International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195317

Efficient and Secure Offline Transaction with Bit Coin Generation

R. Ananthi, Dr. S. Nandhakumar
Department of Computer Science and Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India

ABSTRACT

Disaster is any event that is either occurred naturally or manmade which can create huge loss on people's belonging or lives. Payment through mobile in a disaster field gives the advantage to provide electronic transactions for people buying recovery items like foodstuffs, garments and medicine. Existing *system* uses *a* new *mobile payment* method which makes use *of* infrastructure less *mobile* adhoc networks to permit transactions that permit customers to buy in disaster areas. However, few issues arise in this system while payment is in process. In this paper, proposed a method for secured transaction between a vendor and a customer using offline MANET concept. The customer and the vendor should register with the bank and gets authenticated separately. The protocol used in the proposed system works on two phases. (i) Pairing phase & (ii) Payment phase. At the completion of pairing phase, the vendor and the customer should share their public keys. This is done to improve message integrity & authenticity.

Keywords : Offline Mobile Payment, Mobile Pairing, Bit Coin Generation, Payment Phase.

I. INTRODUCTION

Network security entails the authorization of access to facts in a community, which is controlled with the aid of the community administrator. Users select or are assigned an ID and password or different authenticating statistics that lets in them access to facts and packages within their authority. Network protection covers a spread of computer networks, each public and private that are utilized in ordinary jobs; engaging in transactions and communications amongst agencies, authorities' organizations and individuals. Networks may be personal, which include inside a organization, and others which might be open to public access permission. Network protection is involved in agencies, firms, and other kinds of institutions. It does as its identify explains: It secures the community, in addition to defensive and overseeing operations being done. The most common and simple way of protecting a network aid is by means of assigning it a completely unique call and a corresponding password.

1.1.1 Network Security Concept

Network protection starts with authenticating, generally with a username and a password. Since this requires just one detail authenticating the person call—i.e., the password—that is sometimes termed single factor authentication. With two phase authentication, something the client 'has' is likewise used (e.g., a protection token or 'dongle', an ATM card, or a mobile phone); and with three factor authentication, something the person 'is' is also used (e.g., a fingerprint or retinal test).

Once authenticated, a firewall enforces access to regulations consisting of what services are allowed to be accessed by the community users. Though effective to prevent unauthorized access, this aspect

might also fail to check probably harmful content material including system worms or Trojans being transmitted over the network. Anti-virus software program or an intrusion prevention machine (IPS) helps stumble on and inhibit the motion of such malware. An anomaly-based totally intrusion detection machine may additionally reveal the network like cord-shark traffic and may be logged for audit functions and for later excessive-level evaluation. Newer structures combining unsupervised system getting to know with complete network traffic analysis can stumble on energetic community attackers from malicious insiders or centered external attackers that have compromised a user gadget or account.

Communication among two hosts the usage of a network can be encrypted to hold privateness. Honeypots, basically decoy community-reachable property, may be deployed in a network as surveillance and early-warning device, because the honeypots aren't normally accessed for legitimate purposes. Techniques utilized by the attackers that try to compromise those decoy resources are studied in the course of and after an assault to preserve a watch on new exploitation strategies. Such evaluation may be used to in addition tighten protection of the real network being included with the aid of the honeypot. A honeypot also can direct an attacker's interest far from valid servers. A honeypot encourages attackers to spend their time and energy at the decoy server while distracting their interest from the statistics at the actual server. Similar to a honeypot, a honeypot is a network installation with intentional vulnerabilities. Its reason is also to invite assaults so that the attacker's strategies may be studied and that information can be used to growth network safety. A honeypot normally consists of one or more honeypots.

1.2 SECURITY MANAGEMENTS

Security control for networks is special for all types of conditions. A home or small workplace can also most effective require fundamental protection while massive organizations can also require excessive-renovation and superior software and hardware to prevent malicious attacks from hacking and spamming.

