ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 11, November 2014**

# Password less Authentication Using Keystroke Dynamics: A Survey

[1]Jhalak Modi, [2]Hardik G. Upadhyay, [3]Mitesh Thakor

[1]ME Student, Department of Computer Engineering, Merchant Engineering College, Basna, India.

[3]Assistant Professor, Department of Computer Engineering, Merchant Engineering College, Basna, India.

[2]Assistant Professor, Department of Computer Engineering, GPERI, Mehsana, India.

**ABSTRACT:** Biometrics technologies are gaining high popularity today world they provide effectively authentication and verification. Keystroke dynamics is most secure and confidential in today's scenario. Computer are use in each and every field for store user credential and personal information so its need to make it secure. There are many techniques use in biometrics authentication like Fingerprint Recognition, Face Recognition, Eyes-Iris Recognition, Signature Recognition, and Voice-Speaker Identification. All above techniques are not so much secure and very costly for implementation. Keystroke dynamics allows users to be recognized based on their way of typing on a keyboard. In keystroke dynamics password less authentication mechanism, it would be recognized without typing any specific password to identify legitimate user. This paper tries to review the different keystroke method and also provide keystroke mechanism with existing system helps to improving security.

**KEYWORDS:** Keystroke Dynamics, Biometrics, user authentication, identification and security.

## I. INTRODUCTION

Technological developments during the last few decades have transformed our world into a worldwide nation, a lay where information no longer has been any kind of obstruction. Biometric technologies are defined as automated method to easily verifying and recognizing technique to identity of a living person which are based on physiological or behavioural characteristics. Biometrics techniques are mainly used for user authentication. The confidential information can be secured from unauthorized users by providing authentication. User authentication is defined as the process of verifying the identity claimed by an individual. User authentication are basically classified into three categorized such as Knowledge based, Object or token based and Biometric based authentication. The knowledge-based authentication is based on something one knows and is characterized by secrecy. The examples of knowledge-based authenticators are commonly known passwords and PIN codes. The object-based authentication relies on something one has and is characterized by possession. Biometrics can be classified into two categories: Physiological biometrics and Behavioural biometrics.

Physiological Biometrics characteristics refer to what the person is, or, in other words, they measure physical parameters of a certain part of the body. Physiological characteristics is an identifies the user which are based on fingerprints, eye retina, iris scanning, voice, hand-geometry, face, palm-print etc., and Behavioural characteristics are related to what a person does, or how the person uses the body. Behavioral is based on gait, signature, keystroke dynamics and voice. Keystroke dynamics is the process of authenticating individuals based on their typing style. It is a process of analyzing the way a user types at a terminal by monitoring the keyboard in order to identify the users based on habitual typing rhythm patterns. Moreover, unlike other biometric systems, which may be expensive to implement, keystroke dynamics is almost free as the only hardware required is the keyboard.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

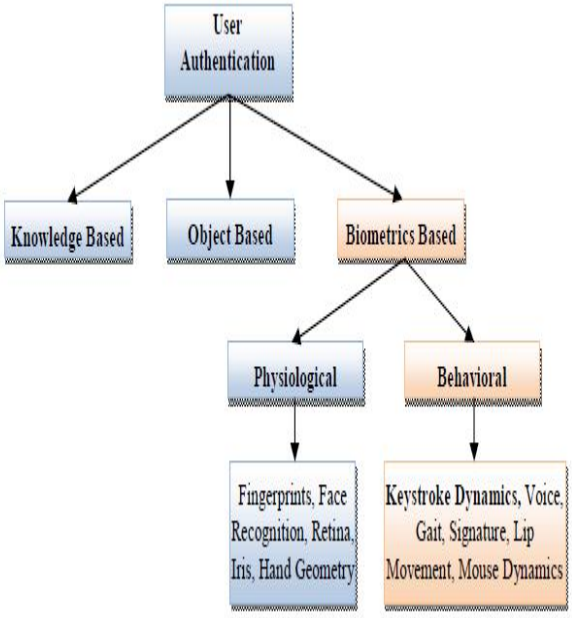


Fig. 1 User Authentication

Keystroke recognition measures the feature of an individual's typing pattern. This technique is including the time spacing of all words. This technique mostly used for identifying person who may generate unworthy email or conduct tricky activity on the Internet. Keystroke or typing recognition technique software is installed onto the computer. When a person uses it their typing patterns on his/her computer they will be easily logging or work on them. It incidence depends on an individual using the same keyboard as different types may create a variance in the keystroke pattern can be defer.

There are mainly two phases that a user has to go through for authorized by keystroke dynamic which are the enrolment phase and log-in phase. The first phase is done with collecting data from user which have credential information like username and password in addition to capturing the user's typing pattern 7061ehaviour. System stores the keystroke times. In this phase user data stored in database in correspondence to the user's other detail. Another second phase takes place whenever user needs to use of the system.

