International Research Journal of Engineering and Technology (IRJET) e-ISSN:2395-0056
Volume: 07 Issue: 04 | Apr -2020 www.irjet.net p-ISSN:2395-0072

A TWO FACTOR AUTHENTICATION SYSTEM FOR TOUCH SCREEN MOBILE DEVICES USING STATIC KEYSTROKE DYNAMICS AND PASSWORD

Ms. Ruchi Goel[1], Manu[2], Mahima Bhatt[3], Nikita Pal[4]

[1] Professor, Dept. of CSE, Krishna Engineering College, Mohan Nagar-201007, Ghaziabad, Uttar Pradesh, India [2, 3, 4] Student, Dept. of CSE, Krishna Engineering College, Mohan Nagar-201007, Ghaziabad, Uttar Pradesh, India

Abstract- *Keystroke Dynamics System is a two-factor authentication system that uses keystroke dynamics that is biometric, which can be used to add an extra layer of security to our existing systems using our typing rhythm. The application will register the user's pattern and use them to authenticate during login time. The purpose of this system is to deliver an authentication system that is simple and cheap which uses a biometric system to establish the identity of the user without needing to add any new hardware to the existing system. There will still be traditional systems in place like a username-password combination that will make up the first factor of the authentication, and then there will be the Keystroke Dynamics System that will act as the second factor of the two-factor system. Even one incorrectly entered factor will never allow user to access the system.*

Key words: Authentication, Two-factor authentication, Biometric authentication, Keystroke dynamics, Performance measures, features extraction.

1.INTRODUCTION

With the growing speed of technological advancement, Smartphones have become the essential components to access and store confidential information like banking transactions, etc. As we look for convenience, we also seek for secure authentication mechanisms in the digital space. So, for this Authentication works as a process of verifying the identity of a person or device. Authentication is one of the most commonly used procedures for controlling access to any system. An example of authentication is log in to a website by entering a username and password. Entering the right login data lets the website recognize your identity and that it is you accessing the website. While a username or password combination, Biometric, PIN, OTP are some common way to authenticate your identity, many other types of authentication mechanisms exist.

Rather than this, an additional authentication process is needed to enhance password security. Keystroke dynamics is one of the important behavioral measurements that use the typing rhythm of the user for authentication purposes. In keystroke dynamics no additional hardware is needed, in this, no extra effort is involved, and it provides continuous authentication which makes it more suitable for authentication purposes.

2. AUTHENTICATION

Authentication is a process of knowing a user's identity and it helps in determining whether someone is the one who he is claiming to be or not. An authentication mechanism is helpful in providing a basis for controlling access to various systems in order to ensure security to the system. It has four main types-

2.1 What the user "Knows"

- This type basically depends upon the knowledge basis means on something that is already known by the user such as password, PIN(personal information number), and any security question.
- The main advantage of this type of authentication is that in this there is no requirement for extra hardware, all we need to store a password in the database.
- Its main disadvantage is that a password can easily be stolen, forgotten, or guessed by another person.

2.2 What the user "Has"

- This type depends upon something owned by the user like smartphones, credit cards, smart cards, etc. This type is used in an Automated teller machine (ATM). The logic used here is if the user has a smart card then he/she must be the owner of the account.
- The main problem associated with this type is that if a card may be stolen, lost then another person may act as the owner of the account

2.3 What the user "Is"

- This type depends upon biometric features or characteristics of the human body such as fingerprint, iris, hand geometry, retina. In this human attributes can be scanned and digitally documented.
- Its main advantage is that biometric could neither be stolen nor lost.
- In this, extra hardware is used for scanning purpose which may act as a disadvantage. Besides, biometric authentication requires some specific conditions that are not available at all times. For example- for the fingerprint authentication finger that needs to be clean and not sweaty, iris authentication must be performed in a good light.

2.4 What the user "does"

- This type of authentication is basically related to the Behaviour of users like typing rhythm, a pattern of mouse movement, a pattern created by tapping on touch screen mobile phones, etc. Typing rhythm is the most efficient way of behavioral authentication and it is also known as keystroke dynamics. It is the cheapest way of authentication as it does not require any extra hardware just a keyboard or keypad.

3. TWO FACTOR AUTHENTICATION

Two-factor authentications basically consist of multifactor authentication. In this authentication is performed in more than one step. Nowadays password is not sufficient to authenticate users remotely especially when it is related to personal data or banking system. So now two-factor authentication has become the standard method that helps in providing an extra layer for verification, authentication, and security. In this process, the user is verified on an extra level and ensures or guarantee that only authorized users can gain access to any application.

