Advanced Security Mechanism in ATM

Mr. S. Manikandan

Assistant Professor,
Department of CSE, PSR Engineering College, Virudhunagar dist, India

***Abstract*: Authentication is a critical part of any computing system which ensures that, only individuals can to log on to the system. ATM machines generally authenticates by using ATM card and PIN number to perform transactions. ATMs enable customers to perform financial transactions like cash withdrawal, check balances or credit mobile phones with the help of the machine and without any human intervention. A plastic ATM card with a magnetic stripe or a plastic smart card with a chip and a unique card number and security information is used for the transaction. Authentication is done by using the Personal Identification Number (PIN). In the existing system four-digit pin is used as weak authentication system, offering just 10,000 variations (even fewer when your account for the fact those certain common combinations, such as 9999, aren't allowed by most banks). The proposed system emoji passcode offers a choice of 44 emoji, and four slots, offering 3.8 million different passcodes. Our brains are capable of processing and storing large amounts of pictorial data with ease. The emoji password schemes provide a way of making more human-friendly passwords.**

***Keywords*: Pins, Security, Encryption, AES, ATM**

I. INTRODUCTION

Now a day the use of ATMs has increased to a huge amount. More than 95 % people can use ATMs. The 1.5 million ATM installed around worldwide. Along with the use of ATM, the frauds on ATM money transactions have also increased. In existing system, a numerical four-digit pin has been used. A numerical four digit pin was weak authentication system and more fraud transaction occurred in this existing system. Hence the proposal of a new security system wherein the normal 4-digit number pins is being replaced with Emoji's.

A numerical four-digit pin is used as weak authentication system, offering just 7290 combinations (even fewer when your account for the fact those certain common combinations, such as 9999 aren't allowed by most banks). By contrast, the emoji passcode offers a choice of 44 emoji, and four slots, offering 3.5 million different passcode combinations.

Hence it will provide a higher-level security as compared to the older system. Hence to overcome this problem we can adopt a new encryption standard known as the Advanced Encryption Standard (AES). AES is a symmetric key encryption & decryption method.

II. LITERATURE SURVEY

Passwords are the most commonly used method for identifying users in computers and communication systems. Generally, passwords are strings of letters and digits, i.e. they are alpha numeric. Such passwords have the disadvantage of being hard to remember. The existing authentication system suffers from many drawbacks.

The users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks.

In the existing system when a user chooses a new password, they find it very difficult to remember the new password if it is created in the random way that is usually required. The lack of understanding of what constitutes a strong password can lead to the creation of weak passwords that are vulnerable to attack. It is rare for training to be provided on how to create a secure password. Without appropriate help and advice when a weak password is selected, the user's inaccurate understanding of security remains uncorrected, and security is undermined. This means that the utility of mechanism that is designed to help provide for security is poor. This in turn reflects on the inability of those people responsible for security to understand that the very measures they have implemented are not secure, and illustrates their failure to design truly secure system.

III. PROPOSED SYSTEM

In proposed system, introduce emoji based authentication system for ATM Machine. Human beings live and interact in an environment where the sense of sight is predominant for most activities; our brains are capable of processing and storing large amounts of pictorial data with ease. While we may find it very hard to remember a string of numbers and letters, we are easily able to remember faces of people, places we visited, and things we have seen.

Thus, emoji password schemes provide a way of making more human-friendly passwords while increasing the level of security.

The proposed scheme entitles the following features:

i. The normal 4-digit number pins being replaced with Emoji's.

ii. A randomized virtual keyboard for security enhancement.

iii. In the proposed scheme a new encryption standard known as the Advanced Encryption Standard (AES) is being used for higher security.

