from the network packet being transferring on the network by using sniffer.

Spoofing: In this attack, the attacker attempts to gain unauthorized access to a user's system by pretending as a user.

V. PROPOSED MODEL OF SECURE OFFLINE MICROPAYMENT SOLUTION FOR AN E-COMMERCE SYSTEM

In these, we have introduced a solution, which is based upon strong physical unclonable functions (PUF) i.e, the device physical properties not able to be replicated. These device properties are distinct to those devices that are utilized for validation purpose. The secure offline micropayment solution for an e-commerce system that is able to withstand a point of sale data breaches. Coin values used in these models are simply digital form of a cash, which are not linked to anybody other than the user.

A secure offline micropayment solution do not need specific USB device other than a identity element and the coin element, which would be either attached to a user device or directly enclosed into the device. Therefore, the identity element and coin element are thought of tamper-proof devices with a secure execution and storage of delicate data.

5.1 Architecture of a secure offline micro-payment system:

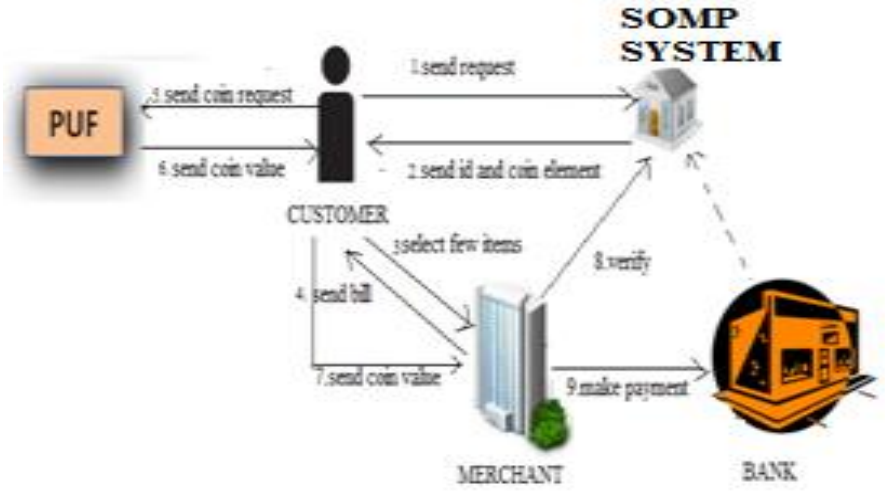


Figure 2 architecture of a secure offline micropayment system

The design of a secure offline micropayment solution is designed with two important elements they are identity element and the coin element. A coin element can be any hardware device that is enclosed with in a physically unclonable function (i.e., USB drive or an SD card) where physical properties of the device cannot be replicated. The coin element is used to generate coin value and this coin value is transmitted securely by encrypting it. The identity element is enclosed with the user device and it is used to match a coin element to a particular user.

The process of these systems, where the customer will send a request for an identity element and coin element to the SOMP(secure off-line micro-payment) system. SOMP system will generate identity element and coin element by using key bunch matrix cryptography and issue the identity element and coin element to a customer. Then, the customer will search for a few items and select the items from the merchant. Then, the merchant will generate a bill for those items and send the payment request to the customer. Then the identity element embedded in a customer device will communicate with the coin element internally, which is built on physically unclonable function for coin value. Coin element will generate coin value on-the-fly by using key bunch matrix cryptography and send the coin value with hard-coded ID to the merchant in order to avoid the forgery attacks. Merchant will receive the coin value and send the coin value to the bank in a secure manner.

The design of secure offline micropayment solution provides authentication in two steps process for the user. Indeed, the coin element is linked with particular identity element, it is impossible for an adversary to steal coins and utilize them that belongs to other users.

5.2 Mathematical models used in this proposed system:

Mathematical models used in this system are a block cipher involving key bunch matrix including with another key bunch matrix preceded with XOR operation. E is an encryption key bunch matrix and keys for it are chosen from odd numbers lying between [1-255]. F is an additional key matrix preceded with XOR operator, keys for it are chosen from the integers lying between [0-255]. D is a decryption key bunch matrix is computed with the multiplicative inverse of E.

