**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 3, Issue. 2, February 2014, pg.666 – 674***

**RESEARCH ARTICLE**

# Improvising Authenticity and Security of Automated Teller Machine Services

**Srivatsan Sridharan[1], Gorthy Ravi Kiran[2], Sridhar Jammalamadaka[3]**

[1]Department of Computer Science, IIIT-Bangalore, India
[2]Department of Networking and Communication, IIIT - Bangalore, India
[3]Department of Software Engineering, IIIT - Bangalore, India
[1] vatsan.s@rediff.com; [2] grkmss@gmail.com; [3] sridhar.jammalamadaka@gmail.com

***Abstract—This work aims at improvising the security and authenticity of the Automated Teller Machine (ATM) using a trusted third party application. This system would in turn benefit all the customers who have a valid ATM card registered officially with their mobile number. This system provides 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- Passkey (Pk) validation through the mobile. 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 the major threat yet to be addressed. A basic solution is the ATM systems having a two tier authentication Pk and Random Security Question (RSQ) are being generated and validated from the user's input from the ATM Terminal 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 dual tier authentication implementation, the issues arise along with them and the solvencies to these issues related to the generation of the RSQ and Pk independent and unique for each session are addressed.***

***Keywords— Automated Teller Machine; Authenticity; Encryption; Random Security Question; Security***

## I. INTRODUCTION

Automated Teller machine (ATM) is a system that is in place to provide the users with instant cash [1]. But the system functions with a single tier of security - called the Personal Identification number. The ATM is an electronic cum telecommunication device that allows the financial institutions customers to directly use a secure method of communication to access their bank accounts. The ATM is a self-service banking terminal that accepts deposits and dispenses cash at a lightning speed. The idea for an ATM was to simply replace and reduce the workload of the employees in the bank [2]. The ATM would help reduce banks overheads as mainly the wages would be decreased. Any ATM machine installed operates while the card is inserted int the machine. Some legacy systems take-in the card, process it and returns it after the transaction is complete. Some modern system establishes the transaction with the help of just the Swipe of the ATM Card. But the primary step of the functioning is the insertion of the ATM Card into the system. This process is followed by the phase that requests for the PIN of the ATM card inserted. PIN (in India) is generally four digits that are kept in secrecy by the user. This PIN entry determines the transaction to continue or abandon. Also the three times wrong entry of a PIN would lead to the blocking of the ATM card [3] in sensing a possible fraudulent transaction. Once the ATM PIN number is successfully validated, the user is given options regarding the financial services to be performed. Once on selection of a particular financial service, the service is rendered by the ATM and the transaction is said to have come to an end. The main problem associated with this kind of mechanism is that the security threats associated with the user due to the absence of the multi-level security system in place. One of the other drawbacks could be inter-bank operation becomes transactional cumbersome and so the financial institutions charge an extra amount after a certain withdrawal from any other financial institution. This is related to the need for introduction of a trusted third party application into the play. As the possibility of means of eaves dropping [4] of the PIN and the abuse of the ATM cards have dramatically increased all around the globe, the need for multi modal authentication phenomenon has emerged for replacement of the current existing authentication procedures. This paper deals with an effective way of the handling such issues with dual tier authentication phenomenon and also the architecture that is being developed to implement such a system that could be much more resistant towards such attacks and support with full ease, the inter-bank operations.

Section II deals with the existing system, the current mechanism by which the ATM Terminals work to dispense and accept the deposits of the customers of that financial institution. It is followed by the sections on proposed system and architectural components which briefly describes the proposed mechanism of introduction of the trusted third party application and the internal architecture of the proposed system in detail respectively. Section VII deals with modules that are being implemented in the proposed system. It mainly concentrates on the pass key and random secret question generation. It is followed by the phases of the proposed system. The failures that are present in the existing methodology and its remedies are discussed in the section V and VI. The final section deals with the implementation issues of this proposed system and shows the implementation of the current system in detail.

## II. EXISTING SYSTEM

Automated Teller Machine, fondly called as Ant Time Money is one of the convenient way that was brought into this world as an replacement to the old banking system of the cash withdrawal. The main intention behind the invention of this system is to provide cash to the customers of the bank at the lightning speed when needed. The major sequential operations [5] [6] that are currently involved in the ATM services are as follows,

1. Inserting or Swiping the ATM card in the respective ATM Terminal.
2. Entry of the secret Personal Identification Number (PIN) with respect to the ATM card by the card holder.
3. Transaction selection (Financial aspects like balance enquiry, withdrawal, deposits).
4. Completion of the transaction and termination of the session.

