Introducing Secured Offline Payments using FRoDO

P.S.V.S Sridhar, T.V.S. Rohitkumar, G. Dharani, V.B.S. Akhila

Abstract: ***The theft of debit cards and the credit cards are common from the earlier days which is part of the cyber crime. In most of the cases attackers focus on the POS (point of sale) system and they steal the customer data. The point at which customer steals the data is known as POS. The POS is a combination of software and hardware. It allows merchants to perform the transactions and simplifies the business operations that happen day to day. POS consists of running software and these are the powerful computer systems. When the customer gets disconnected to the network we cannot assure the secure online payment. Here in this paper we introduce FRODO which enables the offline micro payments which are better compared to the POS systems. In terms of security and flexibility FRODO is the better option. The POS breaches is common now a days hence as per our knowledge the FRODO is the first approach which introduces the secure offline payments possibly reducing the cyber attacks. In this paper we describe about the algorithm of the FRODO, approaches and the architecture. In detail we discuss about the security and functional properties of the FRODO and at what extent it is viable and effective.***

Keywords: Frodo architecture, point of sale (POS), cyber attacks, fraud protection

I. INTRODUCTION

As per the market prediction the traditional market place was overtaken by the mobile payments which provide the convenience to the customers and companies. Internet banking is the most important application for the financial transaction and it provides the facility to make the payment from anywhere in the world [1]. It also provides the customer friendly service for 24 hrs a day. In recent times cyber crimes are popular; it includes stealing of the credit and debit card details and using the credentials. Because of providing the personal identification information there are large number of chances of attacking the data by an attacker [2]. The attackers try to steal the personal data of the credit or debit card details by infecting the POS systems.

The decentralized payment systems and the crypto currencies are becoming popular but they are not reliable since there are unsolved issues like lack of security, limited interoperability and lack of standards which are widely accepted[2].

Main Objectives and Challenges

Past few years the organizations and retailers are the victims of these POS breaches and the transaction data has been lost.[3].In this paper Frodo is the first solution that does not require the third parties to give protection against the frauds and it ensures that the customers are free from those frauds.[5] Many mobile payments are existing which are peer to peer rather than the merchant payment environment. These mobile payments includes the authentication and identification of the sim which simplifies the current infrastructure of the mobile payment. Since the POS breaches are decreasing still they are remunerative undertake for criminals. POS act as gateways and require the network connection for the communication between the customers and credit card processors. To reduce the cost and maintenance the POS approaches try to manually manage the internal networks.[4]. Brute force attacks are one of the most common attacks which can happen in the case of POS systems.

II. SECURITY BREACHES

Lamentably, the reason for information breaks is POS interruptions or framework interruptions that enable access to POS information. Fraudsters are extending their venture not exclusively to take client information, however fake it for some time later. To process charge and credit cards organizations set up a point of offer framework. Traders must guarantee their POS devices satisfy security guidelines, including PCI consistence, to diminish their risk of digital wrongdoing in view of their dealer card preparing innovation. The latest POS attack is MICROS previously attacking more than 330,000 customer websites including the marketing and hospitality. The attacks in the POS systems are multi staged. They need to gain access to the network rather than the card-holder data through this he can access the victims' network. After this the information is sent to the back office server waiting for exhilaration. PoS system hacking is done either by exploring the merchants software, by the brute force attack or by cracking the password.

Revised Manuscript Received on May 05, 2019.

P.S.V.S Sridhar, Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur-522501

T.V.S. Rohitkumar, Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur-522501

G. Dharani, Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur-522501

V.B.S.Akhila, Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur-522501

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Tough networks can be protected from these attacks it is just one of the sophisticated attack approaches.

III. ALGORITHM

Bit Exchanging Method: Encryption taken on the secret message files using simple bit shifting and XOR operation. The bit exchange method is introduced for encrypting any file.

