International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-4, Issue-3, March 2016

User Verification Using Typing Patterns for Secure Login

Suvarna S. Jadhav, Jayshree G. Mali, Sonali R. Patil, Amoli V. Pawar

***Abstract*— Day by day security is big concerns. In day to day life there are many applications or systems where we require login. Normally we type Login ID and Password and if it is correct we easily get access to the system. But what if unauthorized person or hacker gets our password? So this system is really helpful from security point of view. In this system the user is authenticated using ID and Password but along with this user are identified using typing patterns. Because of this one extra level of security added to the existing system without any additional cost. Within the last decade several studies proposed the use of keystroke dynamics as a behavioral biometric tool to verify users. In this system collection of tying patterns are obtained using consecutive keystrokes. The proposed method considers clustering di-graphs based on their temporal features.**

***Index Terms*— keystrokes dynamics, clustering diagraph, temporal features.**

I. INTRODUCTION

All previous login systems uses User D and Password for logged in to the system. But is no secure way because sometimes user ID and password is stolen and there is risk of unauthorized user get access to the system. This may lead to loss of important data and sometimes lead to big financial loss.

There are various previous systems are invented and are mainly classified into two groups and are *Physiological* and *behavioral*. Physiological biometrics includes to physical measurements of the human body, such as fingerprint, face, hand geometry and iris. Physiological biometrics also includes of the scanning, of user is more suitable for a single authentication, rather than for continuous verification. However, most of the physiological biometrics e.g. iris scan, Fingerprints are not include continuous verification, because they are intrusive, costly, not available and inappropriate for most of applications such as web applications. In the other side behavioral biometrics close to a specific behavior of a human along time while performing some task, such as signature writing, speaking, typing and others.

Along with this, techniques like graphical passwords, captcha, security questions are most popular in web based applications. In other hand use of *Physiological* system are costly as it requires extra cost for hardware for measuring physical parameters so they are not a good solution in many cases.

So the proposed system is very useful, for collecting and representing the typing patterns and joining similar pairs of consecutive keystrokes. The proposed method considers clustering di-graphs based on their temporal features. If the typing patterns of authorized user matched with stored patterns then and then only he/she gets access to the system otherwise not. So if anyone other than valid user gets user ID and password then he is not able to get access to the system .The proposed method detection performance is better than that of existing methods. In addition of this when user logged into the system user gets SMS on their mobile for telling user that he/she logged in .So in the case of unauthorized user got user ID and Password also his typing patterns matched with valid user, the authorized/valid user gets SMS that some illegal person access his system and he is able to block the session remotely only by sending LOGOUT to reply for Login SMS.

Suvarna S. Jadhav, Jayshree G. Mali, Sonali R. Patil,Amoli V. Pawar, Department of Computer Engineering, NDMVPS's K.B.T.College of Engineering. Nashik.Savitribai Phule Pune University.

II. LITETATURE REVIEW

Existing approaches:

1) system:

In this system two temporal features, the interval time and the dwell time of di-graphs, for a purpose to build a user profile. These profiles were used to identify a new session depend on one of three proposed classifiers. Euclidean distance classifier, "non-weighted probability classifier" and "weighted probability classifier ".The performances of the three classifiers were very weak in the task of free text verification. The third classifier (weighted probability) was the superior classifier, but its accuracy was only 23%.

2) Typing rhythm system:

This system was originally designed to compress sequences via variable rate coding for a purpose to verify users based on their typing rhythm. Their method built a weighted tree (Mu) from the typing of the user u, based on Lampel-Ziv algorithm. Then, the algorithm determines the probability estimate for traversing from a parent node to one of its children. In the authentication process, the user u is authenticated as the user who typed the session if the probability of the session, given her weighted tree, is higher than a predefined threshold. They also introduced two improvements to the standard LZ algorithm: "input shifting "and "back shift parsing". Disadvantage of this system is amount of data is insufficient and their method should be validated on a much larger data collection.