TYPES OF ATTACKS

Networks are problem to assaults from malicious sources. Attacks can be categorized into two classes namely Active and Passive. Passive is defined as when a community intruder intercepts records traveling via the network, and Active in which an intruder initiates commands to disrupt the community's everyday operation or to behavior reconnaissance and lateral motion to discover and benefit get right of entry to property available via the community.

TYPES OF NETWORK SECURITY

Access control

Not each user has to have get access to on your network. To preserve our capability attackers, you need to understand each person and every device. Then you may enforce your security rules. You can block non compliant endpoint devices or provide them only authorized users. This manner is called Network Access Control (NAC).

Antivirus and antimalware software

"Malware," brief for "malicious software program," includes viruses, worms, Trojans, ransom ware, and spyware. Sometimes malware will infect a community but lie dormant for days or even weeks. The first-class antimalware packages not most effective experiment for malware upon entry, but also constantly tune files in a while to find anomalies, cast off malware, and connect damage.

Application security

Any software you operate to run your business wishes to be protected, whether your IT workforce builds it or whether you buy it. Unfortunately, any utility can also contain holes, or vulnerabilities, that attacker can use to infiltrate your network. Application protection encompasses the hardware, software program, and procedures you operate to close the ones holes.

Behavioral analytics

To detect abnormal network behavior, you ought to know what regular activities looks as if. Behavioral analytics tools mechanically change activities that deviate from the norm. Your security group can then higher pick out indicators of compromise that pose a potential problem and quickly remediate threats.

Email protection

Email gateways are the primary risk vector for a safety breach. Attackers use personal facts and social engineering processes to build sophisticated phishing campaigns to deceive recipients and ship them to sites serving up malware. An email safety software blocks incoming attacks and controls outbound messages to prevent the loss of sensitive information.

Firewalls

Firewalls put up a barrier among your relied on inner network and untrusted outside networks, which include the Internet. They use a set of described policies to permit or block traffic. A firewall can be hardware, software, or each. Cisco offers unified thread management (UTM) devices and hazard-focused subsequent-era firewalls.

Intrusion prevention systems

An intrusion prevention system (IPS) scans network traffic to actively block attacks. Cisco Next-Generation IPS (NGIPS) appliances do this by correlating big amounts of worldwide chance intelligence to now not best block malicious activity but also tune the development of suspect documents and malware across the community to prevent the spread of outbreaks and reinfection..

Mobile tool security

Cybercriminals are an increasing number of concentrated on cellular devices and apps. Within the following three years, 90 percent of IT organizations may additionally help corporate programs on personal cellular devices. Of route, you want to control which devices can get access to your community. You will even need to configure their connections to keep network site visitors non-public.

Network segmentation

Software-defined segmentation puts network traffic into exceptional classifications and makes imposing protection regulations simpler. Ideally, the classifications are based on endpoint identification, now not mere IP addresses. You can assign access permission based on position, region, and extra in order that the proper degree of get right of entry to is given to the proper humans and suspicious gadgets are contained and remediated.

Security facts and event control

SIEM merchandise pull collectively the statistics that your security body of workers needs to identify and respond to threats. These products are available diverse forms, along with bodily and digital home equipment and server software program.

Web security

Web security provides the solution to manage your personnel's internet use, block internet-based

threats, and deny access to malicious websites. It will guard your internet gateway on site or in the cloud.

II. RELATED WORK

Battistoni, et al.[1] The network administrators need tools to support analysis and audit tasks and to detect intrusions and malicious activities. Suppose, for example, that in a time interval an attacker is able to exploit a node new vulnerability to attack other nodes of the network. If the administrator has not the right tool, she cannot detect neither the node generating the attack, nor when the attack started. In this type of context, tools that allow reconstructing the entire activities of a system in a determined time interval, collecting evidences of the activities carried out in that interval, are needed. To date, there are two possibilities to accomplish this goal: traditional Computer Forensics (CF) and Live Digital Forensics (LDF). While the former technique is a static analysis of digital helps only after a harmful event, the latter is able to constitute the nation of a stay device for a decided time period. The FOXP architecture is composed of a set of software sensors, once for every network node, that log node activities and then send these logs to a FOXP collector node; this collector node analyzes collected data and manages the sensors activities.

