An Improved User Verification in Online Learning Systems Using Behavioral Profile

[I]P.V. Praveen Sundar, [II]A.V. Senthil Kumar
[I,II]PG and Research, Dept. of Computer Applications,
Hindusthan College of Arts and Science, Coimbatore, India

Abstract

Online learning is an up growing research area in educational domain, it's key success is delivering content over internet and can be accessed by students from anywhere and anytime. In an online learning systems, Each and every student has separate username and password for their learning process. Based on their learning skills, attendance and examination marks, an instructor can decide whether the learner is engaged or disengaged in the course. From the Instructor's point of view, he can judge the student's performance using the information stored in their account. The instructor doesn't have a knowledge of who are actually involving the academic activities. The present method of authenticate the user is username and password authentication. Username and password Authentication is considered as a static authentication. Using those authentication, we can't validate the logged user is genuine user or not, because anyone who knows the username and password can logged into the system and access the online learning system has a genuine user. Hence we need a dynamic and Continuous Authentication(CA) for an entire logged session. For Continuous Authentication, Key stroke dynamics and Mouse dynamics is considered as an effective authentication procedure in a current atmosphere. The Proposed work analysis the user behavioral profile using Keystroke Dynamics(KD) and Mouse dynamics(MD). The Proposed work has obtained 84% accuracy of identifying the legitimate and imposter users. Hence the proposed work is efficient in authenticating the imposter attacks on online learning system.

Keywords

Computer mouse usage characteristics, Key Stroke Dynamics, Mouse dynamics, Behavioral patterns, Continuous Authentication, Improved Genetic Algorithm (IGA)

I. Introduction

In the current worldwide with Internet-centered world, the process of user validation and authentication have been developing into further significant area [1-2]. The inspirations of e-learning systems strength go through from dishonest behavior of students,particularly where the result of online measurement is guarantee or measure. One-time validation by means of password mightn't protect touching remote user impersonation [3]. The mode of strengthen password security of an account might be completedby means ofusing biometrics, particularly behavioral distinctiveness of users. Usual input devices present information such as keyboard and computer mouse practice distinctiveness with the intention demonstrates good results in demonstrate identity more over when accessing account or constantly following his/her logging in [4].

Designed for extremely perceptive systems such as online banking, it is fundamental in the direction of protected users' accounts and protects their property beginning malicious hands. Even in smaller amount critical systems such as desktop machines in a computer laboratory, online forums, a capture session can be misused to spread viruses, probably harmful a user's standing and additional systems. The majority of usual approach in the direction of protected access in the direction of systems is the utilization of a password [5]. Unfortunately, passwords experience beginning two serious problems: password cracking and password theft [6]. Once a password is cooperation, an adversary is able to straightforwardly misuse a victim's account. Consequently, there is a huge demand toward rapidly and correctly authenticate with the purpose of the person calculating a known user's account is who the user maintains toward be named as re-authentication [7].

In the literature some of the user verification and re-authentication techniques necessitate human involvement, such as given that secret response toward agreed-upon questions. However, these methods only offer one-time authentication and the authenticated users are still susceptible toward together session hijacking and the divulging of the secret information. In the direction of attain an appropriate response toward an account breach, further continuous user verification is required. Continuous verification requires a verification decision to be made upon each new keystroke [8-10]. On the other hand, frequent authentication should be inactive and visible toward users, as frequently necessitate a user's interest designed for re-validation is excessively conspicuous and difficult to be acceptable.

Mouse dynamics evaluates and determines a user's mouse-behavior features designed for make use of biometric. When compared to other biometrics authentication such as face, fingerprint and voice [11], mouse dynamics is less disturbing, and needs no particular hardware toward confine biometric information. Consequently, it is appropriate designed for the present web environment. When a user attempts toward log into a computer system, mouse dynamics simply needs her toward give the login name and toward execute a definite series of mouse operations. Extracted features, depending on their mouse movements and clicks, are related to a legitimate user's profile. Equivalents validate the user; elsewhere her access is left without. Moreover, a user's mouse-behavior features are able to be frequently examined throughout her following procedure of a computer system designed for individuality monitoring. Yampolskiy*et al.* present an evaluation of the field [12].

