2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), and 2015 IEEE 12th International Conf on Embedded Software and Systems (ICESS)

Authentication and Identification Methods Used in Keystroke Biometric Systems

Md Liakat Ali*, Charles C. Tappert†, Meikang Qiu‡, and John V. Monaco§
Seidenberg School of Computer Science and Information Systems
Pace University, Pleasantville, NY 10570, USA
*Email: *ma03901n@pace.edu, †ctappert@pace.edu, ‡mqiu@pace.edu, §jmonaco@pace.edu*

***Abstract*—Keystroke dynamics authentication is not as widely used compared to other biometric systems. In recent years, keystroke dynamic authentication systems have gained interest because of low cost and integration with existing security systems. Many different methods have been proposed for data collection, feature representation, classification, and performance evaluation. The work presents a detailed survey of the most recent research in keystroke dynamic authentication. Research is evaluated by the conditions under which data was collected, classification algorithms used, and system performance. This work also identifies some shortcomings of the current research issues that need to be addressed for keystroke dynamics to mature. Some recommendations for future research are made, with the goal of improving keystroke dynamics system performance and robustness.**

***Keywords*-Keystroke dynamics, authentication, identification, biometrics, classification, machine learning;**

I. Introduction

Computers have become a staple in our everyday lives. We heavily depend on computers to store and process sensitive information. Intruders are everywhere, and capable of attacking an individual's or large organization. As a result, keeping information secure from intruders has become a central question in computer security. It would be desirable to develop a foolproof measure against unauthorized access of information.

User authentication is one of the first lines of defense in preventing unauthorized access. Password-based authentication is by far the most common method to protect data from intruders. Although some password rules, such as the combination of capital letters, special character(s), and digit(s), make them it hard to crack, these are also difficult for the user to remember. Additional mechanisms are needed to enhance or replace the security of password-based authentication.

Like written signatures, typing patterns contain individually-unique neuro-physiological patterns. Biometric recognition based a users typing rhythm is not only noninvasive, but also cheap and transparent [49]. Moreover, it is very easy to capture data as keyboards are common and no special hardware is necessary. Data can be also be captured after the initial authentication for in-application continuous authentication.

Keystroke dynamics have advantages such as low cost, transparency to the user, and being noninvasive, as well as being able to provide continuous authentication. However, the main disadvantage of keystroke dynamics is low accuracy when compared to other biometric systems [71]. Current research aims at improving the accuracy in the keystroke biometric authentication systems. This study outlines the design and performance of existing keystroke biometric systems by considering factors such as: how the data is captured, preprocessing and feature extraction methods, and classification algorithms. By understanding the performance and limitations of various existing systems, this work proposes some guidelines to enhance the accuracy and performance of keystroke dynamics biometric system.

The structure of this paper is as follows. Section II depicts some related works in surveying biometric authentication system. Section III explains the keystroke biometric authentication system and evaluation criteria. Section IV includes the finding of this survey and compares different classification methods. Finally, Section V concludes the survey with recommendations and future research directions.

II. Meta-Survey

Using keystroke dynamics (KD) for authentication is a relatively new concept compared to other biometric systems, and there have been several other survey works on this topic. In mid 2004, A. Peacock et al. [55] evaluated KD systems based on classifier accuracy, usability, and privacy. They suggested that performance of a KD system is greatly influenced by the number of samples. They also recommended the creation of public datasets and introduction of schemes that ensure privacy of collected data.

Another KD survey was conducted by H. Crawford [14] in 2010. The author reviewed a representative subset of concurrent research in KD and provided recommendations for future work. The survey found that high quality results from different researchers were obtained by neural network pattern classification. The study also recommended not to use same participants as both authorized and unauthorized users when evaluating system performance.

An extensive survey of KD research was conducted by S. P. Banerjee [6] in 2012. The survey compared different algorithms used in KD systems and discussed explicitly the factors that affect system performance. The study concluded that KD authentication systems have potential to grow in the

978-1-4799-8937-9/15 $31.00 © 2015 IEEE
DOI 10.1109/HPCC-CSS-ICESS.2015.66

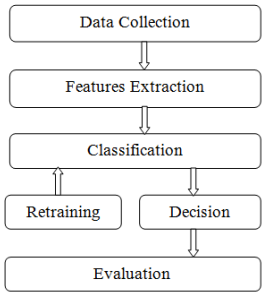

Figure 1. Typical keystroke dynamics authentication system architecture.

area of cyber-security and biometric monitoring since it is both non-intrusive and cost-effective.

A similar surveying of KD research was conducted by Teh et al. [71] in 2013, where the authors claimed that KD is unlikely to replace existing authentication mechanisms entirely. They concluded that some properties, such as the ability to operate in stealth mode, low cost, high user acceptance, and ease of integration with existing security systems, made KD promising.

III. Keystroke Dynamics Overview

A typical KD authentication system consists of six components including: data collection, feature extraction, feature classification/matching, decision making, retraining, and evaluation. Figure 1 shows an overview of a typical KD authentication system.

