International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-10, Issue-2, April 2023
https://doi.org/10.55524/ijirem.2023.10.2.19
Article ID IJIR2359, Pages 103-107
www.ijirem.org

Fraud Resistant Off-Line Card Micropayments Using FRoDO and PUF

**Mr. Janardhan Reddy D[1], Giribabu Sadineni[2], V.V. Tejaswini[3], D. DivyaSree Bhavani[4]
N. Kaveri[5], and V. Divya Archana[6]**

[1]Assistant Professor, Department of Computer Science & Engineering, PACE Institute of Technology & Sciences, Ongole, Andhra Pradesh, India
[2]Associate Professor, Department of Computer Science & Engineering, PACE Institute of Technology & Sciences, Ongole, Andhra Pradesh, India
[3,4,5,6] Student, Department of Computer Science & Engineering, PACE Institute of Technology & Sciences, Ongole, Andhra Pradesh, India

Correspondence should be addressed to Mr. Janardhan Reddy D; janardhanreddy_d@pace.ac.in

ABSTRACT- The internet payment system, which is a widespread cybercrime, is a major issue nowadays. Attackers concentrate on point of sale (POS) systems, the point at which a bank or merchant initially obtains customer information, with the goal of stealing confidential customer information. Effective computer systems with a card reader and specialised software are POS architectures. In this situation, the attacker might utilise malicious software (MS) to steal card statistics. If the customer and the supplier are consistently cut off from the network in, no online payment is practical. If the community fails, attacker's side will attempt to steal the password from the users throughout the price, therefore a safe online transaction price may not be achievable. Due to the PoS information breaches, we recommend an offline micro-fee solution that is secure and protects privacy for the persistent attackers in our paper. We use the FRoDO protocol to make the payment simple and secure from attackers. This protocol not only checks the client's coins but also confirms the client's identity by using identification details. This protocol increases flexibility and security and boosts the device's efficiency by infusing a comfortable micro-charge between the client and carrier.

KEYWORDS- POS systems, Malicious Software, Micro-fee solution and FRoDO.

I. INTRODUCTION

PoS systems function as gateways and need a few different kinds of community connections in order to communicate with external credit card processors. To validate transactions, this is necessary. PoS gadgets can be remotely managed across those internal networks to lower cost and streamline management and maintenance. The mobile pricing options put forth up until this point can be classified as fully online, partially offline, weakly offline, or completely offline. The previous piece, Force, used a PUF-based architecture and, like FRoDO[1], was constructed using this method. Force provided a shoddy prevention strategy that was solely dependent on statistical obfuscation and did not address the most relevant attacks targeted at endangering consumer sensitive data, leaving it open to numerous more advanced attack methods. Cellular billing is expected to supersede traditional billing in the future, offering customers more ease and providing numerous agencies with new streams of income. Due to this scenario, traditional credit cards will be replaced by innovative processes like mobile-based payments, opening up new business opportunities for new market entrants. Even if it is heavily backed by cutting-edge hardware, cell charge technology is still in its infancy. Yet, it is widely expected to advance in the near future, as evidenced by the rising popularity of cryptocurrencies. Cryptocurrencies and decentralised price systems have grown in popularity recently, encouraging a transition from physical to digital.

Network security guards against unauthorised access and other threats to an organisation. Organization managers have a responsibility to take precautions to protect their organisations from potential security risks. Computer networks that are used for regular correspondence and exchanges inside public bodies, individuals, or organisations need to be secure. Giving a resource an intriguing name and a contrasting secret key is the most well-known and simple method of protecting it. A firewall is the security architecture of an organisation that monitors and controls the organization's traffic according to predetermined norms. A firewall creates a barrier between a closed-off internal organisation and the internet. Firewalls are both a programming tool for a spike in equipment demand and a security measure.

Firewalls are both equipment machines and programming tools for abrupt spikes in equipment demand. Equipment-based firewalls offer additional features as well, such as serving as a DHCP server for that organization. The majority of PCs employ firewalls with programming-based protection to keep themselves safe online. On the other hand, many firewalls can perform crucial steering functions, and many switches that transmit data between networks incorporate sections for firewalls. In order to prevent unauthorized access to intranets or confidential organization's websites, firewalls are frequently used. The firewall examines each message coming into or going out of the intranet to ensure its security. The best firewall configuration includes both hardware and programming-based devices. Moreover, a firewall aids in granting remote access to a secure organization.

