ISSN: 2278 – 1323
*International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*
*Volume 5, Issue 6, June 2016*

# Securing Transaction using Alphanumeric Keys and Biometric.

Ms.Sneha R.Dighe.
Ms. Puja S.Joshi.
MCA (IMCOST), Mumbai University
C-4,Wagle Industrial Estate, Near Mulund (W)
Check Naka, Thane (w) - 400604

**Abstract— Security of electronic transaction over insecure communication channel is a challenging task that includes many critical areas as secure communication channel, strong data encryption technique and trusted third party to maintain the electronic database. The conventional methods of encryption in Secure Electronic Transaction can only maintain the data security. The confidential information of customer could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption methods to enhance data security as well as authentication of data communication. Two most important techniques to provide secure electronic transactions. First is instead of only using four digits password we have to provide combination of numeric, alphabets and special characters as a password. Second is we should have to provide finger prints mechanism to identify authenticated user.**

**Keywords— Secure Electronic Transaction, Data Encryption, Data Security.**

## I. INTRODUCTION

Traditionally, numeric passwords have been used for authentication, but they are known to have security and usability problems. Now day's alphanumeric passwords and finger prints are other alternatives. Our paper reports to the comparison study between the different alphanumeric password, finger prints schemes and the numeric passwords. The passwords require the following fundamentally requirements so that the problems with passwords arises [1].

(a) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.

(b) Passwords should be secure, i.e. they should look random and should be hard to guess.

### 1.1. Main problems with numeric passwords.

The main problem with the numeric passwords is that once a password has been given to the user must be able to recall it to log in. But, people regularly forget their passwords. If a password is not frequently used it will be even more susceptible to forgetting. The recent surveys have shown that simple passwords that are easily guessable, numerical passwords contains 0-9 digits only so that they can be easily hacked [2].the most important issue is having a password that can be remembered reliably and input quickly.

### 1.2. Need of alphanumeric passwords and fingerprint.

The alphanumeric passwords provide more security than numeric password. Alphanumeric password also helps to generate large number of combination of passwords. The require alphanumeric password and require both numbers and letters settings specify whether or not the password should consist of letters, numbers, and special characters. When enabled, the device client is required to use a "Strong Alphanumeric" password, which consists of lowercase letters, uppercase letters, numerals, and special characters (@, #, &, etc.).

Fingerprint scanning essentially provides an identification of a person based on the acquisition and recognition of those unique patterns and ridges in a fingerprint. The actual fingerprint identification process will change slightly between products and systems. The basis of identification, however, is nearly the same. Standard systems are comprised of a sensor for scanning a fingerprint and a processor which stores the fingerprint database and software which compares and matches the fingerprint to the predefined database. Within the database, a fingerprint is usually matched to a reference number, or PIN number which is then matched to a person's name or account. In instances of security the match is generally used to allow or disallow access.

**Example:**

Suppose any person purchase anything from mall then he/she have to follow some steps for paying bill, that time if we provide some strong security then there will be less chances to hacking password And misuse of card:

- First user have to swap their card into the machine.
- then he/she type their personal Pin number which consist of some characters ,numbers or special characters so that password will be more secure than numerical password.
-then user will put their finger on fingerprint scanner. And that scanned result going to match with previously stored database data of user.
-if that password and fingerprints are match properly then he/she is authenticate user and process will go ahead for billing process and pay the bill.
-but if match is not found and he/she is unauthorized user then that card will locked from the bank, and transaction will terminated.

These all things we can achieve by providing those both strong securities.

## II. Techniques for alphanumeric password and fingerprint detection.

For the comparison purpose we studied many techniques for generating the alphanumeric password and fingerprint detection. The brief idea of them is as follows.

### 2.1 Alphanumeric and special characters Based Authentication

If you only use words from a dictionary or a purely numeric password, a hacker only has to try a limited list of possibilities. A hacking program can try the full set in under one minute. If you use the full set of characters and the techniques above, you force a hacker to continue trying every possible combination to find yours. If we assume that the password is 8 characters long, this table shows how many times a hacker may