3) Typing patterns using seven features:

To represent the user typing behavior by only seven features. Four of the seven features were proportion features and three were average features. The proportion features include the "Slur rate", "Press before Release", "Paired Perfect Order" and the "Backspace rate". The three average features are the "Average Tap Time", the "Slur length" and the " Words per Minute. With these seven features to verify users using one class classifier, based on Bayes rule.

III. PROPOSED METHOD

In proposed system, the combinations of Di-graph system and typing patterns are used to verify the user. Fig (a) shows architecture diagram for system.

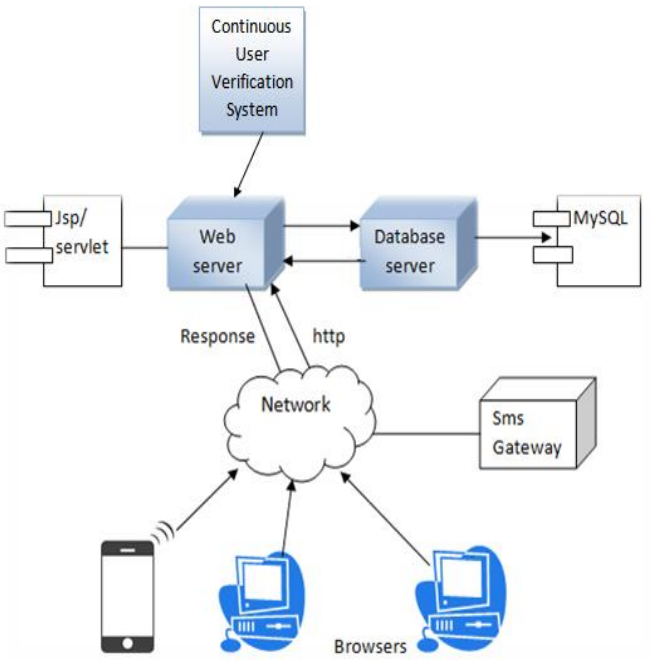

Fig (a).Architecture Diagram

A. Clustering "Similar" Di-graphs

This method is grouped into two parts: Training and Verification phases. Training phase includes build a verification model, which includes of a multi-class classifier and a mapping function, for the user based on all users' sessions. Therefore, a vocabulary that consists of di-graphs is created by extracting the user s unique di-graphs from her training sessions. Then evaluate the mean of the temporal feature for each n-graph in the dictionary based on all its instances in the user training sessions. After that, apply a clustering technique that clusters the means of the temporal features into k clusters. Then call di-graphs that their mean temporal features were clustered to the same cluster, similar di-graphs. The result of the clustering is a function from an n-graph in the main user vocabulary to a cluster. Then transform all the users' sessions to features vectors by first extracting for each user the means of his/her temporal features and then map them to a cluster belonging to the mapping function. Finally train a multi-class classifier. In the authentication phase, given a session to verify, we transform it to a features vector based on the mapping function which was created during the training phase and verify it based on the classifier, given the authentication parameter. As the temporal features are different and have the ability to differentiate among users. Thus for each user, the di-graphs are clustered in another way, which gives to a different classifier. The purpose behind this technique is that similar di-graphs can be considered as the similar feature; hence they have the similar characteristics.

B. Clustering Methodology

For purpose to cluster the di-graphs and to determine which di-graphs are same, first sort the di-graphs based on their temporal features. Then consider the di-graphs whose times difference are small as similar di-graphs and group together k same di-graphs into one grouped cluster. The cluster temporal feature will be the average of the temporal features of all the grouped di-graphs that it contains. Note that when k=1 each n-graph has its own exclusive place in the features vector and no clustering will be performed.

C. User Verification by Classification

To verify a user, a model based on her sessions which is later used to verify each session s features vector.