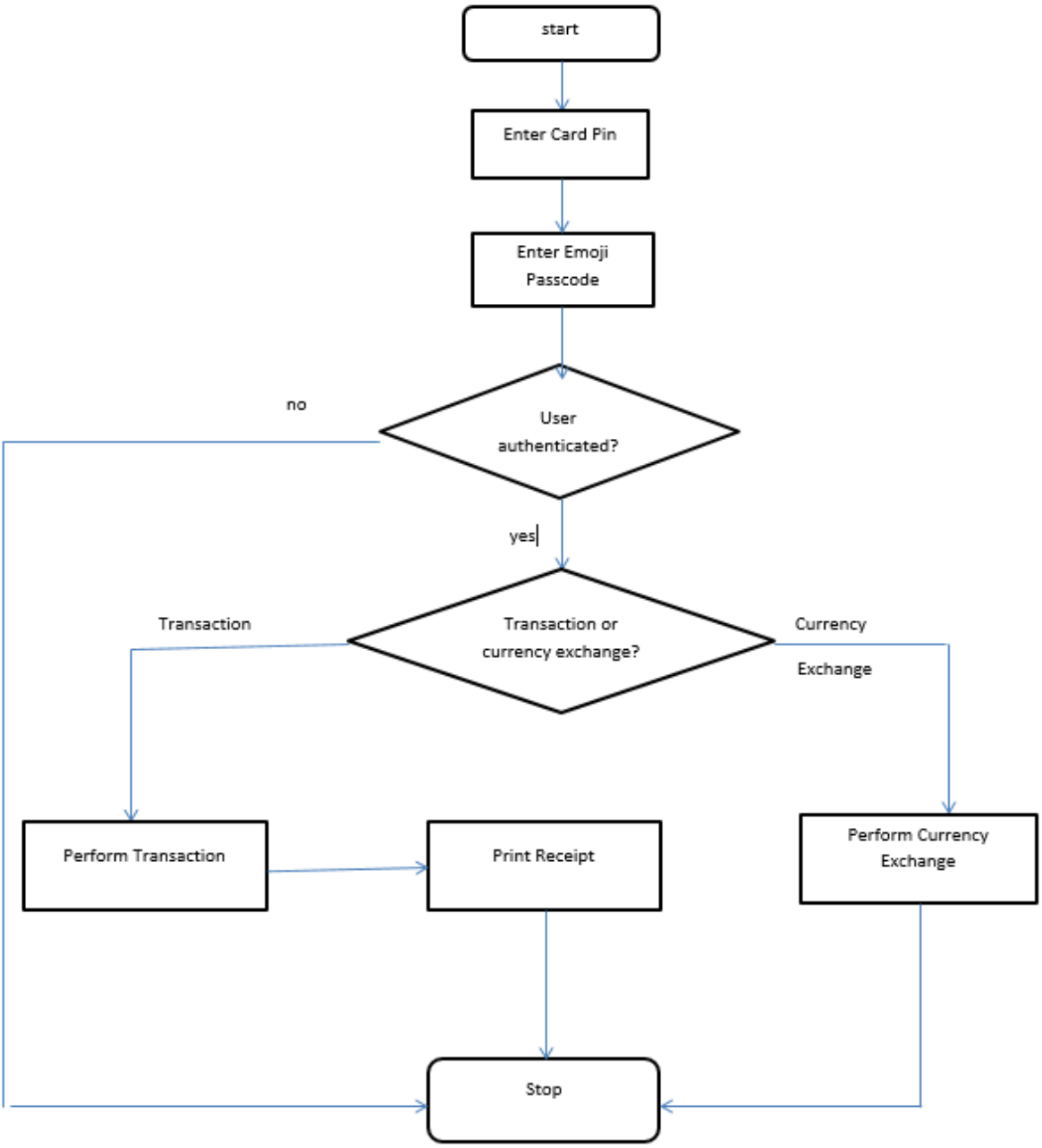

Fig 1: Flowchart of the system

IV. IMPLEMENTATION

A. Visual Basic.NET

Visual Basic is a high-level programming language which evolved from the earlier DOS version called Basic. Basic means Beginners' All-purpose Symbolic Instruction Code. It is a relatively easy programming language to learn.

Visual Basic is also Visual and Event-driven Programming Language. These are the main divergence from the old BASIC. In BASIC, programming is done in a text-only environment and the program is executed sequentially. In VB6, programming is done in a graphical environment. In the old BASIC, you have to write program code for each graphical object you wish to display it on screen, including its position and its color. However, In VB6, you just need to drag and drop any graphical object anywhere on the form, and you can change its properties using the properties window.

In addition, Visual Basic 6 is Event-driven because we need to write code in order to perform some tasks in response to certain events. The events usually comprise but not limited to the user's inputs. Some of the events are load, click, double click, drag and drop, pressing the keys and more. We will learn more about events in later lessons. Therefore, a VB6 Program is made up of many subprograms, each has its own program code, and each can be executed independently and at the same time each can be linked together in one way or another.

Visual Basic .NET is an Object-Oriented programming language designed by Microsoft. With the word “Basic” being in the name of the language, you can already see that this is a language for beginners. Although the language is aimed at noobs and novices, you should not underestimate the power of the language itself. There are people who criticize VB.NET because of the simplicity of the syntax, but VB.NET has the ability to create very powerful and sophisticated applications. VB.NET is a great place

to start because of how easy and straight forward it is. The syntax is easy and you will not find yourself writing hundreds of lines of code as there are many shortcuts that make coding so much easier in this language.

B. SQL

The Structured Query Language (SQL) comprises one of the fundamental building blocks of modern database architecture. SQL defines the methods used to create and manipulate relational databases on all major platforms. SQL is used to communicate with a database. According to ANSI (American National Standards Institute), it is the standard language for relational database management systems. SQL statements are used to perform tasks such as update data on a database, or retrieve data from a database. Some common relational database management systems that use SQL are: Oracle, Sybase, Microsoft SQL Server, Access, Ingres, etc. Although most database systems use SQL, most of them also have their own additional proprietary extensions that are usually only used on their system. However, the standard SQL commands such as "Select", "Insert", "Update", "Delete", "Create", and "Drop" can be used to accomplish almost everything that one needs to do with a database.

