CSEC-472 Authentication Paper

Behavioral Biometric Authentication: Current Trends and Future Needs

Jess Beckwith[1], Alan Dubie[1], Ryne Krueger[1], Matthew Turi[1], and Michael Van Leeuwen[1]

[1]Department of Computing Security, B. Thomas Golisano College of Computing and Information Science, Rochester Institute of Technology

May 12, 2021

Abstract

With the constant development of exploits, bypasses, and a lack of continual authentication, static authentication is no longer enough to ensure the safety of modern computer systems. A new element must be added to increase the effectiveness of authentication systems: behavioral biometric authentication. In this paper, we conduct a literary review of the current state of research in this area and discuss its applicability and validity. We present our findings in a table detailing important statistics across various research papers to give an overview into recent developments in the field. The patterns of high success across 87 analyzed research papers warrants further development of technologies and strategies in behavioral biometrics, particularly keystroke, touch, and mouse dynamics for use in continuous authentication. While promising, our research also demonstrates that the field must address scalability and privacy concerns before these technologies can be deployed across industry.

Keywords

behavioral biometric authentication, keystroke dynamics, touch dynamics, mouse dynamics, continuous authentication

1 Introduction

The world has a heavy reliance on "what you know" type authentication, typically through the use of PINs and passwords. These methods can be hard to remember and are insecure, as they rely on users to choose strong passphrases and not lose them. Furthermore, should they be lost or stolen, there is no sort of detection. Once authenticated, bad actors cannot be detected unless forced to re-authenticate. A key area of research that seems promising to solve this problem revolves around behavioral biometric authentication, the study of using "what you do" to authenticate users.

This type of biometrics has relatively high success rates, is cheap to implement, is scalable, and is able to easily adapt to expected changes in user behavior over time. This makes it a field worth researching, to discover future areas of need and where it currently stands.

In this paper we outline the current state of research in behavioral biometric authentication through the form of a literature review. We analyze the major types, trends, and competing algorithms and establish what norms/algorithms, if any, are currently dominant. We also indicate areas that require further investigation and will need to be thoroughly researched before industry adopts this type of authentication into production systems. We believe this type of authentication is promising as an additional authentication layer and has several use cases, especially for continuous authentication and quelling insider threats. We achieve this by summarizing our findings from 87 established research papers, as well as analyzing the dominant algorithms, type of biometric, scalability, error rates, and other essential metrics in a developed table. These help us establish the current state of research, as well as areas that are underdeveloped.

This research is constructive and imperative, as it provides a comprehensive overview into the

current state of behavioral biometrics. The research space continues to innovate and broaden, indicating a need for summarization to know what current trends, if any, have potential for actual use. Furthermore, security practitioners and industry professionals alike need to know if this type of authentication is truly secure, and if so, where it should be placed in the current authentication stack as a security layer, such as a continuous authentication mechanism. Finally, indicating needs for future research outlines current concerns with the field that must be answered before using these technologies, useful for both those implementing these systems, and for researchers who want to know what areas are ready for further investigation and contribution.

2 Background & Significance

Our research problem is one of determining the viability of biometric authentication as an enhancement to currently established authentication systems. Throughout the course of our research, we narrowed our focus to continuous keystroke dynamics biometric authentication. In our literature review we wish to answer the following questions:

- What is the status of behavioral biometric authentication in current (<5 years) research?
- Where does behavioral biometric authentication fit into existing authentication systems?
- What is the reliability and resiliency of behavioral biometric authentication authentication?
- How scalable is behavioral biometric authentication?
- What are the privacy implications, if any, of the implementation of behavioral biometric authentication?

Our shared interest in overcoming the weaknesses of static authentication motivates this study. Static authentication is a style of allowing access to a system through a single, unmoving method of verifying who a person is [1]. The most common example would be the password: you enter the right combination of characters, and you are granted access. The problem with this method is that there is no way to stop an attacker from abusing their newfound privileges: when a person is in, they are in until they decide to leave.

A solution to this problem is the inclusion of a continuous authentication system. Continuous authentication is a method to constantly verify that a person accessing a system remains who they are throughout their session [1]. If another person was to take over their session, either maliciously or not, continuous authentication would detect this change and revoke access until they could once again verify their identity.

Our initial hypothesis was that biometrics could be used as a potential implementation of continuous authentication, but we were not sure which specific method would work best. Eventually, we began to notice a pattern of potential with keystroke dynamics. Keystroke dynamics consists of people's slight quirks and differences when use a keyboard, or a touchscreen, or even a computer mouse [2]. For example, how long does a person hold down a specific key when typing? What is their average letter-typing cadence? How many words do they type on average per typing "session", with a session being any period of time of continuous interaction/typing.

Akin to a person's penmanship, there are unique (if slight) differences between people's hand movements and key presses that could be used to identify them. Since the usage of a computer system requires semi-regular input into the keyboard/touchscreen/mouse, the ability to match a user's typing quirks to their identity is a tool that can be used throughout the entire session. If a user switches halfway through, or if something not previously authenticated tries to access or manipulate the system, continuous authentication can potentially stop malicious activity before the full extent of their damage is done.

