ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2013.0102

CONCEPTION OF BI-FOLD AUTHENTICATED AGENT – MONITORED TRANSACTION ARCHITECTURE

Srivatsan Sridharan[1] and Gorthy Ravi Kiran[2]
[1]*Department of Computer Science, International Institute of Information Technology Bangalore, India*
E-mail: vatsan.s@rediff.com
[2]*Department of Networking and Communication Systems, International Institute of Information Technology Bangalore, India*
E-mail: grkmss@gmail.com

Abstract
The aim of this paper is to provide an introduction towards the architectural design of a bi-fold authenticated agent-monitored transaction model. The focus is primarily on implementation in ATM systems which provide the following facilities of withdrawing currency at any remote terminal, verification of the end users identity using Personal Identification Number and an authentic One-Time-Session-Dependent Key generation and validation through the mobile. This system requires building up of an third party agent which would establish a secure session to the bank application with the terminal only after a series of authentication mechanism without compromising the privacy of any individual. The customers, without any insider privileges, can withdraw currency without being detected by any mechanisms of theft of card and eaves dropping of the Password from the card holders within the terminal software are also a major threat yet to be addressed. A basic solution is the terminals having bi-fold authentication mechanisms where mobile dependent one time session dependent key is being generated with authenticity being ensured and the confidentiality being maintained. In such a system, the correctness burden on the terminal's code is significantly less as the customers have been given the chance to authorize themselves from their hand-held devices and are allowed to withdraw currency in terminal only after their identity is proved by a series of authentication procedures. In this paper along with the bi-fold authentication implementation, architectural design of the agent which is being introduced is also briefed.

Keywords:
Authentication, Confidentiality, Encryption, Security

1. INTRODUCTION

The need for authentic transactions of any form has now become a primary focus area. Need for integrity, authenticity together with the confidentiality is now being enforced for any operations worldwide. The primary focuses are with respect to the ATM - Automated Teller Machine [5] as these system deals with the delicate matter of currency transfer. Automated Teller Machine is a system which has been installed to give money instantly to the customers at a lightning speed. ATM systems have been installed at various places across the globe by various financial institutions. These systems have been given the secure way of authentication by providing a Personal Identification Number (PIN). PIN is assumed to be kept secret by the ATM card Holder. This PIN will be asked from the customers when their card has been recognized by the terminal [1] [2]. So the process of authentication starts after the card is being sensed by the terminal and stops after the PIN is being entered in the terminal. As the possibility of means of eaves dropping of the PIN and the abuse of the ATM cards have dramatically increased all around the globe, the need for further evolution of authentication phenomenon has emerged for replacement of the current existing procedures. This paper deals with an effective way of the handling such issues with an bi-fold authenticated agent and also the architecture that is being developed to implement such a system that could be more resistant towards such attacks and the phases which ensures the confidentiality associated with these delicate transactions are also maintained at the high stake.

The section 2 of this paper deals with the current existing mechanism of the ATM Terminals and the existing procedure that is being followed for cash withdrawal in the ATM Terminals. Section 3 of the paper deals about the proposed system design and methodologies and the section 4 introduce the concept of the agent and the internal architecture of the agent. Section 5 describes the failures and following section describes the remedies to the failure. Section 7 describes the various functional components of the proposed system and section 9 describes the various modules in the proposed internal agent and the section 10 about the phases in the proposed system.

2. EXISTING SYSTEM

There is increasingly widespread adoption of ATM systems across the globe. ATM system across the globe is known for its famous instant cash delivery to the customers. Customers need to introduce their ATM card provided to them by their financial institutions. Also they are supposed to provide their Personal Identification Number to complete their process of authentication. When their authentication is complete, the customer is allowed to select the type of transaction to be made by them - either balance enquiry or instant cash withdrawal. The authentication of these systems depends upon only the PIN secrecy and the well known fact of the current global situation is that the possibility of eaves dropping of the PIN has exponentially grown over the past few years. Need for enhanced architectural design of this mechanism arises along with the well known fact of maintenance of confidentiality. Also the entire process of the cash withdrawal from the ATM Terminals is done with a help of single governing institute of that particular country, for example the Reserve Bank of India in the mainland of India. The governing body is thus concerned only about the financial aspects and usage of the ATM. Many non-financial services could be achieved by the process of set up of a third party agent, which would help in making ATM used for many non-financial services.

