Sheffield Hallam University

Using keystroke and mouse dynamics for user identification in the online collaborative game League of Legends

DA SILVA BESERRA, I., CAMARA, L. and DA COSTA ABREU, Marjory <http://orcid.org/0000-0001-7461-7570>

Available from Sheffield Hallam University Research Archive (SHURA) at:

http://shura.shu.ac.uk/25384/

This document is the author deposited version. You are advised to consult the publisher's version if you wish to cite from it.

Published version

DA SILVA BESERRA, I., CAMARA, L. and DA COSTA ABREU, Marjory (2016). Using keystroke and mouse dynamics for user identification in the online collaborative game League of Legends. In: 7th International Conference on Imaging for Crime Detection and Prevention (ICDP 2016). Institution of Engineering and Technology.

Copyright and re-use policy

See http://shura.shu.ac.uk/information.html

Sheffield Hallam University Research Archive
http://shura.shu.ac.uk

Using keystroke and mouse dynamics for user identification in the online collaborative game League of Legends

Isaac da Silva Beserra, Lucas Camara, Márjory Da Costa-Abreu*

*DIMAp-UFRN, Natal/RN, Brazil, marjory@dimap.ufrn.br

Keywords: Keystroke dynamics, Mouse dynamics, League of Legends, Online game, User identification.

Abstract

The popularity of computer games has grown exponentially in the last few years. It is not uncommon to find players of online games who can dedicate their whole lives in order to became the best in their favourite game. The best players normally become celebrities and can even get sponsored to compete in game tourneys. It is accepted that each player should follow the his/her own path to increase level, so the experience reflected in the gamer's level is how proficient he/she is in the game. However, this increased popularity has also created a desire on some players to cheat (by paying others more experienced players to play for them) for the progress in the game and thus to improve their status. The companies that develop such games have very strict punishment for such breaking of the rules, but, it can be very difficult to identify when this "account sharing" happens. This paper focus on the collection and analysis of a new online game database for continuous mouse dynamics and keystroke dynamics authentication in order to identify whether who is playing is really the account holder. Our very first results point to very interesting possibilities for security biometric-based applications in this new game analysis area.

1 Introduction

The increased popularity of online games has changed the dynamics of game playing dramatically. Players of online games dedicate their lives to gain visibility in their favourite game and became the best. In the most popular games, it is possible to find items that can be acquired and sold for considerable amounts of real money. This can attract malicious players to steal accounts from other players or it can motivate users to pay in order to "improve" their abilities just for the "status" of being advanced in that particular game.

Major game companies have created alternatives to deal with the account stealing, helping players to protect their accounts. Some of those strategies adopted can include extra-passwords or the linking of a special item to a account, that cannot be traded, and can confirm, by SMS, every time you log on a different computer. These strategies can help, but when the problem is not a stolen account, but a shared account, this detection becomes more challenging.

The main concern, from the point of view of the players, is that some games work with a match-based mechanism. The players on each match are selected based on their skill levels to make the match balanced. But when there is a player who has cheated its level, it will not be able to play evenly with its counterparts making the teams unbalanced. For the company, the main concern is that a game with a large group of "account sharers" will end up making that game less popular, thus losing real players for simply not trusting who they are playing with (or against).

As already mentioned, this is a much harder problem to solve, because the account owner wants to allow another player to use his/her account. A possible security-oriented solution is to make a continuous identification of the account owner.

Although this reality is rapidly changing (specially since the launch of Ingress[1] and Pokemon Go[2]), most online games are played in traditional desktop computers, and this continuous identification could be done by using biometric-based mouse dynamics and keystroke dynamics analysis.

The idea here is that the identification system will work as a traditional biometric-based system, but the data used would be based on the characteristics, specific from the analysed game, of its mouse and keystrokes actions.

This paper presents a new bimodal biometrics database as well as an initial analysis of the possibility of using mouse and keystroke dynamics features for user identification of the popular game 'League of Legends'. We have chosen this game, because it is the most desktop-based played game today. Since, to our knowledge, this is the very first work regarding continuous identification for online games, this paper will mainly focus on the proposal of a data collection protocol as well as a preliminary analysis of the identity predictability of the collected data.

