International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-3, Issue-1, January-2015

Alternative Approach of Handling DOS Vs Mobility Management with Effective Utilization of Client's Needs

Jayamoorthy.S, Gosaladevi.G, Sathiyanarayanan.P.

***Abstract*— Nowadays, a wide range of money flow involved through network communication or wireless communication such as online transaction, mobile transaction, e-payment etc., but yet the 100% security towards the client side opinion not satisfied. Here consider a simple secure authentication criteria for providing security towards ATM's user while cash withdrawal. Because ATM faces lot of security issues such as: Reputation, High rate flooding attacks, Denial of services(DOS), mail bomb, etc., In order to overcome these issues the mobile management authentication is used to provide alternative transaction based solution towards the ATM's user during their normal transaction. Through this better solution obtained between service management for users with immediate response program for entire networks application.**

***Index Terms*—ATM, DOS, mail bomb.**

I. INTRODUCTION

The development technology leads to number of innovative approaches with introduction of every new idea towards the global research. In this way the mobile technology has introduced number of services towards effectively to user. The network communication in early days has limited setup through specified way; it can be optimized by the person one who needs it. But this situation is suddenly/rapidly changed over in the developed countries like U.S, U.K etc., Similarly these countries are maintaining their data in very secured manner. Developing countries like India has facing some problems while implementing the innovative ideas in esteemed manner, because of lack of social and economical factors. Even though these extremes the continuous involvement towards latest technology with new upgradations the innovations still find a next.

In this case of mobile computing it provides number of services towards every individual who involved in network communication. Here discussing about mobile transaction (MT) towards the services provided by ATM. The term ATM (Automated Teller Machine) and in financial purpose we say (Automatic Money Transfer) i.e., transfer of money and withdrawal of money from ATM's anytime, anywhere which is called as Ubiquitous computing.

It is evident from [2] that,

Ubiquitous computing = nomadic + mobile computing.

Whenever a transaction is made through ATM, the actual money is not transferred only the money value can be increased and decreased between the cardholder and the account holder. These are general purpose expected from our innovative towards money transfer. On behalf of it, the number of issues related to usage of ATM's service is called network issues.

These issues are classified based on the following:

1) Denial of services through service provider.
2) Loss of services through legitimate users.

II. RELATED WORKS

There are many articles related to Denial of Services (DOS) attacks in a network environment. Each and every author can revealed lot of alternative solutions to the problem which directly/indirectly support various other network problems or attacks which may be happened in the wireless environment. Whilst the Mori's worm severely disrupted the nascent internet as it existed in 1998, the historical record places the first reported large scale and deliberated Denial of services attack via the public internet.

Limited very soon after that incident, in February 2000, a group of popular e-commerce websites, i.e., yahoo.com, cnn.com and ebay.com also suffered from the DOS attack.

A DDOS attack is one in which a massive amount of compromised systems attack a single target, causing denial of services for users of the target system. Basically DDOS attacks are network traffic jams that temporarily block access to targeted websites, but it was little but different towards ATM based DOS. On the whole both the cases, the services is lost due to some external or internal interrupt or some distortion such changes may happened.

The republic bank doing to prevent DDOS attacks is to limit service interruption and protect client data as well as need to satisfy the user expectation. While DDOS attack can't give assurance of 100% prevention, but it works determinately to deploy effective security measures to protect customer data.

As mentioned in [1], the role of FFIEC (Federal Financial Institution Examination Council) takes measures not only to prevent such attacks, but it also wants them to

Manuscript received December 26, 2015.

Jayamoorthy.S, Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India, +91-9791866601.

Gosaladevi. G, Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India, +91-9750673524.

Sathiyanarayanan.P, Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India, +91-9787138339.

Implement Incident Response Programs (IIRP).

Through the alternative works, it focuses on overall network satisfaction with limited IIRP in current implementation. Here, we provide a little bit extended features supported for DOS happened in ATM's with some mobile agent based alternative solution to this attack is established.

III. EXISTING SYSTEM

The usage of money transaction throughout the world with the electronic medium of services such as e-payment, online-transaction and ATM play an vital role. In this scenario, there will be lot of security measures handled by every banking sector. So, simple transaction management is handled by ATM service centers. Past recently, the ATM services handshake with mobile management it provides the SMS services towards the clients. But it should be limited to certain extent especially in the case of DOS happened during at the point of executing single or multiple transaction. When the customer swipe the card, then enter the password, followed by the system which shows that your service is processing. But within a few seconds, ATM screen shows "ATM is out of services" notice displayed.

This case happened due to the following reasons:

1) The communication line is interrupted
2) Switching server is down state
3) ATM is run out of paper
4) Card reader is failed.

In this case, the above processing results that particular transaction results i.e., SMS is sent to the customer with the help of mobile agent, which is some amount of Rs.XXX is debited from that person's account. But actually cash can't be withdrawn from ATM's due to above discussed points from that last two points based on the "Regular Services Management" monitored by the person's fault. But first two reasons may happened due to network performance and therefore maximizing the server downtime so which may be happened at anytime, anywhere for any one. For this case of failures still there is only one solution/suggestions given by the banking sector i.e., ATM dispensed cash, customer just took card without taking money within 30 seconds. But for failure he should give complaint over the ATM's family bank or in case of cross over services complaint towards the ATM's service bank. For this case, there is no proper solution and authentication towards user needs so still there is an issue of ATM services.

