OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

TOKEN BASED OFFLINE TRANSACTION SYSTEM

Bazeem Ismaeil Khan[1],Prof.B K Patil

Dept of Computer Science Engineering, Everest College of Engineering and Technology, Aurangabad[1 2]

Abstract: **A proposal of offline transaction system in cellular transactions based on the study of micro-transactions. Actually, it is an study of implementation of safer transaction system in cellular network. The past framework has wide usage of PKI and hashing to outfit solid and secure transaction in cellular commerce. The present work has endeavoured to give considerably more light weight secure offline transactions. The observational activity is completed on three sorts of exchange process considering most extreme situation of offline cases. Therefore, the present thought presents two new approaches i.e. mobile agents and token that can guarantee better security and relatively less system overhead**

Keywords: Micro transaction System, Mobile Agent, Hashing, Wireless Adhoc Network

---

I INTRODUCTION

Advancement of internet business and electronic transaction conventions have increased across the globe, Hence Online payment system is the most important tool for making transaction. A transaction includes: the client, the dealer, and the bank [1]. To guarantee the security of transaction, cryptography strategies have been utilized to accomplish verification, protection, and different prerequisites. Obviously, some cryptography methods are not lightweight, for example, open key computerized signature and undeniable irregular number that is presented in [2]; these procedures are generally used to exchange of cash, which are characterized as micropayment

As of late, the PC and system have grown so quickly that confounded open crypto calculation can be productively executed in the settled system stage. These days, versatile web access suppliers are growing bunches of imaginative administrations to make individuals' day by day life more helpful and fascinating with the fame of Smartphone and other hand-held PC, thus, the quantity of online business exchanges including little measure of cash develop quick, particularly that the small esteem impalpable merchandise (non-physical resources, for example, information and data) are blasting. These minor transactions are characterized as micropayment [3].

Micro transactions are being used in every website for a general or a specific purpose, and this can be done over the web by doing electronic checks, but the cost of merchant or bank is a big issue and also a critical part of any transaction. And thus in cellular network this is an obstacle in doing transaction as it costs a lot for micro transaction [4].

The constrained memory, processing force, and battery limit confine the versatile terminal to execute confused figuring. Additionally, the overhead of correspondence is likewise affecting the accessibility of micropayment plot since more adjusts of information trade makes the plan isn't financial. As of late, some micropayment plans have been proposed to fulfill the upgraded highlight for various prerequisites. Proposal Shamir [5], has a primary issue: a trader can't total micropayments of various clients.

The random transactions will be treated as null and the selected transactions will charge the users. Hence the Rivest solves the issues but undergoes into other 2 other problems i.e. (1) interaction (Between the user and the merchand) and (2) user risk.

MR1 conspire takes care of the principal issue, and does not give solution of second problem. MR2 takes care of the both the issues, yet it is feasible for the client and the vendor to cheat Bank. The third approach [MR3] rotates the identifiable information between user and merchand, eliminating the intrigue between the client and the merchand. In option, there is a fundamental fascination: as opposed to making a decent attempt to avert swindling, the bank essentially rebuffs or dispenses with deceiving parties before they can make any generous harm. In spite of the fact that MR2 and MR3 accomplish a progression of prerequisites of micropayment, there maybe a few troubles for actualizing them in portable system. The calculation ought to be lightweight, which is an essential necessity for versatile internet business convention. Every exchange is marked by the client and sent to the trader; the merchand chooses the exchange such as [MR2] or [MR3].

The complexity of the digital signature algorithm or the hashing algorithm affect the performance of the cellular device. Moreover, the privacy should be preserved and lastly the transaction should be economic. Hence, the paper

introduces simple micro transaction framework using hasing and lagrange interpolation method [6].

The rest of this paper is composed as, Segment 2 will depict the related works in the same domain. Unit 3 will show the proposed micropayment technique the fourth unit explains the Outputs of proposed system. Lastly brief conclusion is given in Section 5.

II RELATED WORK

Anonymous Micropayments Authentication is developed by Zhi-Yuan Hu et al for micro payments in cellular devices. But it has some issues in verification process as it uses cryptographic technique [7].

Several schemes has been introduced by Xiaoling Dai et al. and hence proposed a very powerful scheme with the important features such as multiple transactions, anonymity and service provider [8].

A new model named TMR2 is introduced by About et al which guarantees that the user will not be charged if there is an unsatisfactory product. The author has combined the [MR2] scheme with his idea so as to achieve a trusted model [9].

The coin system has been proposed by Lih-Chyau Wuu it says that the coins verification can be done quickly with hashing method and it assures the privacy and protection of the user [11].

Survey of VivekKatiyare.t. al emphasizes the importance of Eliliptical Curve cryptography and More. Husna and Taylor gives the fundamental aspects to mentain a system for ad hoc mobile transaction and its feasibility [12].