Algorithm

Step 1: Read the all Content and Find the all character to covert the ASCII value Step 2: That ASCII value converted in Binary value
Step 3: Encryption taken on the secret message file using simple shifting and XOR operation. Like a 1001110.
Step 4: The bit exchange Method is introduced for encryption any file
Step 5: Read one by one byte from the secret data and convert each byte to 8 bits. Then apply one bit right shift operation. Like this 0100 1110.
Step 6: Divide the 8 bits into to block and then perform XOR operation with 4 bit on the left and 4 bits on the right side (1010).
Step 7: The same thing repeated for all bytes in the file
This FRODO does not require any special hardware component it consists of two components namely coin element and identity element.

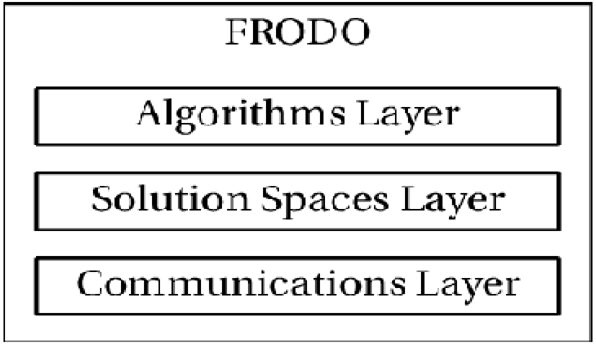


Fig . 1 construction module

Coin elements:

Coin Selects: Responsible for selection of right registers for the output value computed by coin element to obtain the final coin value

Coin re-constructor: It uses helper data stored in coin registers to extract the output of the PUF.
Coin registers: used to store both input and output values of PUF to reconstruct the coin values. Coin registers contain the helper data. Coin seeds and coin registers are used to construct the coin values in case the PUF fails.
Key Generator: It is used to compute private key of the coin element.

Cryptographic Element: used for asymmetric and symmetric cryptographic algorithms for the data received as input and send output by coin element.

IV. FRODO PROTOCOLS

The steps involved in the protocol are:
A query is sent by customer to the vendor for request of some resources

A random value is generated by the vendor which is later encrypted by the coin request for three times. The operations are

$$Eqa(req) = C\ Req$$
$$Eqaj(CReq, salt) = EqaReq$$
$$Eqav(EqaReq) = PrivateReq$$

3) After the request has been built it is directly sent to customer;
4) After receiving the request private key is generated using key generator, after encrypted layers are removed which were generated by vendor.
5) Value of coin is retrieved when the coin request is plain text from the coin element. The value generated by coin re-constructor is first encrypted then with the private key which belongs to authenticity of response and then the private key of vendor for authentication.

$$\begin{aligned} Enq(coin\ value) &= EValueEnqj(CValue)\\ &= EncValueEnqv(EncValue)\\ &= PrivateResponse \end{aligned}$$

6) When the private response is received the coin is read to check whether it is valid or not and then the whole payment can be authorized and verified. At first the vendor decrypts the received response by using private key secondly the result value is decrypted by public key of the identity element finally coin value is decrypted by using public key.

$$\begin{aligned} Dec(Private\ Response) &= EncValuDeck(EncValue)\\ &= CValueDecf(CoinValue)\\ &= CoinValuDecr(CoinValue)\\ &= RawValue \end{aligned}$$

7) The private key is encrypted by the vendor after a new value s stored in the storage device. The coin value is encrypted by the bank using the private key hence it s not possible to imitate digital coins. The whole transaction is said to be valid only if the value obtained after decryption of coin value with public is valid.

ANALYSIS OF FRAUDS:

FRoDO uses both symmetric and asymmetric cryptographic algorithms to ensure the security principles.
1) *Authenticity*: Frodo provides authenticity by computing private keys. Both coin element and identity are used to compute the private key by using the key generator. They are used to encrypt and decrypt the messages in the protocol. Each public key is used by vendor which is signed by the bank. It can always be verified by the vendor.
2) *Integrity*: Each digital coin is encrypted by the bank issuer. Coin helpers and coin seeds are written in registers by issuer and the final coin value is known as the output.