2 The biometric modalities used for desktop-based game playing

Online games have been very popular since its massive commercialisation, in the 80's, but have become very diverse, especially with the popularisation of mobile phones and tablets. Thus, since the interaction with the device can vary, it is possible to use several different biometric modalities related, such as gait, hand shape, keystroke dynamics, mouse dynamics, touch-screen dynamics, etc. Because we have chosen the game

[1] https://www.ingress.com/

[2] www.pokemongo.com/

League of Legends, we have decided to investigate keystroke and mouse dynamics for this particular work which are the two modalities used for this specific game.

Keystroke dynamics or typing dynamics is an automated method for the identification or confirmation of identity of a person through the manner and the rhythm of his/her typing on a keyboard. It uses features as dwell time, which is the time duration that a key is pressed, and flight time, which is the interval between releasing a key and pressing the next key [6].

Mouse dynamics is also an automated method for identification or confirmation of identity, and it uses features such as speed movement and frequency of clicks. The move speed is how fast the user moves the mouse in the 8 possible mapped directions and frequency of clicks is the amount of clicks the users performs in a time interval [4].

As we are proposing a new paradigm of biometric use, we need to understand how the keystroke and mouse dynamics are used in the online game League of Legends. Section 2.1 will introduce the basics of the game.

2.1 League of Legends

League of Legends [3] is a Multiplayer Online Battle Arena (MOBA) game. The game is based on matches which are normally among teams of five players. Before the match starts, each player needs to choose a champion which is a character-avata that already exists in the game. In the same team, two players cannot choose the same character as their champion. The goal of the game is to destroy the "Enemy Nexus" which is a structure located on the enemy base.

Each character has four unique skills, where three are common skill and the last one is an ultimate skill. All those different skills are created by using different combinations of at least two of the keys 'Q','W','E' and 'R'. The unique skills make the characters unique, thus, when selected as a champion, each character will have a different ability. Based on the wide varieties of each character, each player needs to consider carefully his/her choice of champion in order to build a combined a strategy for the team. During each match, the players use the keyboard not only to play but to chat as well.

The main features used in League of Legends from both keyboard and mouse can be described as follows:

- Keystroke dynamics: 'Q','W','E','R' (the unique skills), 'D','F' (The summoner skills - this are the same for every character, but the player must choose only two) and 'B' (which is used to return to the base camp of the team).
- Mouse dynamics: Move the character (with a point and click) and targets the skills direction.

Thus, both mouse and keyboard are essential during the match, so an identification system based on those two modalities has a great chance of reaching a reliable and secure way to make sure each user is playing with his/her own account.

Despite the fact that there are no known game-based databases as such for user identification, the use of keystroke and mouse dynamics for general purpose or verification end is not knew. Sections 2.2, 2.3 and 2.4 will present the most well known referent literature for each modality as well as their combination.

2.2 Related work: Keystroke dynamics

As already mentioned, the existing databases (both for mouse and keystroke dynamics) available do not cover the idea of game-based identification, thus, this session will briefly describe the relevant papers that use keystroke dynamics for user identification.

The very first database that can be found in the literature is presented in [2]. It contains 80 users who had to type five different PINs. Each participant typed 25 times using only the right hand index finger. In [6], the GREYC-Keystroke is presented. It contains 133 users, where each users typed the password "greyc laboratory" between 03/18/2009 and 07/05/2009. The aim of this experiment is to establish the dependency of the keystroke data to the keyboard used.

In [12], each user typed a username and password 4 or 5 times in order to create a new account. The database includes 2057 test samples and 556 training samples from 117 users. This database has a mix of samples with the Dataset A being collected in cybercafe and the Dataset B being collected in the open. In [9], a keystroke database with 110 users is presented and it contains extra information such as gender, age, handedness, and country of origin. Their protocol includes five phrase and the users had to type them with each hand 10 times without errors.

In [3], 44 users are asked to type five times a fixed text of 683 characters. The text used was taken from the famous Italian novels, "I Promessi Sposi" ("The Promised Newlyweds"). In [19], the database collected consists of two phases, with 51 users typing a static text and a free text section in the first stage, and 30 users typing several texts without restriction, each on a different day across the span of a month in the second stage.

