ATM Authentication System using NFC tags and Text Matrix

Madhura Tare, Shweta Kulkarni, Mohak Mehta, Gauresh Salgaonkar

Department of Information Technology
Sinhgad Institute of Technology, Lonavala-410401, Maharashtra
Prof. P. P. Ahire, *Dept. of Information Technology, SIT Lonavala, Maharashtra,India*

***

Abstract - *NFC (Near field Communication) is a short-go remote correspondence innovation whose innovation separation is around 4 inches, and it works in the 13.56MHz recurrence band at a speed of 106Kbps to 424Kbps. The blend of NFC with savvy gadgets brought about enlarging the scope of NFC, which incorporates information trade, benefit revelation, association, e-installment, and ticketing. We are utilizing NFC innovation for ATM enrolment we are giving solid confirmation username, secret key and also NFC label validation and shading watchword verification and lattice watchword verification. We are likewise giving View Balance, Transfer Money, Edit Details - User can utilize the further usefulness of ATM which incorporates adjust enquiry and Edit points of interest.*

Key Words: ATM Transaction, Dash Matrix Algorithm, NFC Tag, Balance, Transfer cash, e-installment, NFC Transmitter, NFC Receiver, Non NFC empowered Phones.

1. INTRODUCTION

A reasonably and progressively regular misfortune including burglary in computerized trade is taking or skimming of ATM cards. Not at all like most different methods for robbery, this is an intrinsic helplessness of the ATM framework and system itself. With a specific end goal to beat this natural shortcoming, we depict framework utilizing a generally new innovation called NFC to implement security amid exchange and utilization. The possibility of this venture is to build up the counteractive action of robbery of the ATM card and to control the use of the ATM card by unapproved individual. The extra component of this venture is that no exchange should be possible without the information of the separate card holder for the cause that NFC exchanges are being executed. To guarantee the wellbeing and uprightness of residential online installments, different banks have presented a three level validation procedure to verify online exchanges. This innovation was initially utilized by Google to upgrade the security of electronic mail account enclosures, taking after the illustration. A few parts, for example, multi-leveled conditions, illustrations, and tables are not endorsed, despite the fact that the different table content styles are given. The formatter should make these segments, consolidating the pertinent criteria that take after. The mix of NFC with brilliant gadgets brought about enlarging the scope of NFC, which incorporates information trade, benefit disclosure, association, e-installment, and ticketing. It is required to supplant Master cards in electronic installment, particularly. As indicated by based installment administrations is relied upon to increment by 11.3 times from $316 million in 2010 to $3.572 billion in 2015, and Juniper look into anticipated that the worldwide NFC installment advertise size would be expanded to $180 billion in 2017. To utilize NFC in electronic installment, security is an essential to be tended to. By and by, NFC security norms characterize information trade design, label sorts, and security conventions, fixating on NFC gathering. It is explicitly stipulated in the NFC security benchmarks that key acquisition is required for mystery interchanges between clients. During the time spent key understanding, both clients ought to trade their open keys. The general population key is gotten from CA (Certificate Authority), and it utilizes a settled an incentive until reissued. Pernicious inside aggressors can make profiles of clients through the securing of open keys of different clients during the time spent key acquisition. On the off chance that NFC is utilized as a part of e-installment thus, the protection of clients can be encroached through profiles made by aggressors.

1.1 Methodology

This segment displays the proposed framework, setup, and Nitti gritty clarification of basic procedures included. A review of the framework is appeared in Fig.1

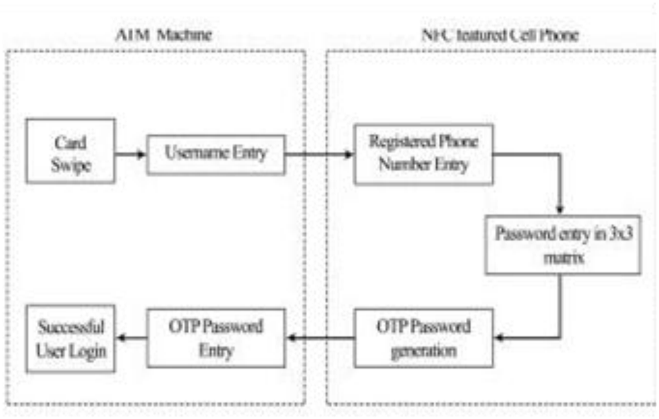


Fig.1 Framework Overview

A. Secured ATM exchanges utilizing NFC

This procedure goes for quicker and dependable dealings without breaking a sweat of utilization for ATM clients. This procedure is further isolated into three sub sectioned procedures.