Mouse dynamics has paying attention further and extra investigate attention over the recent years [13-14]. Even though existing research provides higher results, mouse dynamics is still a recently promising method, and have not been provides higher performance. Many of the recent work proposed based on the approaches designed for mouse-dynamics-based user verification result in less accuracy. Moreover, these mouse dynamics approaches should restrict applicability in real-world application, since many of the users in the WWW not interest to use new authentication mechanism and some of the authors focused to use of this schema to real-world environments over experimentally restricted environments, excluding this realism might origin not premeditated side-effects by means of establishing confusing factors with the purpose of could affect experimental results. Such confounds can make it complex toward characteristic experimental outcomes exclusively toward user behavior, and should not applied to other type of factors next to the time-consuming path of mouse behavior to computing environment [15].

The proposed work presents schema to verify and authenticate the student's identity in sessions depending on their mouse usage patterns. They make use of biometric-based approach toward authenticating users depending on their submissively noticeable mouse movement behaviors. Present preliminary results depending on their first experiment in an e-learning system. Examine appropriateness of distinctiveness such as movement velocity, click duration, etc. It is designed for verification and consistency of the proposed methods depending on this distinctiveness. It calculates the index of Learning Styles depending on their mouse usage patterns with the intention of might be used by means of large benefit in personalizing educational systems. It might be also noticed with the intention of the mouse-dynamics investigation and used information from together the impostors and the honest user towards train the classification or detection model.

II. Related Work

The number of biometric modalities be present able toward basically confine not including disturbing the day by day action of a user, similar to face, voice, keystroke and mouse dynamics. Additional biometrics might be capture, other than achieve require a higher degree of user attachment, designed for instance fingerprint. Voice biometrics capacity undergo beginning music playing, people conversation close by or other sources of noise, and still from the fact with the purpose of people mightn't talk a lot in front of the computer. Face recognition capacity suffer beginning varying light conditions and users altering their location at the same time as working. Keystroke dynamics [16] and Mouse dynamics [17] look toward suffer less from these natural changes in the substantial situation of the user, though it is identified with the purpose of typing behavior determination change depending on the expressive condition of a person.

Additional in recent times, a survey envelops the recent mechanism in mouse dynamics has been performed by means of a proportional experimentation [18]. It points out with the purpose of mouse dynamics investigate must be additional aware toward decrease verification time and obtain the result of environmental variables addicted to account. It has been concluded with the purpose of related to other works, the existing approach in addition obtains high accurateness however simply need a little amount of biometric information. Furthermore, we discover the property of environmental factors such as different machines, mice, and time and show with the purpose of proposed approach is comparatively well across diverse operating system and times.

Graphical passwords [19] are associated types of user authentication; depending on Human Computer Interaction via a pointing machine toward validate a user. The work distinguishes the users based on *how* the users move and click the mouse, higher than *where* the users click. Graphical passwords are recorded where the user clicks on the screen, and consequently use this series as a replacement password. Systems related to the corresponding to the present work, and be able to be deployed together. For example, one capacity makes use of a graphical password scheme at the same time as without interest recording a user's mouse dynamics, make use of the submissively recorded measurements as a resulting fail-safe toward validate the user's identity.

In Ahmed et al.'s work [20], at the same time as attain extremely high accuracy, the number of mouse actions required toward authenticate a user's individuality is moreover high toward be useful. Similarly, the work of [21] proposes a mouse dynamic approach for predicating disengaged learners in online learning.

III. Proposed Work

The proposed work evaluates the results of a continuous authentication system with a variety of diverse examination procedures designed for user authentication approach. The proposed user authentication system includes the following methods: -

A. Keystroke Dynamics

Keystroke dynamics is considered as an automated method of identifying or confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard. Keystroke dynamics is a behavioral biometric, which evaluates based on 'what you do'.The raw measurements used for keystroke dynamics are dwell time and flight time.