3. PROPOSED SYSTEM

The ATM card and the PIN that is being currently being used by the existing system is necessary along with the user Mobile number registered officially with the financial institutions that provide the user with the ATM card. From the globally known

figure that estimates the fact that almost all the populations who have their ATM card are also the user of at least a mobile, this technique is being proposed. Also the challenges of security associated are being addressed. The main issue of improving the authenticity is enforced in this proposed system.

The user inserts the ATM card into the recognizing terminal. The terminal now senses for its validity. Then the terminal does not ask for the PIN number to be entered, instead sends the one time Session-Dependent Password (SDP) to the user officially registered mobile number with the help of the agent. So first a temporary time-dependent session is established between the third-party agent and the Terminal. Agent is provided with only the repository of valid ATM card numbers issued by all the financial institutions (perhaps the possibility of the need for one such agent per country arises) along with the mobile number associated with it. Thus the issue that is pertaining to the eaves dropping is now solved as the SDP is sent to only the officially registered mobile of the customers.

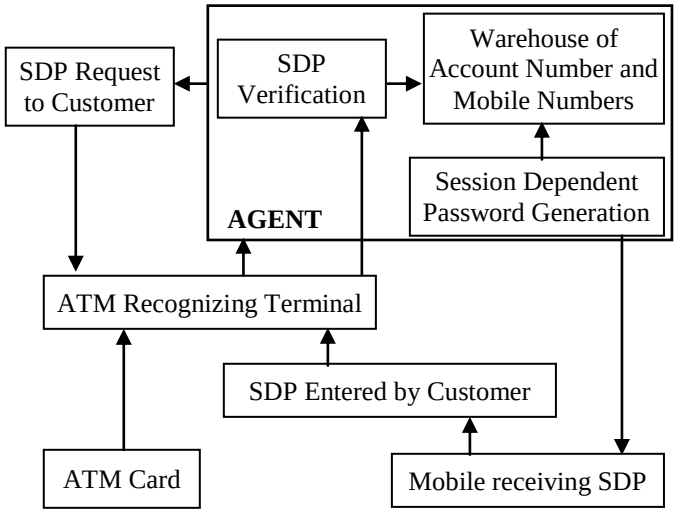

Fig.1. Functional Unit of the proposed System

The bank application is only now approached by the terminal after the session is successfully terminated between the agent and terminal and not aborted. So now the bank application has an extra-level of authentication about the customer that they are both authenticated and validated. Also the SDP and session between terminal (ATM) and agent is time dependent, i.e., the SDP generated expires five minutes and provision of one time regeneration of the SDP is also available in adverse case of the non reception of the SDP to the registered mobile.

The mobile once misplaced shall be brought to the notice to the respective financial institution by the card holder so that the option of change of the mobile number might also be provided. There is a unique back end computation of the SDP with the help of the trusted third party agent so that after this phase only, the PIN number is asked to be entered by the customers. Once the SDP is verified, a secure session as in the existing system is then set up between bank application and the ATM machine for the instant currency withdrawal or for balance enquiry. A chance of entering the SDP sent to the user mobile is fixed to be three so that an additional fold of authentication is also ensured and a leniency towards the end user misread the SDP is also achieved.

The method for computation of the SDP is unique and it is based on the Code number of the Branch of that particular financial institutions and four digits of the account number selected at random followed by an four digit random number (it is chosen as four digit since the PIN is commonly a four digit secret Number). Also the SDP is asked to be entered only preceding the entry of mobile number from the Customer in the ATM terminal which provides another tier of authentication. The third party agent responsible for generation and verification of SDP is only given a read-only version of the customer's account number along with their mobile numbers and refreshed periodically to add, drop and update the account number and their corresponding mobile number.