1. Client Access utilizing NFC labels: Every client will have their remarkable NFC labels. These labels will contain their remarkable id of every client inside the circuit. Client need to put the NFC labels close-by NFC gadget so that the gadget can track the NFC labels. Labels will work just when it is avoided close-by to the gadget at all costs of around 5-8cm.

2. Once NFC labels is been distinguished by the framework, then client can see the points of interest of the bank however exchange and different rights are given simply after second phase of security. approval of the NFC labels are done from the server side.

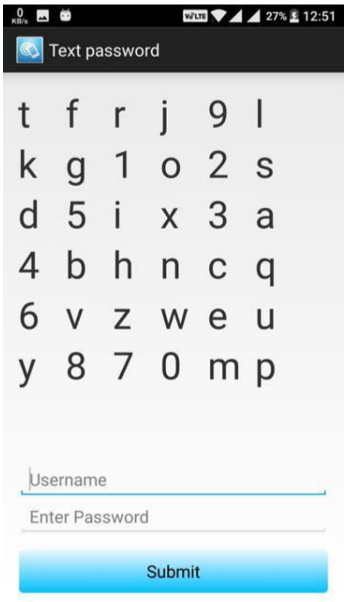
3. Match based Authentication conspire : amid enrollment client presents his secret key. Least length of the watchword is 8 and it can be called as mystery pass. The mystery pass ought to contain considerably number of characters. Session passwords are created in view of this mystery pass. Amid the login stage, when the client enters his username an interface comprising of a lattice is shown. The network is of size 6 x 6 and it comprises of letters in order and numbers. These are arbitrarily put on the network and the interface changes inevitably.

B. NFC Tag perusing

The client peruses the NFC–TAG, by swiping the mobile phone over the NFC tag on the ATM.

C. Matrix Authentication

When the NFC tag authentication is done by the user, then user login into system . The next tab is matrix authentication level. Following is the Matrix,



t	f	r	j	9	l
k	g	1	o	2	s
d	5	i	x	3	a
4	b	h	n	c	q
6	v	z	w	e	u
y	8	7	0	m	p

Fig.2 Matrix Window

1.2 Algorithm

Ones the client peruses NFC label utilizing NFC cell phone, validation screen will show up on screen .User needs to enter the example which demonstrates the secret word. The Pattern Password idea includes another calculation called the Dash Matrix Algorithm (DMA). Following is the algorithm used in the matrix authentication system.

```
    int[] pindex = new
    int[password.length]; int k = 0;

    for (char pchar : password)
      { for (int i = 0; i < 6; i++) {

          for (int j = 0; j < 6; j++) {

            if (textMatrix[i][j] == pchar) {
              pindex[k] = (k % 2 == 0) ? i : j;

            }

          }

      }

      if (k % 2 != 0) {

          sessionPassword +=textMatrix[pindex[k -

1]][pindex[k]];

      }

      k++;

      }

    out.print(sessionPassword + "<br/>" +
                              pwd +

"<br/>");

    if (pwd.equalsIgnoreCase(sessionPassword))
      { out.print("Login Successful using
      text<br>"); return true;
```

```
        }

      }

      return false;

    }

    private boolean validateUserColor(String
dbcolorpassword, String name, String pwd, String[]
colorMatrix, int[][] cNumMatrix) {

      if (dbcolorpassword != null &&
!dbcolorpassword.equals("")) {

        String sessionPassword = "";

        int[] pindex = new
        int[dbcolorpassword.length()]; int k = 0;

        String[] colors = new String[ccolumns];

        for (char pchar :
          dbcolorpassword.toCharArray()) { switch
          (pchar) {

            case 'r':

              colors[k] =
              "#ff0000"; break;

            case 'g':

colors[k] = "#00ff00"; break;

            case 'b':

              colors[k] =
              "#0000ff"; break;

            case 'y':

              colors[k] =
              "#ffff00"; break;

          }
          for (int j = 0; j < ccolumns; j++) {
            if
            (colorMatrix[j].equalsIgnoreCase(colors[k]))
{
              pindex[j] = k;
            }
          }
          k++;
        }
        for (int l = 0; l < ccolumns; l++) {
          if (l % 2 != 0)
          {sessionPassword += "" +
          cNumMatrix[pindex[l -
          1]][pindex[l]];
          }
        }
        out.print(sessionPassword+"<br/>"+pwd+
"<br/>");
        if
          (pwd.equalsIgnoreCase(sessionPassword)
          ) { out.print("Login Successful using
          color"); return true;
        }
      }
      return false;
```

2. HARDWARE

Different types of NFC tags are used to authenticate
the machine. We will take a look at them.