Data collection is the first step in any KD system. Raw data can be collected via various types of keyboard. Previous KD systems have collected data using devices ranging from normal keyboard [48, 45] to pressure sensitive keyboards [51]. Refs. [68, 13] used a modified keyboard that can detect pressure. Other works have used a special purpose number-pad [38, 24], mobile device [11, 60] and touchscreen device [30, 2]. Due to the limited number of publicly available data sets [20, 37], many researchers collected their own data and the number of participants varies greatly. There were 1254 participants involved in [15] experiment, 118 in [74], and only 3 in [44]. Many works have used 10-20 participants [71]. Most data consist of character-based texts, although some have used purely numerical input [43], or mixed input [30]. Sample sizes are generally categorized as either short-text or long-text. Short-text can be a username [53], password [40], or pass-phrase [7], while long-text can be a paragraph [77].

After raw data is collected, it may undergo preprocessing, followed by feature extraction. Features can generally be classified into two groups: *Dwell time (DT)*, the time between the press and release of a key, and *Flight time (FT)*, the time between the press or release of two consecutive keys. There are four different types of FT features with the most common bing press-press, press-release. In some systems, three or more consecutive keystroke events are used. Other time-based features are frequency of typing errors and typing rate.

The most important step of a KD system is the *classification phase*, where extracted features are to make an authentication decision. Both statistical and machine-learning techniques have been used, with an increasing trend of machine learning over statistical. At present, the Support Vector Machine (SVM) seems to be the most popular classification method due to better higher accuracies with less computational intensity.

Although many works have not explicitly considered retraining, Hosseinzadeh et al. [28] have proposed an adaption algorithm that constantly renews a user's template. This is motivated by the possibility of a user's typing pattern to change with time and environment.

The performance of a biometric system is generally characterized by the receiver operating characteristic (ROC) curve. It can be summarized by the equal error rate (EER), the point on the curve where the fall acceptance rate (FAR) and false rejection rate (FRR) are equal. Other system evaluation criteria include efficiency, adaptability, robustness, and convenience.

IV. Survey

A. Statistical approaches

Table I summarizes KD research that has utilized a statistical approaches, such as mean, standard deviation, Euclidean distance, degree of disorder. Identification accuracy (ACC) is reported as the proportion of correctly identified users.

Gunetti et al.'s experiment focused on using the degree of disorder [26] and combination of degree of disorder, mean, and SD [25]. By combining mean and SD, they achieved less false acceptance rates but higher false rejection rate. Kang et al. [34] used a combination of k-means and Euclidian distance, with a 3.8% EER. Giot et al. [21] used Bayesian decision theory and Euclidean distance features, and achieved 4.28% EER. In another research [19], using Bayesian, Euclidean, and Hamming distance, they achieved EER 6.96%. A comparison between keystroke dynamics on personal computers and smartphones was done by Uno Andre Johansen [31]. The study concluded that the performance on smartphones is less than a MK if only timing features are used. If other smartphone sensors are used, performance became better than the MK.

B. Machine learning approaches

Table II summarizes KD systems based on pattern recognition and machine learning techniques, such as Random Forest Decision Tree, SVM, and k-nearest neighbor, while Table III summarizes works that have used neural networks. Some works have implemented new approaches [4] using

Table I
AUTHENTICATION AND IDENTIFICATION BASED ON STATISTICAL APPROACHES

Paper	Year	Participants	Features	Freedom	Type	Method	Device	Result (%)
[32]	1990	33	FT	Yes	Short	Mean, STD	MK	FAR: 0.25, FRR:16.36
[48]	1997	31	DT, FT	Yes	-	Weighted mean, STD	MK	ACC: 90
[25]	2005	205	FT	Yes	Long	Degree of Disorder, Mean, STD	MK	FAR: 0.5, FRR: 5
[26]	2005	31	FT	Yes	Long	Degree of Disorder	MK	FAR: 1.99, FRR: 2.42
[74]	2006	118	DT, FT	Yes	Long	Euclidian Distance	-	ACC: 97.9
[24]	2008	30	DT, FT, P	-	Digit	Euclidian Distance	NP	FAR: 15, FRR: 0, EER: 10
[11]	2009	30	-	-	Text	Statistical	MP	EER: 13
[44]	2009	3	-	-	Digit	Mean, STD	MP	ACC: 90
[21]	2009	16	DT,FT	No	Short	Bayesian, Euclidean	MK	EER: 4.28
[36]	2010	51	DT, FT	No	Short	Manhattan distance	MK	EER: 7.1
[62]	2011	189	DT, FT	No	Long	Weighted Euclidian, array disorder	MK	FAR: 0.01, FRR: 3
[33]	2011	51	FT	No	Long	Euclidian Distance	MK	EER: 0.84
[66]	2011	20	FT	No	Long	Euclidian Distance	MK	FAR: 2, FRR: 4
[56]	2011	50	FT	No	Long	Degree of Disorder	MK	EER: 10
[31]	2012	42	DT, FT, P	-	Digit	Degree of Disorder	MK, TS	Better: MK(timing feature)