A novel approach proposed by Arogundade et in which the cancelable biometric features are utilized for safely storing the template and generating safe matrix an private keys for applying crypto-techniques. It implements open network system that assures secured transaction to any customer's bank [14].

An important epayment protocol as pay-word is discussed by Mohammad Al Fayoumi and describes its pros and cons and limitations, it guarantees the interaction with safety and privacy [15].

A study of micro-payment and non micro-payment is carried out by Kaylash et al. Smart card based Atm card with biometric based cash for all transactions is given by Isioma Ukpere. Whereas Wang has given a novel system based on smart devices. There are n number of computational processes such as exponential operation for e cash payment. [16].

Date integration in e cash is described by Chang and Curan explained the additional security aspects to strengthen the security framework of Bluetooth devices for e commerce [17].

Wanget suggested a novel transaction system on smart devices, in which users are not restricted to buy e-cash with the fixed face-value. The payment of each transaction is deducted from the customer's account directly; hence, the system can be used with the smart devices effectively [18].

Extensible authentication protocols (EAPs) is used by Natarajan and also used permutation technique, where as it is a process of cubing a random number with a prime one. And these are flexible with all networks with no certificate exchange in between the process [19].

The Token based authentication mechanism is studied by panjwani, it says that a mechanism Eko is already being utilized by the service provider and it explains an another scheme in joint effort with EKo to solve the weaknesses of first. Both the mechanism uses the pins and the codes which are identical for every user for verification and authenticity [20].

III PROPOSEDWORK

The proposed architecture guarantees the security and implements it with authentication and verification mechanism between the mobile agents and the merchants through the tokens. The authorized files are utilized by the merchants to do the transaction and it holds the tokens to resist the unauthorized access from the user, the same mechanism is also implemented with the merchants, hence the architecture consists of the modules like broker agreement, cost and endorsement delivery, broker verification and payments. The explanation is as follows.

A. Broker Agreement

Supplies it's enrolled and approved client a protected and carefully designed token with open key match alongside exceptionally encoded client character. Any micropayment plans like Visa can be utilized for planning the application. The client at that point sends a mark message comprising of hash value and transaction data which is scrambled with open key of dealer. The Agent generates special key value, which consist of a random number, a face value, and size of function, customer identity and expiry of function. The agent private data is affixed with expiry date so as to limit an unapproved client in the scope of versatile system to have an entrance on the classified data executed amongst client and intermediary.

B. Cost and Endorsement Delivery

The sender gives the encrypted cost-request message along with the digital signatures and the private key and asks the destination. The linking nodes adds their certificates to make it easy for the source node to validate the certificates for cost-details. The information is returned back to the source. Once the routing cost is calculated, the secured broker-endorsement is sent to all intermediaries in the group. These are personal data as every user secure it with their private keys, that can be gathered from cost message.

C. Initiating Payment

This progression is tied in with starting transaction in the framework by the client. One sends message in his system and adds a valid hash token from sub-chains. The transaction conspire in autonomous of expanded utilization of hash chain for various transactions by the client guaranteeing considerably less system overhead. In the event that the middle of the road transfer hubs have spellbound the hash chain, it is not possible to decrypt them without broker agreement and its valid signature

D. New Route Consideration

This progression is executed as remote adhoc and frequently changes their topology powerfully. If there arises new path, it is not mandatory to contact any TTP. Overhead is decreased by watching the new hubs in the path and

utilizing them for the circulating protected underwriting. The accompanying calculation clarifies the path arrangement.

Input: grid, number_of_column
Temp A (number_of_column) % 4
noc Å number_of_column
if (temp = 0)
Two_col Å noc
two_col_zigzag (grid,two_col)
Else if(temp = 1)
Two_col Å noc-3
two_col_zigzag (grid,two_col)
three_col_path(grid)
Else if(temp = 2)
Two_col Å noc-2
two_col_zigzag (grid,two_col)
straight_up(grid,noc-1)
straight_down (grid,noc)
else if(temp = 3)
two_col Å noc-1
two_col_zigzag(grid,two_col)
straight_down(grid,noc)
end
horizontal_path(grid)

E. Transferring Tokens

The middle way nodes generates the larger key values in a single chain that is used by the node. The user values then transfer the valid key to the broker along with the digitally signed endorsement. The highly secured information are validated by the broker and the acknowledgement is also issued for the same.

F. Broker Approval:

The Framework allows the multiple-brokers for better communication as it permits any one to get linked with any broker present in the group. A node in one group receives payment from the broker in that group, it says the same node for verifying the digi-docs produced by the nodes in new group as network arrangement modifies. It is pre assumed that the users, brokers and the rest all entities involved are already registered and then performing.