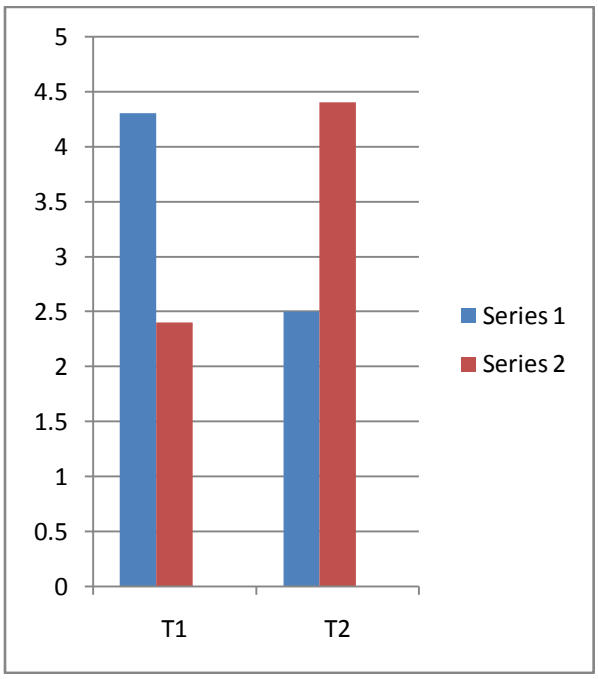
have to before guessing your password. Most password crackers have rules that can try millions of word variants per second, so the more algorithmically complex your password, the better.

**Table I** : Strong password possible combinations

| Character Sets used in Password | **Calculation** | *Possible Combinations* |
|---|---|---|
| Dictionary words (in English): | — | 600,000 |
| Numbers Only | 10^8 | 100,000,000 |
| Lowercase Alpha Set only | 26^8 | 208,827,064,576 |
| Full Alpha Set | 52^8 | 53,459,728,531,456 |
| Full Alpha + Number Set | 62^8 | 218,340,105,584,896 |
| Full Set of allowed printable characters set | (10+26+26+19)^8 | 645,753,531,245,761 |

The longer your password the more secure. If we take the full set of allowed printable characters set and increases the password length, the possible combinations jump exponentially.

- 8 Characters > 645,753,531,245,761 (645 Trillion) Combinations
- 9 Characters > 45,848,500,718,449,031 (45 Quadrillion) Combinations
- 10 Characters > 3,255,243,551,009,881,201 (3 Quintillion) Combinations




**Comparison between the time required for generation the passwords; series 1 for numeric and series 2 for alphanumeric passwords.**

**Advantages of Biometric:**

As with all biometric systems, there are a number of advantages associated with using fingerprint scanning to confirm an individual's identity. Often, weighing the various benefits and costs associated with particular biometric methods greatly affects which systems are implemented by an organization and, in some cases, whether biometric systems are adopted at all. In the case of fingerprint scanning, the relative advantages are reasonably straightforward.

• Acceptance—As most people are familiar with the use of fingerprinting for identification purposes, it is generally accepted as a technology. Most people understand its applicability to access control.

• Accuracy—By and large, fingerprint technology is accurate. There is a small chance of rejection of a legitimate print, i.e., there is a chance of accepting a false print or a chance of rejecting a legitimate print. The chances of accepting a false print are very low.

• Ease of use—Very little time is required for enrolment with a fingerprint scanning system. Unlike other biometric devices, such as retina scanners, fingerprint scanners do not require concentrated effort on the part of the user. Accordingly, one could consider fingerprint scanning to be relatively nonintrusive.

• Installation—Changes in technology have made fingerprint scanners relatively easy to install and inexpensive. Most fingerprint scanners are now very small and portable. Plug-and-play technologies have made installation very easy. In many cases, the scanning device has been incorporated into keyboards, mouse buttons and even notebook computers.

• Training—Due to the intuitive nature of scanning fingerprints, such devices require no training to use and little training to support.

• Uniqueness—As noted previously, fingerprints are a unique identifier specific to the individual.

• Security—Fingerprints cannot be lost or stolen, and are difficult to reproduce. Furthermore, storing fingerprint templates as statistical algorithms rather than complete copies ensures that the ability to reproduce these unique identifiers is significantly reduced.12

**2.2 Fingerprint Reorganization**

Fingerprint recognition describes the process of obtaining a digital representation of a fingerprint and comparing it to a stored digital version of a fingerprint. Electronic fingerprint scanners capture digital "pictures" of fingerprints, either based on light reflections of the finger's ridges and valleys, ultrasonic's, or the electrical properties of the finger's ridges and valleys. These pictures are then processed into digital templates that contain the unique extracted features of a finger. These digital fingerprint templates can be stored in databases and used in place of traditional passwords for secure access. Instead of typing a password, users place a finger on an electronic scanner. The scanner, or reader, compares the subsist fingerprint to the fingerprint template stored in a database to resolve the identity and validity of the person requesting access.

Figure: Fingerprint Authentication

**Fingerprint Identification Algorithm:**

1) The enrollment process: This process consists of capturing a person's fingerprint using a fingerprint capturing device. During the enrollment process, the system saves the persons fingerprint into a database.

2) The authentication process: It is used to authenticate the claimed person. This process consists of comparing a captured fingerprint to an enrolled fingerprint in order to determine whether the two match. If the two fingerprints match, then it allow user to make transaction.