4. ARCHITECTURAL COMPONENTS

The functional units of the proposed system contain the different stand-alone components along with an introduction of an agent which are needed to be interfaced in proper fashion to obtain the desired functioning of the bi-fold authenticated agent monitored transactions. Architecture depicts the various stand alone components which has their specific functionalities which could be efficiently utilized by providing the requisite coordination among each others. The need for proper design of agent is more important as the agent plays a crucial role in integrating authenticity with confidentiality.

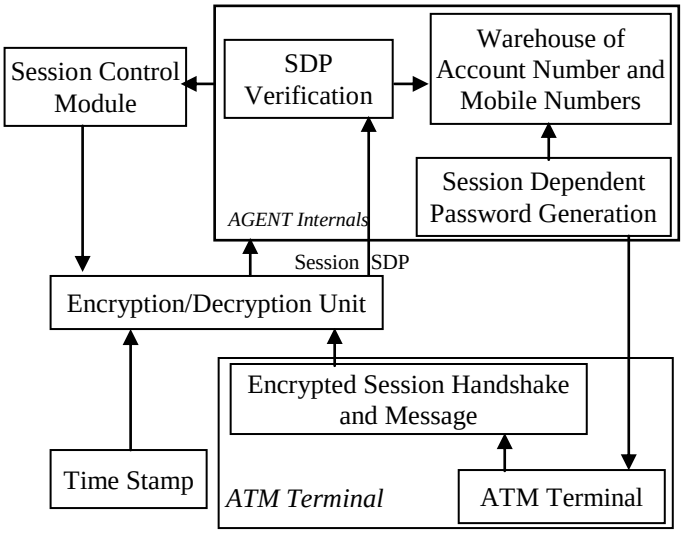

Fig.2. Internal Architecture of Agents

5. FAILURES IN EXISTING SYSTEM

Exploiting the lack of personal weakness of the customers, duplicating the role of a distinct individual, accessing customer's personal possession, and the lack of an internal security mechanism [3] for the complete authentication phenomenon are the main failures in the existing system. An Important failure in the existing system is the lack of the complete authentication phenomenon in the ATM terminal. Any individual is not completely authenticated before they are allowed to perform the transactions in their ATM terminal. Their authenticity is only determined with the PIN they enter in the terminal. The true verification of their identity with any other available means is not the concern of current ATM terminal. As the exploitation of the

weakness of any individual customer has risen exponentially over past few years, the demand for multi-fold distinct and unique authentication has occurred.

6. REMEDIES TO FAILURES

There is a secure complete authentication of the customer in the ATM terminal. The compete authentication is provided with the help of the generation of the SDP and transmitting it to the mobile number of the customer and allowing the customer to enter their the SDP received by their registered official mobile in the ATM terminal which is then preceded by the back-end verification of the SDP entered by the customers in the agent internals depicted in the architecture. All these process of SDP transactions between the ATM terminal and the Agent are encrypted to add an additional fold of security.

The big advantage rested with these systems is that once the SDP is being entered wrongly for three consecutive times, the transaction for that account number is temporarily blocked for next 24 hours and there is no session established between the bank application and the ATM terminal as all the transactions are dealt only between the customer and the agent. To resolve any adverse effect of discrepancies, the possibility of one time regeneration of the SDP is also facilitated. To facilitate the implementation of these remedies to the failures along with the introduction of a third party application - agent, addition of encryption unit in the existing terminal (ATM) is required.

