International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 12 6559 - 6565

# Framework for ATM Card & Safety: Preventing ATM Transaction from Hackers and Frauds

Deepa Malviya
Dept. of CE & IT
Suresh Gyan Vihar University, Jaipur
Raj., India
*er.deepa.malviya@gmail.com*

Sachin Jain
Assistant Professor, Dept. of CE & IT
Suresh Gyan Vihar University, Jaipur
Raj., India
*sachin.jain@mygyanvihar.com*

***Abstract-*** Authentication is possible in several ways namely text password, graphical, bio-metric, and 3 dimensional password authentication. In this paper we have tried to overcome the authentication problem involved due to pin hacking of ATM cards by introducing multi-level authentication technique. The use of ATM card is increasing and making headway day by day among the humans, moreover giving rise to malignant attacks on bank accounts via ATM cards due to limited security & authentication technique i.e., PIN used for ATM transactions. To resolve this problem, paper will focus at concept of graphical-text authentication that will be done by the bank at time of signing-up along with ATM card confidentially to the possessor / owner itself. When possessor will swipe ATM card into machine, as soon as the ATM card will get accepted, the possessor will have to choose an image from 9 images shown and that image must match the image he chose at time of registration. After choosing correct image possessor will have to go through second level of security i.e., he have to choose 4 grid points on that image in a particular sequence that he did at time of registration. If security level is passed with correct grid points then, possessor will get a random encrypted form of PIN number by clicking on chip at ATM window. This will reduce ATM attacks and frauds to a great extent.

***Keywords-*** *ATM, ATM Cards, Image Authentication, DES Algorithm, Hacker*

*****

## I. INTRODUCTION

From previous years, various systems are using alphanumeric passwords for authentication process like some of the ATM cards are still following only numeric password authentication i.e., PIN. For authentication, different methods exist like simple text password, third party authentication, Graphical password, Biometric and 3D password object to access the services firmly. However, it is familiar to say that there is weakness in textual passwords and is insecure for kind of reason as they can be easily breaked and vulnerable to brute force attacks or dictionary attacks. Various problems that are faced with textual password can be:

1. Text-based passwords are afflicted from both security and usability problems as users are likely to choose short and simple strings for easy memorization which can be easily guessed by dictionary attacks.

2. The problem comes around when user forget the textual password. As remembering textual password is not an easy task as compared to image/graphics.

Graphical passwords are based on the thought that users can recall and recognize pictures better than the textual password or alpha numeric strings. Automatic Teller Machines (ATMs) are used by each and every human from years and customers prefer to make out cash withdraw from their accounts through ATM's but these frequent uses of ATM's are leading to attacks on bank accounts by hackers if they come to know the PIN number. However, the wide deployment and sometimes secluded locations of ATMs make them ideal for criminals to turn traceable electronic money into clean cash. The PIN provided with ATM card to customer is the primary security measure against fraud. A hacker or street criminal can easily steal a cash card, but unless he observes the customer enter the PIN at an ATM, he can only have three guesses to match against a possible 10,000 PINs and would rarely strike it luckily. If successful by chance, then also theft cannot exceed the daily withdrawal limit of around $300(it varies from bank to bank). Hackers can steal PIN of a user's ATM card by putting a chip below the keypad of ATM Machine which traces the PIN number pressed by the user. Thus, if PIN is leaked then a user can suffer through huge lose in his accounts.

A corrupt bank programmer can even use a crude method to attack by writing a program that tries all PINs for a particular account, and with average luck this would require about 5000 transactions to discover each PIN.

An approach is to use the combination of the graphical and textual authentication techniques in multi-level authentication, so that the security level is increased to a huge extent. Hence a multi-level authentication technique is introduced in secure transmission for ensuring the strict authentication providing great usability and efficiency. Specifically, proposed methodology mainly consists of three operational steps: image selection, sequence of clicks and encrypted PIN. That is, users' will have to first choose an image from pool of images shown on ATM window. Further, on the chosen image user have to make sequence of clicks in the selected image and code their secrets to be done. At third level of authentication user will have to enter first five

characters of encrypted PIN that is send to its mobile via sms as OTP. This scheme is good at both security and usability, and eventually gives a preliminary security analysis of our scheme against several well- known attacks (e.g., dictionary attack).