The fact that the concept of "micropayments" changes with the crowd and that various frameworks claim to be "Micropayments" is an important aspect of the term. Each of them has the ability to manage small amounts of cash for random reasons. The real problem is saving the money for the one-time transaction; this was never a real problem. This imposes constraints on the pace and expense of handling the installments, as delivery occurs virtually instantly online and frequently in small, sporadic chunks. The bottleneck in handling large products, caring for them, and transporting them, on the other hand, lowers the bar, especially for costs to remain reasonable. Because of the growing importance of elusive (like data) goods in global markets and their speedy delivery at negligible cost, "conventional" installation approaches will typically be more expensive than the genuine article. On the other hand, pricing for small amounts of a good or service reduces the need for security.

II. LITERATURE SURVEY

A. Fee Gateways Are Used To Process micropayments Online

A malicious device or phone one could be used in place of the PoS by an attacker. PoS systems are built on general-purpose operating systems; they are vulnerable to a wide range of attack scenarios that could result in significant data breaches, and the attacker can steal the data using auxiliary tools. We introduce payment gateways to get around this problem, allowing us to stop malware while simultaneously guaranteeing the security of micropayments. A payment gateway[6] is a network that facilitates the payment process. It serves as a liaison between a customer and a retailer. Additionally, it safeguards the client's private payment information, which is transmitted from the client in a way that prevents duplication. In the next years, cell phone installation strategies are anticipated to displace traditional electronic installation methods. However, present solutions are constrained by conventions that assume something like one of the two groups to be online, such as being connected to either a trusted outsider or a shared data collection. Any online payment is obviously absurd in circumstances where the buyer and seller are stubbornly or irregularly cut off from the organisation. This paper introduces Power, a brilliant portable small installation method that enables total disconnection from all complicated gatherings. Our solution relies on modern techniques for installation adaptability and security. In fact, Power completely relies on local knowledge to do the aforementioned tasks and obtain the topological impact provided by the wormhole. Wormhole identification can be done successfully without much help from above or the use of external monitoring equipment.

B. Offline Micro Bills Recover Frozen Frauds

Right here, we are featuring the PUF as the answer to improving the Frodo because, by way of using gateways, the micro bills are secured, but cloning takes place in a specific location. So, to keep away from this, we are imposing the bodily unclonable feature (PUF)[9][10], which no longer needs any pre-determined computed challenge-reaction pair mechanism. With the aid of PUF[7], the physical properties of the tool cannot be cloned or copied. On account of that, it's very vital to have an authentication system within the tool. Such that they're unique to every tool and can be used for authentication purposes. PUF look at the carrier’s information concerning price and activate the carriers. In price verification, PUF checks each identification and coin detail, then the payment is decrypted using the public key. By using Puf, the keys might be generated on demand.

C. Frodo-Friendly Offline Micropayment Solutions

PUF generates the keys so they may be generated on demand, this explains the fantastic answer, which is FRoDo. When a user requests activation, Frodo sees them and activates them. The two components that make up the Frodo structure are the identification detail and the coin [3] detail. Identity Detail creates a private key for the user, and Coin Element converts the customer's account number into a binary code. The charging process is safer with this two-step process. The identifying element's private key is generated using a key generator, and symmetric and asymmetric cryptographic techniques are used to protect the data that is received as input and sent as output.

D. Mobile Transaction And Authentication Using Networks

Many m-payment options have emerged as a result of the expansion of mobile phones' technical capabilities. Applications for mobile payments are created for both online and offline purchases. The Near Field Communication (NFC) technology has a big impact on how mobile devices are used. An existing contactless application infrastructure, such as mobile payment at the point of sale, can be integrated with a mobile phone using NFC [5], a short-range wireless communication interface (POS)[11]. It is crucial to provide a simple method for implementing m-payment systems that offer the user both reasonable protection and ease of use. We suggest a system that integrates USIM identification and authentication capabilities with existing encryption primitives and algorithms, as well as NFC technology[5].

III. RELATED WORK

The cell wallet solutions that have been implemented to date are reportedly totally online or semi-offline; the main issue with the entirely offline price is that it is impossible to verify the validity of the charge in the absence of a third party. It has been the main goal in the last few years. AES is a commonly used encryption method that is supported by hardware and software. When subjected to cryptanalysis attacks [8], AES is virtually undetectable. It's crucial to remember that even though many works were added at the offline payment and overcome the limitations and bring similarly upgraded features, our previous painting FORCE[4], which is very similar to offline micro-bills, was built using PUF architecture. This is despite the fact that many researchers on offline prices are claimed to be reliable.