In [10], the used database consists of 110 users which typed five set of passwords, each user typed 20 times (10 times with one hand and 10 times with two hand) totalling 100 samples per users. In [27], a database with four phase with interval of six months is collected. Each user was allowed to choose their preferable username and password during the enrolment process and they were asked to type one fixed text for fifteen consecutive times.

In [8], the authors analyse the detection of user/password sharing by collecting data sets from 16 graduate students at Seoul National University, each of whom typed a fixed set of 25 username/passwords. Each user typed 30 times with their own keyboards resulting of 480 sample (16 users x 30 patterns) for each password. In [14], the authors also analyse the identification of account sharing. A single keyboard was used by 15 users who trained the system with their own passwords. They were then asked to type the password of the other 14 users 15 times each (that counts for roughly 15^2 training samples, and 15^2 tests which generated $2n$ latency variables each, where n is the length of the password).

[3] http://na.leagueoflegends.com/

Table 1. Keystroke dynamics databases

Ref	users	data	fixed/free	Error
[9]	110	text	fixed	22.00%-4.00%
[19]	81	text	fixed/free	11.00%
[12]	117	text and numbers	fixed	25.00%
[6]	133	text	fixed	-
[3]	44	text	fixed	-
[2]	80	numbers	fixed	4.00%
[10]	110	numbers	fixed	10.00%
[27]	100	text	fixed	9.00%
[8]	16	text and numbers	fixed	7.00%
[14]	15	text and numbers	fixed	11.00%

The table 1 shows the important information of each of the databases. It is interesting to see that the databases are not large compared with other more common modalities and the majority of the available data is of the fixed text. Thus, we can justify the collection of a free game-based keystroke dynamics database.

2.3 Related work: Mouse dynamics

As with the keystroke dynamics, it is possible to find a few relevant mouse dynamics databases for user identification.

The first mouse dynamics database that can be found in the literature is presented in [4]. It contains 28 users which performed a fixed task of moving the mouse trough a fixed path between two lines. In [25], they collected data from five users, each providing free use of the mouse from their workstation. In [23], 20 users were asked to install the data collector on his/her workstation and to continue to work normally. The data includes information of the mouse action timestamp, the mouse action type, the coordinates of mouse cursor on the screen and the receiving process.

In [17], 22 users provided data from free use of their workstations. In [11], 17 volunteers, eight males and nine females, performed a common web browsing task. In [26], 26 subjects were asked to perform a fixed mouse-operation task of 300 repetitions each in a tightly-controlled experimental environment. In [22], 28 volunteers performed Internet surfing, word processing, online chatting and programming for 30 minutes. In [13], 11 users provided file-related operations in Windows Explorer. In [21], 8 users performed 10 times the same fixed task.

In [20], 39 volunteers performed several fixed gestures with the mouse. In each gesture the data collected consisted of the horizontal coordinate (x-axis), the vertical coordinate (y-axis), and the elapsed time in milliseconds at each pixel. In [15], 37 users, 30 males and 7 females, performed a fixed task operation 10 times. In [5], the authors collected data from 28 users, 22 males and 4 females, from their workstations during 30 minutes. The data collected includes the event type, the position at which the event occurred, the timestamp when the event occurred, and the application information in which the event occurred. In [24], 58 users, 46 males and 12 females (all right-handed), performed a fixed task (made to force the user to do several actions types). All the data was collected from the same computer.

Table 2 shows the information about all the databases regarding mouse dynamics. As with the keystroke dynamics, it is interesting to see that the databases are even smaller when compared with other more popular modalities. Also, the main goal of all those databases is very specific to work applications and their aim is to perform user identification. Thus, we can justify the collection of a free game-based mouse dynamics database.

Table 2. Mouse dynamics databases

Ref	users	Fixed/Free	Experiment	Error
[11]	17	Fixed	Controlled	21.00%
[23]	20	Free	Uncontrolled	5.00%
[26]	26	Fixed	Controlled	17.31%
[22]	28	Free	Controlled	1.12%
[25]	5	Free	Uncontrolled	3.00%
[5]	28	Not Clear	Controlled	2.67%
[4]	28	Fixed	Uncontrolled	26.80%
[20]	39	Fixed	Controlled	11.00%
[15]	37	Fixed	Controlled	-
[13]	11	Not Clear	Uncontrolled	5.00%
[21]	8	Fixed	Controlled	25.00%
[17]	22	Free	Uncontrolled	6.25%
[24]	58	Fixed	Controlled	8.81%

2.4 Related work: Combination of keystroke and mouse dynamics

Sections 2.2 and 2.3 presented the referent literature that proposes and/or investigates the acquisition of unimodal databases of keystroke dynamics and mouse dynamics, respectively. As already discussed, it is not possible to find a large amount of such literature, especially for mouse dynamics.