Dwell time

It's the time interval between a key pressed until it releases (press – release). This calculates the time duration for which key holds by the user. The key hold time is the dwell time.

Dwell Time D1 = (Key Release Timing of the Key- Key pressing Time)

Flight time

The time interval between a key press and the successive key press (press – press) is called as flight time. It's the consecutive press key time difference called as press time. The time difference between releases of two consecutive key releases is called as release-release time. Combine of the both the features terms as flight time.

D2= The Key press timing of Key 2- The Key Release Timing of Key 1

D3= The Key Release Timing of Key2 - The Key Release Timing of Key1

D4= The Key press timing of Key 2- The Key press timing of Key 1

Typing speed

Typing speed is measured as average characters typed per minute. Ofcourse typing speed of the keyboard by individual varies by person to person.

The attributes are calculated using key stroke dynamics are listed in Table-1.

Table 1: Key stroke Dynamics attributes

Factor	Unit	Description
Mean of dwell time	Second	The mean dwell time of a sequence of keystrokes.
Standard deviation of dwell time	Second	The standard deviation of dwell time of a sequence of keystrokes.

Mean of flight time	Second	The mean flight time of a sequence of keystrokes.
Standard deviation of flight time	Second	The standard deviation of flight time of a sequence of keystrokes.
Mean of dwell time per category	Second	The mean of dwell time for each keystroke category in a sequence of keystrokes.
Percentage of occurrences per category	%	The distribution of each keystroke category in a sequence of keystrokes.
Percentage of occurrences of holding multiple keys	%	The percentage of occurrences of holding multiple keys in a sequence of keystrokes.
Average Typing Speed	Character / Second	The average typing speed of a sequence of keystrokes.

B. Mouse Dynamics

Mouse dynamics is a part of behavioral biometrics which can authenticate the user based on the usage of mouse while handling the system. Mouse dynamics is divided into two parts, static authentication and dynamic authentication. If the authentication uses mouse based features at the starting point, then it is called as static authentication. Authenticating a person even after the entry point leads to dynamic authentication. The Proposed work uses the following features for evaluation: -

1. Category of action such as 1: Mouse Move; 2: Silence; 3: Point and Click; or 4: Drag and Drop. 5: Double Click.
2. Travelled distance in pixels.
3. Searching time in second via a 0.25 second Sampling Interval.
4. Mouse direction: The value among 1 and 8 related to the movement of the mouse. Consider an example from Figure 1 designed for which direction related to which value.

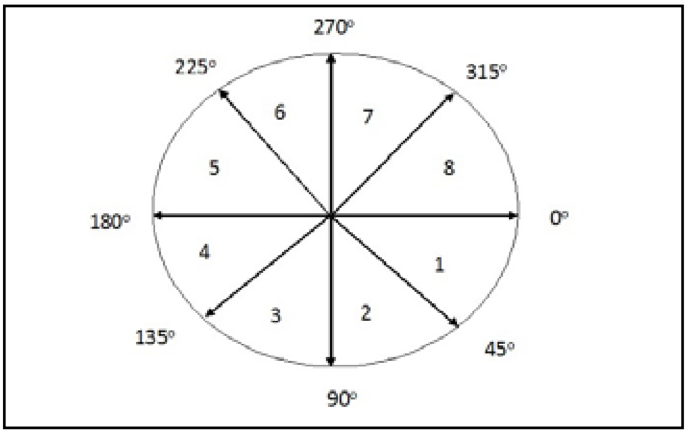

Fig. 1: Direction of the Mouse movements

In this phase, mouse dynamic features were extracted based on the behavior of mouse operations, and were characteristically prearranged addicted towards a vector representation with the series of mouse functions in one implementation of the mouse-operation. Distinguish mouse behavior depending on two basic category of mouse operations—mouse click and mouse movement.