IV. EXISTING SYSTEM

PoS systems serve as gateways and need to be connected to the internet in order to communicate with outside credit card processors. Over these internal networks, remote management of PoS devices is possible. Mobile payment options[2] have so far been categorised as fully online, partially offline, weakly offline, or completely offline. The project is known as FORCE, and FORCE offered a flimsy data obfuscation-based preventive method and neglected to address the most pertinent attacks targeted at endangering consumer critical data, leaving it open to numerous sophisticated attack techniques.

V. PROPOSED SYSTEM

The main solution that does not rely on third parties, bank accounts, or gadgets is FRoDO. The digital currency used in FRoDO is just a virtual representation of actual coins; as a result, it no longer has any connection to anyone other than the owner of each identifier and the coin details. An identifying detail to verify the buyer and a coin detail, where money is computed on the spot as needed rather than being saved locally, are two examples of FRoDO features. Cash from the buyer is no longer immediately inspected during a transaction. In order to identify the user, the dealer best sends the identity information. The main benefit is a simpler, faster, and more consistent interaction between the relevant actors and entities.

VI. RESULTS AND DISCUSSIONS

The Results and Discussion section Explained with the help of Fig 1,2,3.These figures 1,2,3 explains these Frodo and PUF Logins and their implementations and fig 4 explains about user registrations page and fig 5 explaining about User Payment page. with these following figures we are trying to explains the whole scenario.