There are four key press latencies:

1. P-P (Press-Press) – the time interval between successive key presses the speed of the typing will be defines.
2. P-R (Press-Release) – the time interval between the press and release of the key. How much attempt the user should make to type the key.
3. R-P (Release –Press) – the interval between the releasing one key and pressing another.
4. R-R (Release-Release) – the time interval of releasing two successive keys When user wants to access to a system, he selects an account and types target strings login, password, first name, last name.

Keystroke data is captured and the sample is created. The sample will contain the features (duration of the key and keystroke latency) of that are calculated using the data.

The paper is structured as follows: the next section gives the identification and verification in keystroke dynamics. Section III explains the methods and metrics of keystroke dynamics. Section IV discusses the various performance measures. Existing approaches are discussed in Section V. The Sixth and Seventh Sections discuss about the security and challenges of keystroke dynamics respectively and final section concludes the topic.

## II. KEYSTROKE DYNAMICS AS BIOMETRICS

Keystroke dynamics is a one of the most important technique of behavioral biometric. Keystroke dynamics is the process of a user types at a terminal by monitoring the keyboard to identify the user based on habitual typing rhythm

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

patterns. Keystroke dynamics is almost free and it does not require any sophisticated hardware as the only hardware required is the keyboard.

**1. Merits of using Keystroke Dynamics**

- It does not require any special equipment.
- It is user-friendly and noninvasive.
- Flexible enrollment is possible.
- The typing rhythm of the person cannot be lost or forgotten.
- If the template is stolen or guessed, the new one can be easily generated. So it is the only resettable biometric.
- It can be used for remote applications over the Internet.
- Keystroke dynamics can be combined with other authentication technologies

**2. Keystroke Dynamics Approaches**

**a) Static Approach**

In Static approach, the system checks the user only at the authentication time. It provides additional security than the username/password. It also provides more robust user verification than simple passwords. In this approach, the analysis is performed on typing samples produced using the same predetermined text for all the individuals under observation. The static analysis is done at login time in conjunction with other authentication methods such as passwords.

**b) Continuous approach**

System checks the user continuously throughout the session and the user's typing behavior is every time monitored person typing time using by the keyboard. It means that even after a successful login, the user typing patterns are constantly analyzed.

**c) Statistical Algorithm**

Statistical Method consists of computing the mean and standard deviation technique in keystroke dynamic. In statistical method, there are many algorithms and distance measure used for keystroke dynamics which are absolute distance, weighted absolute distance, Probability measure and Euclidian distance. Major of work in statistical method should be done by developing authentication and identification. Main disadvantage of using statistical algorithm, it does not provide good result. It is also lack of training stage which are used for identify the pattern.

**d) Neural Network**

Neural network is also known as the artificial network. Neural network is more adaptive non-linear statistical data modeling tools which have been inspired by biological interconnection of neurons. There are two ways in which the weights can be assigned supervised learning and unsupervised learning. One of the most popular methods in supervised learning is called the backpropagation. One of the popular methods in unsupervised learning is the Hopfield neural network. Other algorithms such as perceptron, Sum of Products (SOP), Adaline and weightless neural networks have been used to classify users based on their keystroke dynamics.

**e) Pattern Recognition and learning based algorithms**

Pattern recognition is nothing but the different pattern or objects which are classifying into different categories based on different algorithm. It contains simple machine learning algorithms such as the nearest neighbor algorithms and clustering to much more complex algorithms such as data mining, Bayes classifier, Fishers linear discriminant (FLD), support vector machine (SVM) and graph theory. Support vector Machine (SVM) is supervised learning algorithm which gives better result for both identification and authentication.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 11, November 2014**

## III. METHODS FOR KEYSTROKE DYNAMICS

**a) Static**

Static keystroke is depend on authenticate typing pattern which are based on a known keyword, phrases or some predetermined text. It compares the original captured typing pattern to recorded typing pattern which are stored during enrollment.

**b) Periodic dynamics**

Using periodic dynamics, user authenticate to his/her typing pattern with comparing a logged session. Data is already captured in logged sessions which are compared to achieve typing pattern to determine the deviation.

**c) Digraph latency**

Digraph latency is the metric that is most commonly used and it typically measures the delay between the key-up and the subsequent key-down events, which are produced during normal typing.

**d) Trigraph latency**

Trigraph latency extends the digraph latency metric to consider the timing for three successive keystrokes.

**e) Continuous dynamic**

Continuous keystroke analysis is capturing data to the entire duration of the logged session. And it is also continuously stored the data into database. The continuous nature of the user monitoring offers significantly more data upon which the authentication judgment is based. Furthermore, an impostor may be detected earlier in the session than under a periodically monitored implementation.

**f) Application specific**

Application-specific keystroke analysis further extends the continuous or periodic monitoring. It may be possible to develop separate keystroke patterns for different applications.

## IV. PERFORMANCE MEASURES

Performance analysis in keystroke dynamic is measured in term of various types which are False Accept Rate (FAR) and False Reject Rate (FRR). False Accept Rate is the probability of an impostor posing as a valid user being able to successfully gain access to a secured system. FAR Ratio is also known as Type II error. FRR measures the percent of valid users which are rejected on authenticate to impostor in keystroke dynamics. It is also known as type I error. If FRR ratio should be minimized than it does not possible any unauthorized user to login. In keystroke dynamic, both FRR and FAR ration always measured in equal rate. So it is known as Equal Error Rate (EER) and also known as Cross over Error Rate (CER).