Table II
AUTHENTICATION AND IDENTIFICATION BASED ON PATTERN RECOGNITION AND MACHINE LEARNING APPROACHES

Paper	Year	Participants	Features	Freedom	Type	Method	Device	Result (%)
[17]	1980	7	FT	No	Long	t-Test	MK	ACC: 95
[7]	1990	26	FT	Yes	Short	Baysian, Minimum Distance classifier	MK	FAR: 2.8, FRR: 8.1
[58]	1998	10	DT, FT	Yes	Short	Inductive Learning Classifier	MK	FAR: 9, EER: 10
[49]	2000	63	DT, FT	Yes	-	KNN	MK	ACC: 83.2-92.1
[29]	2002	7	DT, FT	-	Digit	KNN, MLP	NP	EER: 78-99
[75]	2003	21	DT, FT	Yes	Short	MLP, SVM	MK	FAR:0, FRR: 0.814
[51]	2004	41	DT, FT	No	Short	Random forest decision tree	MK	EER: 2
[28]	2004	41	DT, FT	Yes	Short	Gaussian mixture modeling	MK	FAR: 4.3, FRR 4.8, EER: 4.4
[38]	2005	9	DT, FT,P	-	Digit	ANOVA	MK	EER: 2.4
[59]	2006	20	-	-	Digit	Hidden Markov model	MK	EER: 3.6
[57]	2007	30	DT, FT	No	Short	Sequence alignment algorithms	MK	FAR: 0.2, FRR: 0.2, EER: 0.4
[34]	2007	21	DT, FT	Yes	Short	k-means, Euclidian	MK	EER: 3.8
[3]	2007	24	DT, FT	Yes	Long	SVM	MK	FAR: 0.76, FRR: 0.81, EER: 1.57
[42]	2007	5	P	-	Digit	SVM	MK	FAR: 0.95,FRR: 5.6
[69]	2010	35	FT	No	Long	Kolmogorov-Smirnov	MK	EER: 7.55
[65]	2010	21	DT, FT	Yes	Long	Random forest decision tree	MK	FAR:3.47, FRR:0, EER: 1.73
[43]	2010	28	DT, FT	-	Digit	Random forest decision tree	MK	FAR: 0.03, FRR: 1.51, EER:1
[76]	2010	120	DT, FT	-	-	KNN	MK	EER: 1.00
[70]	2010	100	DT, FT	Yes	Text	KNN, Euclidian	MK	EER:2.7
[45]	2011	55	-	Yes	Long	Spearmans's foot rule distance metric	-	FAR: 2.02, FRR: 1.84
[72]	2011	100	DT, FT	No	Short	Gaussian PDF, Direction similarity measure	MK	EER: 1.401
[67]	2011	30	DT,FT	No	Digit	KNN	-	EER: 0.5
[39]	2011	117	DT, FT	Yes	Short	SVM	MK	EER: 11.83
[23]	2011	100	DT, FT	No	Short	SVM	MK	EER: 15.28
[5]	2011	33	DT, FT	No	Long	Naive Bayesian	MK	EER: 1.72
[46]	2013	40	-	-	-	KNN, Euclidian Distance	MK	ACC: 88.2-91.5
[73]	2013	152	FT, DT, P, FA	-	Digit	k-means	MP	FAR: 4.19, FRR: 4.59
[18]	2014	300	FT, DT	-	Short	SVM	TS	TPR= 92, FPR= 1
[30]	2014	30	FT, DT, P, FA	No	Digit	SVM	MK, TS	EER (MK): 10.5, EER (TS): 2.8

MK - Mechanical Keyboard, MP - Mobile Platform, TS - Touchscreen, NP - Number Pad, STD - Standard Deviation, LVQ - Linear Vector Quantization

different methods. Table IV summarizes the works that have used a combination of different algorithms.

Harun et al. [27] used a Multilayer Perceptron (MLP) neural network to recognize authentic users and reject impostors with more than 80% accuracy. Antal et al. [2] examined keystroke data with and without touchscreen-based features (pressure and finger area). Performance was obtained using several algorithms, such as Nave Bayes, Bayesian Network, C4.5(J48), K-NN(IBk), SVM, Random forest, and MLP. The best performance was achieved by Random forest, Bayesian nets, and SVM respectively. The addition of touchscreen-based features to timing features increased accuracy by 10% for each classifier. The study showed that the lowest error (12.9%) was obtained by Manhattan distance using both timing and touchscreen-based features. Similar to Antal et al. findings, Jain et al. [30] studied the combination of timing and non-timing features. Data was collected from 30 participants over several days and one-class SVM for classification. They achieved a 10.5% EER using timing features, 3.5% EER using non-timing touchscreen features, and 2.8% EER using all features. The result suggests that performance on a smartphone touchscreen is superior to that on hardware keyboards.