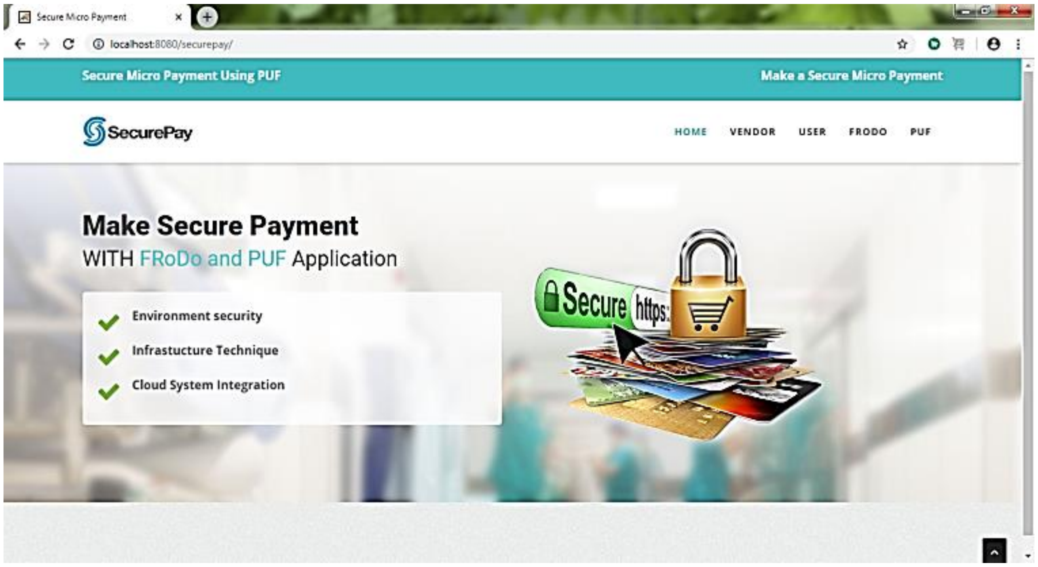


Figure 1: Home Page

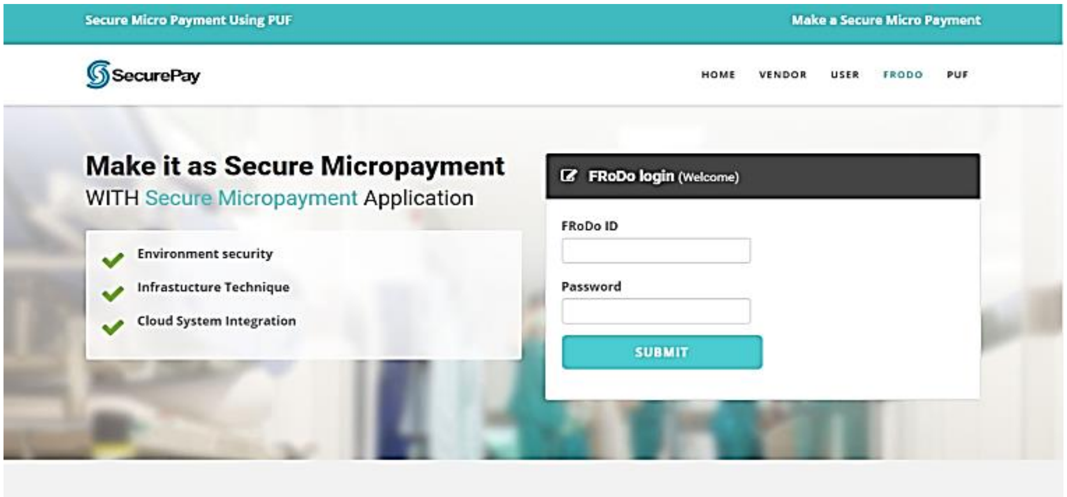


Figure 2: Frodo Login

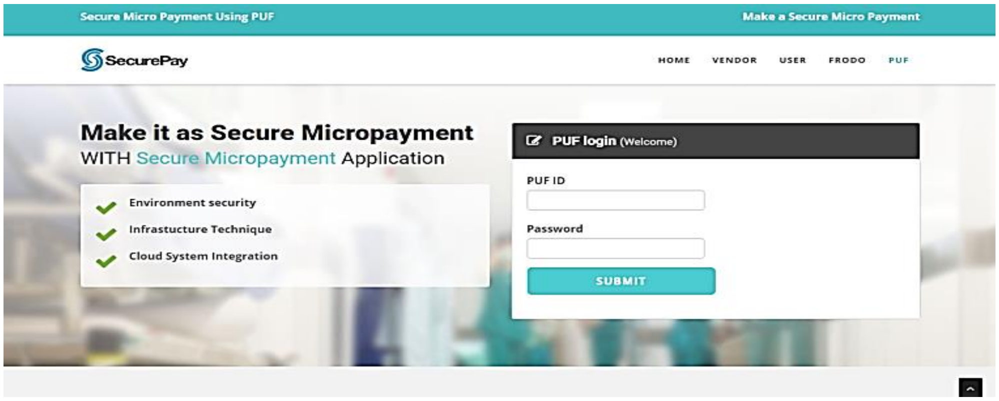


Figure 3: PUF login

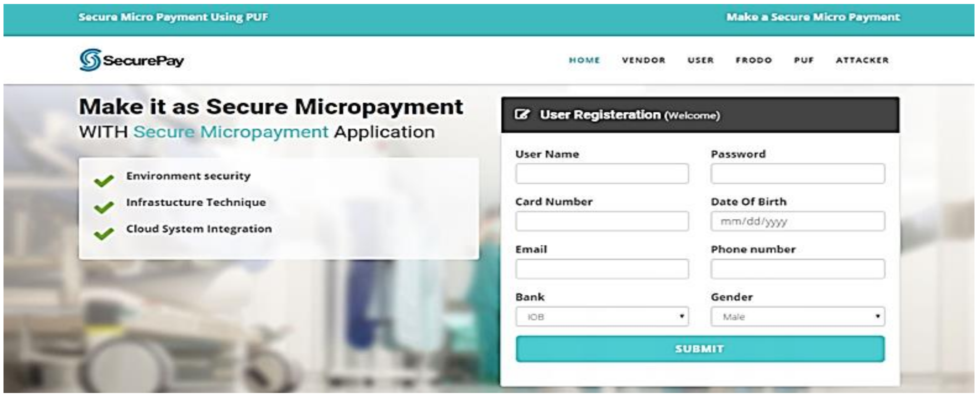
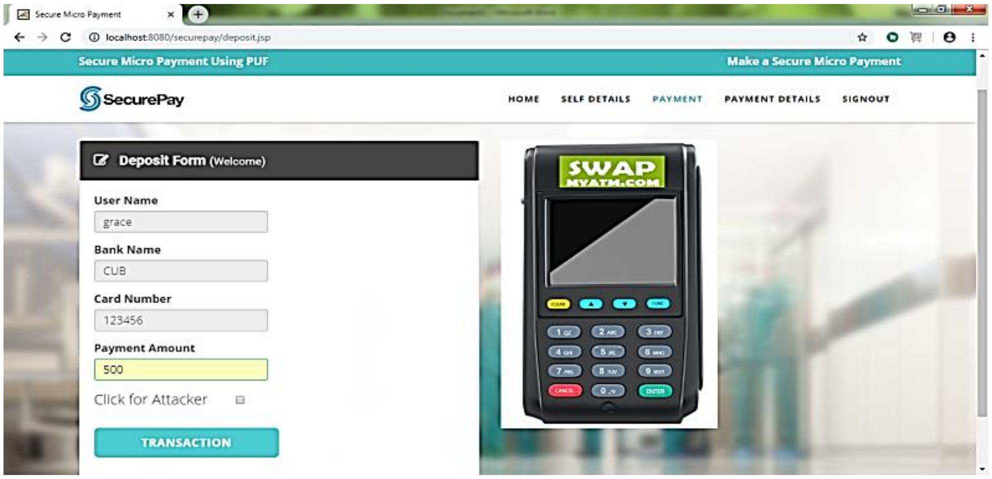