D.SMS module

After all these next stage is SMS module. When user login to the system, user gets SMS for this. In worst case if unauthorized user log in to the system valid user gets SMS that user is login to the system. So that he reply that SMS just by sending "LOGOUT" message .When user send logout the system will blocks remotely. Fig (b) shows state transition of the system. And Fig (c) shows data flow diagram of the system.

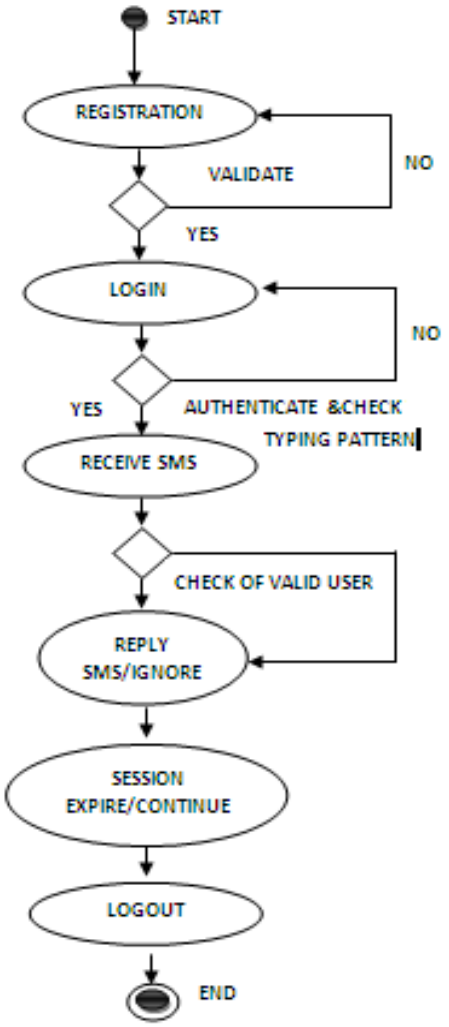

Fig (b) State transition of the system

IV. CONCLUSION

In a proposed method, we saw the concept of Keystroke dynamics and how it is used to calculate typing patterns of user. Here we used the combinational method like Clustering Di-graph system and typing patterns. As there is increase the need of verifying user the proposed system adds one extra level of security to existing system without any additional cost. The proposed system is useful in all types of login systems including applications.

V. FUTURE SCOPE

The proposed systems are worked on di- graph and their corresponding interval times but we can apply the similar technique to any other n-graph type like tri-graphs, fourth-graph and so on and on any other temporal feature.

REFERENCES

[1] Tomer Shimshon, Robert Moskovitch, Lior Rokach, Yuval Elovici. "Clustering Di-Graphs for Continuously Verifying Users according to their Typing Patterns".978-1-4244-8682-3/10/$26.00 ©2014 IEEE.
[2] R. V. Yampolskiy, V. Govindaraju, "Behavioral Biometrics: a Survey and Classification, Int. J. Biometrics, Vol. 1, No. 1, 2008".
[3] E. Yu, S. Cho. "Keystroke dynamics identity verification - its problems and practical solutions". Computers & Security (2004) 23, 428-440.
[4] F. Monrose and A. Rubin. "Authentication via keystroke dynamics". In Proc. of the 4th ACM Conf. on Computer and Communications Security. ACM Press, New York, 48 1997.
[5] K. Fukunaga, "Introduction to Statistical Pattern Recognition". San Diego, CA: Academic, 1990
[6] M. Nisenson, I. Yariv, R. El-Yaniv, and R. Meir. "Towards behaviometric security systems:Learning to identify a typist". In Principles and Practice of Knowledge Discovery in Databases.LNAI 2838, pp. 3634, Berlin, 2003. Springer-Verlag.
[7] J. Ziv and A. Lempel. "Compression of individual sequences via variable rate coding". IEEE Transactions on Information Theory, 24:530 536, 1978.
[8] K. Hempstalk. "Continuous Typist Verification using Machine Learning", PhD thesis, University of Waikato, 2009