2.1 What is NFC tags?

NFC technology is pretty common these days and features in most high-end smartphones. As well as phone to phone communication, small little NFC tags can also be used to store and transfer information. You will probably have noticed small NFC tags next to advertisements near bus stops, stickers in shops, or may have even come across the clever idea of using NFC enabled business cards. These tags can store wide ranges of information, from short lines of text, such as a web address or contact details, to links to apps in the Google Play Store. It's a quick and efficient way to quickly push information to your phone and these little tags can replace bar and QI codes, and could even be used instead of Bluetooth in some cases.

2.2 How it works?

NFC tags are passive devices which means that they operate without a power supply of their own and are reliant on an active device to come into range before they are activated. The trade-off here is that these devices can't really do any processing of their own instead they are simply used to transfer information to an active device, such as a smartphone. In order to power these NFC tags, electromagnetic induction is used to create a current in the passive device. We won't get too technical on this, but the basic principle is that coils of wire can be used to produce electromagnetic waves, which can then be picked up and turned back into current by a another coil of wire. This is very similar to the techniques used for wireless charging technologies, albeit much less powerful.

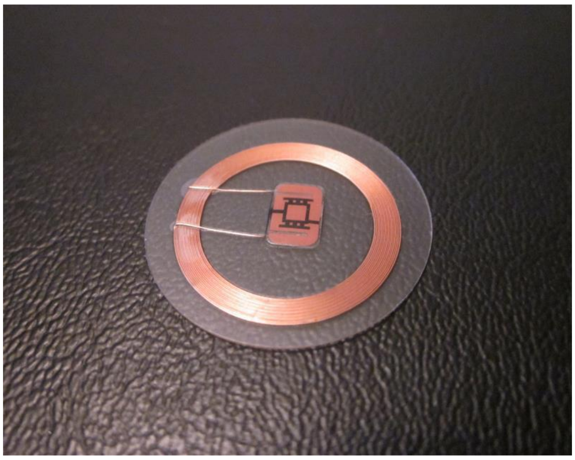


Fig.3 NFC tag

2.3 Different types of NFC tag

The different NFC tag type definitions are as follows:

1) Tag 1 Type: The Tag 1 Type is based on the ISO14443A standard. These NFC tags are read and re-write capable and users can configure the tag to become read-only. Memory availability is 96 bytes which is more than sufficient to store a website URL or other small amount of data. However the memory size is expandable up to 2 kbyte. The communication speed of this NFC tag is 106 kbit/s. As a result of its simplicity this tag type is cost effective and ideal for many NFC applications.

2) Tag 2 Type: The NFC Tag 2 Type is also based on ISO14443A. These NFC tags are read and re-write capable and users can configure the tag to become read-only. The basic memory size of this tag type is only 48 bytes although this can be expanded to 2 kbyte. Again the communication speed is 106 kbit/s.

3) Tag 3 Type: The NFC Tag 3 Type is based on the Sony FeliCa system. It currently has a 2 kbyte memory capacity and the data communications speed is 212 kbit/s. Accordingly this NFC tag type is more applicable for more complex applications, although there is a higher cost per tag.

4)Tag 4 Type: The NFC Tag 4 Type is defined to be compatible with ISO14443A and B standards. These NFC tags are pre-configured at manufacture and they can be either read / re-writable, or read-only. The memory capacity can be up to 32 kbytes and the communication speed is between 106 kbit/s and 424 kbit/s.

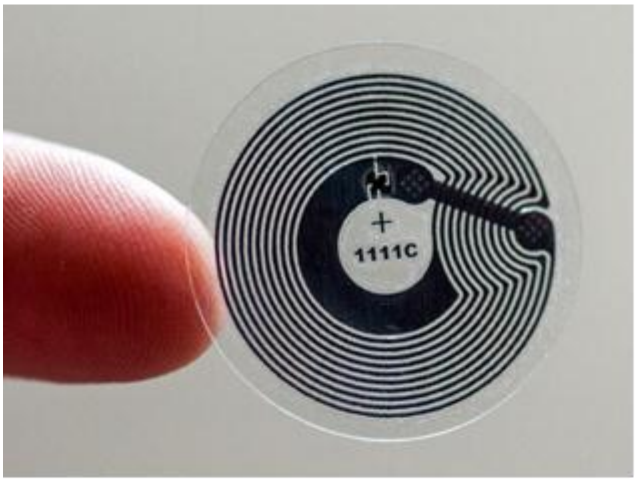


Fig.4 Type 1 tag

From the definitions of the different NFC tag types, it can be seen that type 1 and 2 tags are very different to type 3 and 4 tags, having different memory capacity and makeup. Accordingly it is expected that there is likely to be very little overlap in their applications.