Every mouse operation was then examined independently, and transformed into many mouse features

The Table-2 shows the mouse move and drag-drop features used in this research.

.

Table 2: Mouse Dynamics Biometric Features

Factor	Unit	Description
Average click time	Second	The average of mouse clicks time.
Silence ratio	%	The percentage of silence occurrence of a sequence of mouse actions.
Percentage of mouse action per mouse movement direction	%	The percentage of mouse action occurrence of a sequence of mouse actions in each mouse move direction.
Percentage of distance per mouse movement direction	%	The percentage of mouse move distance of a sequence of mouse actions in each mouse move direction.
Percentage of mouse move time per mouse movement direction	%	The percentage of mouse move time of a sequence of mouse actions in each mouse move direction.
Average distance per mouse movement direction	Pixel	The average distance in each mouse movement direction.
Average speed per mouse movement direction	Pixel / Second	The average speed in each mouse movement direction.
Average velocity in X axis per mouse movement direction	Pixel / Second	The average velocity in X axis in each mouse movement direction.
Average velocity in Y axis per mouse movement direction	Pixel / Second	The average velocity in Y axis in each mouse movement direction.
Average tangential velocity per mouse movement direction	Pixel / Second	The average tangential velocity in each mouse movement direction.

The Proposed work splits the mouse dynamic operation features as four categories which are discussed as follows:

Holistic features with the purpose of distinguish the entire characteristics of mouse behaviors at the time of interactions, such as single-click and double-click statistics with four different actions. 1) Mouse Single Click Action, where the feature be indistinguishable as Single Key Action. 2) Mouse Double Click Action, where the features were time of the initial and second click and the latency among the clicks. 3) Mouse Move Action, 4) Mouse Drag-Drop Action. Depending on the data presented by means of information confine software be able to mine a diversity of trajectory regarding features designed for mouse move and mouse drag-drop actions.

C. Improved genitic algorithm (IGA)

In this research work,Improved Genetic Algorithm (IGA) is used to analysis the behavior of mouse key dynamics which consists of several operators. Figure 2 illustrates the flowchart of IGA with each iteration is spitted into two phases namely 'selection phase' and 'recombination phase'.

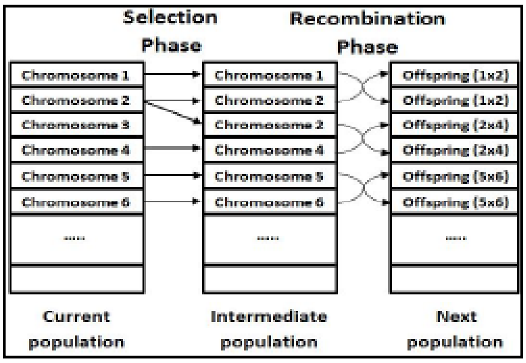

Fig. 2 : Each generation is modified during selection and recombination phase and creates new generation of candidates

To perform IGA, Fitness function f(x) is evaluated by measuring the distance between two mouse dynamic features of the different users. In the initial stage of the work selection phase, lowest fitness value users are considered as normal user and the remaining users is considered as the unauthorized user in the current-population, at the first iteration [22].

After completion of the selection by using fitness function assesses then new candidates is used for next crossover operation. If all the operations in the IGA are completed then stop the current iteration, if it is not then increase number of iterations in the current-population, at the time of selection operation. Here selection operation is performed based on the 'roulette wheel'. Then perform crossover and mutation operations in the recombination phase stage in the current population. Crossover operator selects a pair of samples in the current population. Then new population is found by using two types of crossover operations like: 1-point crossover, 2-point crossover, etc.[22]. The Figure-3 illustrates the 1-point crossover operations.