Zack et al. [76] developed a long-text input KD system that collected data over the Internet. They collected data from 120 participants and achieved a 1% EER. Higher performance was obtained with a closed system of known users than an open system. A similar experiment was conducted by Maxion et al. [43], where 28 users typed the same 10 digit number using only the right-hand index finger. The authors used a random forest classifier and achieved a 10% EER. Saevanee et al. [61] studied KD combined with finger

Table III
AUTHENTICATION AND IDENTIFICATION BASED ON NEURAL NETWORKS

Paper	Year	Participants	Features	Freedom	Type	Method	Device	Result (%)
[8]	1993	24	FT	Yes	Short	Perceptron	MK	FAR: 8, FRR: 9
[12]	1999	10	DT, FT	-	Short	RBFN	MK	ACC: 97
[54]	2007	100	DT, FT	No	Short	MLP	MK	FAR:1, EER: 8
[41]	2007	100	DT, FT, P	-	-	ARTMAP-FD	MK	EER:11.78
[13]	2007	32	FT	Yes	Long	FF MLP	MP	EER: 12.8
[61]	2009	10	DT,FT,P	-	Digit	Probabilistic Neural Network	TS	EER: 1
[68]	2009	30	DT, FT,P	-	-	RBFN	MK	FAR: 2
[1]	2009	7	P	-	-	Multilayer feed Forward	MK	FAR:0, FRR: 0
[35]	2010	25	FT, DT	-	Digit	Back Propagation NN	MK	ACC: 92.8
[50]	2010	20	DT, FT, P	-	-	Fast ANN	MK	FAR: 4.12, FRR: 5.55
[16]	2014	13	FT, DT, P, FA	-	-	ANN	TS	FAR: 14 FRR: 2.2

Table IV
AUTHENTICATION AND IDENTIFICATION BASED ON HEURISTICS AND COMBINATION OF DIFFERENT ALGORITHMS

Paper	Year	Participants	Features	Freedom	Type	Method	Device	Result (%)
[52]	1995	15	DT, FT	Yes	Short	ART-2, RBFN, LVQ	MK	EER: 0
[64]	2005	43	DT, FT	No	Long	Decision trees, Monte Carlo	MK	FAR: 0.88, FRR: 9.62
[77]	2006	-	DT,FT	No	Long	Decision tree c4.5.j48	MK	ACC: 93.3
[10]	2006	20	-	-	Digit	Euclidian, Mahalanobis, FF-MLP	TS	FAR: 0, FRR: 2.5
[60]	2009	25	DT, FT	Yes	Short	Gauss, Parzen, K-NN, K-mean	MK	EER: 1.00
[22]	2009	100	DT, FT	No	Short	Bayesian, Euclidean, Hamming distance	MK	EER: 6.96
[4]	2013	30	-	Yes	Long	Dichotomy Classifier, LOOCV	-	EER(Pass): 8.7, EER(Num): 6.1
[2]	2014	42	FT, DT, P, FA	No	Short	Naive, Bayesian, C4.5(J48), KNN, SVM, MLP, Random forest	MP	EER: 12.9
[63]	2014	10	P	-	digits	J48, Naive Bayes,K*, MLP	TS	ACC: 84.2

MK - Mechanical Keyboard, MP - Mobile Platform, TS - Touchscreen, NP - Number Pad, STD - Standard Deviation, LVQ - Linear Vector Quantization, RBFN - Radial Basis Function Network, MLP - Multilayer Perceptron

pressure. The study showed a 99% ACC was achieved using finger pressure. Since each user entered a different phone number, only the FRR could be measured.

C. Limitations

Many works used a small number of participants, and they were mainly students, researchers, or academic staff. None of the researches were conducted on users with low typing proficiency. Touchscreen features such as pressure and finger area, have only been considered under tightly controlled environments, and ignore such effects as using different devices. In many works, data was collected in only one session. Most research ignores template aging, and it is not clear how the system would perform over time as a user's behavior changes. Many researchers have collected their own data because publicly available KD benchmark databases are very limited. Many studies used fixed text and the same keyboard for enrollment and testing. Researchers sometimes fail to justify a choice of algorithm for classification and verification and provide no explanation one method is superior to other.

V. RECOMMENDATIONS

Most KD studies have used subjects from institutes, including students and faculty. This subset is unlikely to be representative of the greater population. Additionally, the consideration of other demographic factors, such as age, gender, and education level, may help understand and predict the performance of a KD system. One of the key points for better performance in a KD system is introducing new classification algorithms and feature engineering. Features should be designed to be platform-independent. As more sensors are considered, fusing data from various sources also becomes a problem.

Many researchers have not paid attention to the computational cost of training and testing a KD system. A robust KD system should be responsive, especially if the application requires real-time interaction. Several works have been conducted on free or long text input, but they have used only English as the primary language of communication. An investigation of the portability to other languages is warranted. Future research should also place greater emphasis on mobile devices with a vast array of sensors. Many devices support multi-touch screens, pressure sensitive panels, accelerometers, and gyroscopes, all of which could be incorporated into a KD system.

Data collection in most studies was performed over a relatively short period of time. The typing behavior of individuals may change due to age, health condition, or emotional state. Only recently have we seen studies that attempt to detect cognitive load from typing behavior [9] and how user handicaps affect KD system performance [47].

