SECURE ATM USING NFC AND ADAPTIVE AUTHENTICATION

Sophia S. [1], Indhumathi R S[2] , Divya S[3] , Divyashree V[4], Dharshan Shankar S[5]
[1]Assistant Professor, [2,3,4,5]UG Students,
Department of Computer Science and Engineering
Dr. T. ThimmaiahInstitute of Technology, Karnataka, India- 560100
[1]sophia7selvaraj@gmail.com, [2]indhushyla1997@gmail.com,
[3]divyas11223@gmail.com, [4]divyacharya97@gmail.com,
[5]dharshan.ttit@gmail.com

Abstract
ATM has become a most used means for people to withdraw money from their bank accounts, but ATM Cards are no longer secure because a skimmer can be fixed on ATM machine and the account details can be easily hacked . The thesis provides the development of Multi-Factor authentication along with Near Field communication, where Multi-factor authentication includes the design of risk engine proportion with the system to check the users past login records and generate suitable pattern using machine learning algorithm and calculate the risk score, based on the user risk profile it provides different means of authentication. Thus the adaptive authentication helps in providing high-security to its users.

Keywords: Near Field Communication (NFC), Risk based authentication, Adaptive authentication

I.INTRODUCTION

ATM is an electronic telecommunications device. It enables customers to perform several operations, such as cash withdrawals, deposits, Transfer funds, or obtaining account information, at any time without direct interaction with bank staff. By using an ATM, customers can access their bank deposit or credit account s in order to make a variety of financial transactions. Moreover, passwords/PIN are simply knowledge basedinformation that can be shared amongst users that led to a major drawback of Single-Factor authentication. Thus, two factor authentication or Muti-Factor authentication is preferable due to its improved security levels. Multifactor authentication includes Risk based authentication which modify itself according to the risk profile of the user. Risk profile is formed by comparing the usersbehavior such as login time, location, Device type, Number of failed attempts, the amount tin the user account, Risk level/score will be generated by using Risk engine that is integrated with the risk based authentication system. And the proposed system works based on the Machine learning Algorithms and Adaptive authentication. Machine learning algorithms are trained to learn patterns from existing data and predict the unknown value when provided with the new set of data.And Adaptive authentication is a method for selecting the right authentication factors depending on a usersrisk profile. By considering the Risk profile of the user, he/she is been challenged with different authentication methods. Any how the actual user need not required to pass multiple factors of authentications to prove his identity, while a suspicious user needs to pass all authentication methods he is required with, this ensures high security to its users. The remaining paper is arranged in the following manner- Section 2 briefly tells about the research works, enlancingtheir advantages and disadvantages. Section 3 elaborated the detailed structure of proposed method. Experimental results are depicted in Section 4 and Section 5 presents the conclusion.

II. LITERATURE SURVEY

Different studies have been done on secure ATM using NFC and machine learning based adaptive authentication having its own advantages and

DOI: 10.21276/ijcesr.2019.6.6.33

disadvantages. The Naïve Bayes classifier algorithm adopts conditional independence; it consider that an attribute value of a given class is independent values of other attributes.

Nagaratna et al. [1] has suggested multiple bank accounts into single ATM card using finger print based authentication and face recognition which provides high security. The hardware used in the system are mobile phone, face recognition, fingerprint scanner. Inputs are given by user and its verified with the previously stored data in the database and as output the user is authenticated.

Anirudhanadukkathayar [2] proposed 4-digits PIN as the knowledge factor, and NFC enabled smartphone, the input like 4-digit pin number and NFC card is given by the user for process of authentication. If the NFC card is valid the the user is allowed to enter the 4-digit pin number. This pin is verified for the process of authentication.

Anusha mandalapuet al. [3] describes three factor authentication scheme employing NFC, Dash matrix algorithm and one timepassword in this three factor Authentication. user can also block his ATM card if itsmissed using negative pattern which is already registered when the user create the account.

Dasgupta et al.[4] implemented a design for selecting factors dynamically for multifactor authentication. Trustworthy values were calculated for each factor using mathematical objectives functions. This selection of factors was affected by the device, media and external conditions like noise and light. This techniques reduced the repetitive selection of the same set of authentication factors.

Akio Ogiharaet al. [5] implemented a system using biometrics. It is performed by using 10 types of biometric feature of hand shape, which are extracted from key strokes provided in an ATM operation. Moreover, it calculates the similarities between current ATM operator and genuine user in consideration of key- press timing. The components used in this systemsare biometrics sensors which are embedded in ATM Machine.

