# SURVEY PAPER ON SECURE DIGITAL CASH PAYMENT THROUGH COIN MANAGEMENT

C.Jayaprakash[*1], Dr.P.Chandra Sekhar[*2]
*PG Student, Department of CSE, JNT University, Ananthapur, AP,*
*Department of CSE, SK University, Ananthapur, AP,*

**ABSTRACT**

Cybercrime is the most popular crimes in the recent times. Cybercrime involves stealing credit card and debit card information details and utilizing those credentials for 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.

## 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

### 2.1FRODO: Fraud Resilient Device for off-Line Micro-Payments

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 [2]. The identity element is used to authenticate the user and the coin element where the coins are not locally stored but are computed on the fly when needed. In cryptography physical unclonable function is a entity which is used in a physical structure and is easy to evaluate but hard to predict [6]. An individual PUF device is easy to manufacture but practically impossible to duplicate. PUFs depend on the uniqueness of their physical microstructure. Main issue with the fully offline approach is the difficulty of checking the trustworthiness of a transaction without a trusted third party i.e., because bank doesn't involve directly in transaction processing as it requires a third party authentication to process the transaction [10].Keeping track of past transactions becomes difficult with no available connection to external parties or databases. It is difficult for vendor to check the past transactions (history) without a reliable connection.

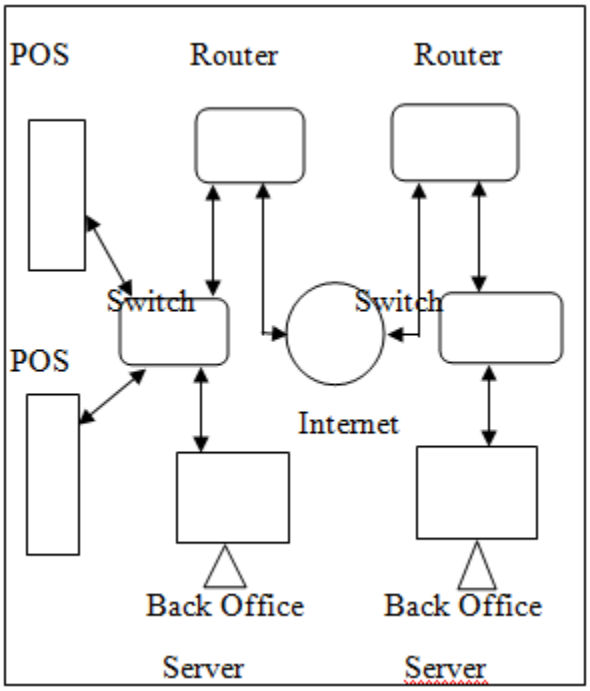


Fig1: Point-of-Sale Architecture

In the point-of-sale system the transaction gets processed by using a single step authentication process and this leads to the stealing of the data i.e., credit card and debit card data as soon as the customer card details are entered in the point-of-sale devices [4].Whenever the customer card data is read by the retailer then it asks for the personal identification number to process the transaction. Once we enter the PIN number and it is valid then the transaction is successfully completed. The Personal Identification Number is static. One can gain access to the information if the security level is low. There might be a chance to modify the data as the personal identification number is static.

### 2.2 Introduction to Bitcoins: A Pseudo-Anonymous Electronic Currency System

Sergio Martins and Yang Yang proposed the concept of Bitcoin. Bitcoin is a digital currency introduced in 2009, based on proof, rather than trust in a manner that is similar to cash. Bitcoin work based on coins and coin ownership verification [14]. Bitcoin is a peer-to-peer version of electronic cash which would allow online payments to be sent directly from one party to another without the involvement of third party institutions. Payment of Bitcoins can be made from one person to another irrespective of geographical location or jurisdiction [15].Payments are relatively fast, the initial notification is sent within seconds and it settles within an hour. A network of computers validates and keeps track of bitcoin payments and ensures that they are recorded.