In this user claimed identity is confirmed by using a combination of two factors:

1. Something user know
2. Something user have or something user is

For Example – Withdrawing of money from ATM is an important example of two-factor authentication. In this only correct combination of the bank card(which is already known by the user) and a PIN(which users have) allow transactions to be performed.

One most common example is of providing One Time Password(OTP) generated by the authenticator that only possess by the user.Nowadays may internet services such as Amazon, Google uses Time Based One Time Password which provides OTP for a limited time period only after extension of time period OTP becomes invalid.

4.BIOMETRIC AUTHENTICATION

Biometric authentication is a process, that provides security by measuring and matching biometric features of a user to recognize that the person trying to access a particular device is authorized to do or not.Biometric Authentication is also described as a security process that based on the unique biological characteristics or features of an individual to verify that he is who says he is.

Biometric features are generally the physical and biological characteristics of a person. These characteristics are unique to an individual person and are easy to compare with authorized features already saved in a database. This system compares a biometric data capture dynamically to stored data. If both samples of biometric data match, then authentication is confirmed and the user can access the system.There are four common types of biometric authentication,

4.1 **Eye Scanners:** Various types of eye scanners are already available, some of them are retina scanners and iris recognition, etc. These eye scanners are present as hand-free verification options, but they can still create inaccuracies if person or individual were eyeglasses or contact lenses. Photographs can be used as a trick eye scanner and by this invalid user can get access to a system, so this method becomes less practicable as scanners become more knowledgeable in their verification plan.

4.2 **Facial Recognition:** Facial recognition is a technology based on matching dozens of different features from an approved face to the face of a user trying to gain access to a system, after creating face prints. Nowadays facial recognition has been used in several smartphones and other popular devices, though it has some disadvantages like it can be inconsistent in comparing faces when viewed from different angles, or it can't distinguish between people who look approximately similar, such as close relative or twins.

4.3 **Fingerprint Scanners:** Fingerprint scanners are the latest or digital version of ancient ink and paper fingerprint. It completely based on recording the unique framework of turn and ridges that make up an individual's unique fingerprint. It is one of the most known, commonly used and accessible modes of biometric authentication. This is the most popular and utilized biometric technique used in office, banks, schools & colleges, etc for everyday consumers.

4.4 **Voice Identification:** Voice identification technologies measure the verbal or vocal characteristics of a person to distinguish and authentication. Like face scanners, they recognize and combine a number of data points like pitch, sound, wavelength, etc of voice and create a voiceprint profile to be matched or compare with the database. These technologies basically focus on measuring and examining a user or speaker's mouth and throat for the formation of different shapes and sound qualities.

5. KEYSTROKE DYNAMICS

It is a type of behavioral biometrics which helps in authenticating the user on the basis of typing rhythm. In these features like key hold time, latency, etc are extracted in order to find out or store the rhythm of a particular user. Its main advantages are-

- No extra hardware is needed.
- Cost-efficient.
- Typing is what user dose so no need for extra efforts.
- Continuous authentication can be done.

It involves two ways studies that are Static based and Dynamic Based. Static based means fixed data so the user has to enter the same text several times. Dynamic based also known as free text mode and in this data can be collected from any typed text, in this user may be required to type long text to collect features.

Basic features involved in keystroke dynamics are-

- **Hold(H):** Time interval between the key pressed and released.
- **Latency or Up Downtime(UD):** Time interval between releasing key and pressing the next key.
- **Down-Down (DD):** Time interval between two successive keys down the press.
- **Trigraph latency:** It is a latency between every three consecutive key down presses.
- **Up-Up(UU):** Time difference between key up of the first key and key up of the second key. It is equal to UD+H.
- **Down-Up:** Time interval between key down of first and key up of the second key
- **Releasing Time:** It is a time key is released.
- **Overall speed:** Variation of speed moving between specific keys.
- **Finger Choice:** which finger is used on the keyword.
- Capital letter and special character.
- Distance between letters.
- Consecutive Key Press Time.

6. PERFORMANCE MEASURES

The performance of such keystroke analysis is typically measured in terms of various error rates, namely False Accept Rate (FAR), False Reject Rate (FRR) and Equal Error Rate (EER).

6.1 False Reject Rate (FRR):

It measures the total percent of valid users who are refused as impostors. In statistics, such kind of errors is considered as a Type I error.