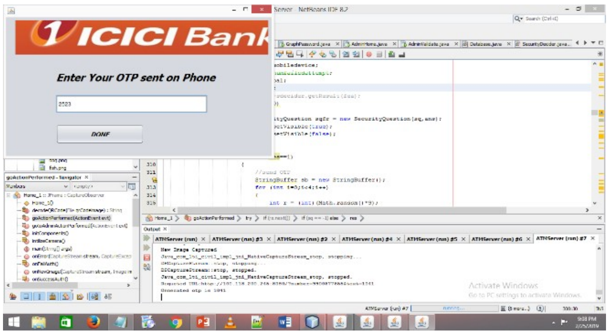
Diep et al. [6] present a mathematical risk based techniques called multifactor evaluation process that assigned numerical weights to risk elements based on confidentiality, integrity and availability of the outcomes. The risk is measured based on contextual information, requested services and the type of transaction.

III PROPOSED WORK

The proposed section presents the systems set up and detailed explanation of essential processes involved. The implementation of secure ATM system uses two new methodology:

1)NFC
2)Risk Score Authentication.

An overview of the system is shown in Figure.1



```
ityQuestion sqfr = new SecurityQuestion(sq,ans);
setVisible(true);
setVisible(false);
//send OTP
StringBuffer sb = new StringBuffer();
for (int i=0;i<4;i++)
{
    int r = (int)(Math.random()*9);
```

```
New Image Captured
Java_com_lti_civil_impl_jni_NativeCaptureStream_stop, stopping...
DSCaptureStream::stop, stopped.
Java_com_lti_civil_impl_jni_NativeCaptureStream_stop, stopped.
```

Figure 1:System Overview

The process aims at reliable dealings with banks and ensures ease of use for ATM users. This process is further divided as follows:

A.NFC Card Validation

System instead of ATM card, NFC enabled mobile phone can be used to login to ATM. With the use NFC there is no need for swiping. The user is required to tap the cell phone on the NFC tag which is fixed on the ATM. Upon successful NFC tagging, a webpage on the Cell phone's browser requests for a pre-registered phone number and PIN as a user input. When user provides it, the user phone number and PIN is sent to ATM Server. It is used to validates the NFC card access and if it is a valid card, it passto the next step of authentication.

B. Risk score calculator

Risk score calculator is a core component of our system which can predict the risk level of a user. In this paper, the risk score calculator is designed using a Naïve Baiyesclassifier which is a machine learning algorithm.

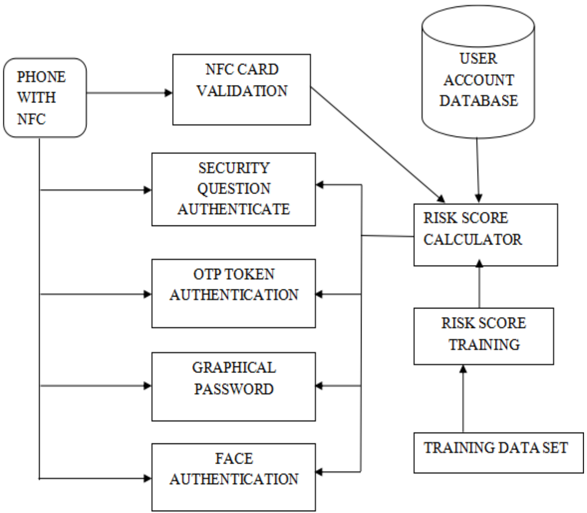
Likelihood Class Prior Probability

$$P(c\mid x)=\frac{P(x\mid c)P(c)}{P(x)}$$

Posterior Probability Predictor Prior Probability

Further the calculator is divided as follows:

Score Training**:** This module trains the Naïve Baiyesclassifier to find the risk score for the user account based on the access attributes and user attributes.



Naive Bayes Risk Score	Risk Level	Authentication Method
1<s<6	1	Security Question
7<s<18	2	OTP token
19<s<29	3	Graphical Password
30<s< 36	4	Face Authentication

Risk Score Calculator: This module uses the trained Naïve Baiyesclassifier to calculate the risk score and based on calculated risk score, it chooses the authentication method.

Below Table I represent the Risk score value and corresponding authentication method.

Table I Risk Score Value

Security Question Authentication: This method provides a security question to user which user has registered during the creation of account and as verifies the user answer. Based on the results allows the user to transaction stage.

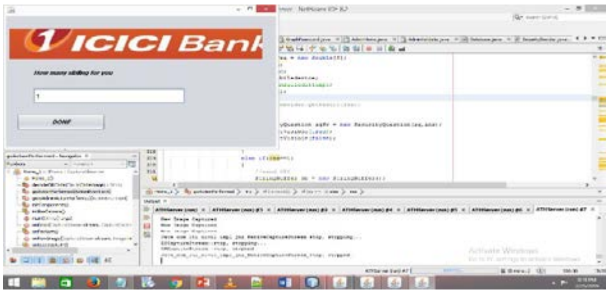


Figure 2: Security Question

OTP Token Authentication: A four digitOne-Time Password (OTP) is generated on the mobile screen which is valid only for few seconds, say 60seconds asinFigure2.If it exceeds the timeout, then a OTP is regenerated. The user wantto enter the same OTP on ATM keypad. If its correct OTP token, it allows user to transaction stage.

