International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 07 | July 2020 www.irjet.net p-ISSN: 2395-0072

Artificial Intelligence and Aadhaar Based Smart ATM

M. Ravi Prasad M.Sc, M.Tech,

Assistant Professor, Department of CSE, S V College of Engineering, Kadapa.

Abstract - *Generally ATM transaction will be perform by customer by entering 4 digit PIN, but it may be traceable by unauthorized user and sometimes an unauthorized user can perform the transactions using dummy card. To handle these type of scenarios and to provide high security for Customer Bank Account from Miscellaneous ATM transactions suggesting a new technique in this paper. The suggested technique is combining features of Artificial Intelligence and Aadhaar ID. Everyone knows AI has huge prominence in the current trends in technology. By using AI Customer Face will be recognized and by using Aadhaar ID will verify Finger Image of the customer, by using these two will have high security to perform the ATM transactions by the Customer.*

Key Words: Artificial Intelligence, Smart ATM, Aadhaar ID based, Biometric Based, Secured ATM Transactions.

1. INTRODUCTION

The automated teller machine (ATM) is an automatic banking machine (ABM) that allows the customer to complete basic transactions without any help from bank representatives. There are two types of automated teller machines (ATMs). The basic one allows the customer to only draw cash and receive a report of the account balance. Another one is a more complex machine that accepts the deposit, provides credit card payment facilities and reports account information.

It is an electronic device that is used by only bank customers to process account transactions. The users access their accounts through a special type of plastic card that is encoded with user information on a magnetic strip. The strip contains an identification code that is transmitted to the bank's central computer by modem. The users insert the card into ATMs to access the account and process their account transactions. The automated teller machine was invented by john Shepherd-Barron in the year of 1960.

So, with ATM lot of benefits are having for the customer and also having many security problems. As technology place a very important role in this Application I have to provide better solution to overcome the problem. In the existing papers few are suggested the only Artificial Intelligence or Aadhaar based solutions. To provide high security in this paper I am grouping the two techniques of AI and Aadhaar.

As the customer Account linked with Aadhaar ID the same data is going to furnish in the ATM card and as well the Customer Facial image with AI. When a Customer insert an ATM card first Account data will be fetched along with that it also fetch facial image and finger print based on AI and Aadhaar ID. Customer will be authorized by reading the current facial image with Cam and Fingerprint by device and will go for validation. After successful validation only Customer can perform the transaction. So, this will be leads to high level security in ATM transactions

2. LITERATURE SURVEY

2.1 Artificial Intelligence based Security

If a Customer want to perform any Transaction through ATM he should be validate first with Face recognition by AI. At the time of Customer registration in Bank itself will go for Face capture by Digital camera. The same will be stored in Bank Customer Account database. Every time when a Customer visits ATM to perform transaction Face recognition will be done by AI.

Customer inserts an ATM card into the machine while reading Account details it also fetch stored Facial image and Aadhaar ID. While retrieving the details the current facial image will be capture from the Camera which was fixed on the machine. Mean while it retrieves stored finger image based on the Aadhaar ID. Once the stored Facial Image and Current Captured image is retrieved will go for AI validation. If success will go for next Aadhhar based finger print validation.

2.2 Aadhaar based Security

Once the AI validation is success then application will go for Aadhaar based finger image validation. Based on retrieved Aadhaar ID linked with Account it will fetch the stored Finger images from UIDAI database. Mean while current Customer finger image will capture from the Biometric device which was connected to ATM machine. Once the store Finger images and Current captured Finger is image is retrieved will go for another Validation. If this

also success then it continues to the next level in Transaction system.

3. EXISTING METHOD

When ATM card is inserted into card slot the information present on the magnetic strip is read by two card readers present in the card slot. One card reader looks for special code which confirms that card is real. Second card reader grabs account number and password to check against what you entered. If authentication is successful then ATM connects with bank server through telephone network. Now user can perform bank transactions and when transaction is completed card comes out through ATM slot and user automatically logs out. Counting machine is present to count number of notes and receipt comes through printer which gives you information about transaction completed.