Dodis, et al.[2] Cryptography traditionally relies on uniformly distributed and precisely reproducible random strings for its secrets. Reality, however, makes it difficult to create, store, and reliably retrieve such strings. Strings that are neither uniformly random nor reliably reproducible seem to be more plentiful. For example, a random peoples fingerprint or iris test is clearly now not a uniform random string, nor does it get reproduced exactly on each time sequence was measured. Similarly, a protracted pass-word (or answers to 15 questions [FJ01] or a list of favourite films [JS02]) isn't always uniformly random and is tough to remember for a human user. This work is about using such non uniform and unreliable secrets in cryptographic applications. Our approach is rigorous and general, and our results have both theoretical and practical value.

Maes, et al.[3] The theoretical study of a cryptographic scheme aims to provide a well defined and quantitative understanding of its security. However, while the scheme enters the realistic domain, extra parameters join in the game. A security application does no longer simplest want to be as protect as possible, but also as less expensive, fast, power-efficient and exile as viable, which regularly approach that the safety is decreased on the way to improve those sensible traits. Moreover, the vast expansion of physical attacks on cryptographic implementations has shown that certain assumptions upon which the theoretical security of a scheme is based do not necessarily hold in practice, e.g. the existence of secure key storage. Private keys often need to be stored in publicly accessible devices, e.g. smart cards or RFID-tags, allowing adversaries to physically attack the implementation. Tampering attacks, in which an attacker physically invades the device in order to extract sensitive information, are among the strongest known physical attacks and are in general always able to obtain the private key if no specific countermeasures are taken.

Bosch, et al.[4] Field Programmable Gate Arrays (FPGAs) are gaining widespread acceptance as substitutes for ASICs in many applications. In fact their re-programmability has made them very attractive in the embedded market, where software and functionality updates can be common and desirable by customers. As a result of this shift, it is increasingly the case that the functionality of an embedded system is presented in the form of a bit configuration file or, in the case of microprocessors, in the form of a program. Thus, the very belongings that makes FPGAs so appealing (their programmability) also makes it very smooth for

counterfeiters to copy an IP developer's configuration report and create a comparable product without the up-the front fee of Intellectual Property (IP) improvement. A PUF on an FPGA they could expand protocols that permit binding of a specific IP to a selected FPGA. Their protocols additionally allow proving authenticity of the IP to the hardware platform. The authors similarly reduce the computation and conversation complexity of the protocols in and introduce the concept of Intrinsic-PUFs based on the start-up values of SRAM memory values. Both based their protocols on symmetric-key primitives.

Yu, Meng, et al.[5] PUFs have two broad classes of applications. In some authentication applications, the silicon tool is authenticated if the regenerated reaction is near sufficient in Hamming distance to the provisioned response. To prevent replay attacks, challenges are never repeated. This means the PUF must be resistant to software model-building attacks to be secure. Otherwise, an adversary can create a software model or clone of a particular PUF. If, instead of Hamming-based authentication as we've described, the PUF is to serve as a secret-key generator, only a fixed number of secret bits need to be generated from the PUF. These bits can serve as symmetric key bits or as a random seed to generate a public-private key pair in a secure processor. However, in order for the PUF outputs to be usable in cryptographic applications, the noisy bits must be error corrected, with the aid of helper bits; these helper bits are commonly referred to as a syndrome. The more the environmental variant a PUF is problem to, the greater the feasible distinction (noise) between a provisioned PUF response and a regenerated reaction.

III. EXISTING METHODOLOGIES

Online banking, additionally known as internet banking, e-banking or virtual banking, is an digital charge device that enables customers of a bank or other monetary institution to conduct a range of economic transactions through the economic group's internet site. The on line banking device will commonly connect to or be a part of the center banking system operated by using a financial institution and is in assessment to branch banking which become the traditional manner customers accessed banking offerings. Online transactions are used for the banking system. FORCE technique makes use of a read-once reminiscence to randomly shop digital cash and a physical unclonable function to recover their layout. Online banking, also called net banking, e-banking or virtual banking, is an electronic fee machine that enables clients of a financial institution or different financial organization to conduct a number financial transactions via the financial group's internet site. The on line banking device will typically connect to or be part of the core banking machine operated with the aid of a bank and is in comparison to department banking which was the conventional way clients accessed banking services.

