

Keystroke Dynamics Authentication with Project Management System

Abhijeet Patai¹ Kirti Chandratre² Gaurav Kamlaskar³ Vikas Thorat⁴

^{1,2,3,4}Department of Computer Engineering

^{1,2,3,4}R. H. Sapat College of Engineering, Management Studies & Research, Nashik, Maharashtra, India

Abstract— Generally user authentication is done using username and password that is called as login process. This login process is not more secure because, however a login session is still unprotected to impersonator when the user leaves his computer without logging off. Keystroke dynamics methods can be made useful to verify a user by extracting some typing features then, after the authentication process has successfully ended. From the last decade several studies proposed the use of keystroke dynamics as a behavioral biometric tool to verify users. We propose a new method, for representing the keystroke patterns by joining similar pairs of consecutive keystrokes. The above proposed method is used to consider clustering the di-graphs which are based on their temporal features. In this project, authentication system is provide to project management system that make more Secure management system without acknowledging unauthorized user. The Project Management System addresses the management of software projects. It provides the framework for organizing and managing resources in such a way that these resources deliver all the work required to complete a software project within defined scope, time and cost constraints. The system applies only to the management of software projects and is a tool that facilitates decision making.

Key words: Keystroke Dynamics, Temporal Features, Clustering Digraph, Project Management System

I. INTRODUCTION

Currently most of the system use basic security technique or many hardware or network devices to secure his personal computer and industrial computer. Basically now use technology for user authentication is username password and extends one step toward use biometric hardware system. But such technology is not user friendly and flexible in some cases. This biometric system make work more complicated, lengthily and more costly. There also exist another user behaviour authentication system this system uses image processing technology, but there also create some limitation because of camera.

In this paper we introduce Keystroke Dynamics Authentication with Project Management System it uses keystroke dynamics technology for user authentication without using any camera and biometric hardware. This system uses simple computer keyboard, therefore it is easy to maintain number of systems or personal computer security. Keystroke Dynamics Authentication system provides security to project management system for securing the project information and data or file which are share between PMS employees. We are providing security in three steps first step is examine user typing behavior, second step is one time password (OTP) it is second verification step and the third step is image verification step in this step select security point on image. Therefore strength of security will be increased.

This paper will focus on past research done on the field of keyboard dynamics authentication. Then, the

reasoning behind the final method and a de-tailed explanation of the final method are stated. This is followed by test results, how efficiently the algorithm works and in periodic time for better results as well as how we used to test it and possible future improvements.

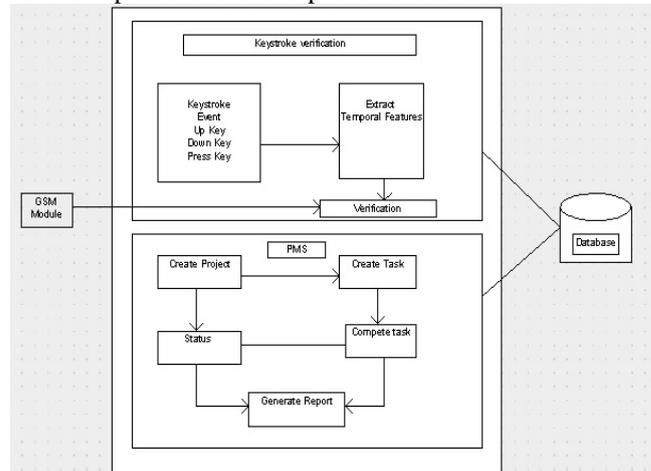


Fig. 1: Architecture of Keystroke Dynamics Authentication with Project Management System”

II. MOTIVATION

Nowadays web security is most important for many organizations, because of hacking. Most of the hacking activity is performed for extracting some valuable information without permission or in unauthorized way.

Traditionally we secure our valuable information by using username and password technique, but it is not sufficient for provide security to distributed network environment. Therefore we introduced keystroke Dynamics Authentication System, this system use machine learning approach for network security. This system learns the user typing behavior to secure user network environment. Additionally it also provides second and third step verification for improving the security. In this paper proposed system is used to provide security for project management system which is handles huge size industrial project. The PMS system perform main role in managing the project efficiently and reliably without requirement of any message passing system or communication system.

III. LITERATURE SURVEY

A. Previous Research on Keystroke Dynamics Authentication:

The effective studies done on this topic have some resemblance. The consensus on feature selection is that key-down to key-down produces the best results. Key-down to key-down is the time that revealed from the user fully depressing a key on the keyboard to the time the user fully depresses the next key on the keyboard. For each key press combination, that time is calculated and used as the prevalent feature[1].