Finally, developing benchmark datasets for the KD authentication will be a promising future research. KD datasets should consider variables such as input device, input type, and input length, so that KD systems can be evaluated based on these criteria. Future work should also attempt to offer an explanation why a particular method achieves better performance. Development of a standardized protocol for KD systems might help make different works comparable. KD research is still in the initial stage and a very limited number of researches have been conducted so far compared

to other biometric systems. Although it has advantages such as low cost, transparency, noninvasive for the user, and continuous authentication, it has low accuracy compared to other biometric systems.

REFERENCES

[1] H. Ali, W. Wahyudi, and M. J. E. Salami. "Keystroke pressure based typing biometrics authentication system by combining ANN and ANFIS-based classifiers". In: *Proceedings of the 5th International Colloquium on Signal Processing and Its Applications (CSPA 09)*. Vol. 1. Kuala Lumpur, Mar. 2009, pp. 198–203. DOI: 10.1109/CSPA.2009.5069216.

[2] M. Antal, L. Z. Szabo, and I. Laszlo. "Keystroke Dynamics on Android Platform". In: *INTER-ENG 2014, 8th international Conference Inerdisciplinarity in Engineering*. Tirgu Mures, Romania: Elsevier, Oct. 2014, pp. 114–119.

[3] G. L. F. Azevedo, G. D. C. Cavalcanti, and E. C. B. Filho. "An approach to feature selection for keystroke dynamics systems based on PSO and feature weighting". In: *Proceedings of the IEEE Congress on Evolutionary Computation (CEC 07)*. Singapore, Sept. 2007, pp. 3577–3584. DOI: 10.1109/CEC.2007.4424936.

[4] Ned Bakelman, Sung-Hyuk Cha John V. Monaco, and Charles C. Tapper. "Keystroke Biometric Studies on Password and Numeric Keypad Input". In: *Proceedings of the 2013 European Intelligence and Security Informatics Conference(EISIC '13)*. 2013, pp. 204–207. ISBN: 978-0-7695-5062-6. DOI: 10.1109/EISIC.2013.45.

[5] K. S. Balagani et al. "On the discriminability of keystroke feature vectors used in fixed text keystroke authentication". In: *Pattern Recognition Letters* 32.7 (2011), pp. 1070–1080.

[6] S. Banerjee and D. Woodard. "Biometric Authentication and Identification using Keystroke Dynamics: A Survey". In: *Journal of Pattern Recognition Research* 7.1 (July 2012), pp. 116–139.

[7] S. Bleha, C. Slivinsky, and B. Hussien. "Computer-access security systems using keystroke dynamics". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 12.12 (1990), pp. 1217–1222.

[8] S. A. Bleha and M. S. Obaidat. "Computer users verification using the perceptron algorithm". In: *IEEE Transactions on Systems, Man and Cybernetics* 23.3 (1993), pp. 900–902.

[9] David Guy Brizan et al. "Utilizing linguistically-enhanced keystroke dynamics to predict typist cognition and demographics". In: *International Journal of Human-Computer Studies* (2015).

[10] A. Buchoux and N. Clarke. "Deployment of Keystroke Analysis on a Smartphone". In: *Proceedings of the 6th Australian Information Security Management Conference*. Perth, Western Australia, Dec. 2006.

[11] P. Campisi et al. "User authentication using keystroke dynamics for cellular phones". In: *IET Signal Processing* 3.4 (2009), pp. 333–341.

[12] N. Capuano et al. "User Authentication With Neural Networks". In: *Proceedings of the 5th International Conference on Engineering Applications of Neural Networks (EANN 99)*. Warsaw, Poland, Sept. 1999, pp. 200–205.

[13] N. L. Clarke and S. M. Furnell. "Authenticating mobile phone users using keystroke analysis". In: *International Journal of Information Security* 6.1 (2007), pp. 1–14.

[14] H. Crawford. "Keystroke dynamics: characteristics and opportunities". In: *Proceedings of the 8th International Conference on Privacy, Security and Trust (PST 10)*. Aug. 2010, pp. 205–212.

[15] S. Douhou and J. R. Magnus. "The reliability of user authentication through keystroke dynamics". In: *Statistica Neerlandica* 63.4 (June 2009), pp. 432–449.

[16] B. Draffin, J. Zhu, and J. Zhang. *KeySens: Passive User Authentication through Micro-behavior Modeling of Soft Keyboard Interaction*. Vol. 130. Springer International Publishing, 2014, pp. 184–201. DOI: 10.1007/978-3-319-05452-0_14.

[17] R. S. Gaines et al. *Authentication by keystroke timing: some preliminary results*. Tech. rep. Calif, USA: R-2526-NFS,Rand Conporation,Santa Monica, 1980.

[18] H. Gascon et al. "Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior". In: *Proc. of GI Conference Sicherheit*. Vol. P-228. Mar. 2014, pp. 1–12.