User needs to perform one of the following transactions:

1 Cash transfer
2 Cash Withdraw
3 Balance Enquiry
4 Password change

This is just general method of what happens.

4. PROBLEM STATEMENT

There are several methods through person can hack into the customer's account can steal the money from the customer's account. This is as follows:

1. Skimming: A device is been installed into the card slot and all the information is read from onto the card. A small pinhole camera is fixed above the keypad which takes up all this information. By the help of this information a duplicate card is made by the criminal and can access the customer's account.

2. Lebanese Loop: In this type of fraud, the criminal installs the device due to which card gets locked into the slot the time when transaction completes that time the machine pushes out the card now since the card is locked. The customer moves away from him place for complaining and by the time criminals comes out and will unlock the card and will draw all the money from users account.

3. Lost or stolen card: If the card is lost or stolen that time too there is possibility that users account can be access by criminal. By many such techniques criminals can access your account. If biometric with some additional security is used then these frauds can be minimized.

5. PROPOSED METHOD

In our proposed Iadding the features of AI and Aadhaar ID for validation of the Customer. The process will be shown below.

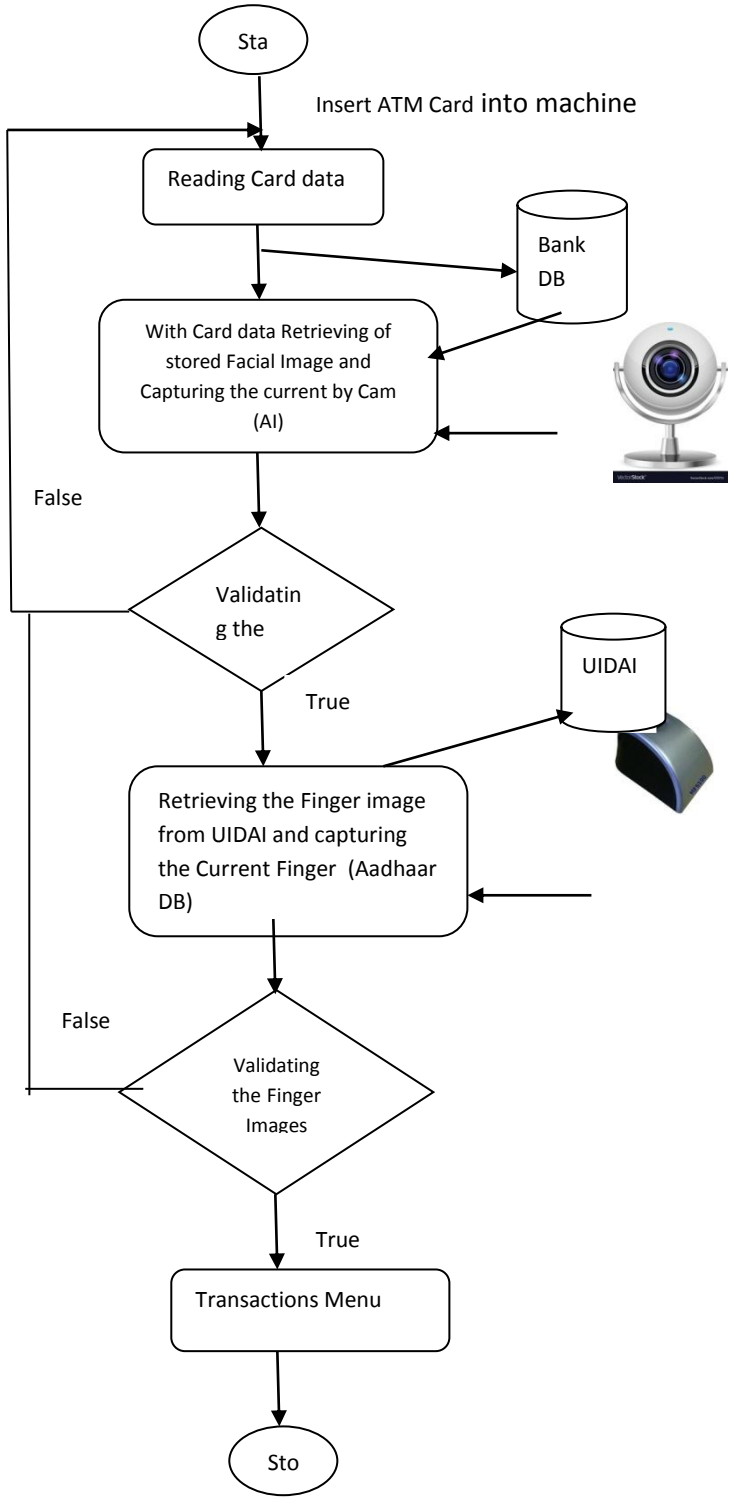

Fig: Process of AI and Aadhaar Based Smart ATM

Requirements to Implement AIASA

To implement the proposed system there is need of few Hardware and Software requirements.

1. Web Camera
2. Biometric Device
3. Module to Link AI algorithm for Capturing and validating the Facial Image.
4. Module to link the UIDAI for retrieval of stored finger images and validating with captured images.
5. Module to Read Account data and Aadhaar ID.

Some algorithms and Methods to implement AI validation and Aadhaar validation.

- Eigenfaces/Principal Component Analysis
- Local Binary Patterns Histograms (LBPH)
- Fisherfaces
- Scale Invariant Feature Transformation (SIFT)
- Speed Up Robust Features (SURF)

Machine Learning Algorithms

- Neural Networks
- Support Vector Machines
- Nearest Neighbor
- Decision Trees

By using of the above Algorithms will compare the Face Comparison. And also will perform Biometric finger validation.