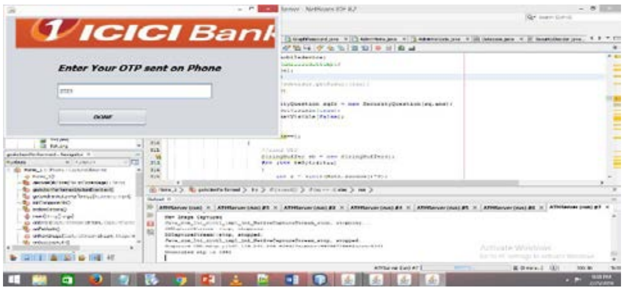


Figure 3: One Time Pad

Graphical Password: User registers graphical password in form his favorite animals, vegetables, fruits in a series , The pictures are shown and user must choose the correct order as he registered. If the selection is correct, it allows the user to transaction stage.

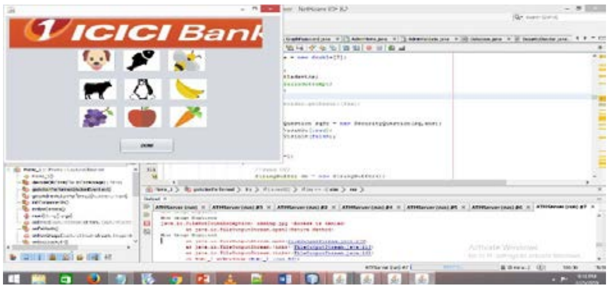


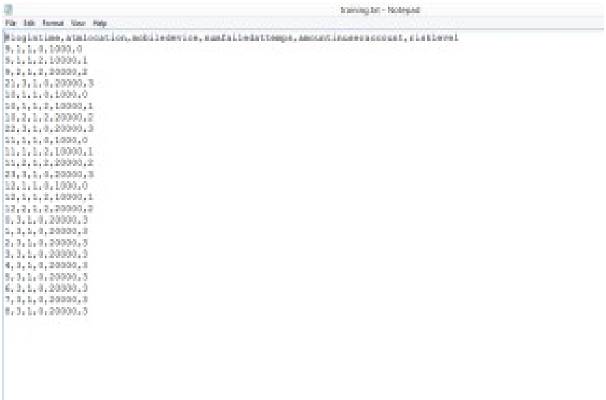
Figure 4: Graphical Questions

Face Authentication: This method captures the face image and compares to the registered face image, if it is similar, it allows the user to transaction stage.

When the user enters to the a ATM the user should tap his mobile phone on the NFC tag. If the NFC card is validated then user is allowed for further process. Then the risk engine is activated and the user is asked for some of security questions, suchas security question authentication, OTP Token Authentication, graphical password, face authentication according to risk score value if conditions satisfies then the user is authenticated user and he is allowed for further process, and allowed for transaction. The risk score value is calculated using some of the user behavior which considered as the training data set and this is stored in database.

Following parameters is used as test cases

1. Login time
2. ATM Location
3. Mobile Device
4. No of failed attempts
5. Amount in the Users account



```
#logintime,atmlocation,mobiledevice,numfailedattempts,amountinuseraccount,risklevel
9,1,1,0,1000,0
9,1,1,2,10000,1
9,2,1,2,20000,2
21,3,1,0,20000,3
10,1,1,0,1000,0
10,1,1,2,10000,1
10,2,1,2,20000,2
22,3,1,0,20000,3
11,1,1,0,1000,0
11,1,1,2,10000,1
11,2,1,2,20000,2
23,3,1,0,20000,3
12,1,1,0,1000,0
12,1,1,2,10000,1
12,2,1,2,20000,2
0,3,1,0,20000,3
1,3,1,0,20000,3
2,3,1,0,20000,3
3,3,1,0,20000,3
4,3,1,0,20000,3
5,3,1,0,20000,3
6,3,1,0,20000,3
7,3,1,0,20000,3
8,3,1,0,20000,3
```

Figure : 5 Naïve Bayes

The below Figure 6 represents Flow Chart of Secure ATM. When the user enter the ATM firstly it will collect the NFC informationrom the user and it will check whether the card is valid or invalid. If the card is invalid it again ask user for proper NFC information card. If the card is valid it moves to further process, it will collect the user attributes such as login time, OS version, location of ATM, Amount present in user account and it will access the attributes. Now the risk engine is initiated for calculating the risk score.

According to the risk score.

1)If the risk score value is r < 6 then it will ask for some security questions.
2) If the risk score value is 6 < r < 18 then it will ask for OTP token.
3)If the risk score value is 18 < r < 29 then it will ask for some graphical password.
4) If the risk score value 29 < r < 36 then it will ask for face image of user.