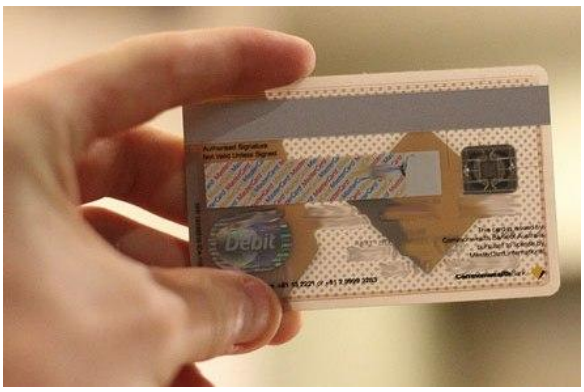

Fig. 1 ATM Card

## II. BACKGROUND AND RELATED WORK

The system and network security is reinforced by passwords, that may be a vital a part of associate Authentication method. Most ordinarily associate Authentication methodology exploitation either alpha-numeric password or Graphical password, that has crucial drawbacks like dictionary attacks and shoulder-surfing. The Grid primarily based Graphical Text password authentications are emerged as an alternate solution to beat the potential vulnerabilities thanks to typical schemes. In addition, originating the "Grid Systemization and Text Enlargement Technique" for classifying a most popular theme Image. By clicking the grid thereon theme Image it enlarges a next sequence of watchword. This methodology depends on "Image-Image-Alphanumeric password" and therefore the serial bearing depends on previous choice. This theme has been deed prominence, attributable to its integrity and security furthermore because the Grid Systemization and Text Enlargement Technique. Swiping of ATM card into the machine and entering a PIN number for performing any activity is getting risky day by day for consumers. Attackers may do fraud by inserting a magnetic strip inside the ATM machine keyboard that can easily trace the PIN number entered by consumer.

Usually a permanent PIN number is provided by the bank for each ATM card, which is used for every transaction. Knowledge Based Authentication System is one that deals with what information the user knows. Remembering PIN number might get difficult for some people, and they choose to write it somewhere on a piece of paper or in mobile phones. For ex., we can consider most popular E-mail Service Providers like Gmail, hotmail and yahoo mail systems that ask for a specific user-id and password from particular user and then check if they properly match with the previously stored id-password. The user enters his/her user-id and a textual password. This system allows remote access but is vulnerable to various attacks like dictionary and brute force attacks. A new approach of graphic-text and generating random encrypted PIN number at each transaction will reduce the burden of remembering PIN number and will increase the level of authentication.

### 2.1 Image Authentication

Image authentication is important in many areas like military target images, images for evidence in court, digital notaries' documents, and pharmaceutical research and quality control images. All these images have to be secured to avoid false judgments. Image authentication can be divided in two groups:

A. Strict authentication

B. Selective authentication.

Strict authentication is used for systems and applications where no refinements in the protected image are allowed. On the other side, selective authentication is used when some image processing operations must be tolerate such as compression, different filtering algorithms and/or even some geometrical transformations...[92, 158]. For type of strict authentication, solutions include conventional cryptography and fragile watermarking that provide good results and also which satisfy users. While Selective authentication, uses techniques based on image content signature or semi-fragile watermarking to provide some kind of robustness against specific and desired refinements. Also, strict image authentication methods do not tolerate any changes in the image data. These methods can be further separated in two groups according to the techniques that are used: methods based on conventional cryptography and methods that use fragile watermarking.

## III. IMPLEMENTATION

ATM is one among most used machine that has modified the standard system of exchanging cash with bank. In world of science and technology, every customer will prefer ATM transaction than moving to bank for accessing account as people are trusting ATM for cash dealing, deposit and transfer, because it is straightforward and time intense. The magnetic strip on back of the ATM card that record the customer's activity is the forgery security as it keep day to day record of transaction by the card. Swiping of ATM card into the machine and coming into a personal identification number for playacting any activity is obtaining risky day by day for customers. Hackers or Attackers can do fraud act by inserting a magnetic strip under the keypad of ATM machine keyboard that may simply trace the personal identification number entered by client. Thus, having PIN as the only security measure is not at all safe for us.