This can be incredibly useful to any business or government who wishes to keep highly sensitive information on lockdown. For organizations, continuous authentication would allow them to strengthen the security of their devices in order to overcome user weaknesses (i.e., weak passwords/PINs, shoulder surfing, disgruntled friends/family/associates). For average people, the promise that this form of authentication shows has all sorts of implications, such as ease of use, quality of life, and privacy.

We believe that this matter is pressing and worth researching as many stakeholders are involved. From the average smartphone user to government agencies attempting to negate insider threats, traditional one-factor and "what you know" authentication is no longer suitable. We seek to build on top of existing literature by generating a table as well as challenging common research topics by indicating under-researched,

yet critical issues.

Our approach to this literature review consisted of conducting online research into databases and search engines like Google Scholar and IEEE. Our database queries match the keywords of this research paper. We analysed 104 separate research papers, drawing conclusions based on those that focused on continuous keystroke dynamics authentication with patterns of similar conclusions. Our specific methodology and implications will be detailed in following sections.

3 Related Work

There has been significant research into behavior biometric authentication and the field continues to develop each year. To serve as a baseline for our understanding and analysis of current trends, as well as to consider under-searched areas, we found several literature reviews to analyze.

Recent advances in mobile touch screen security authentication methods: A systematic literature review [3] surveyed the all the different authentication methods relating to securing a mobile device. This includes authentication methods such as PIN-based authentication, pattern, gesture, biometrics, graphical passwords and others. There are a total of 67 references in this paper, 11 of which are specifically references to behavioral authentication models.

A Review of Continuous Authentication Using Behavioral Biometrics [4] is a review of papers which are related to the topic of using behavioral authentication for continuous authentication. The authors surveyed papers that used authentication methods such as walking gait, touch gestures, multi-modal biometrics, input patterns and location familiarity. They used a total of 46 references in this survey. Their conclusion is that behavioral biometrics is a promising alternative, and additional research is needed to evaluate its efficiency. We disagree that behavioral biometrics can be used as the only authentication method at this time. We believe that behavioral biometrics is best used in conjunction with another authentication method such as "something you know."

Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey [5] is a survey on using the sensors on a mobile device for continuous authentication using behavioral authentication. This survey reviews 140 papers. This includes motion based authentication, gait-based authentication, keystroke-based authentication, touch gesture-based authentication, voice-based authentication, and multi-modal authentication. The authors concluded that behavioral biometrics can be used to offer efficient continuous authentication by leveraging various embedded sensors.

Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective [6] is a review of papers that are about continuous behavioral authentication. This review goes through 167 papers. This includes methods such as keystroke, touchscreen, eye movement, gait, body gesture and others. The authors see several challenges with continuous authentication based behavioral traits. The first challenge is how behavior changes over time, the second is cross-device continuous authentication, and the third is privacy concerns. In our paper, we believe that privacy concerns will be a critical topic that requires further research.

In summary, all related works mentioned are highly detailed, many of which cover more sources than we had the ability to in our limited research timeline. Despite this, we believe that our research is necessary and constructive as these sources primarily covered existing literature and research trends, with little focus on topics within behavioral biometric authentication that require further research. We seek to both analyze existing research as well as indicate where it is lacking.

4 Research Design & Methods

We performed a literature review on a set of sources regarding behavioral biometric authentication. Experimental research sources are used to generate a table outlining types of behavioral biometrics, algorithms, error rates, etc., thus offering insight into current trends and effectiveness ratings. We also sought to analyze the content itself, with a particular interest to the benefits, where they fit in the current authentication chain (replacement, MFA, continuous authentication), etc. Furthermore, we set out to search for concerns/topics that may not be covered in current literature, such that we can propose directions needed for future practitioners and researchers.

4.1 Procedures

Our research was broken into three stages: initial, developing, and challenging. In initial research, basic behavioral authentication topics were searched for as we started to discover and

classify the prominent types of behavioral biometrics used in authentication such as keystroke, gait, etc. This stage of research was primarily used to discover the most prevalent trends for us to focus on and continue researching in the following stages. Keywords used here were generic, including but not limited to "behavioral biometric authentication", "keystroke authentication", "touch dynamics", "behavioral authentication", and "gait authentication". The second stage, developing research, honed in on our identified main types of authentication: keystrokes, touch, and mouse. We determined these by analyzing the frequency of the types that we read, and jointly decided to focus on these in order narrow the scope of our research. Finally, in challenging research we tackled more advanced topics such as scalability, usability, privacy, and attack methods. All stages contributed sources for the table, while the final stage primarily contributed to any extra concerns/areas mentioned for future resource needs.