6. FUTURE SCOPE

- Here proposed system is applicable for only ATM based transactions. It is identifying the Customer Physically authorized or not.
- If the Customer want to perform the same Transaction through Online either with mobile app or internet banking there the Customer is identifying only with Password or PIN number to perform transaction. Therefore Cybercrimes are growing rapidly.
- In future I am going propose this technique i.e AI and Aadhaar based algorithm to validate customer. Here no need of the Additional devices required because now a days every mobile is having a feature of Camera and Fingerprint scanner so, to implement this technique in the Mobile or Internet banking application becomes low cost effective.

7. CONCLUSION

Here I am proposing the solution of the existing problem of low Security. In the existing system Security level is very low because of no particular technique to decide whether Customer is authorized or Unauthorized. In this paper I am proposing the technique of AI and Aadhaar ID algorithms where AI will identify the Customer by validating the Facial image and also Aadhaar based Finger Image Verification to decide the Customer is authorize or not. From this paper it is going to provide High Security for Customer Bank ATM transactions.

REFERENCES

[1] Ankitha Mahajan, Radhika Mande, Avinash Mhaske, Parth Shete & Dr S.B. Dhooth, Dept. of ETE, Govt Polytechnic Aurangabad,Maharastra. “Artificial Intelligence based Smart ATM”.

[2] Manoj V, Moulishankar R, Sasipriya S, Usha Devi E, Devika t.UG student knowledge institute of technology, Salem “Multi authentication ATM theft prevention using Ibeacon”.

[3]”Biometric authentications to control ATM theft” Ahmad Tasnim Siddiqui, College of computers and IT Taif University, Kingdom of Saudi Arabia.

[4] “Design of highly secured automatic teller machine system by using Aadhar card and Fingerprint” Mr. Abhijeet S.Kale Prof. Sunpreet kaur nanda ISSN: 2319-6734, ISSN(print) : 2319-6726 www.ijesi.org volume 3 Issue 5||May 2014||pp.22.

[5] “A-ATM: Aadhar based security in Atm” Abdul rahmana shaik Vemuri Kusuma priya b, ISSN: 2395 - 0056, p – ISSN : 2395 – 0072 volume : 03 ISSUE:12/dec-2016.

[6] “Card less cash access using Biometric Atm security System” by Nine preetam Harsh gupta ISSN:2319-7463,vol.3 ISSUE 11,November-2014,pp:(13-7), Impactfactory:1.252, Avilable online at:www.erpublications.com.