These factors were incorporated into this system with the help of the ATM card that is provided to the each customer. The entire ATM cards are associated in one to one with the unique Personal Identification Number (PIN). This PIN should be maintained with high secrecy by any individual. A recent finding has concluded that it is a 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. The need for reduction in the complexity of the transaction associated with that of the ATM with respect to inter-bank financial operations has dramatically increased. The motivation behind the implementation of the proposed system rests in the fact as follows,

- There is a lack of secure authentication phenomenon other than the secrecy of the PIN, which could be useful in the security aspects of the individuals with regard to the financial transactions.
- There is a demand that is growing to incorporate fewer transactions and less complexity in those transactions that could finally reduce the load on the financial institutions server and the monetary aspects involved between the multiple financial institutions.
- Complete authentication of the individual through any other means other than PIN with no additional cumbersome financial burden on the financial institution for its setup.

## III. PROPOSED MODEL

The ATM card and the PIN that is being currently being used by the 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 fact that estimates that almost all the populations who have their ATM card are also the user of at least a mobile, this technique is being proposed. 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 passkey (pk) to the user officially registered mobile number. Thus the issue that is pertaining to the eaves dropping is now solved as the Pk is sent to only the officially registered mobile of the customers.

Also the Pk is time dependent, i.e., the Pk generated expires five minutes and provision of one time regeneration of the password is also available in adverse case of the non reception of the Pk 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 Pk with the help of the trusted third party applications so that after this phase only the PIN number is asked to be entered by the customers. Once the Pk 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. The additional tier of security is added with the introduction of the Random Security Question (RSQ) in between the ATM Terminal and the trusted third party application.

The method for computation of the Pk is unique and it is based on the Code number of the Branch of that particular financial institutions from where the user obtained their ATM Card and four digits of the account number selected at random followed by an four digit random number (Four digit since the PIN is commonly a four digit secret Number). Also the Pk could be asked to be entered only preceding the entry of mobile number from the Customer in the ATM terminal which could provide an additional tier of authentication. The third party application responsible for generation and verification of Pk 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 so that the integrity and secrecy of the Data is also maintained. Since the PIN is not provided to them nothing secret has been disclosed to the public.

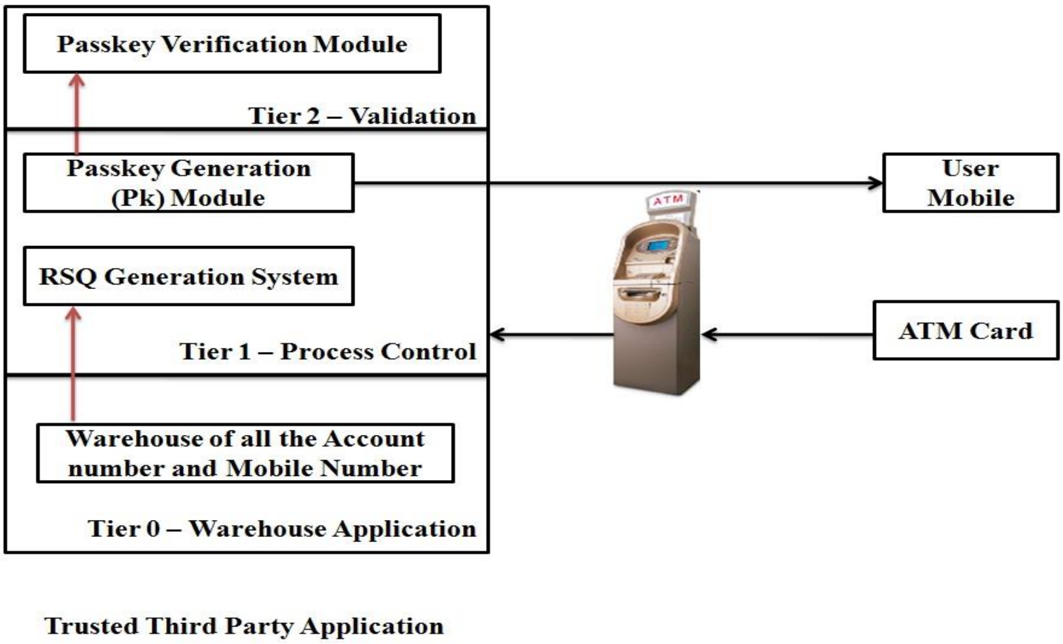

Passkey Verification Module
Tier 2 – Validation
Passkey Generation (Pk) Module
RSQ Generation System
Tier 1 – Process Control
Warehouse of all the Account number and Mobile Number
Tier 0 – Warehouse Application
Trusted Third Party Application
ATM
User Mobile
ATM Card

Figure 1. Proposed Model of Third Party Application integrated with the ATM Terminal

## IV. Architectural Components

The functional units of the proposed system contain the different stand-alone modules which are needed to be interfaced in proper fashion to obtain the desired functioning of the Dual Tier architecture. Architecture depicts the various stand alone modules which has their specific functionalities which could be efficiently utilized by providing the requisite coordination among each others. The necessary components are just needed to be added to the existing system, such as the Trusted Third Party Application, so that the Existing ATM Terminal components need not be discarded to incorporate the proposed system features. The figure 1 shows the entire internal architecture of the proposed model with the help of the third party application. It consists of the three tiers of application involved and interacting within each other. The first tier is tier 0 which represents the tier responsible for storing all the account number and mobile number information. Tier 1 is the process control tier which deals with the Passkey and the Random security Question (RSQ) generation, verified in the tier 2.