[19] R. Giot, B. Dorizzi, and C. Rosenberger. "Analysis of template update strategies for keystroke dynamics". In: *Proceedings of the IEEE Workshop on Computational Intelligence in Biometrics and Identity Management (CIBIM 11)*. Apr. 2011, pp. 21–28.

[20] R. Giot, M. El-Abed, and C. Rosenberger. "GREYC keystroke: a benchmark for keystroke dynamics biometric systems". In: *Proceedings of the IEEE 3rd International Conference on Biometrics: Theory, Applications and Systems (BTAS 09)*. Sept. 2009, pp. 1–6. DOI: 10.1109/BTAS.2009.5339051.

[21] R. Giot, M. El-Abed, and C. Rosenberger. "Keystroke dynamics authentication for collaborative systems". In: *Proceedings of the International Symposium on Collaborative Technologies and Systems (CTS 09)*. May 2009, pp. 172–179.

[22] R. Giot, M. El-Abed, and C. Rosenberger. "Keystroke dynamics with low constraints SVM based passphrase enrollment". In: *Proceedings of the IEEE 3rd International Conference on Biometrics: Theory, Applications and Systems (BTAS 09)*. Washington, DC, Sept. 2009, pp. 1–6. DOI: 10.1109/BTAS.2009.5339028.

[23] R. Giot et al. "Unconstrained keystroke dynamics authentication with shared secret". In: *Computers and Security* 30.6-7 (2011), pp. 427–445.

[24] N. J. Grabham and N. M. White. "Use of a novel keypad biometric for enhanced user identity verification". In: *Proc. IEEE International Instrumentation and Measurement Technology Conference(IMTC08)*. IEEE, May 2008, pp. 12–16.

[25] D. Gunetti and C. Picardi. "Keystroke analysis of free text". In: *ACM Transactions on Information and System Security* 8.3 (2005), pp. 312–347.

[26] D. Gunetti, C. Picardi, and G. Ruffo. "Keystroke analysis of different languages: a case study". In: *Advances in Intelligent Data Analysis VI*. Vol. 3646 Lecture notes in Computer Science. Berlin, Germany: Springer, 2005, pp. 133–144.

[27] N. Harun, S. S. Dlay, and W. L. Woo. "Performance of keystroke biometrics authentication system using Multilayer Perceptron neural network (MLP NN)". In: *7th International Symposium on Communication Systems Networks and Digital Signal Processing (CSNDSP' 2010)*. Newcastle upon Tyne: IEEE, July 2010, pp. 711–714.

[28] D. Hosseinzadeh and S. Krishnan. "Gaussian mixture modeling of keystroke patterns for biometric applications". In: *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews* 8.6 (Nov. 2008), pp. 816–826. ISSN: 1094-6977.

[29] J. Koivumaki J. Mantyjarvi and P. Vuori. "Keystroke recognition for virtual keyboard". In: *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME 02)*. Vol. 2. 2002, pp. 429–432.

[30] L. Jain et al. "Passcode keystroke biomentric performance on touchscreen is superior to that on hardware keyboards". In: *International journal of Research in computer applications and information technology* 2.4 (2014), pp. 29–33. ISSN: 2347-5099 (online).

[31] Uno Andre Johansen. "Keystroke Dynamics on a Device with Touch Screen". MA thesis. Norway: Gjvik University College, June 2012. URL: http://hdl.handle.net/11250/143992.

[32] R. Joyce and G. Gupta. "Identity authentication based on keystroke latencies". In: *Communications of the ACM* 33.2 (Feb. 1990), pp. 168–176.

[33] Y. Kaneko, Y. Kinpara, and Y. Shiomi. "A hamming distance-like filtering in keystroke dynamics". In: *Proceedings of the Ninth Annual International Conference on Privacy, Security and Trust (PST '11)*. Montreal, QC, July 2011, pp. 93–95. DOI: 10.1109/PST.2011.5971969.

[34] Pilsung Kang, Seong seob Hwang, and Sungzoon Cho. "Continual Retraining of Keystroke Dynamics Based Authenticator". In: *ICB'07 Proceedings of the 2007 international conference on Advances in Biometrics*. Vol. 4642. Berlin, Germany, 2007, pp. 1203–1211.

[35] M. Karnan and M. Akila. "Personal Authentication Based on Keystroke Dynamic using Soft Computing Techniques". In: *Second International Conference on Communication Software and Networks (CCSN '10)*. Singapore, Feb. 2010, pp. 334–338. DOI: 10.1109/ICCSN.2010.50.

[36] K. Killourhy and R. Maxion. "Why did my detector do that?!:predicting keystroke-dynamics error rates". In: *Proceedings of the 13th international conference on Recent advances in intrusion detection(RAID'10)*. Ottawa, Canada, 2010, pp. 256–276.

[37] K. S. Killourhy and R. A. Maxion. "Comparing anomalydetection algorithms for keystroke dynamics". In: *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 09)*. July 2009, pp. 125–134.

[38] K. Kotani and K. Horii. "Evaluation on a keystroke authentication system by keying force incorporated with temporal characteristics of keystroke dynamics". In: *Behaviour and Information Technology* 24.4 (2005), pp. 289–302.