The Bitcoin Block chain will be maintaining all the track of payments sitting over thousands of computers across the world which are connected over a network. The bitcoin block chain acts like a ledger which keeps a record of payments [15].When you make a bitcoin payment, a payment instruction is sent to the network. The computers on the network then validate the instruction and relay it to the other computers. After sometime the payment gets included in one of the block updates and is added to the bitcoin block chain file on all the computers across the networks. The distribution of data works on a peer-to-peer basis. Peer-to-Peer is like a gossip network where everyone tells a few other people about new transactions and eventually the message reaches to everyone in the network.

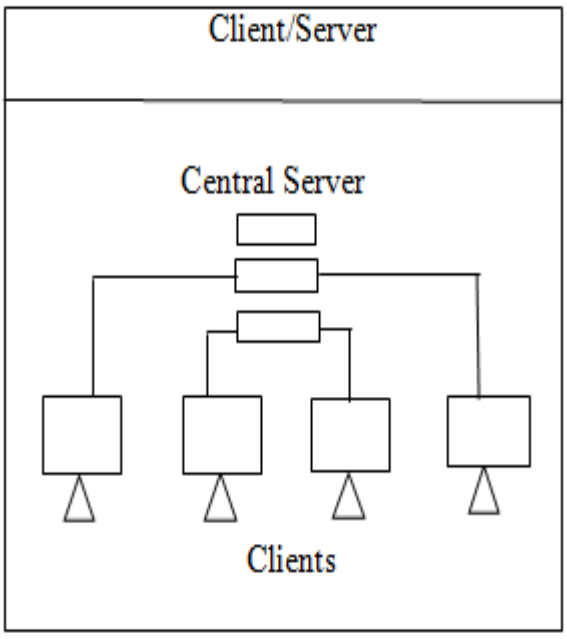


Fig2: Client-server System

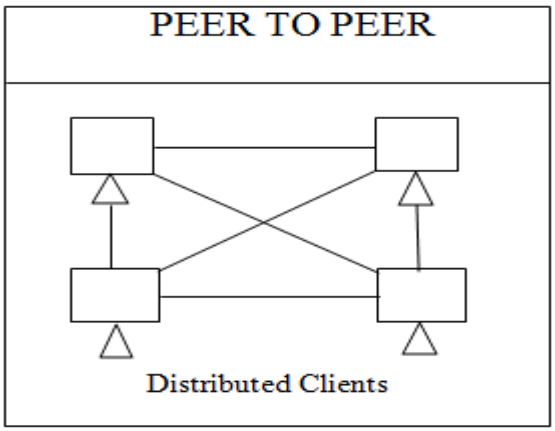


Fig3: Peer-to-Peer System

To make a successful bitcoin transaction we need address and the private key of that bitcoin respectively.

It is possible to send and receive money from any part of the world at any time.There is no central authority in the Bitcoin network. The address and private key of bitcoin are very difficult to read. Bitcoin is volatile because of limited amount of coins and demand gets increased day-by-day.

**2.3 Point–of-Sale System Breaches, Threats to the Retail and Hospitality Industries**

Trend Micro Corporation have proposed Point-of-Sale system breaches. Point-of-Sale systems have been found around in one form or another for decades. Businesses in the retail and hospitality industries use these systems not only to accept payment, but to provide other operational information such as accounting, sales tracking. Many point-of-sale terminals are built using embedded versions of Microsoft windows [8]. This means that it is trivial for an attacker to create and develop malware that would run on a Point-of-Sale terminal. Thus, the attacker can gain access to the terminal. Point-of-Sale systems are difficult to secure mostly because of their role and their location in the network [5].An attacker can find a way to infect a Point-of-Sale device before deployment i.e., in the vendor's factory.

Network-level hacking is another technique used where the attackers may try to check for access to the point-of-sale system through the network that the system belong to.Network level hacking can also be made possible through different methods. One can be shared connections between the systems in an establishment [12].Point-of-Sale systems that share the common connection with the Wi-Fi hotspot provided to the customers.Even though the point-of-sale terminals are connected using a closed Wi-Fi network, the attacker still be able to crack its passphrase [8].The attackers will find a way to breach the servers which holds responsible for all the Point-of-Sale information.