## V. Failures in the Existing System

The main failures associated with the existing model [7] is as follows,

- *Exploiting the lack of personal weakness of the customers*: Simple definition of this would be theft - The procession of the personal belongings of any individual illegally and manipulating with the same.
- *Duplicating the role of a distinct individual:* With the help of illegal possession of the individual's property, trying to work on the same (by overhearing could also be the case) for their personal gains. It could also be termed as accessing customer's personal possession.
- *Lack of the internal security mechanism for the complete authentication*

- Over dependent only on the integrity and secrecy of the password - PIN.

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 which is a serious threat to current System's Integrity. Also any multi level of authentication for these type of highly sensitive financial transactions is absent.

## VI. Remedies to the Failures

There is a secure complete authentication of the end user in the ATM terminal. The compete authentication is provided with the help of the generation of the passkey and transmitting it to the mobile number of the customer and allowing the customer to enter their mobile number followed by the Pk preceded by the back-end verification of the Pk entered by the customers. The big advantage rested with these systems is that once the Pk 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 third party application. This is now providing a relief to the National Financial Switch by prevention of un-wanted and intentionally wrong transaction routing to the bank application and ATM Terminal.

Also the main improvement with respect to the financial system application is the additional tier of individual distinct authentication by the presence of the Random Security Question (RSQ). This question pops up in the screen (similar to that of the online banking) asking the user to answer. These are kept only numeric as the institutions is not burdened to replace the keypad existing in the ATM Terminals. This could also add as additional benefits. Though the possibility of the loss of mobile, ATM card and eavesdropping of PIN by the individual becomes negligible, if so happens the RSQ could not be traced, thus making the system much more fool proof against any security threats from the user's perspective. It acts as an additional level of authentication. As these third party repositories does not have the PIN number associated with the ATM Card, lapse of the personal secrecy and compromise on the same is avoided.

## VII. Modules in the Proposed System

*Tier 0 - Trusted Third Party Application* 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 Pk to the respective mobile number of the user and also called Pk Generation Component.

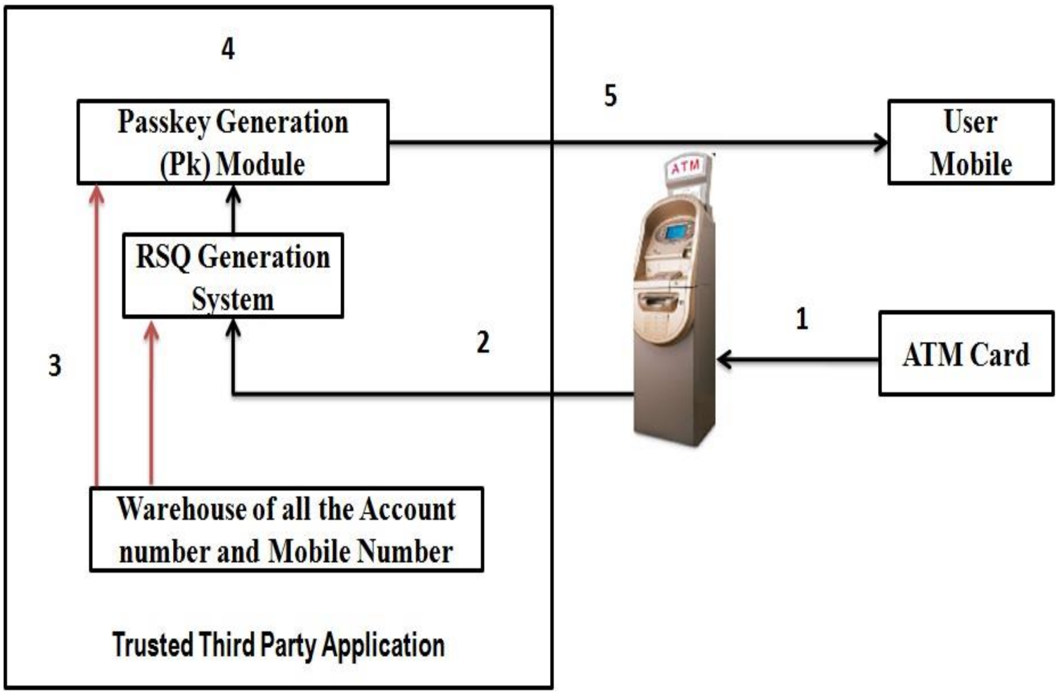

4
Passkey Generation (Pk) Module
5
User Mobile
RSQ Generation System
3
2
1
ATM Card
ATM
Warehouse of all the Account number and Mobile Number
Trusted Third Party Application