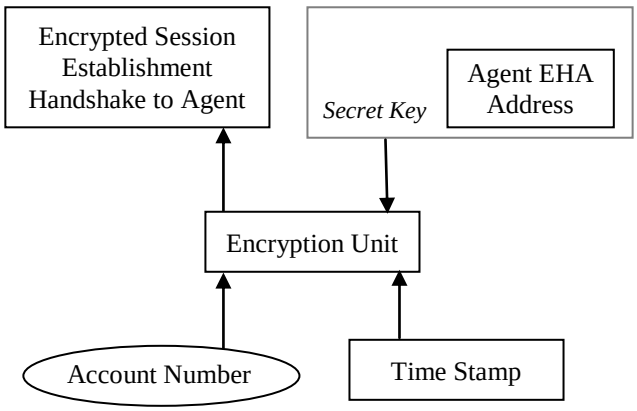

Fig.3. Session Establishment Handshake message

7. MODULES IN PROPOSED SYSTEMS

Agent is a trusted third party application which has a warehouse of only the Mobile number and ATM account number of the customers' which is helpful in the recognition of the valid ATM account number of the user and transmitting the SDP to the respective mobile number of the user and also performs the process of SDP verification. The architecture of the agent must cover the aspects of both authentication enforcement and the secure transaction establishment. Any mechanism of fraudulent action is being restricted by the SDP generation component as the session is established between the bank application and the ATM terminal only after the session dependent password is validated and verified. Agent has internally two software oriented module namely the SDP generation module, and Session Control Module (SCM). Agent needs to be commissioned country-wise across the globe as the norms and regulations differ amongst the countries.

SDP Generation is a module which is basically a software embedded with the agent to generate the SDP to the intended mobile of the users. It uses the warehouse provided and refreshed periodically by the financial institutions which holds the information about account number and their respective, mobile number. This is intended to generate a unique and non-repetitive SDP's for different customers which can be treated as first level of the authentication provided at the terminal. After SDP generation it updates the secondary dynamic repository.

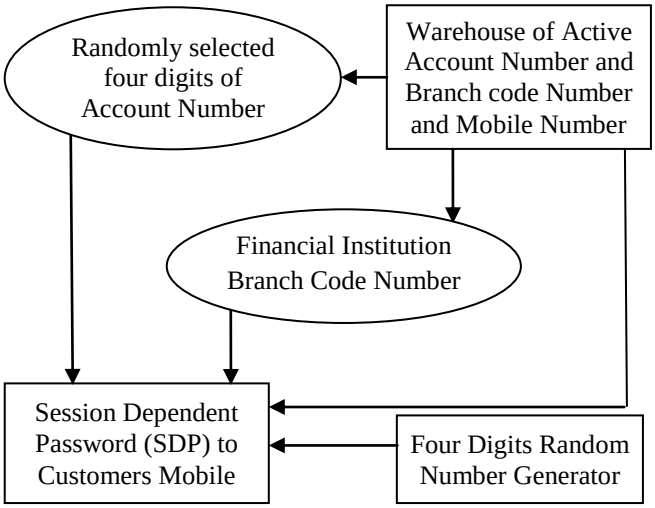

Fig.4. Session Dependent Password Generation Module

Session Control module is responsible for the acceptance of encrypted session establishment handshake message and the SDP validate request encrypted session message from the terminal. The encrypted session establishment handshake is depicted in the Fig.3. Once this message is received by the SCM it decrypts with its private key (EHA) - Ethernet Hardware Address and validates the ATM Account Number from the repository. If the ATM account number entry is present in its warehouse then the SDP generation module generates the SDP and sends SDP Request message to the ATM Terminal. This SDP Request Message has the account number encrypted with the secret key, the EHA.

The SDP validate request encrypted session message is depicted in the Fig.5. Once it validates the SDP to be true then the session existing between ATM Terminal and the agent is now transferred smoothly to the intended financial institutions application. Agent here acts as an authentication gateway and the financial institutions are made earlier aware about the agent application and therefore accept any incoming session transfer request message from the agent and now session between agent and ATM terminal terminates and between that of bank application and terminal begins. This session transfer request message is obtained from the SDP validate request encrypted session message after SDP validation dropping the SDP and encrypting again with EHA.