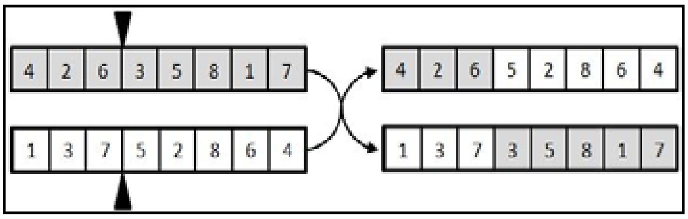

Fig. 3 : 1-point crossover cuts candidate's arrays from 'break point' then it replaces primary or secondary pieces

IMPROVED GENETIC ALGORITHM (IGA)

```
Initial-population  greedy←initializing(n)
current-population Initial←population
for iter = 1 :maximum-iteration
    for i=1: k
        fitness-value[i]fitness←function(current-population[i])
    end of inner for
    if solution is found
        break;
    end of if
    intermediate-populationselection(current-population)
    temp←crossover(intermediate-population)
    temp←mutation(temp)
    temp←minimal-conflicts-algorithm(temp)
    next-population←temp
    current-population←n_population
end of for
k :population size
```

At the final stage of the work then perform mutation operation by adding new mouse dynamic user behavior. The value of the current population should be determined via the computation of the probability P.

IV. Dataset Preparation

The dataset used in this studies is collected from an online learning system [23]. The dataset in this research work consists of information regarding to mouse dynamics of 49 users. The users were of various age, occupation and level of computer use experience. Each user was working on their own personal computer/laptop. The system records the key stroke values and mouse activities in their specified log file.

The dataset formation can be divided into two phases.

1. Training phase
2. Testing phase

While in the Training Phase, Initially the user has to login into the system using their own login and password, After the successful login, the user is guided to Keystroke Registration. Keystroke registration focuses on the entering a fixed paragraph containing 1000 to 1500 words. After completion of this procedure, the user is allowed to learn the online materials. On those duration, there mouse activities are recorded. For first 10 times the same procedure is followed. Based on the Keystroke values extract from the user's static passphrase and their Mean, Standard deviation, Minimum and maximum range is calculated for the user and the same is stored in the database. After successful keystroke and mouse usage registration, based on the values stored in the database. separate template has been created for each and every user. The training process covers the three ways of confidential information. Username-password, keystroke and mouse data collect from registration process.

Testing phase consists of three sub phases. The first part focuses on the existing functionality of the identifying user. Username and password enter by the user in this phase. The data get validate by the application and if the details don't match then user gets deny. If username and password match, then the user is allowed to learn the online materials, while in background the system records the new mouse movement values and keep on checking them with the values stored in database. If the details didn't match means then the user is guided to keystroke authentication, where keystroke authentication focuses on entering a fixed passphrase. Keystroke values extract from the user's passphrase (5 times entry of passphrase) and data get validate by the application and if the details don't match then user gets deny and his account is locked. If details match with the store data, then the user is allowed to continue learning process.

V. Experimental Results and Discussion

In order to validate our approach, 49 users are involved in our testing process. Each and every user has spent 10 to 20 sessions in online learning. Initially first 10 sessions the users are logged in their own username and password. Out of 49 users, 10 users are wrongly classified as an imposter and the system guides those users for keystroke authentication. On key stroke authentication, their key stroke values prove that they are wrongly classified in mouse dynamic authentication. The main goal of our proposed work is to minimize the uncomfortable for the genuine users and give maximum security from imposters. once they identified as legitimate user, the system immediately unlocks their account and allows them in online learning like earlier. At the end of the first stage of testing process, we found that mouse dynamics authentication has wrongly identified 10 genuine users as imposters, but keystroke authentication will judge them as a legible user and concludes the 100% accuracy of our work. With the help of key stroke authentication, we conclude that none of the users account has locked in our first stage of testing process.

On the next level of testing process, we allow the users to login with other users account, i.e., the system allows the users to access the users to access the username and password of other users in order to allow impersonation attacks. Out of 49 users, 21 are the genuine users even though they know the fellow user's authentication details they logged in their own account only. Due to the curiosity, remaining 28 users have try to login with their fellow user's authentication details.