Figure 2. Task Performed by Tier 1 - Process Control

Any mechanism of fraudulent action is being restricted by the Pk generation component as the session is established between the bank application and the ATM terminal only after the Pk is validated and verified. *Pk Generator* is the module which is software intended to generate the Pk to the intended mobile of the users. It uses the warehouse provided and refreshed periodically the warehouse of financial institutions account, mobile number and generates a unique and non-repetitive Pk's for different customers as first tier of the authentication at ATM terminal. The steps followed are explained as below,

1. The ATM Card is inserted into the ATM terminal by the user.
2. Once the ATM terminal senses the presence of the ATM Card, the session is established between the ATM Terminal and the trusted third party application. So no session primarily is established between the ATM terminal and the financial institution's server reducing the possibility of fraudulent actions to a greater level.
3. Tier 0 is first initiated by this session request and the session thus is verified to be true by validating the ATM Card number sensed by the terminal from the warehouse of the account number. Once the validation is successful, the interaction between the tiers happens and thus the Tier 0 is consulted by the Tier -1, process control tier to generate the Pk and the RSQ.
4. The generation of the Pk is the next step that could be immediately followed in the process. The process of the Pk generation is explained as a separate module in the Pk generation module.
5. The tier 0 interaction again happens to retrieve the mobile number of the ATM Card holder and the Pk generated is thus transmitted to the user mobile retrieved. RSQ is popped on the ATM Terminal screen.

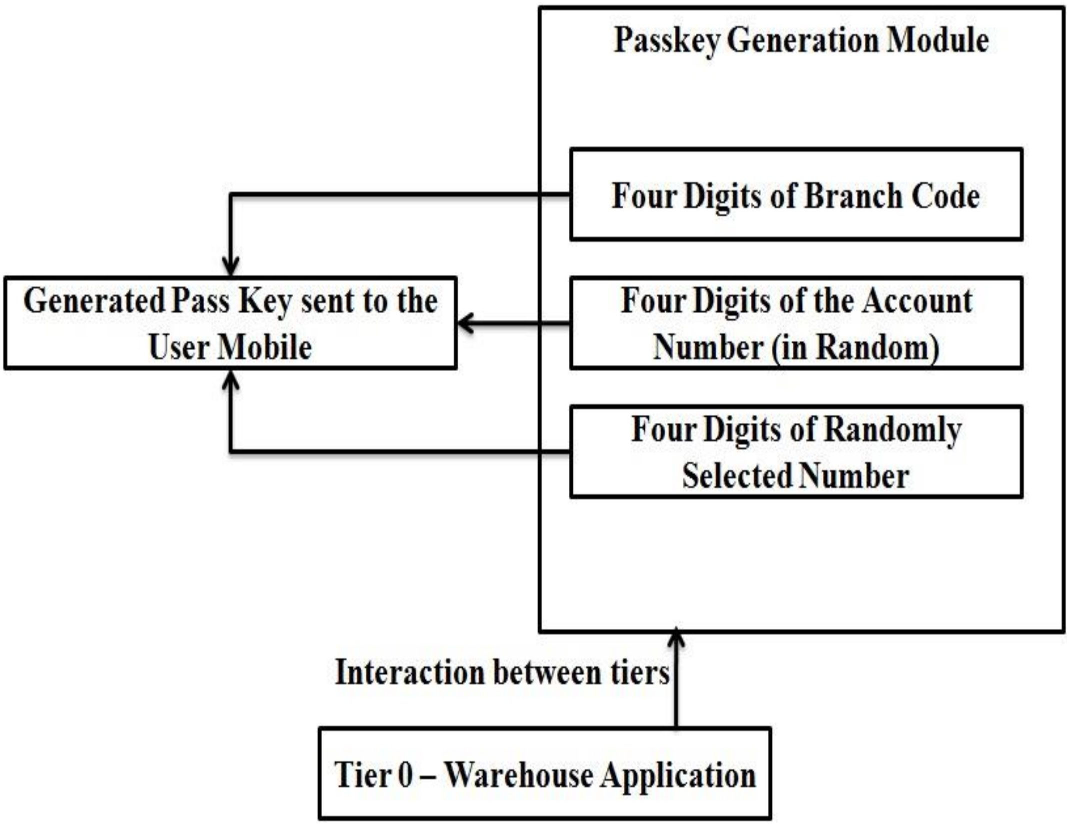

Passkey Generation Module
Four Digits of Branch Code
Generated Pass Key sent to the User Mobile
Four Digits of the Account Number (in Random)
Four Digits of Randomly Selected Number
Interaction between tiers
Tier 0 – Warehouse Application