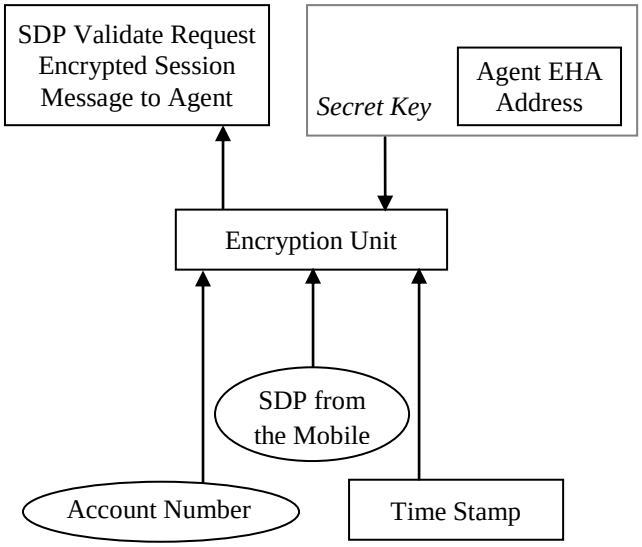

Fig.5. SDP Validate Request Encrypted Session Message

The secret key is the Agent Ethernet Hardware address (EHA) for both bank application to accept the incoming session transfer request message from agent and encryption of session messages between the terminal and the agent. Identity theft (or EHA spoofing) occurs when a cracker is able to listen in on network traffic and identify the EHA address of a computer with network privileges. Most wireless systems allow some kind of EHA filtering to allow only authorized computers with specific EHA IDs to gain access and utilize the network. EHA filtering is effective since it provides protection against the spoofing and also spoofing is local only to broadcast domain. The Secret key used therefore could be ensured to be a private key known only by the agent to decrypt the process. Also intra-terminal communication could be blocked to provide additional fold of security. The account number sensed from the ATM terminal along with the time stamp is encrypted with the EHA as the key and sent as a session transfer request message to the bank application which serves as self-authentication of agent to the intended financial institutions. From the Account number, it could now identify its respective financial institution.

There are two separate *repository designed*, one the primary repository acting as a configured warehouse for the SDP generation which is provided by the financial institutions comprising of the mobile number and the account number of the customer. Second repository is dynamic in nature named as secondary repository containing the account number, Branch code number and mobile number along with the SDP generated which helps in the session establishment between the bank application and the ATM terminal after bi-fold authentication mechanism is completed. The respective account entry in the secondary repository is kept active for exactly five minutes from the generation of the SDP and updation of the flag in the primary repository provided by the financial institutions if the SDP mismatch occurs for more than three times against the SDP generated or request for new SDP generation is made more than two times consecutively. Both the respective repositories are maintained separately for each financial Institution.

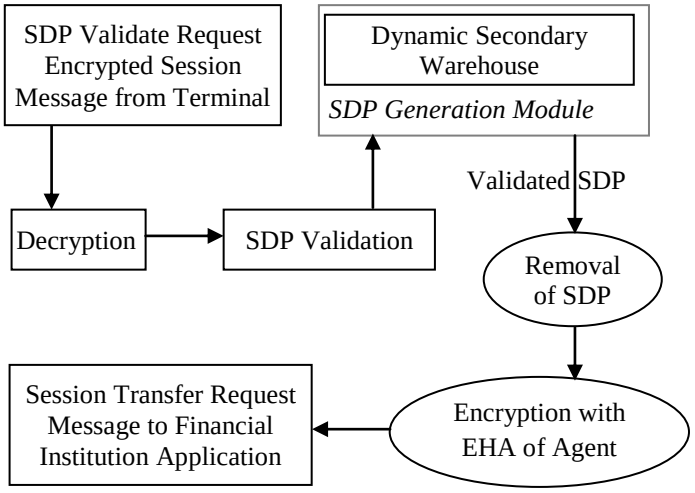

Fig.6. Session Transfer Request Message

In such cases the suspect for fraudulent action is sensed dynamically and the corresponding account number of such happening is deactivated for next 24 hours denying any further service. Also the update on the warehouse on behalf of request by financial institutions on change of the mobile number is also entertained. As these agent repositories does not have the PIN number associated with the ATM Card, the secrecy between the financial institution and the customer is not spoiled along with the dual-fold authentication also made possible. Also as sensing the fraudulent activity is made dynamic associated with the agent application, the financial institution worry about the absence of completely authenticated transactions is therefore abolished.