C. AES

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption.

AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Each round of processing works on the input state array and produces an output state array. To appreciate the processing steps used in a single round, it isbest to think of a 128-bit block as consisting of a 4×4 matrix ofbytes, arranged as follows:

$$\begin{bmatrix} byte_0 & byte_4 & byte_8 & byte_{12} \\ byte_1 & byte_5 & byte_9 & byte_{13} \\ byte_2 & byte_6 & byte_{10} & byte_{14} \\ byte_3 & byte_7 & byte_{11} & byte_{15} \end{bmatrix}$$

Fig 2: Matrix Table

Therefore, the first four bytes of a 128-bit input block occupy thefirst column in the 4 × 4 matrix of bytes. The next four bytes occupy the second column, and so on. Unlike DES, the decryption algorithm differs substantially from the encryption algorithm. Although, overall, very similar steps are used in encryption and decryption, their implementations are not identical and the order in which the steps are invoked is different, as mentioned previously.

High-level description of the algorithm:

i. KeyExpansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

ii. InitialRound

iii. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

iv. Rounds

v. **SubBytes**—a non-linear substitution step where each byte is replaced with another according to a lookup table.

vi. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

vii. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

viii. AddRoundKey

1. Final Round (no MixColumns)

ix. **SubBytes**

x. ShiftRows

xi. AddRoundKey

V. RESULTS

Fig 3: Login Screen Layout

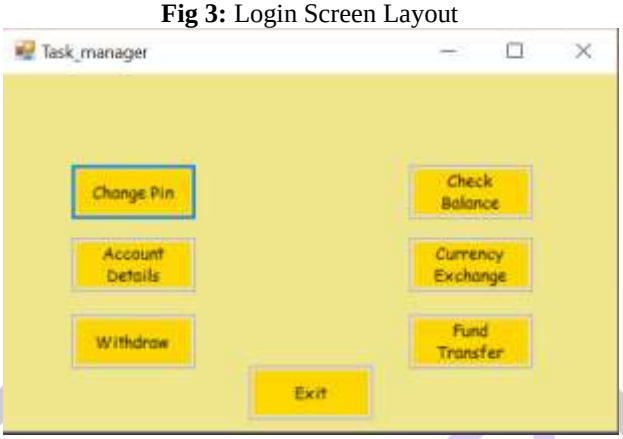

Fig 4: Functional Screen Layout

V. CONCLUSION AND FUTURE WORK

Emoji Passcodes offers about 3.5 million combinations compared to 7999 combinations offered by numeric PINS. Emoji's are pictorial form of an emotion or a memory. We remember more information when it is in a pictorial form, that's why the Emoji passcode is better than numeric PINs. The Advanced Encryption Standard (AES) feature adds support for the new encryption standard AES, along with Cipher Block Chaining (CBC) mode, to IP Security (IPsec). There are no Physical keyboards available which contains EMOJI, we propose to make a virtual keyboard which is more secure than a physical keyboard.

The main goal is to provide a secure authentication system wherein the pins are being replaced with emoji's providing an enhanced level of security. The system approves the following objectives:

Password encryption and decryption through AES algorithm:

This algorithm has different block size and keys. Thus, making it difficult for the intruder to break the code. AES has power to implement an anti-theft system.

Encoding and decoding the emoji's:

Transmitting in the form of image makes it complex for the intruder to detect the presence of secured information.

Randomized Virtual Keyboard:

Every time the user inputs the password the emoji's will be randomly placed so as to enhance the level of security.

REFERENCES

[1] A. Fiat and M. Naor. Broadcast encryption. Advances in Cryptology - CRYPTO'93, volume 773 of Lecture Notes in Computer Science, 1994.

[2] Implementation of a Low Cost Hybrid Automated Teller Machine (H-ATM) with Integrated Currency Exchange Capability, 2012 7th International Conference on Electrical and Computer Engineering 20-22 December, 2012, Dhaka, Bangladesh.

[3] Kannan, P (2013) and Ms P. Meenakshi Vidya. "Design and Implementation of Security Based ATM theft Monitoring system".

[4] Automatic Teller Machine, Lockergnome Encyclopedia 2004 [Retrieved from web March 25th, 2005].

[5] Cryptography and Network Security, Principle and Practice 3rd ed., William Stallings 2003 [Retrieved from text March 20th, 2005].

[6] Data Encryption Standard (DES), Federal Information Processing Standards Publication 46-2 1993 [Retrieved from web March 25th, 2005].

[7] Bruce Schneier; John Kelsey; Doug Whiting; David Wagner; Chris Hall; Niels Ferguson; Tadayoshi Kohno; et al. (May 2000). "The Twofish Team's Final Comments on AES Selection" (PDF).