Figure 3. Passkey Generation Module

There are two separate *repository designed,* one which acts as a configured warehouse for the Pk 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 which contains the Account and mobile number along with the Pk generated which acts as the session establishment between the bank application and the ATM terminal. It is also called the *Temporary Warehouse Instance* which also holds the Ethernet Hardware Address (EHA) of the ATM terminal from which the session generation request originated. The respective account entry in the temporary instance of the warehouse is kept active for exactly five minutes from the generation of the Pk and updation of the flag in the primary repository provided by the financial institutions if the PK mismatch occurs for more than three times against the PK generated or request for new PK generation is made more than two times consecutively. 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 third party repositories does not have the PIN number associated with the ATM Card, the secrecy between the financial institution and the customer is not given up along with the double tier authentication also made possible.

## VIII. PHASES IN THE PROPOSED SYSTEM

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 party Application Vendor. Thus the Pk Generator generates as soon as the ATM Card recognizing terminal validates the card and the customer mobile is sent with the Pk generated at the third Party application. If the Pk is wrongly entered thrice or the request for new generation of Pk exceeds the limit allowed the corresponding account is temporarily blocked for 24 hours suspecting suspicious activities. Else only after the Pk validation session transfer happens i.e., the existing mechanism of secure session establishment between bank application and the ATM terminal is facilitated.

*Session Establishment with the trusted third party application*. Before a transaction takes place, one of the first things the ATM terminals must do is to establish a session (one-time) between the ATM terminal and the Third Party Application. This is done by sending the first token of the ATM card account number along with the ATM terminal MAC address encrypted with the Third party MAC Address as the shared - secret key so that the Third Party application can only decrypt it and the ATM Terminal can only encrypt it as itself is maintained with high secrecy. Prior to it all the ATM terminals are loaded with the MAC address of the Third party Application and refreshed for any change. This is then followed by the messaging of the Pk to the customer mobile number. This time while user provides the PK the encryption is done with the same MAC - EHA (Ethernet Hardware Address). So during decryption the mobile number associated with the Account number is used for decryption. If the MAC used for the previous encryption process does not match it becomes impossible to decrypt for Pk Validation Procedures and thus the additional tier of authentication is being achieved. Once decrypted and the Pk is validated to be true then the session as in the existing system is established between the bank application and the ATM terminal. Decryption becomes impossible as the instance of the warehouse holding the account number and the user mobile number has only the MAC address from which terminal (ATM) did the request for session establishment originated.