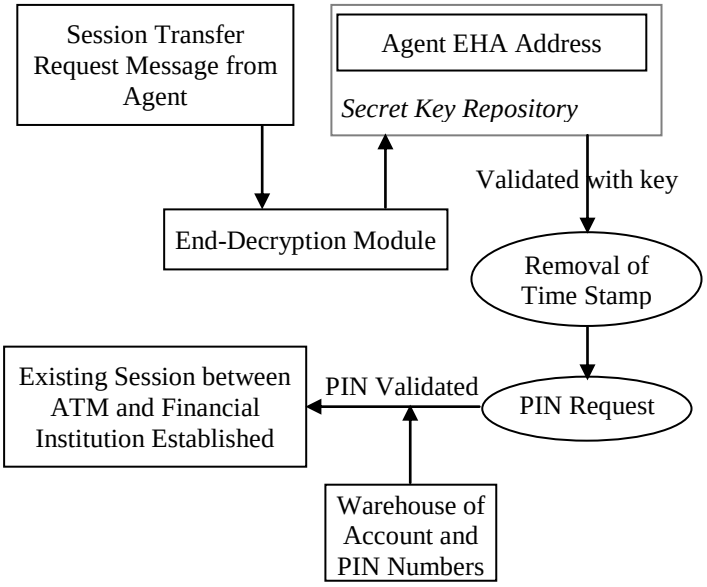

Fig.7. End-Decryption Module introduced in Existing System

End-Decryption Module is the additional module need to be incorporated into the current existing financial institutions application. This module has in the repository, the Agent EHA address - the secret key. It becomes more convenient as the agent can be proposed on the national basis and the norms of financial institutions are generally country - dependent. In this module, the decryption with the Agent EHA Address is facilitated and then the original message from the ATM terminal forwarded via agent is

obtained. Then the time stamp is removed which facilitates the PIN request (PIN that corresponds to the Account Number) from the customer from the ATM Terminal. Then PIN is validated and the session that is now existing between the ATM Terminal and financial institution comes into the picture.

8. FUNCTIONAL COMPONENTS

Customer must be given an ATM card by the financial institutions and can make use of it in the ATM terminal where the session first is established between the ATM terminal and trusted third part Agent. Thus the SPD generator generates as soon as the ATM card recognizing terminal recognizes the card as well as the agent validates the account number and the customer mobile is sent with the SPD generated at the third party application. If the SPD is wrongly entered thrice or the request for new generation of SPD exceeds the limit allowed the corresponding account is temporarily blocked for 24 hours suspecting suspicious activities.

Else only after the SPD validation, the existing mechanism of secure session establishment between bank application and the ATM terminal happens and further transactions is facilitated. This mechanism also facilitates the complete removal of the fraudulent activity of usage of the forged ATM cards as the mobile with respect to the forged ATM card is not available with them. This approach also prevents additional fraudulent activities of eaves dropping as the session between the agent and the ATM Terminal is encrypted before the process of validation. The Fig.5 shows the functional flow of the entire proposed system. The flow between the current ATM Terminal and the Bank Application is separated now by a encrypted flow of session through the Agent to achieve a complete authentication phenomenon.