In [28], 24 subjects were asked to perform a fixed task on their own computer. The classifier had an EER (Equal Error Rate) of 8.21%. The mouse dynamics isolated had a EER of 22.41% and the keystroke dynamics isolated had a EER of 24.78%.

In [16], 25 volunteers participated in the experiment, four different machine learning approach were used, Decision Tree (DT), Counter-Propagation Artificial Neural Network (CPANN), ANN and SVM. In this work, was obtained an identification accuracy of 62.2% in a closed-set experiment and a Detection and Identification Rate of 58.9% in an open-set experiment.

Since the two cited papers were the only found in the literature that combined mouse and keystroke data, even though it can be considered obvious that the automatic authentication in traditional desktops should be done with both. Thus, we believe the work presented here has a lot of relevance and validity for this type of security application.

3 Database protocol and collection

As the main goal of this paper is to present a data collection protocol as well as an initial analysis of this first database, we have to describe in detail how this collection was made. Thus, this section will present the protocol and an initial data analysis.

We have collected all the samples from the same set of computers. In each experiment five (the number needed in order to play a match on League of Legends) volunteers had to play a match together.

Table 3. Data captured during the collection

Event type	Code	Attribute 2	Attribute 2	Attribute 4	Attribute 5
KeyBoard press down	0	Button pressed	Time span	(none)	(none)
KeyBoard press up	1	Button pressed	Time span	(none)	(none)
mouse move	0	x pixel coordinate	y pixel coordinate	Time span	(none)
mouse click down	1	Button clicked	x pixel coordinate	y pixel coordinate	Time span
mouse click up	2	Button clicked	x pixel coordinate	y pixel coordinate	Time span
mouse wheel up	3	x pixel coordinate	y pixel coordinate	Time span	(none)
mouse wheel down	4	x pixel coordinate	y pixel coordinate	Time span	(none)

During the collection, each volunteer could freely decide which of the five available computers to use and, then started to interact with the other volunteers to develop a strategy. Therefore, in all cases, each user had a different function on the team (support, mid laner, top laner, AD carry and jungler are the possible functions) which provided more heterogeneous samples in relation to the functions on the game. Each user was free to choose whichever character as his/her champion and play normally like he/she would at home. During the collection, the matches lasted from 30 to 50 minutes on average. The volunteers team played against a random team, chosen by the system of the game.

For further analysis, it is important to separate the data collected based on each possible function, because each of those functions would create a different style of playing, therefore, providing different characteristics for the data. Even on the same function on the game, each character will have a different style to play, thus we have identified not just the function that the volunteer selected, but the champion as well.

In order to make the environment more controlled, we have used a program that runs in the background and captures every command executed by the keyboard and the mouse. This program was developed in C#, and, for each collection, it started to run when the key "Home" is pressed, so we could control the moment of the game when the collection started.

We have collected simultaneously, the keyboard information which are the action press-0 or released-1 respectively, the key pressed or released, and the time span when the action happened; and the mouse information which are the value 0 (representing the action moving), the values for action, the coordinates of pixel X and Y and the time span, the values 1 (for click down) or 2 (for click up), as well as the actions, key (left click and right click) coordinates of pixel X and Y (place where has been clicked) and the time span, and the values 3 and 4 which represents the action of mouse wheel, and the time span. Table 3 shows how the data is stored in each file.

Section 4 will present a preliminary statistical analysis of the database we have collected so far as well as some classification preliminary results.

4 Preliminary results and analysis

We have presented, so far, the motivation for this new data collection as well as the protocol used to collect this first set of users' data. We have collected samples from 55 users (all males) within a period of four months. Among the samples, we have 53 users right-handed and all users were between the age of 18 and 30 years. Threes of the users played more than once, however, they never played with the same character as their champion.