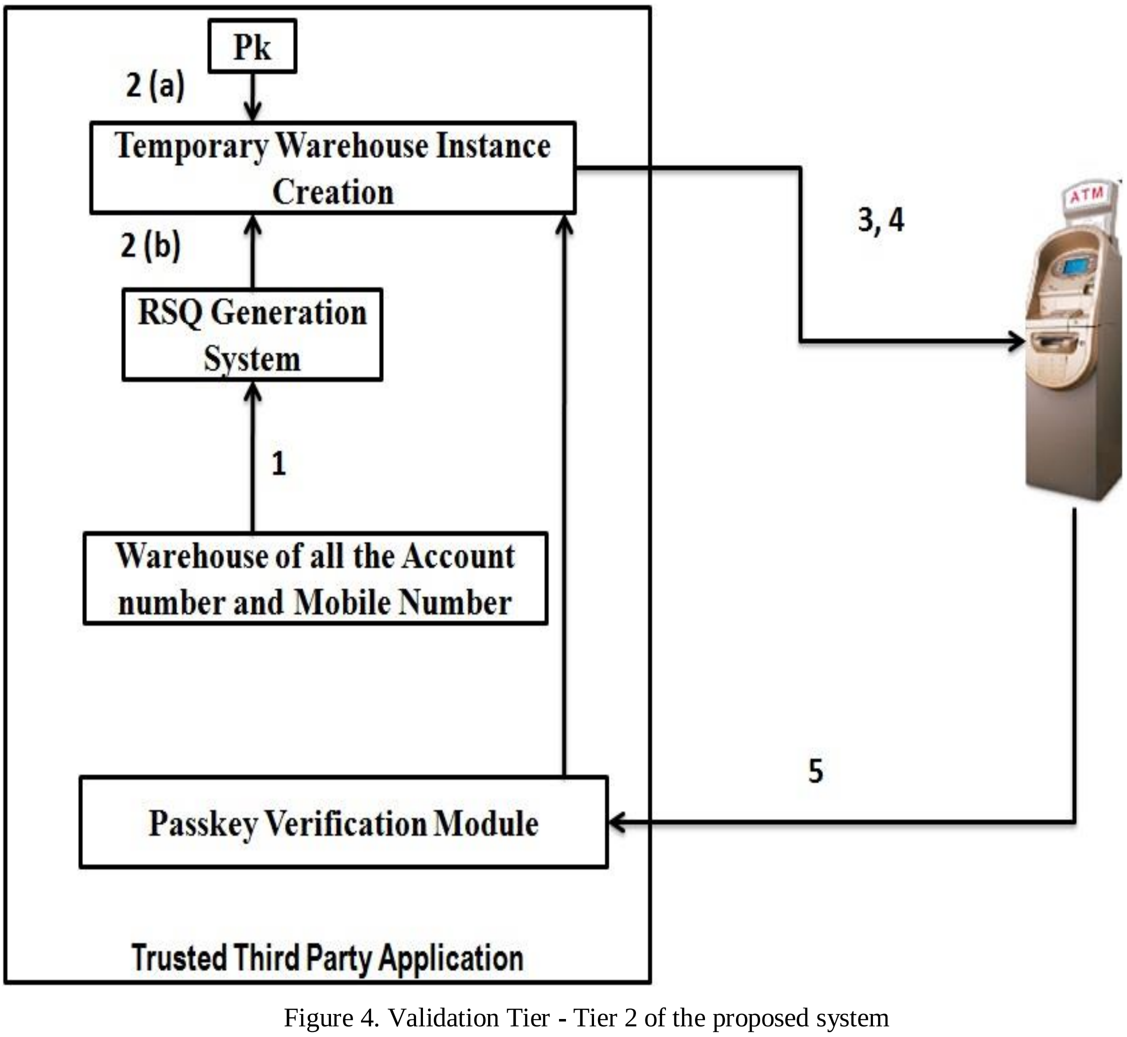

Pk
2 (a)
Temporary Warehouse Instance Creation
2 (b)
RSQ Generation System
1
Warehouse of all the Account number and Mobile Number
Passkey Verification Module
Trusted Third Party Application
3, 4
ATM
5

Figure 4. Validation Tier - Tier 2 of the proposed system

*Validation Module*. Once session is established, the PK generator combines randomly four digits of the account number along with the financial institutions branch code and the four digit random number. This is forwarded only to the mobile, RSQ is popped up in the screen and the steps followed are explained as below,

1. Interaction with the tier 0 happens to retrieve the RSQ that has been stored against the account number.
2. (a) The main intention of the interaction with the tier 0 is to store the retrieved information about the account number, Pk generated, user mobile number, RSQ generated along with the EHA address of the ATM terminal from which session request originated for using it as a secret key.
   (b) Another main intention is to obtain the time duration for which the Pk will be available and thus determining the time at which the instance created should be destroyed and no longer be used.
3. Now the communication happens between this temporary instance created and the ATM Terminal for the receipt of the information for the validation purpose.
4. The RSQ popped up in the screen and the Pk is sent to the mobile. Both the inputs are requested from the user. As mentioned to avoid change of numeric key pad only numeric RSQ are asked from the user. The RSQ would contain the information extracted from the Know Your Customer norms such as their day or year of birth or reverse of their KYC information randomly. Each time the question generated is not same and is selected from a subset of already available (under high level of privacy) questions.
5. The entry of the Pk and the RSQ followed by the transfer of the process control and session control to the validation module happens.
6. Once within the given framework of time, the Pk and the RSQ are validated to be true the session encrypted with the EHA of that particular Application server is transferred barring the account number. The encryption is not mandatory as the account no. is only sent with the source. The decryption with the available EHA happens, id needed and the current secure method of connection establishment is done with an additional guarantee of prior dual-tier authentication mechanism.