Type 1 and type 2 tags are dual state and may be either read/write or read-only. Type 3 and Type 4 tags are read-only, data being entered at manufacture or using a special tag writer.

3. CONCLUSIONS

In proposed system, every client will have their extraordinary NFC labels. These labels will contain their one of a kind id of every client inside the circuit. Client need to put the NFC labels adjacent NFC gadget so that the gadget can track the NFC labels. Labels will work just when it is avoided close-by to the gadget at all costs of around 5-8cm. Once NFC labels is been identified by the framework, then client can see the points of interest of the bank yet exchange and different rights are given simply after second phase of security. approval of the NFC labels are done from the server side. We are utilizing NFC innovation for ATM enlistment we are giving solid validation username, secret word and in addition NFC label verification and shading watchword confirmation and grid watchword confirmation.In existing framework the mix of NFC with brilliant gadgets has prompted broadening the usage scope of NFC. It is required to supplant Visas in electronic installment, particularly. In such manner, security issues should be routed to vitalize NFC electronic installment. To utilize NFC in electronic installment, security is an essential to be tended to. By and by, NFC security gauges characterize information trade arrange, label sorts, and security conventions, centering on NFC gathering. NFC is a short-extend remote correspondence innovation. Because of its separation restrictions, the short-go remote correspondence innovation is by all accounts more secure than wired correspondence innovation, which truly is definitely not. On the off chance that correspondence is performed through RF field, alongside NFC, information can be acquired notwithstanding when clients remain close to the transmitter. In this area, the security prerequisites met by techniques that break down security dangers of NFC are found. In Proposed System we are utilizing NFC innovation for ATM enrollment we are giving solid validation username, watchword and in addition NFC label verification and shading secret word confirmation and framework watchword confirmation. We are additionally giving View Balance, Transfer Money, Edit Details - User can utilize the further usefulness of ATM which incorporates adjust enquiry and Edit subtle elements.

REFERENCES

1. Anusha Mandalapu, Daffney Deepa V, Laxman Deepak,Raj Anish Dev J "A NFC included three level confirmation framework for viable exchange and edited version of ATM card blocking complexities" , 978-1-4799-6908-1/15/$31.00 ©2015 IEEE
2. http://www.radioelectronics.com/info/wireless/nfc/ne ar-field-communications-tags-types.php
3. Thivya.G, Amutha.C "Deployment of NFC for Security Purposes and Efficient Transaction in Real World" (An ISO 3297: 2007 Certified Organization)

   Vol. 3, Special Issue 2, April 2014
4. C.Balakumar, A.M.Adrean mel Clinton, J.Karthikumar "NFC ACCEPTANCE BY AN ADVANCED ATM MACHINE" Proceedings of 4th IRF International Conference, Chennai, 9th March-2014, ISBN: 978-93-82702-64-1
5. J. A. Ang, R. F. Barrett, R. E. Benner, D. Burke, C. Chan, J. Cook, D. Donofrio, S. D. Hammond, K. S. Hemmert, S. M. Kelly, H. Le, V. J. Leung, D. R. Resnick, A. F. Rodrigues, J. Shalf, D. Stark, D. Unat, and N. J. Wright. Unique machine models and intermediary structures for exascale figuring. In Proceedings of the first International Workshop on Hardware-Software Co-Design for High Performance Computing, Co-HPC '14, pages 25–32, Piscataway, NJ, USA, 2014. IEEE Press.
6. Bradford L Chamberlain, Sung-Eun Choi, Steven J Deitz, David Iten, and Vassily Litvinov. Composing client characterized area maps in Chapel. In CUG 2011, 2011.
7. Young-Gon Kim and Moon-Seog Jun, "A plan of User Authentication framework utilizing QR code distinguishing strategy", sixth International Conference on Computer Science and Convergence ,Information Technology, IEEE Transactions, pp. 31-35, Nov-Dec 2011.
8. Zhengming Li, Lijie Xue and Fei Tan, "Confront recognition in complex foundation in view of skin shading highlights and enhanced AdaBoost Algorithm" Progress in Informatics and Computing (PIC), 2010 IEEE International Conference, Vol. 2 , pp. 723-727, Dec. 2010
9. Carlos de Blas Cart'on, Arturo Gonzalez-Escribano, and Diego R Llanos. Easy and productive disseminated information apportioning in direct variable based math. In High Performance Computing and Communications (HPCC), 2010 twelfth IEEE International Conference on, pages 89– 97. IEEE, 2010.
10. Chris Karlof, U. Shankar, J. D. Tygar and D. Wagner, "Dynamic pharming assaults and bolted same-starting point strategies for web programs" in CCS'07:proc. fourteenth ACM Conf. PC Communications Security, New York, 2007, pp. 58-71, ACM.