In this section, we will present an initial statistical analysis of some features that could be used to verify their representatives. The data used in order to calculate the features is listed below:

- 12 mouse features: The move speed of the 8 directions, 'Down', 'Down + Left', 'Left', 'Up + Left', 'Up', 'Up + Right', 'Right' and 'Down + Right, represented by 'Dir-0','Dir-1','Dir-2','Dir-3','Dir-4','Dir-5','Dir-6','Dir-7' respectively, and the Frequency of clicks of right and left (fre R & L) and the Latency of clicks right and left (lat R & L).
- 7 keystroke features (the press speed of the 7 most common keys used during the game 'Q','W','E','R','D','F' and 'B').

Since the main goal of this research is to investigate if it is possible to identify if the user logged into the LoL game is the owner of that specific account, we have performed some initial classification experiments. From each user we have applied the mean data collected during 5 minutes of the feature. Each user played for 30 to 50 minutes, which gave us exactly 336 samples.

For simplification, based on the collected samples, we have decided to use the 16 most common actions performed by the players on the game (presented in Section 4) because they were likely to provide the most recognisable data. We have used all the mouse features but only the 'Q','W','E','R' because those are the more used for the keystroke though out all the different players.

When calculating each user feature we have decided to calculate the arithmetic mean of each 5 minutes of the game play. If there is no data for that specific feature, we have set its value to zero. Since during the first five minutes of the game it is common that the players do nearly no command, we have decided to ignore the data from this period. Each round lasts for around between 30 and 45 minutes, we have a variation of 5 to 8 samples per user.

In order to have a global feel of how the database can be used and since the game needs to be played by mouse and keystroke dynamic actions, we have used both biometrics in a single identification focused classification task.

Since this can be considered a benchmark database, we have selected a wide range of classifiers for user identification

Table 4. Mouse % accuracy first results

Algor	All mouse	8 dirs	lat R & L + 8 dirs	lat R & L	fre R & L + 8 dirs	fre R & L	lat and fre R & L
KNN	75.8929	36.9048	59.8214	28.8690	62.7976	52.0833	83.0357
SVM	83.0357	43.7500	69.0476	28.5714	71.4286	52.0833	86.0119
MLP	73.5119	19.0476	36.6071	6.2500	56.2500	6.2500	18.4524
RFor	85.4167	38.6905	71.7262	29.4643	75.8929	51.1905	80.6548

in order to understand the different results they will produce. We have chosen three well known classifiers from the Weka toolbox [4].

The algorithms selected from this toolbox were the Multi-Layer Perceptron (MLP - 'hiddenLayers' = a, 'learningRate' = 0.001, 'momentum' = 0.9, 'trainingTime' = 50000, 'validation-Threshold' = 500, 'validationSetSize' = 20) [7], the Support Vector Machines (SVM - 'c' = 45, 'checksTurnedOff' = true, 'debug' = true, 'kernel' = Puk) [18], the K-Nearest Neighbours (KNN - 'knn' = 1, 'crossValidate' = true, 'distanceWeighting' = 1/distance, 'nearestNeighbourSearchAlgorithm' = LinearNNSearch) [1] and the Random Forest (RFor - all the default parameters) [5].

Table 4 shows the preliminary results using only the simplest mouse data. In the case of the mouse, since we have a greater quantity of data than the one produced by the keyboard during each game round, it is expected that we have better results when compared with the keystroke results. The difference, however, is very considerable. The best accuracy result is just over 86%, which is a lot more than the best results using only keystroke information. It is also interesting to note that the results of using only the frequency of clicks, in two cases (KNN and SVM) are better than when using all the mouse features. In the same way we did with the keystroke, we wanted to investigate as well if there is any feature that has a bigger impact on the accuracy than the others. From the results, it is possible to note that the combination of frequency of clicks and their latency is likely to have a bigger impact than the directions of the mouse, thus having more individual information.