Figure 4: User Register Page



User Name: grace

Bank Name: CUB

Card Number: 123456

Payment Amount: 500

Click for Attacker □

Figure 5: User Payment Page

VII. CONCLUSION

To our knowledge, FRoDO is the first entirely offline, privacy-preserving micropayment method. Security research demonstrates that FRoDO does not impose any assumptions about reliability. Moreover, FRoDO is the first solution in the literature that prevents system compromise by preventing assaults on client device data from being exploited. This was principally accomplished via a novel protocol design and erasable PUF architecture. Also, our ideas were carefully examined and contrasted with current best practices. Our investigation shows that only FRoDO delivers the flexibility needed for a safe micropayment solution while taking payment mediums (different types of digital currency) into account. Finally, a few unresolved problems that need further investigation were found. The prospect of distributing digital change over numerous offline transactions while retaining the same level of security and usability is of special interest to us.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, and Matteo Signorini, "Frodo: Fraud Resilient Device For Off Line micro Payments", Dependable and Secure Computing, IEEE Transactions On (Volume: PP,Issue: 99), 12 June 2015.

[2] R. L. Rivest, ― Payword and micromint: two simple micropayment schemes, in CryptoBytes, 1996, pp. 69–87.

[3] S. Martins and Y. Yang, ―Introduction to bitcoins: a pseudo-anonymous electronic currency system, ‖ser. CASCON '11. Riverton, NJ, USA: IBM Corp., 2011, pp. 349–350.

[4] V. Daza, R. Di Pietro, F. Lombardi, and M. Signorini, FORCE Fully Off-line secure Credits for Mobile Micro Payments, in 11th Intl. Conf. on Security and Cryptography, SCITEPRESS, Ed., 2014.

[5] W. Chen, G. Hancke, K. Mayes, Y. Lien, and J. - H. Chiu, using3G network components to enable NFC mobile transactions and authentication,in IEEE PIC '10, vol. 1, Dec 2010, pp. 441 –448.

[6] M. A. Salama, N. El-Bendery,and A.E. Hassanien, "Towards secure mobile agent-based e-cash system," in Intl. Workshop on Security and Privacy Preserving in e-Societies. New York, NY, USA: ACM, 2011, pp. 1–6.

[7] J. Guajardo, S.S. Kumar, G.J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," ser. CHES '07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 63–80.

[8] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," SIAM Compute, vol. 38, no. 1, pp. 97–139, mar 2008.

[9] B. Kori, P. Tuyls, and W. Ophey, "Robust key extraction from physical unclonable functions," in Applied Cryptography and Network Security ser. LNCS, J. Ioannidis, A. Keromytis, and M. Yung, Eds. Springer Berlin Heidelberg, 2005, vol. 3531, pp. 407– 422.

[10] M.D. Yu, D. M. Raihi, R. Sowell, and S. Devadas, "Lightweight and Secure PUF Key Storage Using Limits of Machine Learning," in CHES 2011, ser. LNCS, B. Preneel and T. Takagi, Eds. Springer Berlin Heidelberg, 2011, vol. 6917, pp. 358–373.

[11] C. R. Group, "Alina & Other POS Malware," Cymru, Technical Report, 2013. [12]. N. Kiran and G. Kumar, "Reliable OSPM schema for secure transaction using mobile agent in micropayment system," in ICCCNT 2013, July 2013, pp. 1–6.