The content which was stored can be backed up and transferred to make it more secure for an adversary to delete the transactional history.

3) *Confidentiality:* The communication between the customer and vendor as well as the coin element and identity the asymmetric encryption primitives to assure the confidentiality.

4) *Availability*: The offline digital coins are used which allows the guaranteed availability of the proposed solution. It completely removes the communication requirement and it would be helpful in the extreme situations without the internet.

V. ATTACKS REDUCTION

Double spending: The computation of same coin twice is prevented by PUF [30].Since the request of the vendor is only calculated by customer he private keys of identity and coin elements are needed to decrypt the request of vendors. Even if fake vendor read all those coins, it is not possible to spend all the coins sue to inability to decrypt those coins. The coin element or private keys are said to be valid only if they are signed by the bank. The coin element having fake bank signature would be declared as invalid and the messages sent by the coin element are rejected.

Emulation: Original responses would be different from responses computed by fake PUF'S. These coins cannot be imitated in software or hardware.

Coin imitated: It is not possible to forge new coins since each coin is encrypted by bank or element issuer.

Information Forgery: No confidential information is kept in coin element or identity. Physical access to hardware is not provided by coin elements or identity so the stealing of information is not possible.

Paused Transaction: The output is obtained with the help of the access key which is private, These coin elements does not contain any information in the form of the plain text or in the encrypted form.

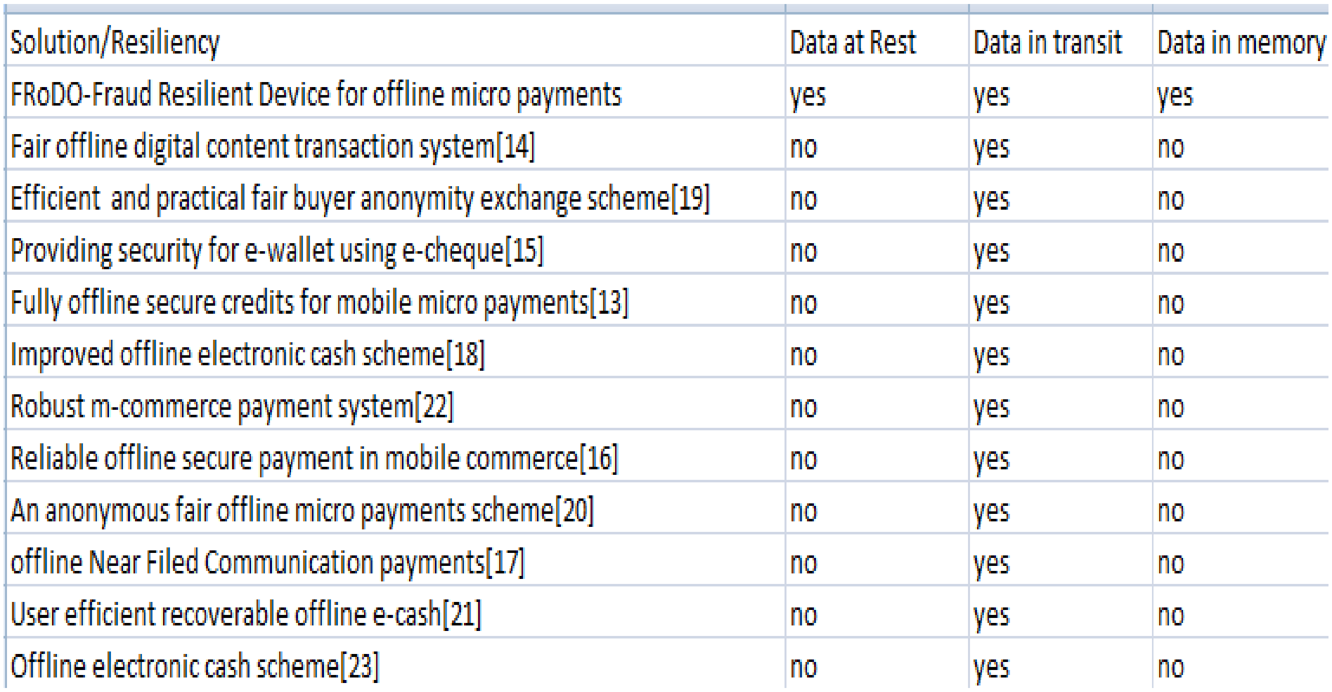
Replay: Each coin is related to transaction. Random salt generated is different for each transaction generated by the vendor.