Sources are primarily located in IEEE, Springer, and ScienceDirect, found through Google Scholar. The RIT Wallace Library is utilized to gain access to restricted academic journals. All sources have been published within the last five years. This ensured we were only looking at recent trends in literature to help enforce our recommendations for future trends, at the disadvantage of excluding some older, foundational research sources. Using this recent time window helped us to only categorize "hot" topics in behavioral biometrics, while ignoring some older, yet somewhat proven effective trends, such as gait.

Source quality is determined through a combination of the paper ranking as well as the citation count. The CORE Journal and Conference Portals are used to check the grade of each paper's conference. Most sources are analyzed if they had a B rank or higher, although some unranked or lower quality sources are still considered if the overall purpose/experiment was determined to be relevant. Relevancy is determined based on the previously discussed focuses (keystroke/touch/mouse). Should the paper's conference or journal not be found within the CORE database, H-indexes are checked. Citation counts have a less strict evaluation process: papers with higher citation counts are favored, relative to the year of release. If a paper is released in the current year or year prior, citation counts are largely ignored if they were minimal, as this did not give a proper timeline to establish the usefulness of the research.

The vast majority of sources are experimental research, as we are primarily searching for a breadth of sources utilizing various types of behavioral biometrics, algorithms, and dataset sizes, resulting in a final accuracy and EER. All of this data was paramount to making our table for analysis. We also sought after some literature reviews, albeit to a lesser extent. Five literature reviews serve to base our own research on, as well as to see where new research is needed. These are detailed further in Related Works.

4.2 Interpretation

We are left with a large dataset (87) of experimental research sources that are highly ranked and recently published. From these, we analyze the current research trends and effectiveness through construction of a table, shown in Table 1, which classifies the type of biometric, algorithm used, error rates, accuracy, timing, and other important factors. From this, we demonstrate which behavioral biometrics and algorithms are the most prominent and promising, showing signs of current trends, as well as indicating areas that lack research. By aggregating these sources in the table, as well as offering general commentary into concerns/topics seen throughout our research, we generate an easy-to-view, yet fairly comprehensive overview into the current trends of behavioral biometrics.

4.3 Pitfalls

While we believe this is the most efficient way to analyze current trends, alternative methods could have been chosen. Automated methods could have been developed to scrape a more diverse and larger dataset of behavioral biometric research. Further, rather than analyzing efficiency and overall metrics, we could have focused on the frequency of types/papers themselves over time, showing the overall interest and amount of research in this field to indicate what areas are growing or shrinking. We believe that our method is the most effective to show their use in actual systems, but these alternative ideas are certainly valid, and could be considered for future research.

4.4 Timeline

This paper was conceived and finalized over the course of a twelve-week semester. The first two weeks were dedicated towards developing a concrete research direction. Next, sources were sought after. All sources were found over the course of ten weeks, with each researcher finding and analyzing two or more sources per week. The initial research stage made up the bulk of

the research, taking four weeks, while developing and challenging research each took up three weeks. The final two weeks were spent aggregating all of the sources into our main focus, the table, for analysis in this paper.

5 Findings

Analyzing the compiled information in Table 1, we can see that the majority of existing studies focused around keystroke authentication systems and that those systems generally tend to have fair accuracies, averaging well over 90%. Also worth noting are the small dataset sizes. Most studies averaged around 100 users or less, with only 4 exceeding 10,000 users, and one exceeding 100,000 users. Further work can be done to evaluate these systems with larger datasets.

Our analysis of existing literature has identified that there are many actively researched areas in behavioral biometrics, but that there are primarily three main schemes with more focus and that show more promise than others; those being keystroke dynamics (KD), mouse dynamics (MD), and touch dynamics (TD) [5].

Furthermore, existing research has identified that the various biometric authentication schemes that were previously mentioned are not suitable on their own to completely replace password authentication. They are better served as components of a multi-factor or continuous authentication solution [1].

Finally, we identified that across the various studies that we have reviewed there is a lack of research into areas concerning the scalability of the proposed biometric authentication mechanisms as well as end user opinions on the privacy implications posed by them.

Through our analysis of the existing research, some of the following implications are offered.

Finding 1: KD/MD/TD lowers the cost of adoption for biometric authentication solutions due to their reuse of existing hardware vs. other biometric solutions [1]. Keyboards, mice, and touchscreen devices are ubiquitous in today's world, lowering the barrier to entry into adopting KD/MD/TD based systems. Compared with other biometric systems that require specialized (and frequently more expensive) hardware such as iris scanners, fingerprint readers, etc., KD/MD/TD is more feasible.

Finding 2: Continuous Authentication (CA) is not an alternative security solution for initial login; it provides an added security measure alongside the initial login [1]. This is in part due to the risk of a single form of biometric authentication becoming cracked and rendering it unusable [1]. This also stems from the concern of replacing a 1FA system with another 1FA system instead of using both in a 2FA system.