FRR = (Number of correct attempts rejected / Number of correct attempts)*100

6.2 False Accept Rate (FAR):

It measures the percent of impostor who are accepted as valid users and being able to successfully gain access to any secured system. In statistics, such kind of errors is considered a type II error. Both error rates should ideally be 0%.

FAR = (Number of incorrect attempts accepted / Number of incorrect attempts)*100

6.3 Equal Error Rate (EER):

It is considered as a rate as which both accept and reject errors are approximately equal. It is also conversant as the Cross-Over Error Rate (CER).

7. FEATURE EXTRACTION

Feature extraction is used as an important task in the retrieval of a multimedia task. In recent years feature extraction has been investigated extensively. Feature extraction is a process of extracting various features involved in a system, and then these features are used for comparison during the authentication process.

The extraction of features is one of the most important steps of behavior authentication. The error rates involved during this process directly depend on the selection of the right features. The extraction of characteristic features from the input data is the net result of a well pre-processed and represented collection of features in a pattern vector, However, extraction of more extra features increases the computational complexity of the problem.

8. CONCLUSION

In this paper, we have tried to present a comprehensive survey of work done on keystroke dynamics in the field of mobile phones in the past decade and what keystroke is & how it works. But there are some open challenges which are still to be addressed

Password authentication is the extremely used authentication mode for local, network, and internet access. However, password authentication suffers from many drawbacks. Various biometric systems are also present for authentication but they too have many disadvantages. This survey basically focused on various typing behavior strengthening techniques (also called keystroke dynamics) available nowadays. Keystroke dynamics is still in its early stages in the field of mobile devices and a lot of research needs to be done to make it an effective biometric.

9. FUTURE WORKS

The future research work should be focused towards developing a large dataset of keystroke available to the research community, investigating more problem of keystroke biometrics by free text, developing richer keystroke features, analyzing context-dependent sub word and across-word models, seamlessly integrating language model score, that is, the authorship, into the keystroke dynamic system, and minimizing the effect of different hardware and network delay for remote-access applications. Future work should involve more focus towards improving accuracy of currently present keystroke systems.

REFERENCES

[1] Fabian Monrose, Aviel D. Rubin, “Keystroke Dynamics as a Biometric for authentication”, [March 1999]

[2] Yu Zhong, Yunbin Deng, Anil K. Jain, “Keystroke Dynamics for User Authentication”, [March 2012]

[3] Yunbin Deng and Yu Zhong, “Keystroke Dynamics User Authentication Based on Gaussian Mixture Model and Deep Belief Nets”, [Volume 2013]

[4] Soumen Roy, Utpal Roy, D. D. Sinha, “Enhanced Knowledge-Based User Authentication Technique Via Keystroke Dynamics”, [September 2014]

[5] “Authentication Method through Keystroke Measurement of Mobile users in Cloud Environment”; [Int. J. Advance Soft Compu. Appl, Vol. 6, No. 3, November 2014]

[6] “Soft Biometrics for Keystroke dynamics: profiling individuals while typing password”; [IEEE-2014]

[7] Alen Peacock, Xian Ke, and Matthew Wilkerson, “Typing Patterns: A Key to User Identification”, (Massachusetts Institute of Technology); [October 2015]

[8] Md. Asraful Haque, Namra Zia Khan, Gulnar Khatoon, “Authentication through Keystrokes: What You Type and How You Type” , [IEEE 2015]

[9] Ramzi Saifan, Asma Salem, Dema Zaidan, Andraws Swidan, “A Survey of behavioral authentication using keystroke dynamics”, [Volume 1, January 2016].

[10] Soumen Roy, Utpal Roy, D. D. Sinha, “Performance Evaluation of Various Distance-based Data- Mining”, [January 2016 Vol 5 Issue 2].

[11] Baljit Singh Saini, Navdeep Kaur, Kamaljit Singh Bhatia, “Keystroke Dynamics for Mobile Phones A Survey”, [Vol 9(6), February 2016].

[12] Joyce R., Gupta G., “Identity authorization based on keystroke latencies”, [1990].

[13] L. C. F. Ara´ujo, L. H. R. Sucupira, M. G. Liz´arraga, L. L. Ling, and J. B. T. Yabu-uti, “User authentication By various typing biometrics features", [volume 3071, 2004].

[14] F. Bergadano, D. Gunetti, and C. Picardi, “User Authentication through Keystroke Dynamics", ACM Trans. Information and System Security, [2002].