## V. LITERATURE SURVEY

An author at [4] provides supporting evidence to the role software based security systems can bring to the issue of enhanced computer security. The system, based on keystroke dynamics, is not overly burdensome to the user, very cost-effective, and very efficient in terms of the overhead placed on an internet based server. They achieve a very low FAR/FRR (each less than 5%), compatible with those produced by very expensive hardware based systems. In addition, authors have begun investigating additional strategies that can be combined with keystroke hardening, such as keyboard partitioning. Partitioning provides an added layer of security, but requires users to limit their selection of login IDs and passwords. But if security is vitally important to the organization – such as mission critical Ecommerce sites, then this is a small price to pay to remain in business. A single successful attack can literally put a site into financial bankruptcy.

Authors at [2] address the practical importance of using keystroke dynamics as a biometric for authenticating access to workstations. Keystroke dynamics is the process of analyzing the way users type by monitoring keyboard inputs and authenticating them based on habitual patterns in their typing rhythm. They also review the current state of keystroke dynamics and present classification techniques based on template matching and Bayesian likelihood models.
Authors also argue that although the use of a behavioral trait (rather than a physiological characteristic) as a sign of identity has inherent limitations, when implemented in conjunction with traditional schemes, keystroke dynamics allows for the design of more robust authentication systems than traditional password based alternatives alone.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 11, November 2014**

Authors at [5] propose model which work with keystroke dynamics and represent it as a reliable security instrument for authentication. They mentioned that dwell times (how long a key is held pressed) are more discriminatory and therefore more powerful than flight times (time between consecutive press times), confirming a similar finding by Obaidat and Sadoun.

The test based on dwell times tells us that:
if reject a person if the *T*2-test fails once, then it will reject the true owner 5% of the time and recognize a hacker 85% of the time.
If reject a person if the *T*2-test fails twice, then it will reject the true owner 1% of the time and recognize a hacker 84% of the time. They also developed the test statistic under the assumption that the characteristics are independent. This is probably unrealistic and more power can be obtained by allowing for some dependence, perhaps using Markov models.

| Individual Criteria → Providers ↓ | Authentication provided | Classification Method? | Outlier Handling? | Keystroke Hardening | Scalable? | FAR , FRR Ration | Limit ID and Password text | Experiment No. of Users? |
|---|---|---|---|---|---|---|---|---|
| [1] | Y | X | X | X | X | ↑ | X | 9 |
| [2] | Y | Y | X | X | Y | ↓ | Y | 63 |
| [3] | Y | X | Y | X | X | ↑ | Y | 51 |
| [4] | Y | X | X | Y | X | ↑ | Y | 8 |
| [5] | Y | Y | Y | X | X | ↓ | Y | 42 |

Table 2: Detailed Comparative Study

The table2 above show a detailed comparison of available approaches from various authors based on parameter they used in their research. The problem with keystroke dynamics is improper dataset. No one has used the common dataset. The need of classification method can be helpful to the keystroke to achieve the less False Accept Rate (FAR) and False Reject Ratio (FRR).

## VI. CONCLUSION

The different methods used and authenticated by the user are discussed. Amongst them Statistical and Neural network have been widely used methods. The advantages, disadvantages and future work also reviewed. Future works includes keystroke hardening, scalability Etc. The web based enablement of keystroke and adding more feasibility can be part of future works. The size of keystroke data and the reduction in the number of attempts at the time of registration should be part of future works. Some mentioned outline handler as a filter which remove noise which may come in data sets. FAR, FRR and EER should be low down to zero to achieve higher security.

## REFERENCES

**[1]** Mariusz Rybnik, Marek Tabedzki, Marcin Adamski, Khalid Saeed " An Exploration of Keystroke Dynamics Authentication using Non-fixed Text of Various Length" International Conference on Biometrics and, IEEE, 2013.
**[2]** Fabian Monrose A and Aviel D. Rubin B, title "Keystroke dynamics as a biometric for authentication" Future Generation Computer Systems Elsevier Science. 2002
**[3]**Yu Zhong Yunbin Deng and Anil K. Jain, "Keystroke Dynamics for User authentication" Approved for Public Release; Distribution Unlimited. Computer Vision and Pattern Recognition - CVPR , 2012
**[4]**Kenneth Revett, Sérgio Tenreiro de Magalhães and Henrique M. D. Santos, "Enhancing Login Security Through the use of Keystroke Input Dynamics" *Advances in Biometrics: International Conference*, ICB 2006, Hong Kong.
**[5]** Douhou, S. and Magnus, J. R. (2009), The reliability of user authentication through keystroke dynamics. Statistica Neerlandica, 63: 432–449. doi: 10.1111/j.1467-9574.2009.00434.x.