SECURE OFFLINE PAYMENT USING BIT COIN TECHNOLOGY

The proposed method is much more improved when compared to the existing approaches in terms of flexibility and security. This method is the first solution that can provide secure fully off-line payments. The digital coins used are just a digital version of real cash for the transaction. It is the first solution that neither requires trusted third parties, nor bank accounts, nor trusted devices to provide resiliency against frauds based on data breaches in a fully off-line electronic payment systems. Furthermore, by allowing this method, customers are able to be free from having a bank account, makes it also particularly interesting as regards to privacy. The transactions are fully based on the Mobile off-line method. It is important to highlight that the

proposed method has been designed to be a secure and reliable encapsulation scheme of digital coins. This can be applicable to multiple-bank scenarios also. The architecture of this method is composed of two main elements: an identity element and a coin element. The coin element can be any hardware built upon a physical unclonable function and it is used to read digital coins in a trusted way. The identity element has to be embedded into the customer device and it is used to tie a specific coin element to a specific device. The proposed method relies on standard pairing protocols such as the Bluetooth pass key entry simple pairing process. At the end of the pairing protocol, both the customer and vendor devices will share their public keys that will be used for message integrity and authenticity.

METHODOLOGY FOR THE PROPOSED WORK

- User Registration and Login
- Key Generator
- Pairing Phase
- Payment Phase
- Transaction Dispute

USER REGISTRATION AND LOGIN

Users should create an account by providing the basic details username, password, account number etc… These data will be saved in the bank server. The vendor should create account for amount transactions. While login, the entered details will be matched with the available details. If match found, it will proceed to the next step. If match not found, the details should be entered until it matches. This module also used for analyzing fraudulent events. Registered users are only allowed to make transactions.

KEY GENERATOR

User details register into the bank server database for the banking purpose. The details are contains the name, address, contact, and etc. Thus the details are stored on the server database. The secret key has to be writing into the user device. The key generator element is used each within the identification element and in the coin detail. The main responsibility of such an element is to compute on-the fly the private key. Such keys are used by the cryptographic elements to decrypt the requests and encrypt the replies. Key generation is the procedure of generating keys in cryptography. A key is used to encrypt and decrypt something information is being encrypted/decrypted. A tool or software used to generate keys is known as a key generator.

PAIRING PHASE

The coin owner and the receiver devices are pairing with IP address. The source and destination devices will share their public keys that will be used for message integrity and authenticity. This method relies on standard pairing protocols such as the Bluetooth passkey entry simple pairing process. At the end of the pairing protocol, both the customer and vendor devices will share their public keys that will be used for message integrity and authenticity. Furthermore, in order to avoid brute force pairing attacks during the pairing phase, the proposed method adopts a “fail-to-ban” approach. If the number of consecutive bans reaches a security threshold value, the vendor can decide to blacklist the customer. To simplify exposition, all the encryption operations involved in the Bluetooth SPP protocol and used in the pairing process will be omitted here as they refer to standardized protocols.

PAYMENT PHASE

The transaction between users is fully based on the cryptography method. The encryption and decryption process are depend upon the ECC algorithm. The coin value and user details are converted into unreadable format. Off-line banking also called as electronic payment system. The generation and transformation process was fully

based on the ECC (asymmetric) algorithm. The agreement establish between the login user and the bank server. Elliptic curve cryptography (ECC) is a symmetric type based on public-key cryptography approach. This based totally on the algebraic form of elliptic curves over finite fields. It requires smaller keys as compared to non-ECC cryptography to offer equivalent protection. ECC is able to provide the same cryptographic strength as an with much smaller key sizes. The source can be encrypting the coin value used by the destination key.