In a typical attack, target receives an email or an instant message that encourages him to click link or open a file which contains a piece of malware.If the target opens a file containing malware the attackers will have a scope to enter into the server or the database which contains confidential information.Once attackers gain access to the system, they gain access to the entire network of Point-of-Sale systems and are enabled to deploy malware that will steal customer information [12].When the information is read from the card, it can be found inside the point-of-sale device's memory in unencrypted form. Point-of-Sale malware exploit this by capturing the payment card information directly from memory which is known as "RAM SCRAPPING".

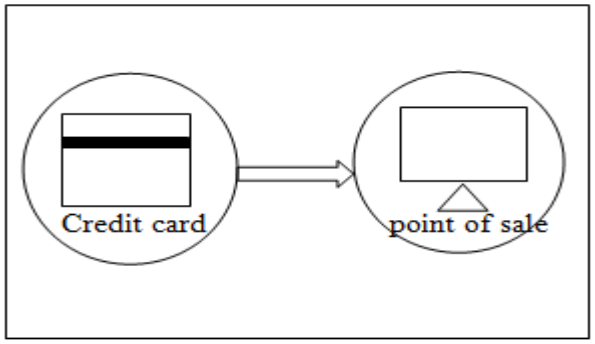


**Fig4: Point-of-Sale System Breach point**

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.

It provides detailed sales reports and helps to reduce the employment. It helps in simplifying the accounting process and gives easy access to the past transactions. Customer information will be lost if the point-of-sale systems are infected.

### 2.4 Pay Word and Micro Mint: Two Simple Micropayment Schemes

Ronald L. Rivest and Adi Shamir proposed two simple micro payment schemes, "Pay-Word" and "Micro-Mint" for making small purchases over the internet.In this paper the players are brokers, users and vendors. Brokers authorize the users to make micro payments to vendors and redeem the payments collected by the vendor.Vendor-user relationship is transient, broker-user and broker-vendor relationships are long-term.Our main goal is to minimize the number of public-key operations required per payment using hash operations [16].Hash functions are about 100 times faster than RSA signature verification and about 10,000 times faster than RSA signature generation.

On a typical workstation one can sign two messages per second, verify 200 signatures per second and complete 20,000 hash function values per second.The first scheme "Pay-Word" is a credit based scheme. The user establishes an account with a broker, who issues her a digitally signed payword certificate containing the broker's name, the user's name and IP address, the user's public-key, the expiration date and other information [17]. Pay-Word does not require the vendors to interact with broker for every payment. The vendor only needs to clear the payment once a day.

"Micro-Mint" is designed to provide reasonable security at very low cost and is optimized for low value payments. Micro-Mint uses no public-key operations at all.Micro-Mint coins are produced by a broker, who sells them to users. Users give these coins to vendors as payments. Vendors return coins to the broker in return for payment by other means.Micro-Mint has a property of generating many coins in a cheap manner. A large investment is required to generate first coin, but then generating additional coins can be made progressively cheaper.The broker will typically issue new coins at the beginning of each month [17]. The validity of these coins will expire at the end of each month.The unused coins are returned to the broker at the end of each month and new coins can be purchased at the beginning of each month.

Micro-Mint scheme can prevent from counterfeit and double spending effectively.Larger payments will not be processed using these schemes. High investment is required to generate the coins.

### 2.5 The Technology of Identification and Authentication of Financial Transactions from Smart Card to NFC Terminals

In recent times the intensive automation and computerization of various fields, security is the main concern. The payment systems are based on identification and authentication on the basis of plastic cards i.e., credit cards and debit cards. In payment systems two types of transactions are supported i.e., online and offline. In online transactions a constant communication channel between the financial terminal and the issuing bank servers [18]. The authorization is carried out on the bank server and the sanction to end the transaction is also given by the bank server. In online payment systems a simple terminal equipment and magnetic striped cards are used .The systems providing the offline transactions do not require the constant communication channel between the financial terminal and the bank servers. In offline transactions the authorization is carried out on the terminal. Two types of authentication methods are carried out i.e., static authentication and dynamic authentication [19]. Static authentication assumes the one sided control of integrity. Only the terminal equipment checks the integrity of a card. Dynamic authentication assumes two sided control of integrity not only the terminal equipment checks integrity of a card, but also the card checks authenticity of the terminal. In this case the basis of cards should be the microprocessor equipped with internal memory and capable to carryout cryptographic transformations.