[39] Y. Li et al. "Study on the BeiHang keystroke dynamics database". In: *Proceedings of the International Joint Conference on Biometrics (IJCB 11)*. Oct. 2011, pp. 1–5.

[40] Daw-Tung Lin. "Computer-access authentication with neural network based keystroke identity verification". In: *Proceedings of the 1997 IEEE International Conference on Neural Networks*. Vol. 1. June 1997, pp. 174–178.

[41] C. C. Loy et al. "Keystroke patterns classification using the ARTMAP-FD neural network". In: *Proceedings of the 3rd International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 07)*. Vol. 1. Kaohsiung, Nov. 2007, pp. 61–64. DOI: 10.1109/IIH-MSP.2007.218.

[42] W. Martono, H. Ali, and M. J. E. Salami. "Keystroke pressurebased typing biometrics authentication system using support vector machines". In: *Proceedings of the 2007 International Conference on Computational Science and Its Applications: Volume Part II*. Kuala Lumpur, Malaysia, Aug. 2007, pp. 85–93.

[43] R. A. Maxion and K. S. Killourhy. "Keystroke biometrics with number-pad input". In: *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 10)*. July 2010, pp. 201–210.

[44] I. V. McLoughlin and M. S. O. N. Naidu. "Keypress biometrics for user validation in mobile consumer devices". In: *Proc. IEEE 13th International Symposium onConsumer Electronics(ISCE09)*. May 2009, pp. 280–284.

[45] A. Messerman et al. "Continuous and non-intrusive identity verification in realtime environments based on free-text keystroke dynamics". In: *Proceedings of the International Joint Conference on Biometrics (IJCB 11)*. Washington, DC, Oct. 2011, pp. 1–8.

[46] J. V. Monaco et al. "Behavioral biometric verification of student identity in online course assessment and authentication of authors in literary works". In: *Proceedings of IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS 2013)*. Arlington, VA, Sept. 2013, pp. 1–8. DOI: 10.1109/BTAS.2013.6712743.

[47] John V Monaco et al. "One-handed Keystroke Biometric Identification Competition". In: *Proceedings of the 8th International Conference on Biometrics (ICB)*. 2015.

[48] F. Monrose and A. Rubin. "Authentication via keystroke dynamics". In: *Proceedings of the 4th ACM Conference on Computer and Communications Security*. Zurich, Switzerland, Apr. 1997, pp. 48–56.

[49] F. Monrose and A. D. Rubin. "Keystroke dynamics as a biometric for authentication". In: *Future Generation Computer Systems* 16.4 (2000), pp. 351–359.

[50] T. T. Nguyen, T. H. Le, and B. H. Le. "Keystroke dynamics extraction by independent component analysis and bio-matrix for user authentication". In: *Proceedings of the 11th Pacific Rim International Conference on Trends in Artificial Intelligence*. Vol. 6230. Daegu, Republic of Korea, Sept. 2010, pp. 477–486.

[51] H. Nonaka and M. Kurihara. "Sensing pressure for authentication system using keystroke dynamics". In: *Proceedings of the International Conference on Computational Intelligence*. Istanbul, Turkey, Dec. 2004, pp. 19–22.

[52] M. S. Obaidat. "Verification methodology for computer systems users". In: *Proceedings of the 1995 ACM Symposium on Applied Computing*. Feb. 1995, pp. 258–262.

[53] M. S. Obaidat and B. Sadoun. "Verification of computer users using keystroke dynamics". In: *IEEE Transactions on Systems, Man, and Cybernetics B* 27.2 (1997), pp. 261–269.

[54] N. Pavaday and K. M. S. Soyjaudah. "Investigating performance of neural networks in authentication using keystroke dynamics". In: *Proceedings of the IEEE AFRICON 2007 Conference*. Sept. 2007, pp. 1–8.

[55] A. Peacock, X. Ke, and M. Wilkerson. "Typing patterns: a key to user identification". In: *IEEE Security and Privacy* 2.5 (2004), pp. 40–47.

[56] K. A. Rahman, K. S. Balagani, and V. V. Phoha. "Making impostor pass rates meaningless: a case of snoop-forge-replay attack on continuous cyber-behavioral verification with keystrokes". In: *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW 11)*. Colorado Springs, CO, June 2011, pp. 31–38. DOI: 10.1109/CVPRW.2011.5981729.

[57] Kenneth Revett, Srgio Tenreiro de Magalhes, and Henrique M. D. Santos. "On the use of rough sets for user authentication via keystroke dynamics". In: *Proceedings of the Portuguese Conference on Artificial Intelligence (EPIA 07)*. Guimares, Portugal, Dec. 2007, pp. 145–159. DOI: 10.1007/978-3-540-77002-2_13.

[58] J. A. Robinson et al. "Computer user verification using login string keystroke dynamics". In: *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans* 28.2 (1998), pp. 236–241.