5.2.1 Cryptographic Key Generation

The cryptographic key generation algorithm is used to generate key element. When a customer sends request to SOMP for identity element and coin element, then the SOMP system will generate identity element and coin element key using cryptographic algorithm. Then SOMP will send the encrypted identity element and coin element to the customer. When the merchant send a payment request to the customer, then the identity element attached to the customer will internally interact with the coin element built on a physically unclonable function. Then the cryptographic key generator within the coin element will compute on-the-fly coin value. This coin value will be sent to the merchant in an encrypted form by using key bunch matrix cryptography. Later the merchant will send the encrypted coin value to the bank.

E is an encryption key bunch matrix and keys for it are chosen odd numbers between [0-255].

$$E = \begin{pmatrix} 119 & 157 & 167 & 87 \\ 41 & 123 & 189 & 177 \\ 177 & 155 & 79 & 225 \\ 197 & 95 & 209 & 151 \end{pmatrix} \qquad (5.1)$$

The decryption matrix keys are computed by selecting keys of encryption matrix in particular manner by using multiplicative inverse in modular arithmetic. d_{ij} is multiplicative inverse of e_{ij} and that are linked by an equation

$$(e_{ij} \times d_{ij}) mod\ 256 = 1$$

i.e, e_{ij} and d_{ij} are odd numbers, lying between interval [1-255].

By using, multiplicative inverse, we get decryption matrix D as

$$D = \begin{pmatrix} 71 & 181 & 23 & 103 \\ 25 & 179 & 149 & 81 \\ 81 & 147 & 175 & 33 \\ 13 & 159 & 49 & 39 \end{pmatrix} \qquad (5.2)$$

5.2.2 Encryption Scheme

The basic equation for encryption of the cipher is given by

$$C = [c_{ij}] = ([e_{ij} \times p_{ij}] mod\ 256) \oplus F,$$
$$i = 1\ ton, \quad j = 1\ ton.$$

Whereas, $C = [c_{ij}], i = 1\ ton,\ j = 1\ ton$ be the ciphertext.

$E = [e_{ij}], i = 1\ ton, j = 1\ ton$ be encryption key bunch matrix.

Algorithm:

1. read n, E, P, F, r
2. For k=1 to r do
   {
3. For i=1 to n do
{
4. For j=1 to n do
{
5. $p_{ij} = ([e_{ij} \times p_{ij}] mod\ 256) \oplus f_{ij}$
   }
}
6. P=[p_{ij}]
7. P=Mix(P)

}

8. C=P
9. write(C)

5.2.3 Decryption Scheme

The equation for the decryption process is in the form

$$P = [p_{ij}] = [d_{ij} \times (C \oplus F)_{ij}] mod 256, i = 1\ ton$$
$$, j = 1\ ton.$$

Where,

$P = [p_{ij}], i = 1\ ton, j = 1\ ton$ be the plain text, $D = [d_{ij}], i = 1\ ton, j = 1\ ton$ be the decryption key bunch matrix,

and, $F = [f_{ij}], i = 1\ ton, j = 1\ ton$be the additional key matrix.

Algorithm:

1. read n, E, C, F, r
2. D=Mult(E)
3. For k=1 to r do
{
4. C=Imix(C)
5. For i=1 to n do
{
6. For j=1 to n do
{
7. $c_{ij} = [d_{ij} \times (c_{ij} \oplus f_{ij}) mod\ 256$
}
}
8. C=[c_{ij}]
}
9. P=C
10. Write(P)

5.2.4 Illustration:

For example,

Consider plaintext, Identity **Element**

By using, EBCDIC code it can be written as:

$$P=\begin{pmatrix} 201 & 132 & 133 & 149 \\ 163 & 137 & 163 & 168 \\ 64 & 197 & 147 & 133 \\ 148 & 133 & 149 & 163 \end{pmatrix} \quad (5.3)$$

And an additional key matrix F is chosen odd numbers lying between [1-255].

$$F=\begin{pmatrix} 147 & 197 & 53 & 139 \\ 79 & 227 & 175 & 163 \\ 209 & 67 & 157 & 137 \\ 187 & 35 & 129 & 215 \end{pmatrix} \quad (5.4)$$

By using E in equation (5.1), P in equation(5.3) and F in equation (5.4) and applying encryption algorithm, and after applying sixteen rounds of iteration process(r=16) ,we get cipher text as

$$C=\begin{pmatrix} 59 & 128 & 170 & 32 \\ 205 & 9 & 41 & 38 \\ 132 & 181 & 146 & 10 \\ 9 & 52 & 138 & 75 \end{pmatrix} \quad (5.5)$$

By using decryption algorithm for the cipher text C, we get result as plaintext P **Identity Element** in equation (5.3).