Finding 3: Passwords/passphrases in combination with KD/MD/TD as a Continuous Authentication (CA) mechanism is more effective than either one individually [49]. As is implied in the above point, using both systems to supplement each other and thus creating a 2FA system increases the overall resiliency against impersonating the user. A continuous authentication system by its nature is not suited for performing initial authentication (at least on its own), as it relies on the mannerisms of the user's input to determine whether they are the legitimate user. Passwords + behavioral authentication can be used together because it would cause an attacker to need to know both what the actual password/passphrase is, as well as the specific mannerisms in how it was inserted [49].

Finding 4: Free-text KD collection poses issues for user privacy as it can contain all sorts of sensitive information (namely PII) [25]. In academic research, this creates an issue where sharing source datasets would introduce privacy issues. In actual real-world implementations, this would present an issue if keystroke data is stored on a remote system and that system gets breached at some point. Huang et. al. [53] proposes a methodology for removing PII from KD datasets while negligibly impacting its ability to authenticate a user. Despite this, there still does not appear to be much research in regards to the privacy concerns of users before entering any of this information into a KD authentication system in the first place.

Finding 5: There are questions regarding the scalability of biometric authentication systems. Most existing literature on KD/MD/TD systems only looks at datasets with a couple hundred users; there is little to no data on how it functions at a multi-million user scale [16]. Acien et. al. (2020) specifically performs a study with 168k users, and concludes that a system at that scale was feasible specifically using siamese networks. This however is only one study, using one particular method; there does not yet appear to be other studies looking at other methods/algorithms at either the same or a larger scale.

6 Conclusions

As we have discussed in this paper, there is clearly a need for solutions that increase the factors necessary for authentication from only "something you know" to include additional factors like "something you do". Through our analysis of different studies in Table 1, we have iden-

Table 1: Summary of Behavioral Biometric Authentication Studies

Study	Year	Type	Method	Dataset Size	EER	FAR	FRR	Accuracy
[2]	2017	Keystroke	Scaled Manhattan verifier	486	0.0232	N/A	N/A	N/A
[7]	2021	Keystroke	Neural Networks	184	1.3	N/A	N/A	N/A
[8]	2019	Keystroke + Swipe	Neural Networks	31	N/A	N/A	N/A	93.15
[9]	2018	Keystroke + Gait	SFFS Algorithm	20	1.0	1.68	7.0	99.1
[10]	2019	Keystroke	Neural Network	42	0.9	0.3	1.5	N/A
[11]	2016	Keystroke	Neural Network	5	5.43	2.2	8.67	N/A
[12]	2017	Keystroke	SVM	30	N/A	0.113	0.331	98.5
[13]	2019	Keystroke	KCMS	100	15.7	15.7	15.7	N/A
[14]	2020	Keystroke	Random Forest	89	N/A	23.34	10.73	N/A
[15]	2019	Random Graph	Random Forest	20	N/A	0.12	0.0	N/A
[16]	2020	Keystroke	RNN	1,000	4.8	N/A	N/A	N/A
[17]	2017	Keystroke	Gunetti/Picardi's	95	N/A	1.0	11.5	98.4
[18]	2018	Gait	Dictionary Learning	20	11.2	N/A	N/A	95.0
[19]	2016	User Behavior	SVM	70	N/A	N/A	N/A	89.28
[20]	2016	Gametrics	Random Forest	118	N/A	0.02	0.02	N/A
[21]	2019	Pattern Lock	1-SVM	64	N/A	N/A	N/A	93.7
[22]	2018	Touch	PSO-RBFN	48	2.4	3.67	4.13	N/A
[23]	2020	Phone Sensors	MLP/Random Forest	20	N/A	6.94	2.55	95.96
[24]	2017	Gait	LDA	12	N/A	N/A	N/A	93
[25]	2019	Keystroke	Gunetti/Picardi.	103	N/A	N/A	N/A	N/A
[26]	2019	Mouse	CNN	10	N/A	2.94	2.28	N/A
[27]	2019	Touch	1-SVM/Isolation Forest	45	N/A	N/A	N/A	89.67
[28]	2017	Gait	Motion Capture	12	9.36	11.95	3.63	N/A
[29]	2018	Keystroke	CNN/XGB	51	0.17	N/A	N/A	98.97
[30]	2021	Passwords	Manhattan Distance	42	N/A	10.33	10.66	89.66
[31]	2019	Phone Use	Siamese LSTM	37	N/A	1	0.1	99.87
[32]	2019	Gait	Li-Gait	12	N/A	N/A	N/A	96.69
[33]	2017	Gait	Gait Cycle Detection	35	13	N/A	N/A	N/A
[34]	2020	Keystroke	Neural Networks	100,000	N/A	N/A	N/A	90
[35]	2019	Keystroke	Convolutional Neural Networks	150	N/A	N/A	N/A	72.8
[36]	2018	Gait	Pearson Correlation Coefficient	10	N/A	N/A	N/A	96.9
[37]	2019	Keystroke	Support Vector Regression	104	8.71	0.028	1.667	N/A
[38]	2020	Keystroke	Recurrent Neural Network	31	N/A	N/A	N/A	94.26
[39]	2018	Keystroke	Support Vector Machines	291	5.33	N/A	N/A	N/A
[40]	2019	Keystroke	K Nearest Neighbor	95	1.70	N/A	N/A	N/A
[41]	2018	Keystroke	Distance-Based Classification	22	7.89	N/A	N/A	N/A
[42]	2020	Password	Frequency Analysis	28	0.31	0.012	N/A	95
[43]	2017	Keystroke	Decision Trees + Logistic Regression	39	N/A	1.4	6.2	97.7
[44]	2020	Hand Gesture	Manhattan Classifier	10	4.27	N/A	N/A	N/A
[45]	2017	Keystroke	Chaotic Neural Network	10,000	N/A	.15	.65	N/A
[46]	2017	Keystroke	Convolutional Neural Network	267	2.3	N/A	N/A	94.0
[47]	2017	PIN + Touch	Fuzzy Interface System	10	N/A	N/A	N/A	39.5
[48]	2017	Keystroke	J84/Random Forests	10	N/A	0.105	1	85
[49]	2020	Passwords	Entropy Analysis	112	14.6	N/A	N/A	N/A
[50]	2019	Keystroke	KNN/SVN	299	4.03	0.0463	0.0833	82.8
[51]	2018	Keystroke	Frequency Analysis	98	N/A	N/A	N/A	N/A
[52]	2018	Keystroke	DTW	17	N/A	0.66	1.85	98
[53]	2017	Keystroke	Gunetti/Picardi algorithm.	95	N/A	1	11.5	98.4
[54]	2019	Keystroke	STFT/CWT	N/A	N/A	N/A	N/A	N/A
[55]	2021	Touch	SVM/KNN	60	2.9	N/A	N/A	85.77
[56]	2018	Touch	SVM	60	N/A	4.95	4.37	N/A
[57]	2019	Keystroke	Neural Network	8	N/A	N/A	N/A	82
[58]	2020	App Use	m-Classification Algorithm	10,000	0.25	1.79	0.25	N/A
[59]	2020	App Use	Learning Classifier System	50,000	N/A	< 10	< 5	N/A
[60]	2017	Keystroke	Pearson-Hamming networks	100	0.6	0.07	0.059	N/A
[61]	2019	Pin Codes	ABC Algorithm	10	N/A	N/A	N/A	90.99
[62]	2019	User Login	WEKA-MLP	5	5.44	2.2	8.68	91.3
[63]	2016	Keystroke	1-SVM	34	0	N/A	N/A	100