[59] Ricardo N. Rodrigues et al. "Biometric Access Control Through Numerical Keyboards Based on Keystroke Dynamics". In: *Proceedings of the 2006 international conference on Advances in Biometrics (ICB'06)*. Vol. 3832. Hong Kong, China, June 2006, pp. 640–646. DOI: 10.1007/11608288_85.

[60] S. Cho S. S. Hwang and S. Park. "Keystroke dynamics-based authentication for mobile devices". In: *Computers and Security* 28.1-2 (2009), pp. 85–93.

[61] H. Saevanee and P. Bhattarakosol. "Authenticating user using keystroke dynamics and finger pressure". In: *6th IEEE Consumer Communications and Networking Conference (CCNC09)*. Las Vegas, NV: IEEE, Jan. 2009, pp. 1–2. DOI: 10.1109/CCNC.2009.4784783.

[62] T. Samura and H. Nishimura. "Keystroke timing analysis for personal authentication in Japanese long text input". In: *Proceedings of the 50th Annual Conference on Society of Instrument and Control Engineers (SICE 11)*. Tokyo, japan, Sept. 2011, pp. 2121–2126.

[63] S. Sen and K. Muralidharan. "Putting Pressure on Mobile Authentication". In: *Seventh International Conference on Mobile Computing and Ubiquitous Networking (ICMU'2014)*. Singapore: IEEE, Jan. 2014, pp. 56–61. DOI: 10.1109/ICMU.2014.6799058.

[64] Y. Sheng, V. V. Phoha, and S. M. Rovnyak. "A parallel decision tree-based method for user authentication based on keystroke patterns". In: *IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics* 35.4 (2005), pp. 826–833.

[65] T. Shimshon et al. "Continuous verification using keystroke dynamics". In: *Proceedings of the International Conference on Computational Intelligence and Security (CIS10)*. Dec. 2010, pp. 411–415.

[66] S. Singh and K. V. Arya. "Key classification: a new approach in free text keystroke authentication system". In: *Proceedings of the 3rd Pacific-Asia Conference on Circuits, Communications and System (PACCS 11)*. Wuhan, July 2011, pp. 1–5. DOI: 10.1109/PACCS.2011.5990168.

[67] J. C. Stewart et al. "An investigation of keystroke and stylometry traits for authenticating online test takers". In: *Proceedings of the International Joint Conference on Biometrics (IJCB11)*. Washington, DC, Oct. 2011, pp. 1–7.

[68] A. Sulong, W. Wahyudi, and M. D. Siddiqi. "Intelligent keystroke pressure-based typing biometrics authentication system using radial basis function network". In: *Proceedings of the 5th International Colloquium on Signal Processing and Its Applications (CSPA 09)*. Mar. 2009, pp. 151–155.

[69] P. Sunghoon, P. Jooseoung, and C. Sungzoon. "User authentication based on keystroke analysis of long free texts with a reduced number of features". In: *Proceedings of the 2nd International Conference on Communication Systems, Networks and Applications (ICCSNA 10)*. Vol. 1. Hong Kong, July 2010, pp. 433–435. DOI: 10.1109/ICCSNA.2010.5588979.

[70] C. Tappert et al. "A keystroke biometric system for long-text input". In: *International Journal of Information Security and Privacy* 4.1 (2010), pp. 32–60.

[71] P. S. Teh, A. B. J. Teoh, and S. Yue. "A Survey of Keystroke Dynamics Biometrics". In: *The Scientific World Journal* 2013 (2013), pp. 1–24. DOI: 10.1155/2013/408280.

[72] P. S. Teh et al. "A multiple layer fusion approach on keystroke dynamics". In: *Pattern Analysis and Applications* 14.1 (2011), pp. 23–36.

[73] Matthias Trojahn, Florian Arndt, and Frank Ortmeier. "Authentication with Keystroke Dynamics on Touchscreen Keypads - Effect of different N-Graph Combinations". In: *MOBILITY 2013, The Third International Conference on Mobile Services, Resources, and Users*. 2013, pp. 114–119.

[74] M. Villani et al. "Keystroke biometric recognition studies on longtext input under ideal and application-oriented conditions". In: *Proceedings of the Conference on Computer Vision and Pattern Recognition Workshops (CVPRW06)*. June 2006, p. 39.

[75] E. Yu and S. Cho. "Novelty detection approach for keystroke dynamics identity verification". In: *Intelligent Data Engineering and Automated Learning*. Vol. 2690. Springer, Berlin, Germany, 2003, pp. 1016–1023.

[76] R. S. Zack, Charles C. Tappert, and Sung-Hyuk Cha. "Performance of a long-text-input keystroke biometric authentication system using an improved k-nearest-neighbor classification method". In: *Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS '2010)*. Washington, DC, USA, Sept. 2010, pp. 1–6. DOI: 10.1109/BTAS.2010.5634492.

[77] Y. Zhao. "Learning user keystroke patterns for authentication". In: *Proceedings of the World Academy of Science, Engineering and Technology*. Vol. 14. Karnataka, India, Dec. 2006, pp. 65–70.