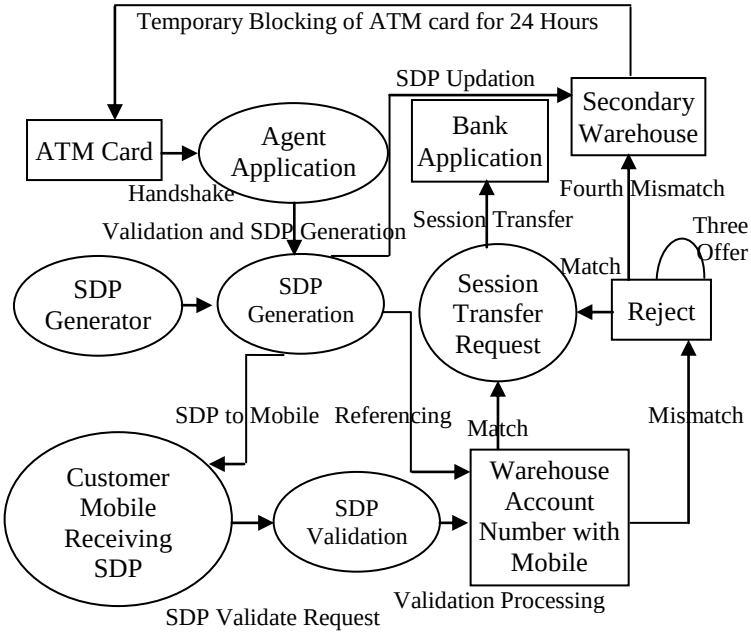

Fig.8. Functional Flow in the Proposed System

9. PHASES IN THE PROPOSED SYSTEM

One Time Session Establishment Before a transaction takes place, one of the first things the ATM terminals must do is the establishment of a one Time session between the ATM terminal and the Agent. It includes the three message flows between the agent and the ATM terminal. These messages are Session Establishment Handshake Message, SDP Validate Request Encrypted Session Message and the Session Transfer Request Message. This is done by sending the first token of the ATM card account number along with exact time stamp encrypted with the Agent secret EHA Address so that agent can only decrypt it, as the EHA address of itself is maintained with high secrecy. The one-time session establishment is helped in checking the authenticity of the user with the help of the agents.

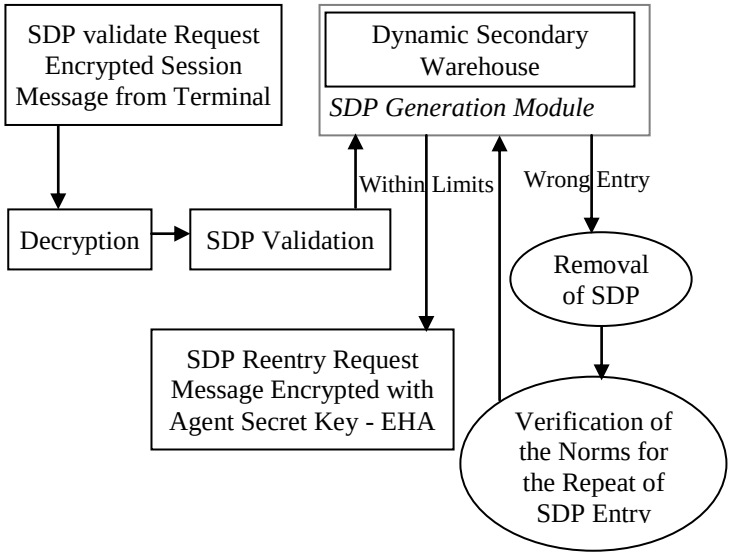

Fig.9. SDP Re-entry Request Message in One-Time Session

Prior to it all the ATM terminals are loaded with the EHA address of the agent and refreshed for any change. On the acceptance of the invalid SDP within the accepted limits a SDP Re-entry request message is sent encrypted with the secret key with the respective Account Number in the data field of the message.