Table 1: Summary of Behavioral Biometric Authentication Studies

Study	Year	Type	Method	Dataset Size	EER	FAR	FRR	Accuracy
[64]	2016	Writing	Multinomial Nave Bayes classifier	11	N/A	N/A	N/A	50.86
[65]	2018	Keystroke	HTER/K-Chen	736	N/A	0.015	0.014	92.25
[66]	2021	Keystroke	Machine Learning	18 data-sets	N/A	N/A	N/A	96.7
[67]	2018	Keystroke	Manhattan distance	30	N/A	0	2.4	87.7
[68]	2019	File Browsing	Gaussian Mixture Model	160	N/A	N/A	N/A	95
[69]	2018	Touch	SVM/Random Forest	41	0.029	0.93	5.3	98.7
[70]	2017	User Login	k-NN	51	0.078	N/A	N/A	N/A
[71]	2017	Keystroke	DeepSecure	51	0.03	N/A	N/A	93.59
[72]	2018	Letter Frequency	Letter Frequency	8	0.52	N/A	N/A	N/A
[73]	2018	Keystroke	Iterative KCA process	100	N/A	N/A	N/A	97.8
[74]	2020	Fingerprints	CNN	90	N/A	0.045	1.39	96.04
[75]	2019	Gait/Gyroscopes	k Neighbors/Random Forest	51	9.3	N/A	N/A	94.8
[76]	2017	Smartphone Sensors	Information Gain Attribute Evaluator	95	N/A	.01	N/A	96
[77]	2019	Smartphone Sensors	AnswerAuth	100	N/A	N/A	N/A	99.35
[78]	2017	Audio Keystroke Dynamics	Hidden Markov Model	50	4.65	N/A	N/A	97.03
[79]	2017	Keystroke	SVM	39	2.94	N/A	N/A	99.4
[80]	2020	Keystroke + Touch	Few-Shot Learning	89	N/A	23.34	10.73	95.66
[81]	2016	Touch Features	Guassian process	24	N/A	N/A	N/A	90
[82]	2020	Individual Keystrokes	CNN+RNN	260	3.04	4.12	3.04	N/A
[83]	2019	Pattern Lock	Machine Learning	30	5.83	3.25	N/A	97.52
[84]	2016	Keystroke	Gaussian mixture model	157	0.39	N/A	N/A	N/A
[85]	2018	Keystroke	User-adaptive feature extraction method	150	0.44	0.045	0	N/A
[86]	2017	Emotions	K-Fold	9	N/A	12.85	8.78	81.2
[87]	2017	Bio-Hashing	New Distance Metric	10	0.15	0.12	4.78	N/A

tified that keystroke, mouse, and touch based authentication systems generally seem to be the leading areas of research thus far. We also highlight a number of areas where research is still lacking and can be improved through further studies in those areas.