Other researchers are also uses key-press durations as a feature. Key-press duration is the time the key is fully depressed until the key is released. This feature, while useful, does not perform as well as a lone feature, in comparison to key-down to key-down time does. However, if these features are used in combination, the results were improved.

Tyler Highlander, Dale Bassett, Derek Boone proposed "Utilization of Keyboard Dynamics for Unique Identification of Human Users [2]" In this paper they intricate many computer security schemes have been developed over this time period; however, none of these are designed yet. A username and password combination is one of the most popular approaches for securing a computer system, but this system is unprotected because passwords can be stolen or cracked. However, research suggests that it is possible to identify a user based on their typing style by using pattern recognition, neural networks, and other techniques. This paper mainly focuses on using the keyboard dynamics method of the user's password to add an extra layer of security to the log-in process.

Tomer Shimshon, Robert Moskovitch, Lior Rokach, Yaval Elovici proposed "Clustering Di-Graphs for Continuously Verifying Users according to their Typing Patterns [1]" In that they have explain a new method, for compactly representing the keystroke patterns by joining similar pairs of consecutive keystrokes. The proposed method considers clustering di-graphs based on their temporal features. The proposed method was performed on 10 genuine users and 15 impostors. The inspiring results suggest that the proposed method detection performance is better than that of existing methods. Specifically we reach a False Acceptance Rate (FAR) of 0.41% and a False Rejection Rate (FRR) of 0.63%.

E. Yu, S. Cho proposed "Keystroke dynamics identity verification - its problems and practical solutions [3]". In this paper they define Computers & Security; Password is the most widely used identity verification method in computer security system. However, because of its simplicity, it is unguarded to imposter attacks. Use of keystroke dynamics can result in a more secure verification system. Recently, Cho et al. (J Organ Comput Electron Commerce 10 (2000) 295) proposed auto associative neural network approach, which used only the user's typing patterns, yet reporting a low error rate: 1.0% false rejection rate (FRR) and 0% false acceptance rate (FAR). However, the previous research had some limitations: (1) it took too long to train the model; (2) data were preprocessed by a human; and (3) a large data set was required. In this article, we propose the alternative solutions for these limitations with an SVM novelty detector, GA-SVM wrapper feature subset selection, and an ensemble creation based on feature selection, respectively. Experimental results show that the proposed methods are encouraging, and that the keystroke dynamics is able to be done or possible to implement and it is a practical way to add more security for identity verification.

Güven, A. and I. Sogukpinar, proposed "Understanding users keystroke patterns for computer access security [4]" In this paper they have proposed Computers & Secure User authentication is a major problem in gaining access rights for computer resources. A recent

approach to improve the computer access rights is the use of biometric properties as the keystroke rhythms of users. Therefore user authentication for computers can be more secure using keystroke rhythms as biometric authentication. Methods like minimum distance, statistical, vector based, neural network type and data mining techniques have been applied for examining the keystroke patterns. In this paper, a vector based algorithm for a recent approach has been applied in the identification of keystroke patterns. Keystroke Identification system that is a neuron physical characteristic is studied to realize biometric authentication.

D. Gunetti and C. Picardi, proposed "Keystroke analysis of free text, ACM Transactions on Information and System Security [5]" In this paper they elaborate Keystroke dynamics can be useful to discover personal identity even *after* an authentication phase has been passed, provided that we are able to deal with the typing rhythms of free text, chosen and entered by users without any specific constraint. In this paper we present a method to compare typing samples of free text that can be used to verify personal identity. We have tested our technique with a wide set of experiments on 205 individuals, obtaining a False Alarm Rate of less than 5% and an Impostor Pass Rate of less than 0.005%. Different trade-offs are, however, possible. Our approach can rely on what is typed by people because of their normal job, and a few lines of text, even collected in different working sessions, are sufficient to reach a high level of accuracy, which improves relatively to the amount of available information. As an inference, we argue that our method can be useful in computer security as a complementary or alternative way to user authentication and as an relieve for intrusion detection.

D. Bartmann, I. Bakdi and M. Achatz proposed "Design of an Authentication system based on Keystroke Dynamics Using a Predefined Input Text. [6]" In this paper they elaborate the design of an authentication system based on keystroke dynamics is made difficult by the fact that the typing behavior of a person is laid to strong fluctuations and variations. An unsymmetrical method able to handle this difficulty by using a long text on enrolment and a short one at login is analyzed in this article. The results of an empirical study based on an extensive field test are presented. The study shows that the advantages of the analyzed method remain even if a predefined input text is used. The results also show that the method's quality is highly depends on the amount of text typed on enrolment as well as on login, which makes the system scalable to different security levels. They also confirm the importance of using stable characteristics that are due, for example, to the user's right- or left-handedness. The method's learning velocity is shown to be high, which enables enrolment to be kept short. Moreover, the study display that allowing multiple login attempts which significantly improves the recognition performance without sacrificing security.