ISSN: 2321-8169
6559 - 6565

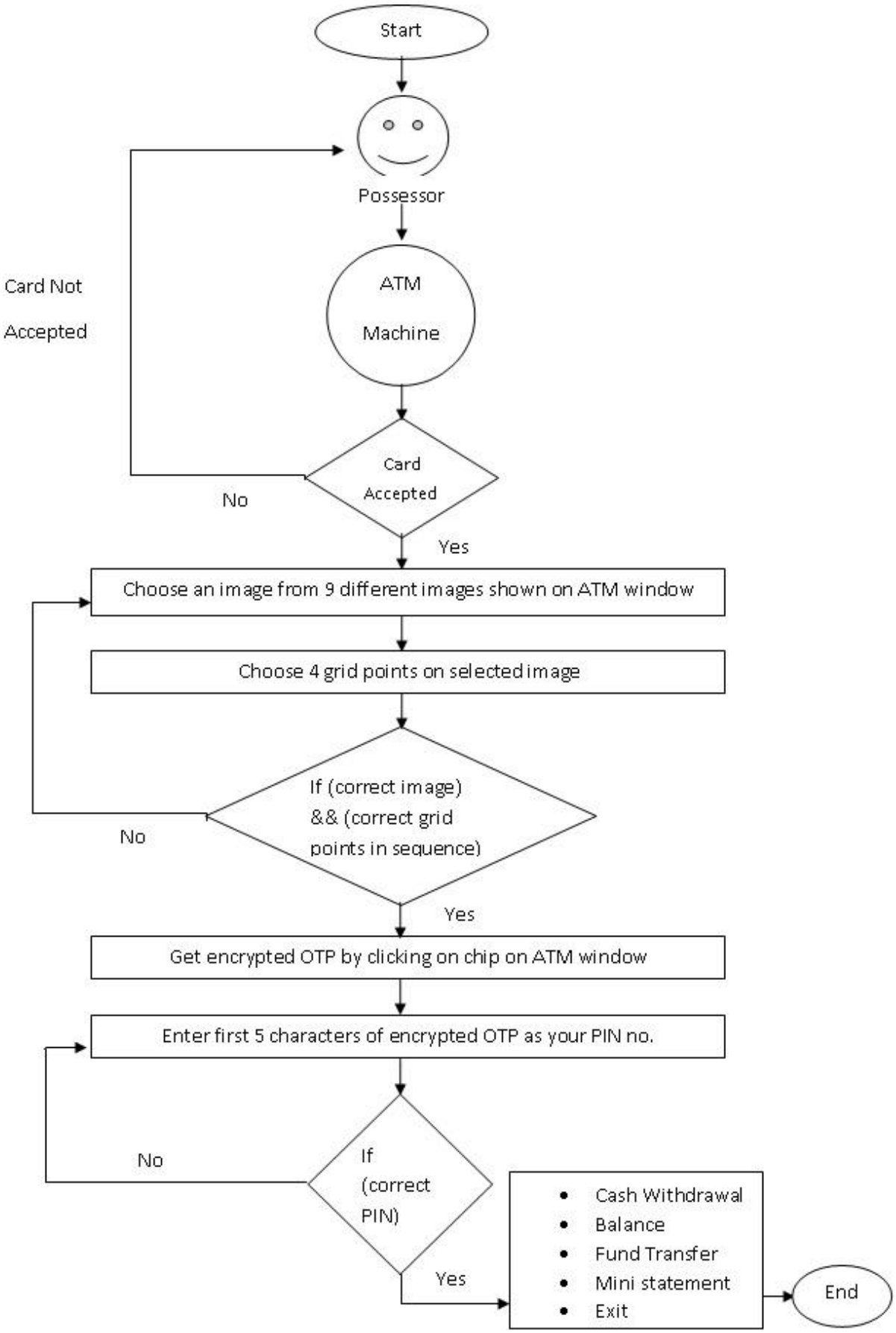


Fig. 2 Work Plan

In our proposed system, Graphical-Text Authentication system for ATM's is done in form of 3 levels i.e., Image Selection-Sequence Click on Image-alphanumeric. There are 3 steps to be considered for their Authentication. 1) The user has to select one Image from the pool of images shown on the ATM window. The image selected will get opened. 2) For every image there are grid points on that Image. User will have to click on 4 such grid points in a sequence that he followed at time of signing up and registration. 3) After correct sequence is matched, user will have to enter an encrypted PIN that is sent to his mobile as OTP. These levels of security will not only increase the security for ATM's but also the efficiency and usability of ATM cards.

Usually a permanent PIN is provided by the bank for every ATM card, which is employed throughout each dealing. Basic cognitive process PIN may get troublesome for a few folks, and that they like better to write it somewhere on a bit of paper or in mobile phones. This will facilitate attackers to steal PIN simply, and might do fraud transactions multiple times. To overcome this authentication, a brand new approach of generating encrypted random PIN and image authentication with sequence of clicks at every dealing can scale back the burden of basic cognitive process PIN. In this new approach, ATMs will work as a knowledge terminal with few inputs and outputs. The input that ATMs will take would be simply the swipe of ATM card, selection of image on screen , clicking of grid points in sequence, alphanumeric encrypted PIN number through keyboard and after authentication further selection of choices like money withdrawal, balance inquiry, transfer cash, etc. Using Visual C# .Net, this project is implemented and executed. The results of this work improve the performance, security and efficiency. Also coming up from the drawbacks of text password authentication attacks i.e., dictionary attacks.