Reverse engineering: Any attempt to steal the information can change the behaviour of the PUF which makes the elements no longer usable.

Man in the middle: An attacker cannot pretend as another customer since it would not be able to generate the private key. Digital coins are encrypted by the bank so any attacker cannot dump the coins in the middle since the digital coins are not present in the memory and they are generated during the execution,

Denial of services: Frodo requires pairing process it requires private key to be, manually entered in the customer device. Each transaction needs to be approved by customer which prevents the breach attacks which generally happens in the POS systems. It is a kind of cyber attack in which the attacker prevents the users from accessing the network. This can be done in several ways which causes the victim a great deal of time and money to handle

Table 1. Data Breach Resiliency



Solution/Resiliency	Data at Rest	Data in transit	Data in memory
FRoDO-Fraud Resilient Device for offline micro payments	yes	yes	yes
Fair offline digital content transaction system[14]	no	yes	no
Efficient and practical fair buyer anonymity exchange scheme[19]	no	yes	no
Providing security for e-wallet using e-cheque[15]	no	yes	no
Fully offline secure credits for mobile micro payments[13]	no	yes	no
Improved offline electronic cash scheme[18]	no	yes	no
Robust m-commerce payment system[22]	no	yes	no
Reliable offline secure payment in mobile commerce[16]	no	yes	no
An anonymous fair offline micro payments scheme[20]	no	yes	no
offline Near Filed Communication payments[17]	no	yes	no
User efficient recoverable offline e-cash[21]	no	yes	no
Offline electronic cash scheme[23]	no	yes	no