So far, we discuss various factors that leads the ATM's service centre facing DOS during the anytime, anywhere, anyone process failures with number of issues related to these criteria are discussed. Here we focus the "Point of Failure". In the mobile ad hoc network, the above failure happened at anywhere in the communication node, it should be monitored by some near hop towards the failure node can take immediate response towards the end user node with the help of monitoring authority(MA). In the similar way, ATM's service centre is also monitored by some main server and some backup server. Whenever that particular ATM's service center fails the sub-server or the monitoring server can take earlier response towards matching that particular customer's mobile number with transaction states are already existed. But further particular focused on the criteria i.e., money which is completely disposed cash towards out of ATM's are not considered and the failure reasons are immediately SMS towards the customer. In order to overcome the feelings of end user along with their transacted money failure reasons are to be known by the customer immediately. Now question arises from lateral thinking people i.e., when ATM's is failure due to above mentioned criteria such as

1) ATM is out of service.
2) Switching server is down, etc.,

Ideal thinker can take further steps towards the back up monitoring server as well as other alternative service provider for this case. Because it is monitored by some backbone machine can take immediate actions on that last processing service user account number with their mobile matching mobile agent module can automatically take responsibilities and send valid SMS towards them, i.e., Reasons for failure and their account status is intimated as service to the customer through this implementation the next level security and trust towards clients is gradually increased.

IV. SYSTEM ARCHITECTURE

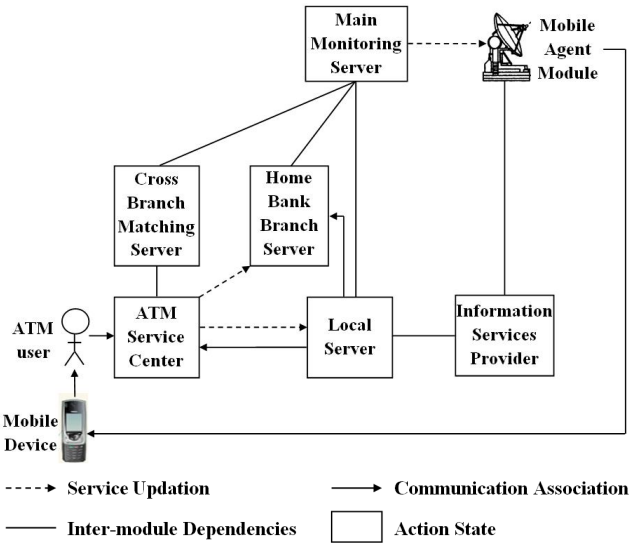

Fig 1: System Architecture

The system architecture depicted in fig.1, shows detailed description about how the DOS is happened during the customer account processing in either home branch or cross home branch ATM's centre. Suppose this case is faced by anyone, anytime anywhere during their cash transaction, this problem is managed by the monitoring server or by the local server can immediately provide the solution with the help of Mobile Agent Module (MAM) through SMS services of sending transaction report along with reason for failure during that particular transactions as mentioned earlier and also if any new attempt of failures status is also processed immediately and instance response towards the customer using ATM's services. Through this next level extend the overall utilization of ATM's centre facility is increased in future.

V. CONCLUSION

Even though the banking sector extends their services through ATM service centre and e-payment transaction services, online transactions etc., but still authentication issues are exist. The financial sector is also increasing their security in number of alternative ways. The problems focused are, when the client debit their money from any home ATM bank or need service from cross ATM's, it will be updated in local and main server. But some time during the customer service is processed by ATM's service centre, if some Denial Of Service is occurred the money not disposed to customer but the SMS sent to the customer about that particular transaction is debited. During this time, the customer/clients face the lots of problem practically. In order to overcome it, the main server or monitoring server can update the last transaction details of every ATM's centre with the result of cash flow in every service centre details. The instant response is SMS towards the client mobile with the matching of account number with mobile number through mobile agent module. Through this way, the next level confident/trust provided towards every end user.

REFERENCES

[1] Amila Karunanayake, Kasun De Zoysa, Sead Muftic, "Mobile ATM for developing countries", MobiArch'08, August 22, 2008, Seattle, Washington, USA Copyright 2008 ACM 978-1-60558-178-1/08/08.
[2] Abdelsalam A Helal, Richard Brice, Bert Haskel, Marek Rusinkiewicz, Jeffery L Caster and Darell Woelk, "Anytime, Anywhere Computing, Mobile Computing Concepts and Technology", Springer International Series in Engineering and Computer Science, 2000.
[3] ATM and Debit Card Questions [Online]. Available: https://www.wellsfargo.com/help/faqs/debit-card/
[4] ATM Based Services [Online]. Available: http://www.banknetvn.com.vn/sites/english/FAQ/1-Local-Switching/Trang/ATMBasedServices.aspx
[5] Consumer Information on Electronic Banking, Federal Trade Commission [Online]. Available: https://www.consumer.ftc.gov/articles/0218-electronic-banking
[6] Frequently Asked Questions [Online]. Available: http://www.firstbanks.com/faq.asp
[7] The Banking Ombudsman Scheme, 2006, [Online]. Available: http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=159
[8] Electronic Funds Transfer Services, [Online]. Available: http://www.scotiabank.com/ca/en/0,,559,00.html

Jayamoorthy.S has completed Bachelor's Degree in the field of Information Technology and Master's Degree in the field of Computer Science and Engineering. He is interested in the area of Vehicular Ad hoc Networks, Network Security and Image Processing. He has published research papers in various domains. He has attended a few workshops and faculty development programs related to his discipline.

Gosaladevi.G has completed Bachelor's Degree in the field of Computer Science and Engineering and Master's Degree in the field of Computer Science and Engineering. She is interested in the area of Network Security. She has attended workshops and faculty development programs related to her discipline.

Sathiyanarayanan.P has completed Bachelor's and Master's Degree in the field of Computer Science and Engineering. His interest is in the area of Vehicular Ad hoc Networks and Network Security. He has published research papers in multiple domains. He has attended a few workshops and faculty development programs related to his discipline.