In the given scheme the issuer, the processing center, the terminal only knows the public keys. The possibility of the card duplicate creation or unauthorized repeated transfer. The absence of the user protection from the persons serving the terminal equipment abusing. The absence of the user

protection from the bank employees abusing. The reliability of the considered scheme can be increased if the successfully completed transaction include the digital signature of the terminal.

### 2.6 Anonymous Subscription Schemes: A Flexible Construction far Online Services Access

Maria Isabel, Gonzalez vasco proposed subscription schemes which allows a set of users to buy access to a limited set of services, in a perfectly anonymous and efficient way. This access is paid to an issuing authority that dispenses connection tokens, which usage is completely determined at issuing time [20]. More precisely tokens are differentiated in terms of their service providers and validity period. This implies that each service provider can locally and non-interactively take control on the different tokens spent in each time slot, thus rejecting any attempt of token misuse. It is the main goal that the information cannot be linked either to the token itself or to the service the token is intended for [21]. One will impose that the view of the issuing authority must be independent of the value of the issued token. Payment is organized in such a way that at the end of a time slot, every service provider sends the collected tokens to the issuer to be paid for the offered service. Unused tokens can similarly be refunded to the users upon request.

Thus the subscription scheme must ensure that no collision of users and service providers can forge new valid tokens and they will furthermore not succeed in getting paid more than once for each issued token. The design basically works as follows users obtain from an issuing agency some tokens consisting of a blind signature on a message including a fresh public key, the identity of a service provider and a time slot [20]. To access the service the user signs a randomly with respect to the public key contained in the token and sends it along with the token itself to the service provider. With this simple setting one can achieve perfect user anonymity with respect to the services he purchased, unforgeability of tokens by a collision of dishonest users and services, valid access tokens cannot be repudiated by the issuing authority.

Efficient management of tokens due to the independence of services and time slots. Efficient access to services for users and very flexible access management for the service provider.

### 2.7 A Complete Secure Customer Centric Anonymous Payment in a Digital Ecosystem

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. Mobile commerce is a powerful technology in which E-commerce is carried out through a mobile device. A general account based payment model involves 4 parties. Card holder, Merchant, Issuer, and the acquirer [22]. An additional party called payment gateway which acts as an interface between the mobile payment world and existing private payment infrastructure. Payment gateway plays a major role between issuer and acquirer for the settlement of the transaction. The complete payment system is operated by payment system provider who maintains a relationship with banks [23]. Three primitive transactions involves in the payment protocols. Payment: customer makes a payment to the merchant for the goods purchased on merchant website. Value subtraction: The customer requests the issuer to debit his amount equal to the price involved in the transaction. Value claim: Merchant requests the acquirer to credit the transaction price involved in the transaction.

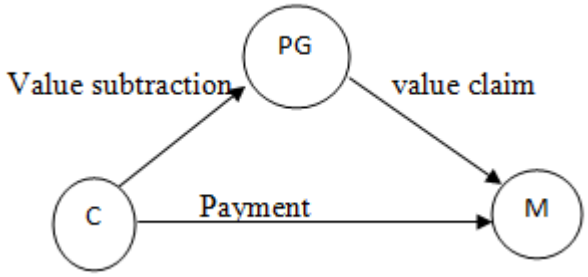


**Fig5: Digital Ecosystem**

### 2.8 Security of Offline Anonymous Electronic cash systems against Insider Attacks by Un trusted Authorities Revisited

In the design of electronic cash system one can usually focus on preventing customer's malicious behavior. However, since authorities such as banks and certificate authorities may have important secret

data of customers the insider attacks by the untrusted authorities also need to be handled carefully. Electronic cash has been one of the important challenging problems in cryptography. Chaum proposed an online anonymous electronic cash system by using the blind signatures [24]. The bank needs to be involved in the payment in order to check double spending of electronic cash.