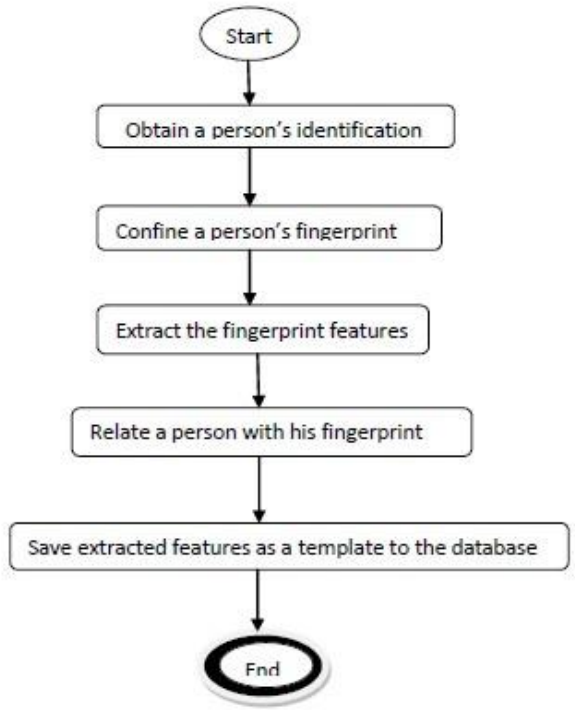



Figure 1: The Enrollment Process

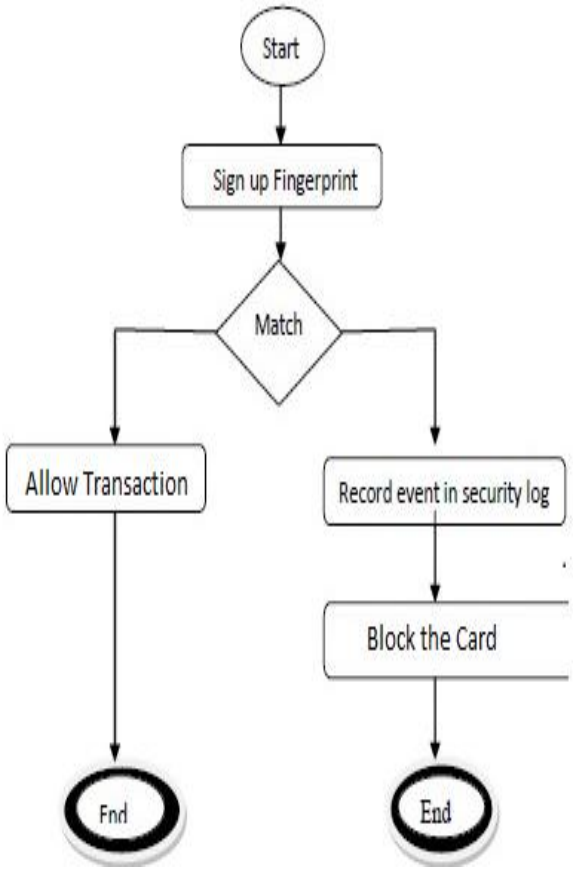



Figure 2: The Verification Process

## III. Conclusion

There are several attacks that try to negotiate a system using a variety of methods such as unauthorized access. These attacks could be reduced if an identification tool is used to complement already deployed intrusion detection system. The most reliable identification systems are based on fingerprints and alphanumeric. Therefore, several biometrics technologies start to accompany host-based Intrusion detection systems

**Acknowledgement**

We thank our colleagues from IMCOST who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper.

We thank Mr. Manish Deo sir for assistance us by providing proper IEEE formats and all faculties for guiding us.

**References**

[1] A. Ahmed and I. Traore. Anomaly intrusion detection based on biometrics. *In 6th IEEE*

[2]Wikipedia: The free Encyclopedia, Technical Weblink:

http://en.wikipedia.org/wiki/Multiple_encryption

[3] ATM security System using fingerprint biometric identifier:

[4] E. Lau, X. LI, C. Xiao, and X. Yu. Enhanced user authentication through keystroke biometrics. In Compute and Network Security, Massachusetts Institute of technology

[5] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer

[6] Ito, K., Nakajima, H., Kobayashi, K., Aoki, T., Higuchi, T.: A fingerprint matching algorithm using phase -only correlation. IEICE Trans. Fundamentals E87-A

[7] J. McHugh. Intrusion and intrusion detection. International Journal of Information Security, 1:14–135, 2001.

[8] ― An Overview of ATM Security Using Biometric Technology‖ By Jaspreet Kaur , Sheenam Malhotra International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 3, March 2014 , ISSN: 2277 128X.

Authors:

1. Sneha Dighe.

Student of University of Mumbai, Appearing for final examination of Masters of Computer Application Course

2. Puja Joshi.

Student of University of Mumbai, Appearing for final examination of Masters of Computer Application Course