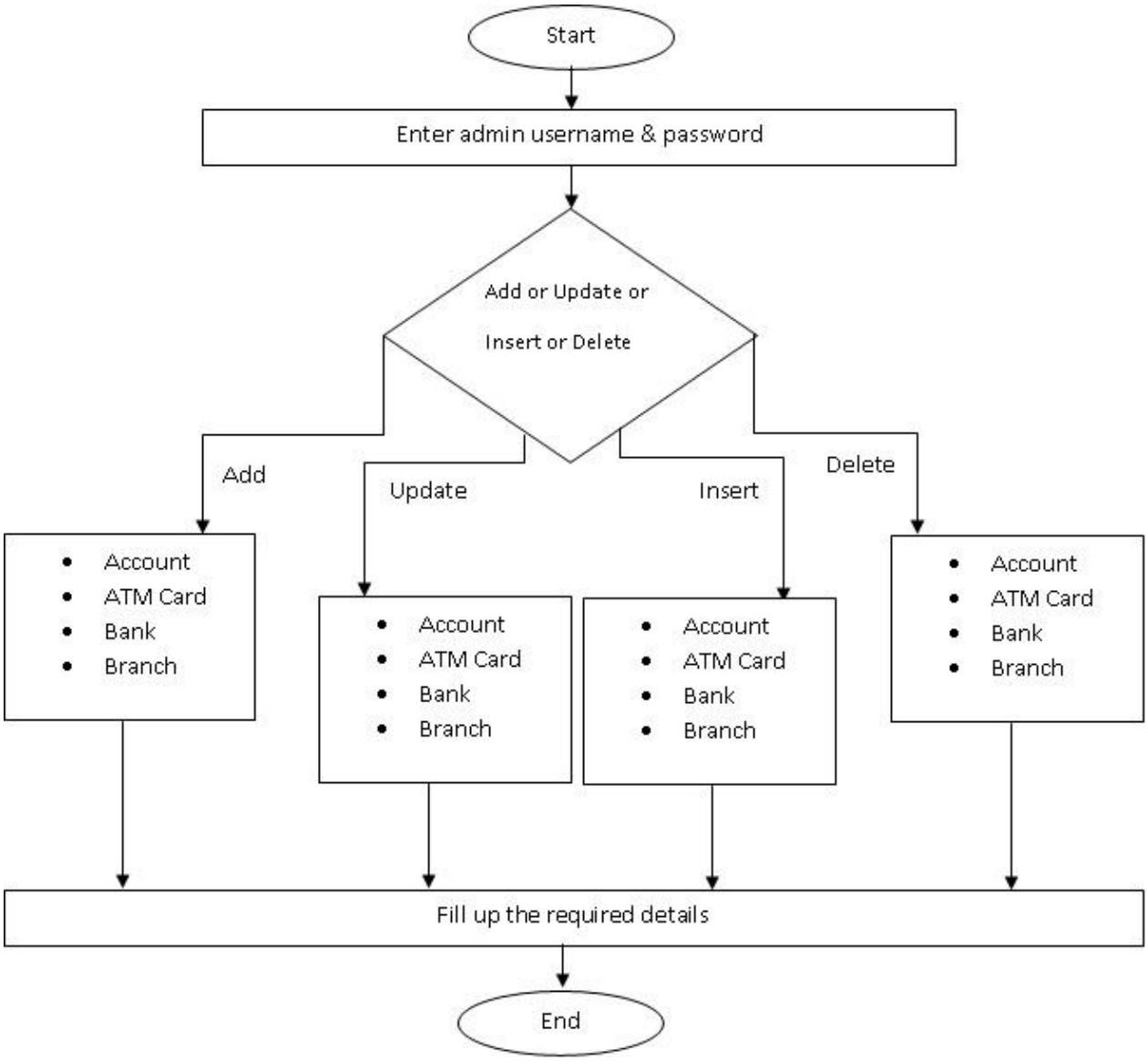


Fig. 3 Admin DFD

ISSN: 2321-8169
6559 - 6565

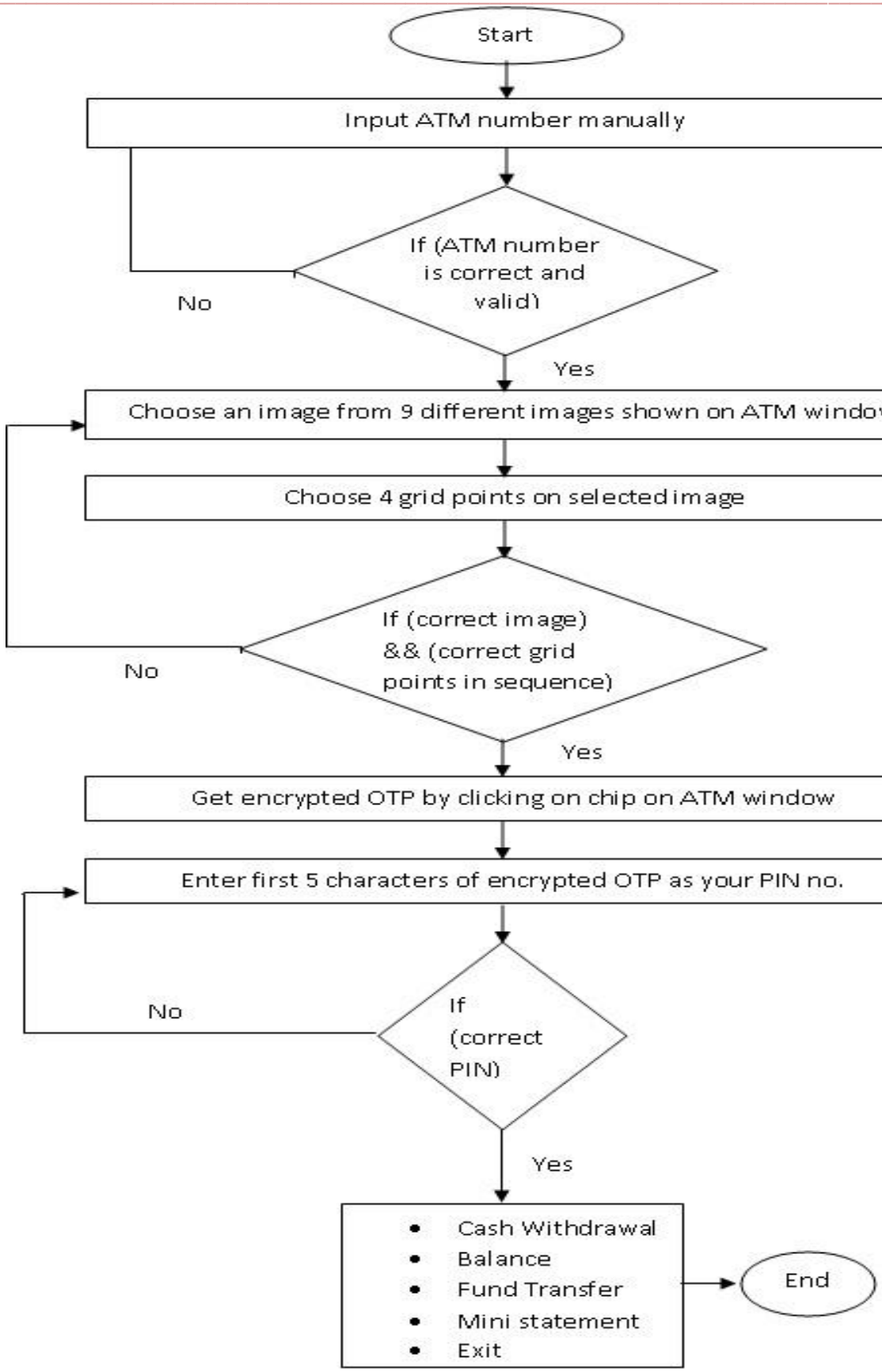


Fig. 4 Client DFD

 ISSN: 2321-8169
6559 - 6565

The implementation part consists of two sections:

A. For the Client or the User Usage
B. For the Bank Administration

*A. For the Client or the User Usage*

This section will behave like ATM machine where the possessor will swipe the ATM card and make it able to access the bank facilities via the image and text authentication which is matched with the original data stored in bank records. In this screen the user can swipe the card, in our case the user will enter the ATM card range. And therefore the card range is then searched within the database to see out its existence and so a user is forwarded to image authentication level where he select a image from pool of images and make sequence of clicks on that image. If the image and sequence of click matches the original data that user selected at time of signing up, then only he is directed to third level of authentication where an encrypted PIN is generated and send to mobile of possessor as OTP. The user will now have to enter first five characters of encrypted alpha numeric PIN and can proceed further with transactions.

*B. Server Part or Admin Part*

The Server part will act as bank server that will deal with the management of the tables or the data which will be required for processing the client or user section working.
In this section, the admin will be first authenticated by entering a valid username and password to validate his or her credentials and after the validation is done, then the admin services are available to the admin in which he can add/update/insert/delete/view various records of banks, branches, registered users, transactions performed by users, etc.