Our paper offers a comprehensive overview into recent research trends in the behavioral biometric space and will help to inform future researchers of critical topics that must be researched, namely in the space of scalability and privacy. Should these be more thoroughly examined and tested, we believe that behavioral biometric authentication, particularly as a continuous authentication model, will have the ability to progress beyond just a research topic and make waves in industry.

7 Acknowledgements

We'd like to give a special shoutout to the StackExchange LaTeX community for giving us the will and means to make a giant table, as well as Justin Pelletier for his critical and constructive feedback.

References

[1] Mondal S, Bours P. A study on continuous authentication using a combination of keystroke and mouse biometrics. Neurocomputing. 2017;230:1–22. Available from: https://www.sciencedirect.com/science/article/pii/S0925231216314321.

[2] Goodkind A, Brizan DG, Rosenberg A. Utilizing Overt and Latent Linguistic Structure to Improve Keystroke-Based Authentication. Image and Vision Computing. 2016 06;58.

[3] Mahfouz A, Mahmoud TM, Eldin AS. A survey on behavioral biometric authentication on smartphones. Journal of information security and applications. 2017;37:28–37.

[4] Stylios IC, Thanou O, Androulidakis I, Zaitseva E. A review of continuous authentication using behavioral biometrics. In: Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference; 2016. p. 72–79.

[5] Abuhamad M, Abusnaina A, Nyang D, Mohaisen D. Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey. IEEE Internet of Things Journal. 2021;8(1):65–84.

[6] Liang Y, Samtani S, Guo B, Yu Z. Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. IEEE Internet of Things Journal. 2020;7(9):9128–9143.

[7] Toosi R, Akhaee MA. Time–frequency analysis of keystroke dynamics for user authentication. Future Generation Computer Systems. 2021;115:438–447. Available from: https://www.sciencedirect.com/science/article/pii/S0167739X19319247.

[8] Tse K, Hung K. Behavioral Biometrics Scheme with Keystroke and Swipe Dynamics for User Authentication on Mobile Platform. In: 2019 IEEE 9th Symposium on Computer Applications Industrial Electronics (ISCAIE); 2019. p. 125–130.

[9] Lamiche I, Bin G, Jing Y, Yu Z, Hadid A. A continuous smartphone authentication method based on gait patterns and keystroke dynamics. Journal of Ambient Intelligence and Humanized Computing. 2018;10(11):4417–4430.

[10] Salem A, Obaidat MS. A novel security scheme for behavioral authentication systems based on keystroke dynamics. Security and Privacy. 2019;2(2):e64. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.64.

[11] Salem A, Zaidan D, Swidan A, Saifan R. Analysis of Strong Password Using Keystroke Dynamics Authentication in Touch Screen Devices. In: 2016 Cybersecurity and Cyberforensics Conference (CCC); 2016. p. 15–21.

[12] Alsultan A, Warwick K, Wei H. Non-conventional keystroke dynamics for user authentication. Pattern Recognition Letters. 2017;89:53–59. Available from: https://www.sciencedirect.com/science/article/pii/S0167865517300429.

[13] Tsai CJ, Shih KJ. Mining a new biometrics to improve the accuracy of keystroke dynamics-based authentication system on free-text. Applied Soft Computing. 2019;80:125–137. Available from: https://www.sciencedirect.com/science/article/pii/S1568494619301577.

[14] Solano J, Tengana L, Castelblanco A, Rivera E, Lopez C, Ochoa M. A Few-Shot Practical Behavioral Biometrics Model for Login Authentication in Web Applications. NDSS Symposium. 2020 Feb. Available from: https://www.ndss-symposium.org/wp-content/uploads/2020/02/23011-paper.pdf.

[15] Mohamed M, Shrestha P, Saxena N. Challenge-response behavioral mobile authentication. Proceedings of the 35th Annual Computer Security Applications Conference. 2019 Dec:355–365. Available from: https://dl.acm.org/doi/abs/10.1145/3359789.3359838.

[16] Acien A, Morales A, Vera-Rodriguez R, Fierrez J, Monaco JV. Typenet: Scaling up keystroke biometrics. In: 2020 IEEE International Joint Conference on Biometrics (IJCB). IEEE; 2020. p. 1–7.

[17] Huang J, Hou D, Schuckers S. A practical evaluation of free-text keystroke dynamics. In: 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA). IEEE; 2017. p. 1–8.