TRANSACTION DISPUTE

This method securely transfer the coins over the off line method. The receiver sides decrypt the element from the source node. After the reconstruction method update the coin value into the destination side. Due to its fully off-line nature, it does not provide any transaction dispute protocol. Such an off-line dispute could be exploited by fraudsters or malicious vendors by injecting fake faults in the transaction or by altering past transactions. To prevent this possibility, direct off-line disputes between vendors and customers are avoided. However, the proposed method is able to provide an on-line redemption, each off-line transaction can be verified by the bank/card issuer at a later time. This renders a fake transaction dispute attempt too risky and unfeasible to both fraudsters and malicious vendors. The receiver collects the data and decrypts it. Finally update the coin value into the device memory.

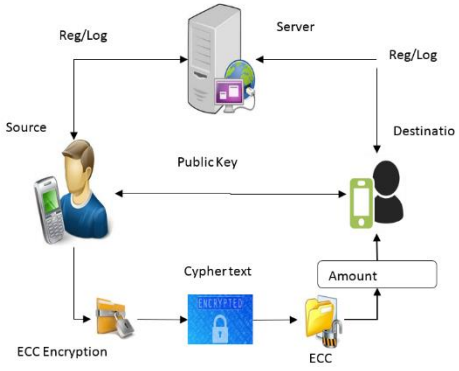

Fig 1 : Architecture for Proposed Work

IV. CONCLUSION

The security evaluation suggests that the proposed technique does no longer impose trustworthiness assumptions. Further, this is also the first solution in the literature where no patron device information attacks may be exploited to compromise the machine. This has been finished mainly with the aid of leveraging a singular erasable PUF architecture and a unique protocol design. The idea has been very well discussed and compared in opposition to the kingdom of the artwork. Proposed evaluation shows that that is the best idea that enjoys all of the properties required to a at ease micro-payment answer, whilst also introducing flexibility whilst considering the payment medium (varieties of virtual coins). Finally, some open issues had been identified which are left as future work.

V. REFERENCES

[1]. Battistoni, Roberto, Alessandro Di Biagio, Roberto Di Pietro, Matteo Formica, and Luigi V. Mancini. "A live digital forensic system for Windows networks." In IFIP International Information Security Conference, pp. 653-667. Springer, Boston, MA, 2008.

[2]. Dodis, Yevgeniy, Leonid Reyzin, and Adam Smith. "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data." In International conference on the theory and applications of cryptographic techniques, pp. 523-540. Springer, Berlin, Heidelberg, 2004.

[3]. Maes, Roel, Pim Tuyls, and Ingrid Verbauwhede. "Low-overhead implementation of a soft decision helper data algorithm for SRAM PUFs." In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 332-347. Springer, Berlin, Heidelberg, 2009.

[4]. Bosch, Christoph, Jorge Guajardo, Ahmad-Reza Sadeghi, Jamshid Shokrollahi, and Pim Tuyls. "Efficient helper data key extractor on FPGAs." In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 181-197. Springer, Berlin, Heidelberg, 2008.

[5]. Yu, Meng-Day, and Srinivas Devadas. "Secure and robust error correction for physical unclonable functions." IEEE Design & Test of Computers 27, no. 1 (2010): 48-65.

[6]. R. L. Rivest, "Payword and micromint: Two simple micropayment schemes," in Proc. Int. Workshop Security Protocols, 1996, pp. 69–87.

[7]. 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.

[8]. T. Micro, "Point-of-sale system breaches, threats to the retail and hospitality industries," University of Zurich, Department of Informatics, 2010.

[9]. 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.

[10]. W. Chen, G. Hancke, K. Mayes, Y. Lien, and J.-H. Chiu, "Using 3G network components to enable NFC mobile transactions and authentication," in Proc. IEEE Int. Conf. Progress Informat. Comput., Dec. 2010, vol. 1, pp. 441–448.

Cite this article as :

R. Ananthi, Dr. S. Nandhakumar, "Efficient and Secure Offline Transaction with Bit Coin Generation ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 3, pp. 51-58, May-June 2019. Available at doi : https://doi.org/10.32628/CSEIT195317
Journal URL : http://ijsrcseit.com/CSEIT195317