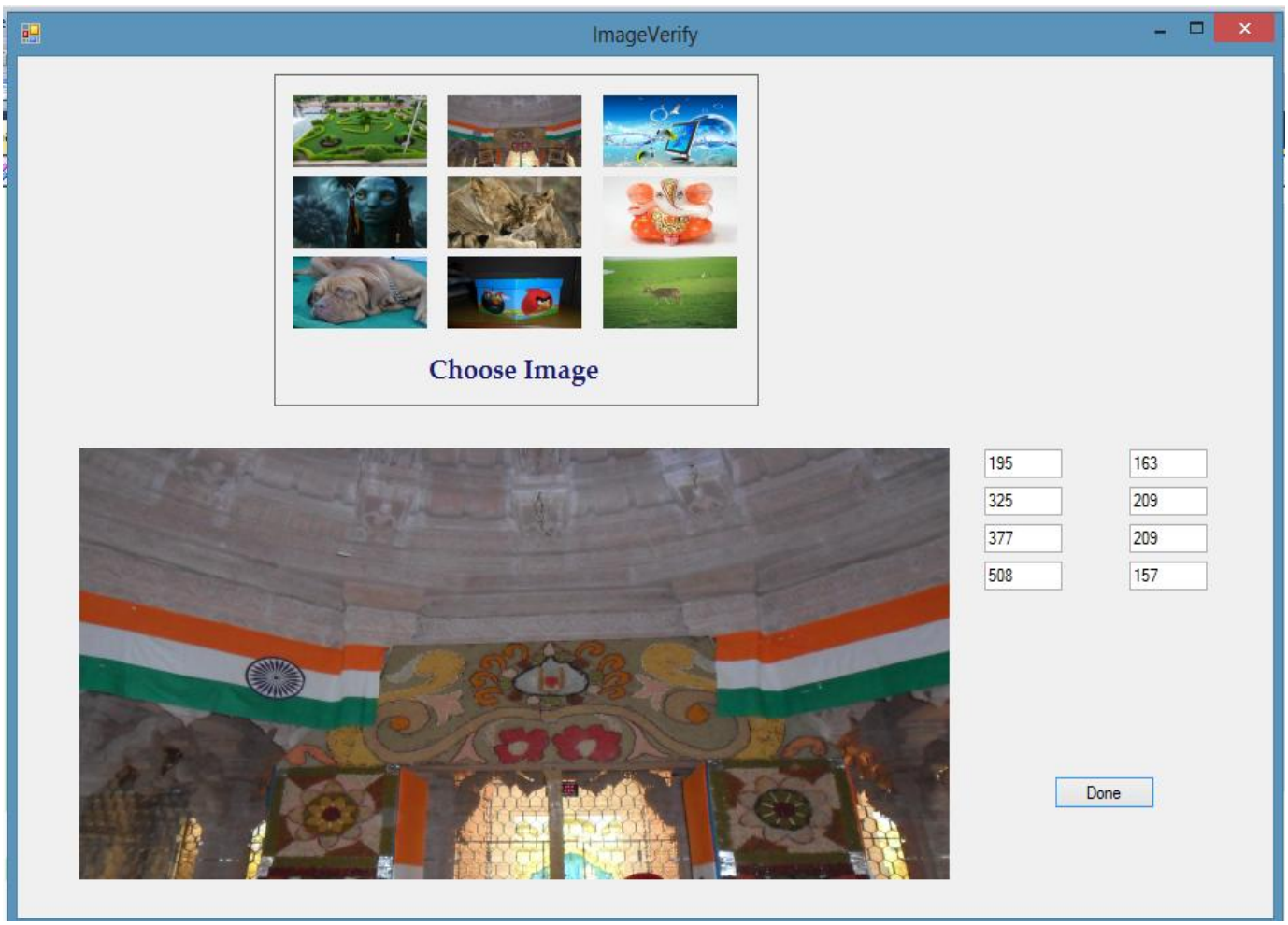


Fig. 5 Image Authentication Form

## IV. CONCLUSION

To resolve the problem of authentication of ATM cards that are being suffered by malicious attacks and loss in bank accounts as PIN as only authentication is not apt for this world. There is need to increase security of ATM cards authentication by increasing level of security. To resolve this, paper has focused at concept of a image-image-text authentication that will authenticate user at three levels in both manner i.e., graphics and alphanumeric authentication.

## REFERENCE

[1] http://akshitkumar.heck.in/decimalisation-table-attacks-for-pin-cra.xhtml

[2] http://ijecs.in/issue/v4-i8/68%20ijecs.pdf

[3] https://www.isc2.org/uploadedfiles/(isc)2_public.../isc2_wpiv.pdf

[4] Vinothini T, Rajesh I and Kirupa Rani D, "Multiple Grid Based Graphical Text Password Authentication", International Journal of Research in Engineering and Technology, eISSN: 2319-1163, pISSN: 2321-7308

[5] S.Yamini and Dr.D. Maheswari, "A Multiple Click Based Graphical Authentication System", Journal of Theoretical and Applied Information Technology, Vol. 62 No.2,April 2014

[6] Rajpreet Kaur Jassal and Ravinder Kumar Sehgal, "Online Banking Security Flaws: A Study" International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3,Issue 8,August 2013

[7] B.Srikanth and G.Padmaja, "Secured Bank Authentication using Image Processing and Visual Cryptography" International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014

[8] R. Sujatha and G. Arumugam, "An Analysis of Text-Based Authentication using Images in Banking System"IISTE, Vol 2, No.4, 2011