[18] Xu W, Lan G, Lin Q, Khalifa S, Hassan M, Bergmann N, et al. Keh-gait: Using kinetic energy harvesting for gait-based user authentication systems. IEEE Transactions on Mobile Computing. 2018;18(1):139–152.

[19] Susuki RS Hiroyaand Yamaguchi. Cost-Effective Modeling for Authentication and Its Application to Activity Tracker. In: Kim D Ho-wonand Choi, editor. Information Security Applications. Cham: Springer International Publishing; 2016. p. 373–385.

[20] Mohamed M, Saxena N. Gametrics: Towards Attack-Resilient Behavioral Authentication with Simple Cognitive Games. In: Proceedings of the 32nd Annual Conference on Computer Security Applications. ACSAC '16. New York, NY, USA: Association for Computing Machinery; 2016. p. 277–288. Available from: https://doi.org/10.1145/2991079.2991096.

[21] Torres J, Santos S, Alepis E, Patsakis C. Behavioral Biometric Authentication in Android Unlock Patterns through Machine Learning. Proceedings of the 5th International Conference on Information Systems Security and Privacy. 2019. Available from: https://www.scitepress.org/Papers/2019/73942/73942.pdf.

[22] Meng W, Wang Y, Wong DS, Wen S, Xiang Y. TouchWB: Touch behavioral user authentication based on web browsing on smartphones. Journal of Network and Computer Applications. 2018;117:1–9.

[23] Liang X, Zou F, Li L, Yi P. Mobile terminal identity authentication system based on behavioral characteristics. International Journal of Distributed Sensor Networks. 2020;16(1):155014771989937. Available from: https://journals.sagepub.com/doi/pdf/10.1177/1550147719899371.

[24] Lee M, Ryu J, Youn I. Biometric personal identification based on gait analysis using surface EMG signals. In: 2017 2nd IEEE International Conference on Computational Intelligence and Applications (ICCIA); 2017. p. 318–321.

[25] Huang J, Klee B, Schuckers D, Hou D, Schuckers S. Removing Personally Identifiable Information from Shared Dataset for Keystroke Authentication Research. In: 2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA); 2019. p. 1–7.

[26] Hu T, Niu W, Zhang X, Liu X, Lu J, Liu Y. An insider threat detection approach based on mouse dynamics and deep learning. Security and Communication Networks. 2019;2019.

[27] Yang Y, Guo B, Wang Z, Li M, Yu Z, Zhou X. BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics. Ad Hoc Networks. 2019;84:9–18.

[28] Sulovská K, Fišerová E, Chvosteková M, Adámek M. Appropriateness of gait analysis for biometrics: Initial study using FDA method. Measurement. 2017;105:1–10. Available from: https://www.sciencedirect.com/science/article/pii/S0263224117302105.

[29] Dwivedi C, Kalra D, Naidu D, Aggarwal S. Keystroke dynamics based biometric authentication: A hybrid classifier approach. In: 2018 IEEE Symposium Series on Computational Intelligence (SSCI); 2018. p. 266–273.

[30] Parkinson S, Khan S, Crampton A, Xu Q, Xie W, Liu N, et al.. Password policy characteristics and keystroke biometric authentication. The Institution of Engineering and Technology; 2021. Available from: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/bme2.12017.

[31] Deb D, Ross A, Jain AK, Prakah-Asante K, Prasad KV. Actions speak louder than (pass) words: Passive authentication of smartphone* users via deep temporal features. In: 2019 International Conference on Biometrics (ICB). IEEE; 2019. p. 1–8.

[32] Musale P, Baek D, Choi BJ. Lightweight gait based authentication technique for IoT using subconscious level activities. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT); 2018. p. 564–567.

[33] Muaaz M, Mayrhofer R. Smartphone-Based Gait Recognition: From Authentication to Imitation. IEEE Transactions on Mobile Computing. 2017;16(11):3209–3221.

[34] Morales A, Acien A, Fierrez J, Monaco JV, Tolosana R, Vera-Rodriguez R, et al.. Keystroke Biometrics in Response to Fake News Propagation in a Global Pandemic. COMPSAC; 2020. Available from: https://ieeexplore.ieee.org/abstract/document/9202723/keywords#keywords.

[35] Maiorana E, Kalita H, Campisi P. Deepkey: Keystroke Dynamics and CNN for Biometric Recognition on Mobile Devices. EUVIP; 2019. Available from: https://ieeexplore.ieee.org/abstract/document/8946206/keywords#keywords.

[36] Sun F, Mao C, Fan X, Li Y. Accelerometer-based speed-adaptive gait authentication method for wearable IoT devices. IEEE Internet of Things Journal. 2018;6(1):820–830.

[37] Wang Y, Wu C, Zheng K, Wang X. Improving Reliability: User Authentication on Smartphones Using Keystroke Biometrics. IEEE Access. 2019;7:26218–26228.