By changing the value in the 4th row and 4th column of the plaintext P in equation (5.3), from 163 to 162, we can examine avalanche effect as one-bit change in plaintext P. By applying encryption algorithm to it, we get ciphertext C as

$$C=\begin{pmatrix} 51 & 19 & 182 & 50 \\ 39 & 169 & 106 & 180 \\ 214 & 109 & 103 & 28 \\ 220 & 51 & 29 & 64 \end{pmatrix} \quad (5.6)$$

By comparing, (5.5) and (5.6), in their binary form, we can see that this two ciphers differs by 55 bits out of 128 bits. From the above we can conclude that the cipher is expected to be a strong one.

we can also examine avalanche effect by changing one bit in the encryption key matrix E in (5.1). By changing the value in 3rd row, 3rd column from 79 to 78, then we can see one bit change. By applying this encryption matrix E with other matrices P and F from equation (5.3) and (5.4) and applying encryption algorithm, we get the output as the cipher text C.

$$C=\begin{pmatrix} 99 & 107 & 125 & 224 \\ 20 & 96 & 46 & 118 \\ 50 & 89 & 43 & 118 \\ 234 & 59 & 81 & 64 \end{pmatrix} \quad (5.7)$$

By comparing, (5.5) and (5.7) in their binary form, we can see that these two ciphers differs by 69 bits out of 128 bits. From these, we conclude that the cipher is strong one.

For preserving the confidentiality of the coin element across the public network between the interacting entities like customer, e-commerce merchant, bank and SOMP system, the similar cryptographic steps are processed as well with the coin element.

VI. SECURITY ANALYSIS

A secure offline micropayment system makes use of key bunch matrix cryptanalysis that the cipher is expected to be strong one which is not even able to broken by any attack. It is able to withstand with different types of cryptanalytic attacks available such as

Ciphertext-only attack: This attack cannot break this cipher by the brute force attack. In these ciphers, we are chosen one Encryption key bunch matrix E which may include all odd numbers between [0-255] and an additional matrix F which includes all integers between [1-255]. The size of two matrices is of size n that are square matrices. Therefore, the key space size is

$$2^{15n^2} = (2^{10})^{1.5n^2} \approx (10^3)^{1.5n^2} = 10^{4.5n^2} \text{ years} \quad (6.1)$$

Time taken to execute the cipher with one E and F in the key space is 10^{-7} seconds. Then, the time taken to execute the cipher with all the keys in the key space is equal to

$$\frac{10^{4.5n^2} \times 10^{-7}}{365 \times 24 \times 60 \times 60} = 3.12 \times 10^{4.5n^2-15} \text{years.} \quad (6.2)$$

If we take n=4, then the time required for these analyses is

3.12×10^{57} years.

As time taken for these cipher too large, so that the adversary cannot break these cipher by brute force attack.

Known plaintext attack: We know required number of plaintext and cipher text. Let consider iteration process with one round(r=1). Then the equation is given by:

$$P = \left(\left[e_{ij} \times P_{ij}\right] mod\ 256\right) \oplus F, i = 1\ ton,$$

$j = 1\ ton.$ (6.3)

$P = Mix(P)$ (6.4)

and

$$C = P \quad (6.5)$$

Here if we know the value of C, then the value of P is also known in the equation (6.5). Then, the value for P on the left-hand side in equation (6.4) is also known. On applying Imix(), we know P on the right-hand side of the equation (6.4). From these, we know the value of P on the left-hand side in equation (6.3). As the equation (6.3) has two key bunch matrices, where (e_{ij}) =E and F, which contains a mod operator, so, it is impossible to determine them by breaking the cipher. From the above we can conclude that, it is impossible for the attacker to break this cipher with one round of iteration process. Here, we are using sixteen rounds of iteration process, so that the attacker not even breaks the cipher with expected values by this attack.

Chosen plain text attack: An attacker will randomly select the plaintext which would be encrypted and get the cipher text. Here we are choosing random odd numbers as plaintext and using multiplicative inverse in iteration process of each round, so that the attacker will unable to break the cipher using chosen plain text attack.