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

VI. RESULTS

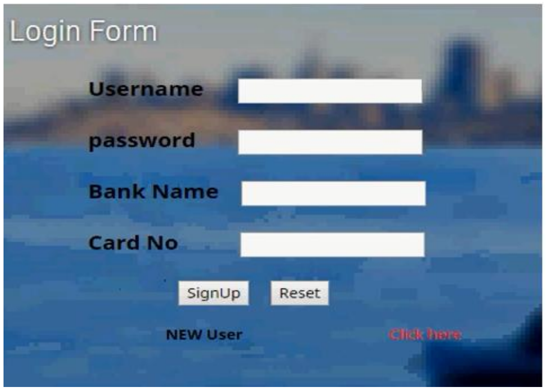


Fig. 2 Login Form

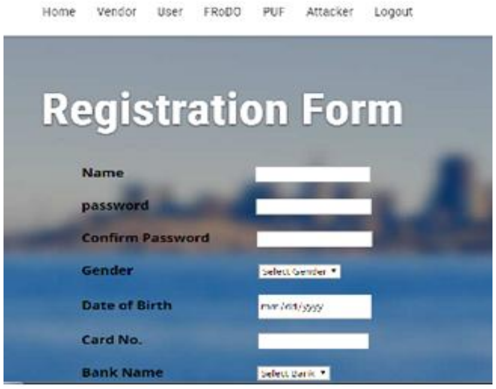


Fig . 3 Registration Form

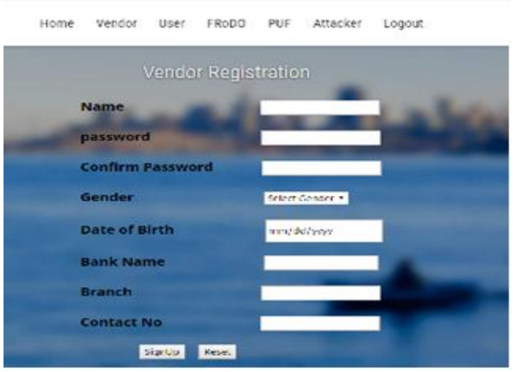


Fig . 4 Vendor Registration

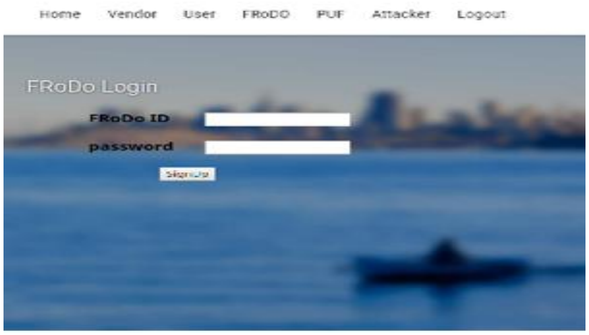


Fig . 5 FRoDo Login

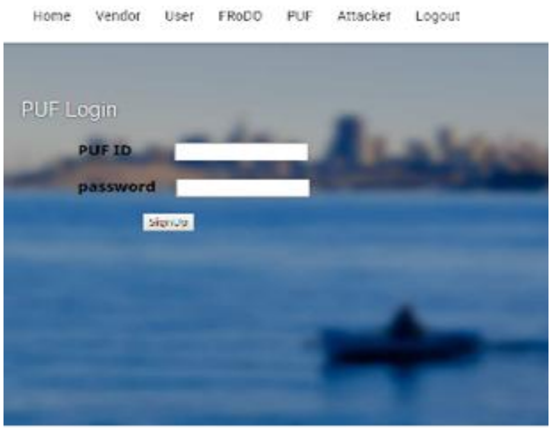


Fig .6 Login

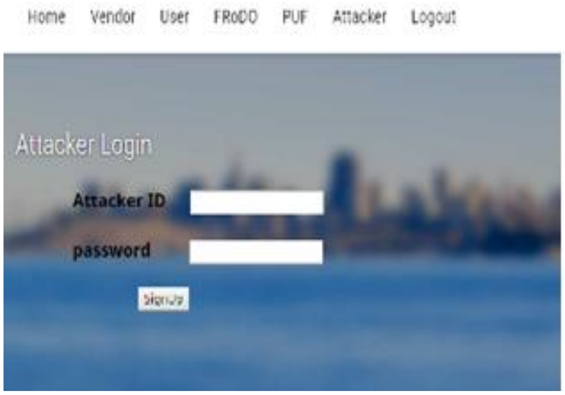
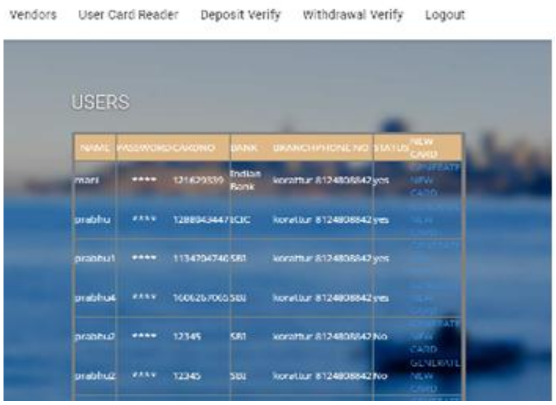