Table 5. Keystroke % accuracy first results

Algor	All-key	Q,W,E	Q,W,R	Q,E,R	W,E,R
KNN	26.7857	21.4286	17.8571	18.4524	16.9643
SVM	27.3810	28.5714	21.1310	26.4881	19.6429
MLP	5.3571	5.3571	4.1667	4.4643	3.5714
RFor	27.6786	23.8095	19.9405	18.4524	14.2857

Table 5 shows the preliminary results using only the simplest keystroke data. We have chosen to use the most used keys in an attempt to have an idea of how the inclusion of keystroke data would improve (or not) the overall result of the system even though we understand that the four keys have very little information on their own. As expected, the accuracies reached only using these specific keystroke data is very poor. The overall results are not higher than 28% which is very low in a security application. We also wanted to understand which of these most used keys carry the most amount of individual information and, based on the results, it can be said that the 'Q', 'W', 'E' together are the most significant information about the users. In fact, in the case of the SVM, the accuracy with 'Q', 'W', 'E' is even higher than the one with all four keys and in the case of the MLP, the results for the cited cases is the same.

Even though the results for the keystroke data are not very significant, we wanted to analyse if, when used combined with mouse, they would still have a positive impact in the overall accuracy. Table 6 shows the preliminary results using the combination of all the keystroke and mouse data. It is possible to notice straight away that the results are very interesting. In the cases of the KNN, the Random Forest and, especially, the MLP, there is a considerable increase in the overall accuracy. The SVM was the only classifier that had a very small improvement.

Table 6. Combination of Keystroke and Mouse % accuracy first results

Algor	All (mouse + keystroke)
KNN	80.9524
SVM	83.3333
MLP	87.5000
RFor	90.7738

We understand this results relate only with very specific characteristics of the initial database, but we believe that they can point out to interesting ways to use this kind of data depending on the game targeted. As an example, we can improve the keystroke dynamics results by adding the information about the "combos" used by the users, and, we can improve the classification by performing a correlation analysis of the features already extracted and used. Thus, we believe that the new proposed analysis can give some directions on how it is possible to benefit by understanding the dynamics of the game playing and biometric data.

5 Conclusion

This paper presented a proposed new way to use biometric-based keystroke and mouse dynamics in order to guarantee the authenticity of game users in the online game League of Legends. We have proposed a new protocol for the game data collection as well as presented a set of possible features that could be used in the identification system.

The literature presents a few mouse or keystroke dynamics

[4] www.cs.waikato.ac.nz/ml/weka/

databases using a fixed task and a controlled computer environment to collect their data. Despite the fact that this can provide a better result, it does not reflect a real situation if we wanted to use the system for a continuous identification. Based on the preliminary analysis of the initial features, it is possible to note that some are more representative than others. Thus, we are able to decide not to use the features with low representatives, therefore improving the classification performance without losing precision.

We understand that this is a very initial data analysis and identification results, but we consider that this pioneer data proposal will have a big impact on the different ways we can use biometrics data in the future.

References

[1] A. Arya. An optimal algorithm for approximate nearest neighbors searching fixed dimensions. *Journal of ACM*, 45(6):891–923, 1998.

[2] F. Bergadano, D. Gunetti, and C. Picardi. User authentication through keystroke dynamics. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):367–397, 2002.

[3] S. Bhatt and T. Santhanam. Keystroke dynamics for biometric authentication a survey. In *International Conference on Pattern Recognition Informatics and Mobile Engineering*, PRIME, pages 17–23, February 2013.

[4] P. Bours and C.J. Fullu. A login system using mouse dynamics. In *The 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IIH-MSP, pages 1072–1077, Sept 2009.

[5] Z. Cai, Z. Shen, and C. Guan. Mitigating behavioral variability for mouse dynamics: A dimensionality-reduction-based approach. *IEEE Transactions on Human-Machine Systems*, 44(2):244–255, April 2014.

[6] R. Giot, M. El-Abed, and C. Rosenberger. Greyc keystroke: A benchmark for keystroke dynamics biometric systems. In *The IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, BTAS 2009, pages 1–6, September 2009.

[7] S. Haykin. *Neural networks: a comprehensive foundation*, volume 13. Cambridge University Press, New York, NY, USA, 1999.

[8] S.-S. Hwang, H.-J. Lee, and S. Cho. Account-sharing detection through keystroke dynamics analysis. *International Journal of Electronic Commerce*, 14(2):109–126, December 2009.