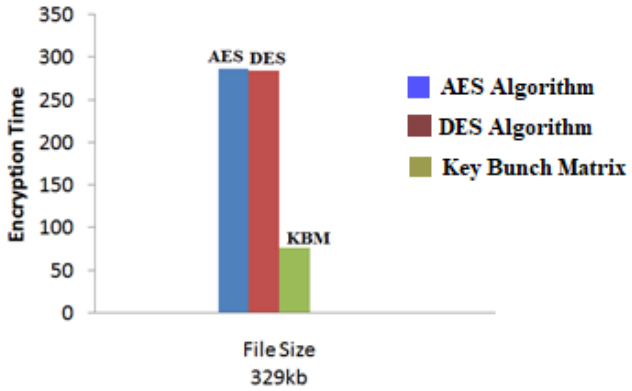
Chosen cipher text attack: This attack is not possible to choose cipher text in manner as required to get the cipher text.

From above, we can conclude the cipher we used in this system cannot be broken by any attack.

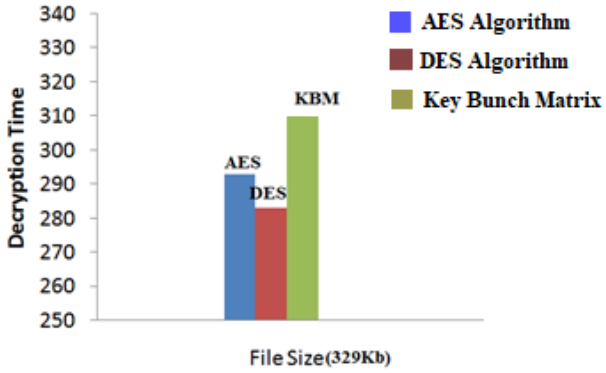
VII. PERFORMANCE ANALYSIS:

The key bunch matrix cryptography used in this system is very strong cipher which cannot be broken. In this cipher, the plaintext is chosen from an odd number randomly. In addition, the change in one bit will differ by many bits which will be unable to expect. By using this cipher we can transfer data in a secure manner. As compared to the DES and AES, this algorithm takes less execution time and takes more time to decrypt the cipher. Therefore, it has better security than DES and AES.

Encryption Execution



Decryption Execution



VIII. CONCLUSION

In this paper, we have introduced a secure offline micropayment solution for an e-commerce system that is able to withstand point-of-sale data breaches. The cryptographic features are embedded to secure the coin element and identity element shared between the interacting parties across the public channel like internet. Thorough analyses of this solution and security properties are provided. This solution addresses the shortcomings observed in the current practices of online payments, thereby offering flexibility and security thereby providing fully secure off-line micropayment.

REFERENCES

[1]. Vanesa Daza, Robert Di Pietro, Flavio Lombardi, Matteo Signorini, "FORCE fully off-line secure credits for mobile micropayments, "2015.
[2]. Ronald L.Rivest, Adi Shamir, "Payword and micro mint: two simple micropayment schemes," 1996.
[3]. Sergio Martins, Yang Yang, "Introduction to bitcoins: a pseudo-anonymous electronic currency system," 2011.
[4]. Miyazaki, K.Sakurai, "Security of offline anonymous electronic cash system against insider attacks by untrusted authorities revisited,"2011.
[5]. V.U.K. Sastry, K.Shirisha, "A block cipher involving a key bunch matrix and including another key matrix supplemented with XOR operation," Oct 2012.
[6]. Sergiy Golovashych, "The technology of identification and authentication of financial transactions from smart cards to NFC terminals," 2005.
[7]. Maria Isabel Gonzalez Vasco, Somayeh Heidarvand, Jorge L. Villar, "Anonymous subscription schemes a flexible construction for online services access," Jan 2012.
[8]. Vorugunti Chandra Sekhar, S Mrudula, "A complete secure customer centric anonymous payment in a digital ecosystem," March 2012.
[9]. Kiran S. Kadambi, Jun Li, Alan H. Karp, "Near field communication-based secure mobile payment service," 2009.
[10]. Trend Micro Incorporated, "Point-of-sale system breaches threats to the retail and hospitality industries," Technical report 2014.
[11]. Helena Handschuh, Geert-Jan Schrijen, Pim Tuyls, "Hardware Intrinsic Security from Physically Unclonable Functions," Oct 2010.

Dr K.Shirisha. "A Secure Off-line Micro-payment For an E-commerce System." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 02, 2019, pp. 64-71.