F. Monroe and A. Rubin proposed "Authentication via keystroke dynamics. [7]" In this paper they elaborate more than ever before the Internet is changing computing as we know it. Global access to information and resources is becoming an integral part of nearly every aspect of our lives. Unfortunately, with this global network access increased chances of malicious attack and intrusion. In an effort to deal with the new threats disclosed by the networking

revolution of the past few years reliable, rapid, and unintrusive means for automatically recognizing the identity of individuals are now being sought. In this paper we examine an emerging non-static biometric technique that aims to identify users based on analyzing usual rhythm patterns in the way they type.

L. Breiman, "Random Forests" proposed "Machine Learning [8]" In this paper they elaborate More than ever before the Internet is changing computing as we know it. Global access to information and resources is becoming an integral part of nearly every aspect of our lives. Unfortunately, with this global network access come increased chances of malicious attack and intrusion. In an effort to deal with the new threats revealed by the networking revolution of the past few years reliable, rapid, and un-intrusive means for automatically recognizing the identity of individuals are now being sought. In this paper we examine an emerging non-static biometric technique that aims to identify users based on analyzing regular rhythm patterns in the way they type.

B. Existing Project Management System:

In most existing Project management system required message passing or communication systems like email system to maintain track of communication between multiple users. And also they required manual updating in task completion and ticket generation or other activity which are performed by user itself. It also not is providing any major security to PMS to secure projects important file which are share between different users. There for we proposed Keystroke Dynamics Authentication with Project Management system.

IV. PROPOSED METHOD

As we see previous research on keystroke dynamics authentication we proposed system is Keystroke Dynamics Authentication with project Management System. The purpose of this system is to secure or protect data from unauthorized access. Keystroke Dynamics Authentication with PMS system (KDAPMS System) work in three sections in that first section has two phases first is training phase and second is verification phase.

In first training phase of KDAPMS system when user perform typing activity on any simple keyboard that time generate three atomic event key up event, key down event, and key press event. Using this atomic event KDAPMS system extract user-temporal future like flight time, interval time, latency time among this value we consider one value which is identity of particular user which stored. After in verification phase at user login time system again generate keystroke identity of that user and check in training set for authentication if it matches with its particular identity then user directly switch to tired section otherwise switch to second section, after three attempt by user for identity.

V. CONCLUSION

The proposed web application provides security in term of unique identification for particular users through its typing pattern and also provide project management system. Hence, we conclude that Keystroke Dynamics Authentication with Project Management System is better than all traditional

existing keystroke dynamics system and project management system.

ACKNOWLEDGMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without mentioning the people who made it possible. We are grateful to a number of individuals whose professional guidance along with encouragement have made it very pleasant endeavor to complete this survey.

It gives us great pleasure in presenting the preliminary project report on 'Keystroke Dynamics Authentication with Project Management System.' We would like to take this opportunity to thank my internal guide Prof. P. P. Kanhegaonkar for giving us all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful.

We are also grateful to Prof. N. V. Alone, Head of Computer Engineering Department, Gokhale Education Society's R. H. Sapat College of Engineering, Management Studies Research, Nashik-5 for his indispensable support, suggestions. In the end our special thanks to Dr. P. C. Kulkarni (Principal of GESRHSCOEMSR) for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for Our Project.

REFERENCES

- [1] Tomer Shimshon, Robert Moskovitch, Lior Rokach, Yuval Elovici "Clustering Di-Graphs for Continuously Verifying Users according to their Typing Patterns". 2014 IEEE 28-th Convention of Electrical and Electronics Engineers in Israel.
- [2] Tyler Highlander, D Ale Bassett, Derek Boone "Utilization of Keyboard Dynamics for Unique Identification of Human Users".
- [3] E. Yu, S. Cho. "Keystroke dynamics identity verification - its problems and practical solutions". 23 2004
- [4] Guven, A. and I. Sogukpinar, "Understanding users keystroke patterns for computer access security," 22, 695-706, 2003.
- [5] D. Gunetti and C. Picardi, "Keystroke analysis of free text. ACM Trans. Inf. Syst. Secur.", 8(3):312-347, 2005.
- [6] D. Bartmann, I. Bakdi and M. Achatz. "On the Design of an Authentication system based on Keystroke Dynamics Using a Predefined Input Text.", 1(2), 1-12, April-June 2007.
- [7] F. Monroe and A. Rubin. "Authentication via keystroke dynamics.", 48-56 1997.
- [8] L. Breiman, "Random Forests", Machine Learning, vol 45(1) 2001.