[9] S.Z.S. Idrus, E. Cherrier, C. Rosenberger, and P. Bours. Soft biometrics database: A benchmark for keystroke dynamics biometric systems. In *International Conference of the Biometrics Special Interest Group*, BIOSIG 2013, pages 1–8, September 2013.

[10] S.Z.S. Idrus, E. Cherrier, C. Rosenberger, S. Mondal, and P. Bours. Keystroke dynamics performance enhancement with soft biometrics. In *IEEE International Conference on Identity, Security and Behavior Analysis*, ISBA, pages 1–7, March 2015.

[11] Z. Jorgensen and T. Yu. On mouse dynamics as a behavioral biometric for authentication. In *The 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, pages 476–482, New York, NY, USA, 2011. ACM.

[12] Y. Li, Y. Zhang, Y. Cao, S. Zhao, Y. Gao, and J. Liu. Study on the beihang keystroke dynamics database. In *2011 International Joint Conference on Biometrics*, IJCB, pages 1–5, October 2011.

[13] C-C. Lin, C-C. Chang, and D. Liang. A new non-intrusive authentication approach for data protection based on mouse dynamics. In *International Symposium on Biometrics and Security Technologies*, ISBAST, pages 9–14, March 2012.

[14] S. Mandujano and R. Soto. Deterring password sharing: user authentication via fuzzy c-means clustering applied to keystroke biometric data. In *The 5th Mexican International Conference in Computer Science*, ENC, pages 181–187, September 2004.

[15] S. Mondal and P. Bours. Continuous authentication using mouse dynamics. In *International Conference of the Biometrics Special Interest Group*, BIOSIG 2013, pages 1–12, September 2013.

[16] S. Mondal and P. Bours. Combining keystroke and mouse dynamics for continuous user authentication and identification. In *IEEE International Conference on Identity, Security and Behavior Analysis*, ISBA, pages 1–8, February 2016.

[17] 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, Part A: Systems and Humans*, 40(6):1345–1353, November 2010.

[18] C. Nello and S.T. John. An introduction to support vector machines and other kernel-based learning methods. *Robotics*, 18(6):687–689, 2000.

[19] J. Roth, X. Liu, and D. Metaxas. On continuous user authentication via typing behavior. *IEEE Transactions on Image Processing*, 23(10):4611–4624, October 2014.

[20] B. Sayed, I. Traore, I. Woungang, and M.S. Obaidat. Biometric authentication using mouse gesture dynamics. *IEEE Systems Journal*, 7(2):262–274, June 2013.

[21] J. Shelton, J. Adams, D. Leflore, and G. Dozier. Mouse tracking, behavioral biometrics, and gefe. In *Proceedings of IEEE Southeastcon*, pages 1–6, April 2013.

[22] C. Shen, Z. Cai, and X. Guan. Continuous authentication for mouse dynamics: A pattern-growth approach. In *The 2012 42Nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, DSN, pages 1–12, Washington, DC, USA, 2012. IEEE Computer Society.

[23] C. Shen, Z. Cai, X. Guan, and J. Cai. A hypo-optimum feature selection strategy for mouse dynamics in continuous identity authentication and monitoring. In *IEEE International Conference on Information Theory and Information Security*, ICITIS, pages 349–353, Dec 2010.

[24] C. Shen, Z. Cai, X. Guan, and R. Maxion. Performance evaluation of anomaly-detection algorithms for mouse dynamics. *Journal Computers and Security*, 45:156–171, Sepember 2014.

[25] C. Shen, Z. Cai, X. Guan, H. Sha, and J. Du. Feature analysis of mouse dynamics in identity authentication and monitoring. In *The 2009 IEEE International Conference on Communications*, ICC, pages 673–677, Piscataway, NJ, USA, 2009. IEEE Press.

[26] C. Shen, Z. Cai, R.A. Maxion, G. Xiang, and X. Guan. Comparing classification algorithm for mouse dynamics based user identification. In *IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems*, BTAS, pages 61–66, September 2012.

[27] R. Thanganayagam and A. Thangadurai. Fusion approach on keystroke dynamics to enhance the performance of password authentication. In *International Conference on Electrical, Computer and Communication Technologies*, ICECCT, pages 1–6, March 2015.

[28] 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. In *The 4th International Conference on Digital Home*, ICDH, pages 138–145, November 2012.