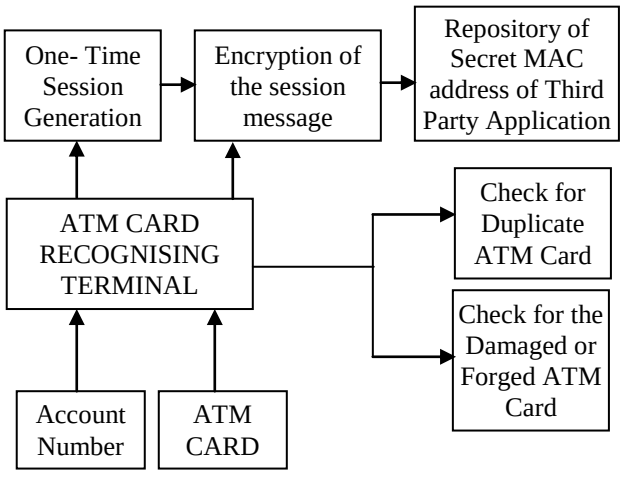

Fig.10. One - Time Session Establishment

Dynamic Repository Updation: The Process of repository updation is made twice once after the Generation of the SDP and other after the receipt of the SDP. Once the Session establishment handshake message is obtained, after the validation of the account number the SDP is generated which in turn adds an entry into the Dynamic Repository with account number, the SDP and the timer

along with the two limit field one for the SDP Regeneration request and other for the SDP Entry for validation. As soon as the Timer expires or the SDP entry or the Regeneration Request exceeds the Limit enforced the flag in the primary repository is updated else the session transfer request message is generated deleting the corresponding entry of account number from the dynamic repository.

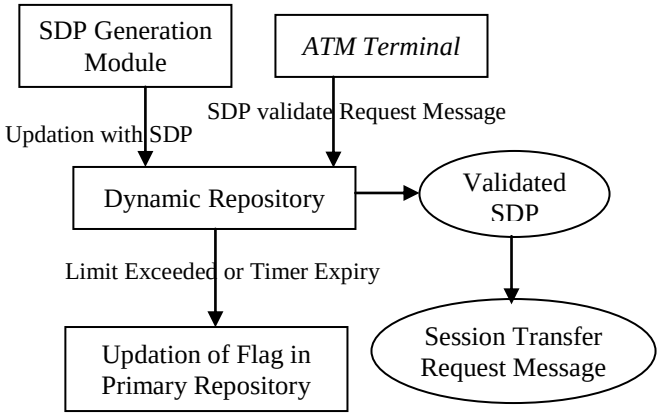

Fig.11. Dynamic Repository Updation Process

10. CONCLUSION AND FUTURE WORK

Also in this model of bi-fold authentication mechanism, the SDP sent to the mobile could be entered from the mobile itself instead of entering it from the ATM Terminals by establishment of connection locally among registered mobile of the customer and ATM Terminals. Also additional prompt could be made after entering the SDP (such as the security questions) which could be randomly chosen from the repository to provide an additional level of authentication and this could also be asked to be entered from the mobile. The bi-fold authentication mechanisms could be adopted also as a part of different phases before the session between the ATM terminal and the bank application is being established and after this session establishment and Personal identification Number Entry into the terminal so that fraudulent action at its next level could also be assured with integrity of the data also being maintained. Any other techniques like the Biometric [4] verification at the ATM terminal at lower cost, economical and at the expense of lesser energy requirement could also be devised along with double tier authentication phenomenon.

REFERENCES

[1] G. Mujtaba, "Adaptive Automated Teller Machine Part-II", *International Conference on Information and Communication Technologies*, pp. 1 – 6, 2011.

[2] G. Mujtaba, "Adaptive Automated Teller Machine Part-I", *International Conference on Information and Communication Technologies*, 2010.

[3] Zhi Zhong et al., "Energy Based Surveillance systems for the ATM Machines", *Eighth World Congress on Intelligent Control and Automation*, pp. 2880 – 2887, 2010.

[4] Yun Yang and Jia Mi, "ATM Terminal Design is based on Finger Print Recognition", *International Conference on Computer Engineering and Technology*, Vol. 1, pp. V1-92 – V1-95, 2010.

[5] A Basic Study on Automated Teller Machine. Available: http://en.wikipedia.org/wiki/Automated_teller_machine/Teller