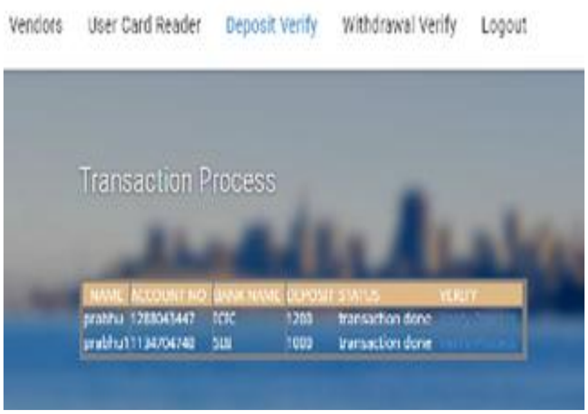
Fig . 7 Attacker Login



USERS

NAME	PASSWORD	CARDNO	BANK	BRANCH	PHONE NO	STATUS	NEW CARD
mari	****	1216293339	Indian Bank	korattur	8124808842	yes	GENERATE NEW CARD
prabhu	****	1288943447	ICIC	korattur	8124808842	yes	GENERATE NEW CARD
prabhu1	****	1134704740	SBI	korattur	8124808842	yes	GENERATE NEW CARD
prabhu4	****	1606267065	SBI	korattur	8124808842	yes	GENERATE NEW CARD
prabhu2	****	12345	SBI	korattur	8124808842	No	GENERATE NEW CARD
prabhu2	****	12345	SBI	korattur	8124808842	No	GENERATE NEW CARD

Fig . 8 Users



Transaction Process

NAME	ACCOUNT NO	BANK NAME	DEPOSIT	STATUS	VERIFY
prabhu	1288043447	ICIC	1200	transaction done	
prabhu1	1134704748	SBI	1000	transaction done	

Fig . 9 Transaction Process

VI. CONCLUSION

In this paper a new concept named FRODO was introduced which does not require the access of any network and helps in secure payments and it is fully secure. The FRoDO does not give any false predictions in case of any security issues. In this model no data attacks are capitalised which belongs to the customer device. This is achieved with the help of erasable PUF architecture and FRoDO protocols. Our propose has been analysed thoroughly and compared with the mobile payment systems. Our paper shows that it achieves all the properties to assure the security in case of transactions it also considers the flexibility considering the payment medium. Some issues were identified which need to be improved in future work. We are surveying on possibility to allow the offline transactions and make it more reliable and faster simultaneously maintaining the security and the ease of use. This FRoDO does not have the chances of data breach which generally happened in case of mobile payments which are attacked on the line of POS systems.