IV EXPERIMENTAL ANALYSIS

For Performance report of the desired micropayment framework, there is a simulation results of the desired systems compared with the payword and PPayword. The two cost are calculated i.e computational and communicational. The communicational cost is the message size of the transmitted payment. The computational cost is the required CPU cycles at the broker end. Experiments are observed in 2 sizes of the chains 10 and 20 and it is partially utilized and not transferable if its size is less than the specified chain-size.

A. Computational Cost of Broker

The Picture depicts the difference of broker load for the desired scheme in contrast with the payword and Ppayword. It is observed that the transactions with transferred chains divides the load by 2, the output confirms the later claims as ppayworld broker load is reduced near by 40 percent. The term semi online refers to the broker load in case to transmitting chain in peers though this transmission is online but offline for payment and does not have any impact on performance. The picture demonstrates that the workload of many of the broker is semi online and very less no of broker's job checking online transaction. The offline and semi online load of broker can be adjusted related to the requirement. For this an upper bound for transmitting chain must be utilized by applying a new column to the broker's database and the value is increased 1 unit/chain transmission and as it reaches the desired upper bound the chain should be blocked.

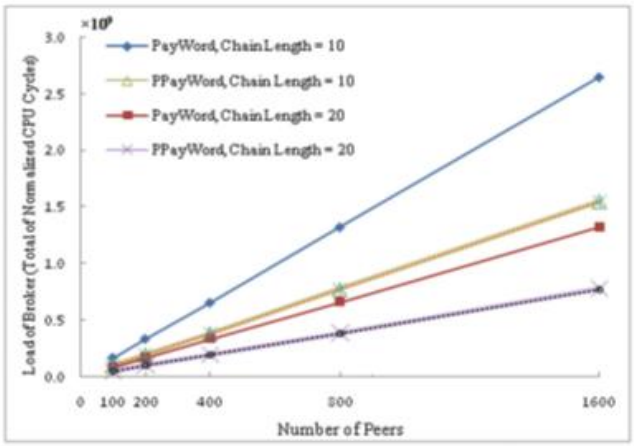

Figure 1. Computational cost

B. Communicational Cost

The second Picture depicts the communication cost in ppayword that it increases related to the size of the chains and the small chain possesses the more committed messages. In next case more no of messages are sent to ppayword. A point to Point Micropayment framework for video captured 89 brokers till the end of the day, the cost in ppayword is segregated over time and without any problem of the payment system. The transfer of maximum chain size possesses the reliability of peers and it can reduce communication cost by eliminating required commitment msgs.

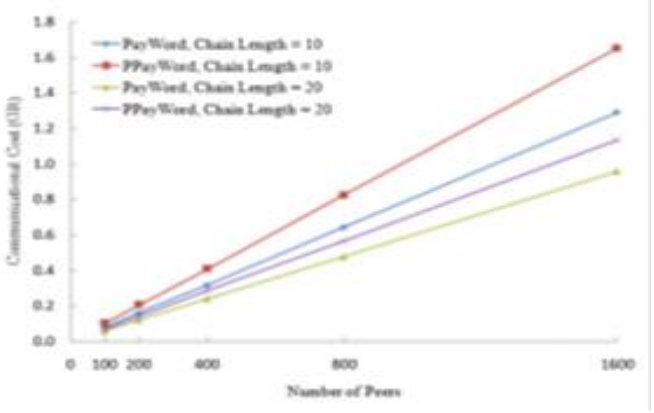

Figure 2 Computational cost

The explained framework in the paper is not customer or merchant specific rather allowing number of merchants to do a secure offline transaction over the group. One of the noteworthy advantages of the proposed scheme is that OSPM transfer the authenticated network channel issues from Mobile-agent and allocates it among the entire merchant. Hence this schema balances the network and processing overhead from merchant over the network. The major benefit of the system is that it guarantees the secure

transaction of the valid tokens as a credit and on the other hand, it also allows the merchants to focus on content-scheduling and agents to perform tasks related to amount management in respective accounts.

The transaction between mobile user and vendor has dual benefits. Primarily, the transfer of the secure message from M1 to M2 does not include any mobile agent and it diminishes the network overhead of the mobile agent. Secondarily, the consecutive secure message posses the m-token of the authorization for which it resists the customer C from any sorts of malicious activities while in offline even when C swaps to another merchant M2. Lastly, the system gives a best, cost efficient and safe network along with enhanced business policy.