The fact that the bank needs to be online for all the payment transactions between a customer and a shop can lead to the bottleneck of the bank system and it prevents realizing practical electronic cash system. Chaum, Fiat, and Naor proposed an offline anonymous electronic cash system where the bank doesn't need to be involved in the payment transaction between a customer and a shop. Many electronic cash systems follow the chaum-fiat-naor approach [25]. A customer withdraws electronic cash from the bank and sends the e-cash to a shop without needing to access the bank system. If the customer spends the e-cash maliciously the bank can extract the identification information of the customers from the double spent e-cash.In the CFN paradigm to realize both the offline property and the detection of double spending, the identification information of a customer is embedded in e-cash and also maintained by authorities such as banks.

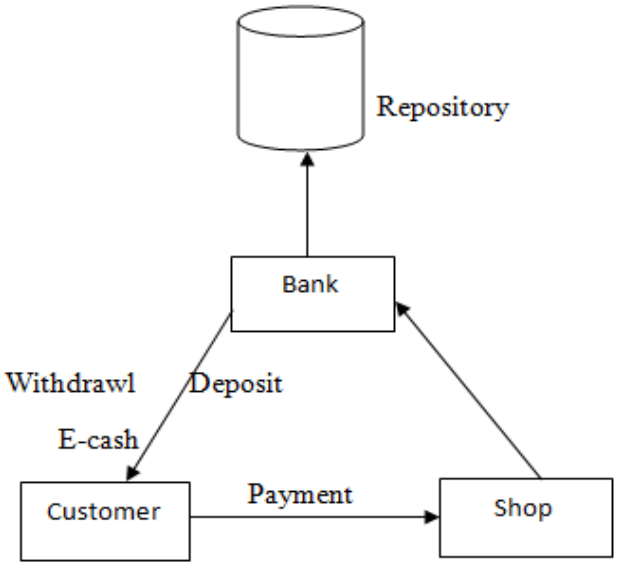


**Fig6: Flow in Electronic cash system.**

Such important identification information needs to be protected so that no malicious persons including bank employees can misuse it.

## III.CONCLUSION:

In this paper we have been sorted out maximum payment strategies which deals with more or less security features. A detailed study has been carried out on the payment mechanisms and able to figure out weak areas of security

## IV.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.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.
4. T. Micro, "Point-of-sale system breaches, threats to the retail and hospitality industries," University of Zurich, Department of Informatics, 2010.
5. Verizon, "2014 data breach investigation report," Verizon, The. Rep., 2014,http://www.verizonenterprose.com/DBIR/2014/
6.https://en.wikipedia.org/wiki/Physical_unclonable_function
7. R. L. Rivest, "Payword and micromint: Two simple micropayment schemes," in Proc. Int. Workshop Security Protocols, 1996, pp. 69–87.
8. Bogmar, "Secure POS & kiosk support," Bogmar,2014,"https://www.bomgar.com/assets/documents/Bomgar_Remote_Support_for_POS_Systems.pdf
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14.https://en.wikipedia.org/wiki/Bitcoin
15.www.computerhowtoguide.com/2016/07/bitcoins-advantages-disadvantages.html
16.https://link.springer.com/chapter/10.1007/3-540-62494-5_6
17. Ross Anderson, Harry Manifavas, and Chris Sutherland. A practical electronic cash system, 1995. Available from author: Ross. Andereson@cl.cam.ac.uk
18. Wolfgang Rankl, Wolfgang Effing. Smart Card Handbook. Hardcover 2 Ed edition. John Wiley & Sons, 2000.
19. Government Smart Card Handbook. U.S. General Services Administration, 2004.

http://www.smartcardalliance.org/pdf/industryinfo/smartcardhandbook.pdf
20. Blanton, M. (2008). Online subscriptions with anonymous access. In Proceedings ofthe 2008 ACM Symposiumon Information, computer and communications security, pages 217–227.
21. Camenish, J., Maurer, U., and Stadler, M. (1997). Digital Payment Systems with Passive Anonymity-Revoking Trustees. Journal of Computer Security, 5(1):254–265.
22. V. Ahuja, Secure Commerce on the Internet, AcademicPress, 1996.
23.G. Horn and B. Preneel, Authentication and Payment in Future Mobile Systems, Proceedings of 5th ESORICS'98, Belgium, 1998, pp. 277-293.
24. D. Chaum, "Blind signatures for untraceable payments," in CRYPTO, 1982, pp. 199–203.
25. 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