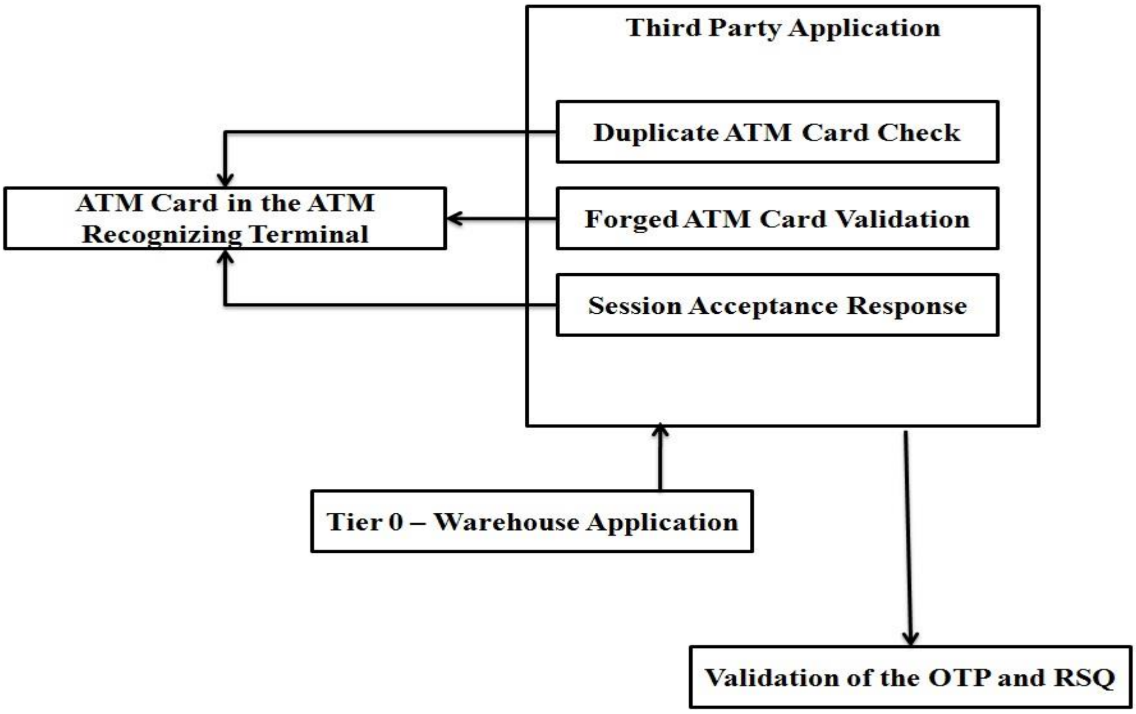

Third Party Application
Duplicate ATM Card Check
Forged ATM Card Validation
Session Acceptance Response
ATM Card in the ATM Recognizing Terminal
Tier 0 – Warehouse Application
Validation of the OTP and RSQ

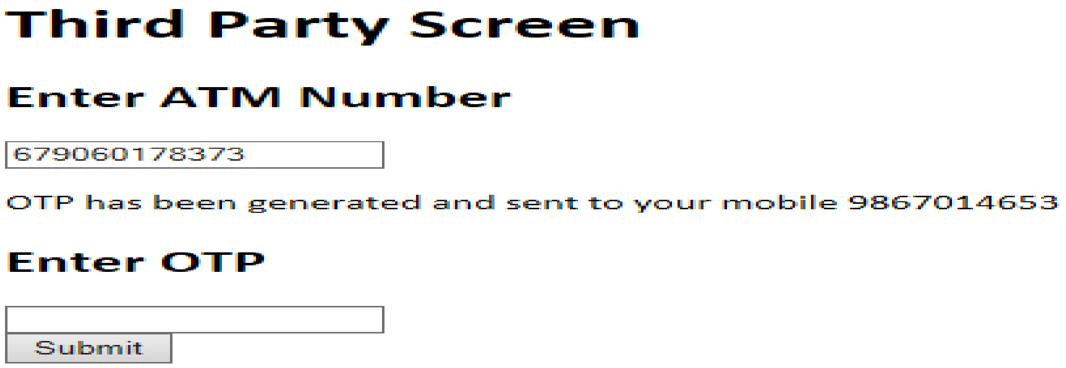
Figure 5. Complete Functional Flow of the Proposed System

*PK Generation Module*. Once session is established, the PK generator combines randomly four digits of the account number along with the financial institutions branch code and the four digit random number. This is forwarded only to the mobile of the user and this the updation in the dynamic repository for validation form the terminal entered PK code within the stipulated time frame that is being provided on the guidelines issued to the third party applications by the financial institutions. Once the PK has been verified by the third party applications it creates a new session between the bank application and the ATM [8] terminal by sending decrypted data from trusted third party application with the source address as the ATM terminal address instead of itself and at this moment act as a forwarding router which has the to match to which bank application process does this packet of data needs to be forwarded with Account Number as data field obtained from the ATM Terminal. The secret key is the trusted Third Party Ethernet Hardware address (EHA) or the MAC Address for the ATM Terminal to encrypt and Trusted third party application to accept the incoming one-time session establishment from the ATM Terminal. 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 or a server with network privileges. Most wireless systems allow EHA filtering to admit only the authorized computers or terminals 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 Trusted Third Part Application for the process of decryption.