V CONCLUSION

Now days the major intension is to develop an secure offline payment module in cellular commerce specially micro transactions. The work has been carried out on the online security with the service operators. But, in this work, it can be seen that SP also requires generating secure supportive hash value for every secure channel data that is sent via smart-phone of the customer C. The service provider sends the valid secured details and the related key values to the merchant for each and every transactions offline. The m-token in system schema considered in customer and merchant dependent. This phenomenon restricts the portability of the secure channel information to a greater extent. The current work therefore has introduced a real time offline payment system from a Mobile-agent and service providers and termed the scheme. The proposed scheme restricts the customers for performing a malicious activity even in offline mode using m-token. Therefore, the proposed system is found to satisfy all the critical security requirements in micro-payment system. The proposed schema is also cost-effective as it does not posses any operation with public key for any types of purchases being made.

REFERENCES

[1] Zygmunt J. Haas, Jing Deng, Ben Liang, Panagiotis Papadimitratos, S. Sajama,"Wireless ad hoc Networks", John Wiley & Sons, Inc, 2003

[2] Yuntsai Chou, Chiwei Lee and Jianru Chung, "Understanding m-commerce payment systems through the analytic hierarchy process", Journal of Business Research, Volume 57, Issue 12, December 2004, Pages 1423-1430

[3] Neal Leavitt, "Payment Applications Make E-Commerce Mobile", IEEE Computer Society, 2010

[4] Rafael Martínez-Peláez, Francisco Rico-Novella, Cristina Satizábal and Jhon J. Padilla, "Performance Analysis of Mobile Payment Protocols over the Bluetooth Wireless Network", Whitepaper, 2008

[5] HeikoKnospe, Scarlet Schwiderski-Grosche, "Future mobile networks: ad-hoc access based on online payment with smartcards", IEEE, 2002

[6] Peter Tarasewich, Robert C. Nickerson, Merrill Warkentin, "Wireless/Mobile E-commerce: technologies, applications, and issues", Seventh Americas Conference on Information Systems, 2001

[7] Zhi-Yuan Hu, Yao-Wei Liu, Xiao Hu, Jian-Hua Li, Anonymous Micropayments Authentication (AMA) in Mobile Data Network, INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies Iss: 7 March 2004,

[8] Min-Shiang Hwang, Pei-Chen Sung, A Study of Micropayment Based on One-Way Hash Chain, International Journal of Network Security, Vol.2, No.2, PP.81–90, Mar. 2006

[9] Al-Fayoumi, M., Aboud, S., Al-Fayoumi, M., "Practical E-Payment Scheme", International Journal of Computer Science Issues, vol. 7, no. 7, May. 2010

[10] Xiaoling Dai, OluwatomiAyoade, and John Grundy, Offline Micro-payment Protocol for Multiple Vendors in Mobile Commerce, Proceeding PDCAT '06 Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, IEEE Computer Society Washington, 2006 R. Hauser, M. Steiner, and M. Waidner, "Micro-payments based on iKP", in Proc. of the 14th Worldwide Congress on Computer and Communications Security Protection, Paris, 1996, pp.67-82, http://www.zurich.ibm.com

[11] Lih-Chyau Wuu, Kuang-Yi Chen, Chih-Ming Lin, OffLine Micro Payment Scheme with Dual Signature, Journal of Computers, Vol.19, No.1, April 2008

[12] VivekKatiyar, Kamlesh Dutta, Syona Gupta, A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment, International Journal of Computer Applications (0975 – 8887) Volume 11– No.10, December 2010

[13] FouziaMousumi, Subrun Jamil, Push Pull Services Offering SMS Based m-Banking System in Context of Bangladesh, International Arab Journal of e-Technology, Vol. 1, No. 3, January 2010

[14] Arogundade O.T, Ikotun A. Motunrayo, OlaniyiAdemola, Developing a Usage-centered e-Payment Model using Open Network System, International Journal of Computer Applications (0975 – 8887) Volume 12– No.6, December 2010

[15] Mohammad Al-Fayoumi, SattarAboud and Mustafa AlFayoumi, Practical E-Payment Scheme, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010

[16] Kaylash Chaudhary, Xiaoling Dai and John Grundy, Experiences in Developing a Micro-payment System for Peer-to-Peer Networks, International Journal of Information Technology and Web Engineering, vol. 5, no. 1, 2010

[17] C. C. Chang and Y. P. Lai, "A flexible Date-attachment Scheme on E-cash", Computers & Security, Vol. 22, No. 2, pp.160-166, 2003.

[18] Jian-Sen Wang, Fuw-Yi Yang, and Incheon Paik, "A Novel E-cash Payment Protocol Using Trapdoor Hash Function on Smart Mobile Devices", IJCSNS International Journal of Computer Science and Network Security, Vol.11 No.6, June 2011

[19] Natarajan Vijayarangan, "A system and design of Extensible Authentication Protocols based on ECC and SKE mechanisms for mobile and wireless communications", Advances in E-Activities, Information Security and Privacy, 2011