If the authentication is success it will allow for transaction else it will display an error and process is terminated.

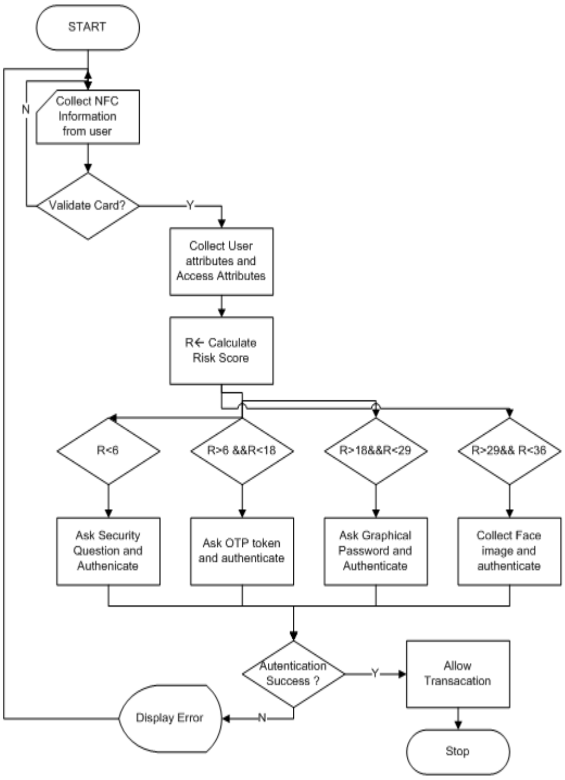
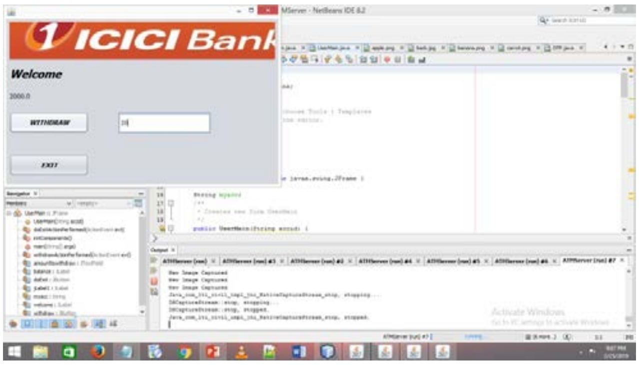

START
Collect NFC Information from user
N
Validate Card?
Y
Collect User attributes and Access Attributes
R← Calculate Risk Score
R<6
R>6 &&R<18
R>18&&R<29
R>29&& R<36
Ask Security Question and Authenticate
Ask OTP token and authenticate
Ask Graphical Password and Authenticate
Collect Face image and authenticate
Autentication Success ?
Y
Allow Transaction
N
Display Error
Stop

Figure 6 : Block Daigram of Secure ATM

V.RESULTS



V. CONCLUSION

The ATM Electronic Transaction is playing very persistent and pervasive role in the present world. The ATM should be made up of robust infrastructure setup to with stand any kind oftheft. In Existing System authentication and authorization is done by using credit card and pin number. It leads to low level of authentication and leads to theft . Hence developed new method called Multi factor authentication using two methodology NFC (Near Field Communication) and Risk Based Authentication. The Benefits of NFC are avoiding skimming of cards, it is easyaccessible to user and reliable, Feasible and Benefits of Risk Based

DOI: 10.21276/ijcesr.2019.6.6.33

Authentication provides High Level security and it provides risk level questions based on user behavior. In this paper it mainly providehigh level of security, avoid bank accounts from different types of theft and attacks, and avoid the usage or Carrying of multiple ATM Card.

REFERENCES

[1] Nagaratna,"Highly Secure Multiple Account Bank Affinity Card- A Successor for ATM Card", IEEE Publisher, 2015

[2] anirudhanadukkathayaer," secure multifactor authentication payment system using nfc",10th International Conference on Computer Science & Education (ICCSE 2015) July22-24, 2015. Fitzwilliam College, Cambridge University, UK

[3] Anusha Mandalapu, "AnNFC featured three level authentication system for tenable transaction and abridgment of ATM card blocking intricacies", IEEE 2015.

[4] Dipankar Dasgupta, Abhijit Nag, and Arunava Roy,"Toward the design of adaptive selection strategies for multi-factor authentication". Computers and security, pp,2016.

[5] Dipankar Dasgupta, Abhijit Nag,andArunavaRoy, " Toward the design of adaptive selection strategies for multi-factor authentication". Computers and security,2016.

[6] DiepN.N.,Y.-KLee, HJ.Lee, S.Lee, "Contextual Risk-based Access control", Security and management,2007

DOI: 10.21276/ijcesr.2019.6.6.33