At the Initial stage of testing process, 49 users are logged into the system with username and password. At the second phase of testing the current mouse activities of the users is compared with their template. Out of 21 genuine users, 5 users mouse dynamics details didn't match with their own template. Hence they will be treated as an imposter. then the 5 users are guided to the third phase of testing with key stroke dynamics. The current values of key stroke values of 4 users are matched with their own template and 1 of the users keystroke values failed on key stroke dynamics too. Even though he is a genuine user he fails to prove himself on both type of verification process. Hence his account is locked and assigned as an imposter.

Similarly, out of 28 imposters 6 of the users has overcome the mouse dynamics authentication their mouse dynamic values will comes under the genuineuser's values. Hence the system didn't detect them as an imposter and considered them as a genuine user. The remaining 23 users are identified as an imposter user in mouse dynamic authentication. They are guided to the keystroke dynamics verification. while in keystroke authentication, 22 users keystroke values didn't match with the template and thus they confirmed as an imposter and one of the user keystroke values matches with the template and the system will be classified as a genuine user.

Table 3: Summary of the authentication accuracy using Improved Genetic Algorithm summarized as a Confusion Matrix

	Legitimate	Imposter	
Legitimate	20	7	0.77
Imposter	1	22	0.96
	0.95	0.79	0.865

Table 3 Summaries the authentication accuracy using Improved Genetic Algorithm(IGA) and summarized as a confusion matrix for the obtained results/ Based on the above confusion matrix, the following values are calculated. The formula used for calculation is presented in Table-4. The experimental results in Table-4 shows that proposed work has 84% accuracy. Precision andRecall values for legitimate users are 74% and 95.23% respectively. Precision and Recall values for Imposter values are 95.65% and 75.86% respectively. F1 Score is 83.3%.

In Table-4, the meaning of the short words used are as follows:

TP→ True Positive,
FP→ False Positive,
P→ Predicted Legitimate values,
N→ Predicted Imposter Values,
TN→ True Negative Values,
FN→ False Negative values.

Table 4: Performance Evaluation values

Measure	Value	Derivations
Sensitivity	0.9524	TPR = TP / (TP + FN)
Specificity	0.7586	SPC = TN / (FP + TN)
Precision	0.7407	PPV = TP / (TP + FP)
Recall	0.9523	R= TP/ (TP+FN)
Negative Predictive Value	0.9565	NPV = TN / (TN + FN)
False Positive Rate	0.2413	FPR = FP / (FP + TN)
False Discovery Rate	0.2593	FDR = FP / (FP + TP)
False Negative Rate	0.0476	FNR = FN / (FN + TP)
Accuracy	0.84	ACC = (TP + TN) / (P + N)
Error Rate	0.1633	ER= (FP+FN)/ (P+N)
F1 Score	0.833	F1 = 2TP / (2TP + FP + FN)
Matthews Correlation Coefficient	0.7041	F1 = 2TP / (2TP + FP + FN)

VI. Conclusion

Basically User authentication in an online learning system is classified into two categories namely static authentication and continuous authentication. The main drawback of static authentication is anyone who knows the username and password can logged into the system as a genuine user. Identifying whether the logged user is genuine user or imposter is not possible in static authentication system. Hence our proposed work authenticates the user using static and dynamic authentication. Initially every user is logged into the system using their username and password. Then the system authenticates the logged user using the combined power of mouse dynamics and key stroke dynamics authentication. Improved Genetic Algorithm is used to classify the genuine and imposter users. Using Improved genetic algorithm system has got 84% accuracy. In the Future Perspective, the proposed work has to be extended to the simultaneously authentication using both key stroke and mouse dynamics authentication. While in the present work, initially mouse authentication authenticates the logged user. if the mouse authentication suspects the user then only key stroke authentication authenticates the user. If mouse authentication fails to identify the imposter then there is key stroke authentication is not possible for the user. To avoid those criteria, the system has to authenticates both methods simultaneously means then the system doesn't allow singe imposter to access the online system and produces 100% accuracy.