## IX. IMPLEMENTATION ISSUES

The system is implemented using RESTful web services in java and the following figures indicates the exposed web services. The primary reason for implementation using RESTful web services is that REST is stateless, which means the server doesn't have to store the state of clients which reduces huge load on servers. Also, REST is simple, flexible, allows multiple representations of data like XML, JSON, Plain Text, RSS, etc. One of the greatest advantages of REST is the Transport Level security which can be accomplished using SSL. The two tier authentication phenomenon is implemented using a RESTful web service. The reason for choosing a RESTful web service is that the service offered provides a way for server not holding all the session and its corresponding states. The client has to hold its session and information about the states.  Some more convincing reason for choosing REST services is as follows,

- REST is cleaner than SOAP and the server is not burdened with maintaining the state. Client has to do the same that server does in a legacy systems.
- Safe encapsulation of Legacy systems which would not provide any financial losses to the institution.
- REST isn't any obscure; it's the way Web works aided with some rules of session and state maintenance.
- There is always a plain text data exchange.
- It has not so many standards to follow other than basic HTTP methods and its encapsulation, becoming easy to get implemented in any legacy systems.



Third Party Screen

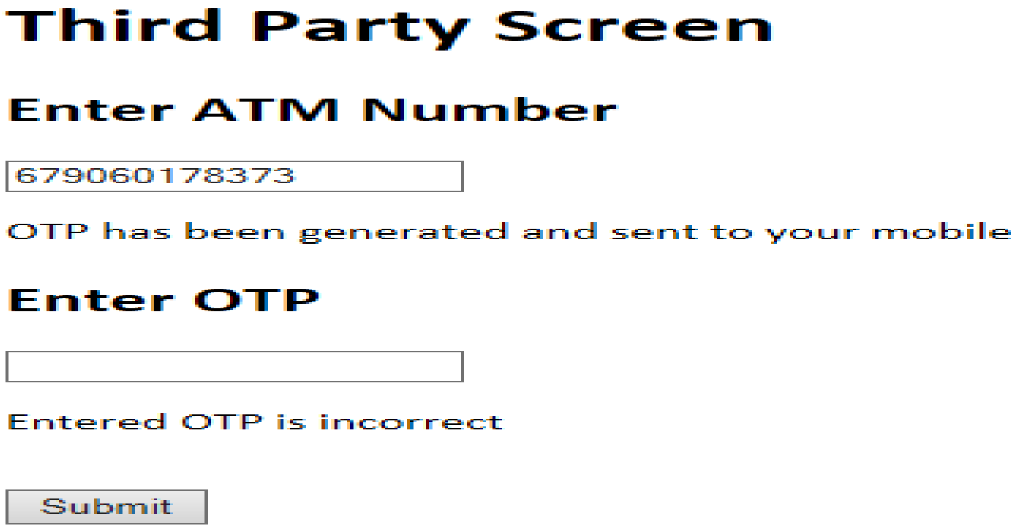
Enter ATM Number

679060178373

OTP has been generated and sent to your mobile 9867014653

Enter OTP

Figure 5. Pk Generation Process using RESTful web service - Simulation Result I



Third Party Screen

Enter ATM Number

679060178373

OTP has been generated and sent to your mobile

Enter OTP

Entered OTP is incorrect

Figure 6. Incorrect Pk Entry. (OTP  = One Time Password = Pk = Passkey) - Simulation Result II

## X. Conclusion

The two tier authentication mechanisms could be adopted also into different phases as, before the session establishment between the ATM terminal and the bank application and after the session establishment between bank application and Personal identification Number Entry into the terminal so that fraudulent action at its next level could also be prevented assuring integrity and data secrecy. Any other techniques like the Biometric verification [4] at the ATM terminal, being economical and at the expense of lesser energy requirement could also be devised. The main future course of action would be the application of the encryption techniques and dividing of the phases involved based on the encryption mechanisms such as Handshake, PK Request messages, PK Validate Request and Session Transfer Request messages along with the capturing of the time stamp associated with each thus ensuring additional level of security being enforced. Each of these messages could be used at every time period as addition level of security reinforcement. Also improvisation in scalability, robustness, performance encryption issues along with the security establishment and energy optimization of the third party application could also be undertaken. This Authentication model can also be extended to various other applications that offer services related to both security and integrity of data being handled such as the Online Ticket Reservation scheme.

## 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]. A.S. Adams, and K. A. Thieben, “Automatic teller machines and the older population”, *Applied Ergonomics*, Vol. 22**,** pp. 85 -90, 11991.

[4]. A. B. El-Haddad, and M. A. Almahmeed, “ATM banking behaviour in Kuwait: a consumer survey”, *International Journal of Bank Marketing*, Vol. 10**,** pp. 25 - 32, 1992.

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

[6]. 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.

[7]. *A Basic Study on Automated Teller Machine (ATM Machines).* Available (Online): http://en.wikipedia.org/wiki/Automated_teller_machine/Teller .

[8]. S. Sridharan and G.R. Kiran “Conception of Bi-fold, Authenticated Agent Monitored Transaction Architecture”, *ICTACT Journal on Communication Technology,* Vol. 4, Issue no. 2, pp. 717-722, 2013.