REFERENCES

1. FRoDO: Fraud Resilient Device for Off-Line Micro-Payments Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, and Matteo Signorini
2. J.Lewandowska.(2013)
3. Available:http://www.frost.com/prod/servlet/press-release.pag?docid=274238535
   S. Martins and Y. Yang, “Introduction to bitcoins: A pseudo anonymous electronic currency system,” in Proc. Conf. CenterAdv. 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. Mandiant, “Beyond the breach,” Mandiant, 2014, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.
6. See Information Systems Audit & Control Association (ISACA) and RSA Confrence, “State of Cybersecurity: Implications for 2015,” http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/Study-82-percent-of-Organizations-Expect-a-Cyberattack-Yet-35-percent-Are-Unable-to-Fill-Open-Security-Jobs.aspx.
7. See Ponemon Institute LLC, “The Economic Impact of Advanced Persistent Threats,” May 2014.
8. .SeeGartnerhttp://www.securityweek.com/global-cybersecurity-spending-reach-769-billion-2015-gartner.
9. See Gartner, Addressing the Cyber Kill Chain Aug 15, 2014 Research note by Analyst Craig Lawson
10. See “2014 Threat Report: MTrends – Beyond the Breach,” Mandiant,April2014, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.
11. G. Vasco, Maribel, S. Heidarvand, and J. Villar, “Anonymoussubscription schemes: A flexible construction for on-line services access,” in Proc. Int. Conf. Security Cryptography, Jul. 2010,pp. 1–12.
12. K. S. Kadambi, J. Li, and A. H. Karp, “Near-field communication based secure mobile payment service,” in Proc. 11th Int. Conf. Electron.
13. Commerce, 2009, pp. 142–151.
14. V. Daza, R. Di Pietro, F. Lombardi, and M. Signorini, “FORCEFully off-line secure credits for mobile micro payments,” in Proc. 11th Int. Conf. Security Cryptography, 2014, pp. 125–136.
15. C.-L. Chen and J.-J. Liao, “Fair offline digital content transaction system,” IET Inf. Security, vol. 6, no. 3, pp. 123–130, Sep. 2012.
16. B. Yahid, M. Nobakht, and A. Shahbahrami, “Providing security for e-wallet using e-cheque,” in Proc. 7th Int. Conf. e-Commerce Develop. Countries: Focus e-Security, Apr. 2013, pp. 1–14.
17. N. Kiran and G. Kumar, “Reliable OSPM schema for secure transaction using mobile agent in micropayment system,” in Proc. 4th Int. Conf. Comput., Commun.Netw. Technol., Jul. 2013, pp. 1–6.
18. G. Van Damme, K. M. Wouters, H. Karahan, and B. Preneel, “Offline NFC Payments with Electronic Vouchers,” in Proc. ACM 1st ACM Workshop Netw., Syst., Appl. Mobile Handhelds, 2009, pp. 25–30.
19. C. Wang, H. Sun, H. Zhang, and Z. Jin, “An improved off-line electronic cash scheme,” in Proc. 5th Int. Conf. Comput. Inf. Sci., Jun. 2013, pp. 438–441.
20. W.-S. Juang, “An efficient and practical fair buyer-anonymity exchange scheme using bilinear pairings,” in Proc. 8th Asia Joint Conf. Inf. Security, Jul. 2013, pp. 19–26.
21. C.-I. Fan, Y.-K.Liang, and C.-N. Wu, “An anonymous fair offline micropayment scheme,” in Proc. Int. Conf. Inf. Soc., Jun. 2011,pp. 377–381.
22. C.-I. Fan, V. S.-M.Huang, and Y.-C. Yu, “User efficient recoverable off-line e-cash scheme with fast anonymity revoking, Math.Comput.Model” vol. 58, no. 12, pp. 227–237, 2013.
23. N.Kiran and G. Kumar, “Building robust m-commerce payment system on offline wireless network,” in Proc. IEEE 5th Int. Conf. Adv. Netw.Telecommun. Syst., Dec. 2011, pp. 1–3.
24. J. Liu, J. Liu, and X. Qiu, “A proxy blind signature scheme and an off-line electronic cash scheme,” Wuhan Univ. J. Natural Sci.,vol. 18, no. 2, pp. 117–125, 2013.
25. G. Hong and J. Bo, “Forensic analysis of skimming devices for credit fraud detection,” in Proc. 2nd IEEE Int. Conf. Inf. Financial Eng., Sep. 2010, pp. 542–546.
26. C.R.Group, “Alina & other POS malware,” Cymru, 2013,https://www.teamcymru.com/ReadingRoom/Whitepapers.
27. Dr.Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T “Review and Analysis of Promising Technologies with Respect to fifth Generation Networks”, 2014 First International Conference on Networks and Soft Computing,ISSN:978-1-4799-3486-7/14,pp.248-251,August 2014.
28. A.Surendar, K. H. Kishore, M. Kavitha, A. Z. Ibatova, V. Samavatian “Effects of Thermo-Mechanical Fatigue and Low Cycle Fatigue Interaction on Performance of Solder Joints” IEEE Transactions on Device and Materials Reliability, P-ISSN: 1530-4388, E-ISSN: 1558-2574, Vol No: 18, Issue No: 4, Page No: 606-612, December-2018.
29. Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.
30. Yadlapati, A., Kakarla, H.K. An Advanced AXI Protocol Verification using Verilog HDL (2015) Wulfenia, 22 (4), pp. 307-314.
31. Murali, A., Hari Kishore, K., Rama Krishna, C.P., Kumar, S., Trinadha Rao, A. Integrating the reconfigurable devices using slow-changing key technique to achieve high performance (2017) Proceedings - 7th IEEE International Advanced Computing Conference, IACC 2017, art. no. 7976849, pp. 530-534.