References

[1]. *A. E. Ahmed and I. Traore. A new biometric technology based on mouse dynamics. IEEE Transactions on Dependable and Secure Computing, 4(3):165–179, 2007.*

[2]. *S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle. Multiple password interference in text passwords and click-based graphical passwords. In ACM Conference on Computer and Communications Security (CCS), 2009.*

[3]. Moini, A., Madni, A.: Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective. In: Systems Journal, IEEE, vol. 3, no. 4, 2009, pp. 469-476.

[4]. Chudá, D., Ďurfina, M.: Multifactor authentication based on keystroke dynamics. In: Proceedings of the International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing, (2009), pp. 1–6.

[5]. S. Chiasson, P. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In USENIX Security Symposium, 2006.

[6]. Y. Zhang, F. Monrose, and M. K. Reiter. The security of modern password expiration: An algorithmic framework and empirical analysis. In ACM Conference on Computer and Communications Security (CCS), 2010.

[7]. M. Pusara and C. E. Brodley. User re-authentication via mouse movements. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pp. 1–8, 2004.

[8]. Kenneth Revett,FlorinGorunescu, Marina Gorunescu and Marius Ene, "A machine learning approach to keystroke dynamics based user authentication",Int. J. Electronic Security and Digital Forensics, Vol. 1, No. 1, 2007.

[9]. I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi and I. Lai, "Combining Mouse and Keystroke Dynamics Biometrics for Risk-Based Authentication in Web Environments," Digital Home (ICDH), 2012 Fourth International Conference on, Guangzhou, 2012, pp. 138-145.

[10]. P. Bours and S. Mondal, "Performance evaluation of continuous authentication systems," in IET Biometrics, vol. 4, no. 4, pp. 220-226, 12 2015.

[11]. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp.125–143, 2006.

[12]. R. V. Yampolskiy and V. Govindaraju, "Behavioral biometric: A survey and classification," Int. J. Biometrics, vol. 1, no. 1, pp. 81–113, 2008.

[13]. H. Gamboa, A. L. N. Fred, and A. K. Jain, "Web biometrics: User verification via web interaction," in Proc. Biometrics Symp., Baltimore, MD, 2007, pp. 1–6.

[14]. P. Bours and C. J. Fullu, "A login system using mouse dynamics," in Proc. 5th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing, Kyoto, Japan, 2009, pp. 1072–1077.

[15]. Z. Jorgensen and T. Yu, "On mouse dynamics as a behavioral biometric for authentication," in Proc. 6th ACM Symp. Information, Computer and Communication Security, Hong Kong, 2011, pp. 476–482.

[16]. J. Stewart, J. Monaco, S.-H. Cha, and C. Tappert, "An investigation of keystroke and stylometry traits for authenticating online test takers," in Int. Joint Conf. on Biometrics (IJCB'11), 2011, pp. 1–7.

[17]. C. Feher, Y. Elovici, R. Moskovitch, L. Rokach, and A. Schclar, "User identity verification via mouse dynamics," Information Sciences, vol. 201, pp. 19 – 36, 2012.

[18]. Z. Jorgensen and T. Yu. On mouse dynamics as a behavioral biometric for authentication. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS '11, pp. 476–482, 2011

[19]. E. Stobert, A. Forget, S. Chiasson, et al. Exploring usability effects of increasing security in click-basedgraphical passwords. In Annual Computer Security Applications Conference (ACSAC), 2010.

[20]. Y. Nakkabi, I. Traore, and A. A. E. Ahmed. Improving mouse dynamics biometric performance using variance reduction via extractors with separate features. IEEE Transactions on Systems, Man, and Cybernetics, 40(6):1345–1353, 2010

[21]. Sundar PVP, Kumar AVS. An enhanced disengagement detection in online learning using Quasi framework. Special Edition of International Journal of Applied Engineering Research (IJAER). 2015 Jun; 10(55):1298–302.

[22]. Whitley, "a genetic algorithm tutorial," statistics and computing, pp. 65-85, 1995.

[23]. Quasi Framework. Available from: www.quasiframework.com