[38] Tse K, Hung K. User Behavioral Biometrics Identification on Mobile Platform using Multimodal Fusion of Keystroke and Swipe Dynamics and Recurrent Neural Network. In: 2020 IEEE 10th Symposium on Computer Applications Industrial Electronics (ISCAIE); 2020. p. 262–267.

[39] Sun Y, Upadhyaya S. Synthetic Forgery Attack against Continuous Keystroke Authentication Systems. In: 2018 27th International Conference on Computer Communication and Networks (ICCCN). IEEE; 2018. p. 1–7.

[40] Mhenni A, Cherrier E, Rosenberger C, Amara NEB. Analysis of doddington zoo classification for user dependent template update: Application to keystroke dynamics recognition. Future Generation Computer Systems. 2019;97:210–218.

[41] Lee H, Hwang JY, Kim DI, Lee S, Lee SH, Shin JS. Understanding keystroke dynamics for smartphone users authentication and keystroke dynamics on smartphones built-in motion sensors. Security and Communication Networks. 2018;2018.

[42] Khan H, Hengartner U, Vogel D. Mimicry Attacks on Smartphone Keystroke Authentication. ACM Trans Priv Secur. 2020 Feb;23(1). Available from: https://doi.org/10.1145/3372420.

[43] Crawford H, Ahmadzadeh E. Authentication on the Go: Assessing the Effect of Movement on Mobile Device Keystroke Dynamics. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). Santa Clara, CA: USENIX Association; 2017. p. 163–173. Available from: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/crawford.

[44] Shen C, Wang Z, Si C, Chen Y, Su X. Waving gesture analysis for user authentication in the mobile environment. IEEE Network. 2020;34(2):57–63.

[45] Baynath P, Soyjaudah KMS, Khan MHM. IEEE; 2017. Available from: https://ieeexplore-ieee-org.ezproxy.rit.edu/document/8311590.

[46] Çeker H, Upadhyaya S. Sensitivity Analysis in Keystroke Dynamics using Convolutional Neural Networks. IEEE; 2017. Available from: https://ieeexplore-ieee-org.ezproxy.rit.edu/document/8267667.

[47] Xin Ci Loh S, Ow-Yong HY, Lim HY. IEEE; 2017. Available from: https://drive.google.com/file/d/1mpCCKzfYsGOp54UA3owMOrPFlzN0Gxl1/view.

[48] Mohlala M, Ikuesan AR, Venter HS. User attribution based on keystroke dynamics in digital forensic readiness process. IEEE; 2017. Available from: https://ieeexplore.ieee.org/abstract/document/8270436.

[49] Bhana B, Flowerday S. Passphrase and keystroke dynamics authentication: Usable security. Computers & Security. 2020;96:101925.

[50] Mhenni A, Cherrier E, Rosenberger C, Amara NEB. Double serial adaptation mechanism for keystroke dynamics authentication based on a single password. Computers & Security. 2019;83:151–166.

[51] Smriti P, Srivastava S, Singh S. Keyboard Invariant Biometric Authentication. In: 2018 4th International Conference on Computational Intelligence Communication Technology (CICT); 2018. p. 1–6.

[52] Alshehri A, Coenen F, Bollegala D. Keyboard Usage Authentication Using Time Series Analysis. In: Madria S, Hara T, editors. Big Data Analytics and Knowledge Discovery. Cham: Springer International Publishing; 2016. p. 239–252.

[53] Huang J, Hou D, Schuckers S. A practical evaluation of free-text keystroke dynamics. IEEE; 2017. Available from: https://ieeexplore.ieee.org/abstract/document/7947695/keywords#keywords.

[54] Alpar O, Krejcar O. Frequency and Time Localization in Biometrics: STFT vs. CWT;. .

[55] Li W, Meng W, Furnell S. Exploring touch-based behavioral authentication on smartphone email applications in IoT-enabled smart cities. Pattern Recognition Letters. 2021;144:35–41.

[56] Meng W, Li W, Wong DS. Enhancing touch behavioral authentication via cost-based intelligent mechanism on smartphones. Multimedia Tools and Applications. 2018;77(23):30167–30185.

[57] Vysotska A Olenaand Davydenko. Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor Authentication. In: Hu SDIHM Zhengbingand Petoukhov, editor. Advances in Computer Science for Engineering and Education II. Cham: Springer International Publishing; 2020. p. 356–368.

[58] Yamaguchi S, Gomi H, Kobayashi R, Thao TP, Irvan M, Yamaguchi RS. Effective Classification for Multi-modal Behavioral Authentication on Large-Scale Data. In: 2020 15th Asia Joint Conference on Information Security (AsiaJCIS). IEEE; 2020. p. 101–109.

[59] Irvan M, Nakata T, Yamaguchi RS. User authentication based on smartphone application usage patterns through learning classifier systems. In: 2020 IEEE International Conference on Big Data (Big Data). IEEE; 2020. p. 4462–4466.

[60] Sulavko AE, Eremenko AV, Fedotov AA. Users' identification through keystroke dynamics based on vibration parameters and keyboard pressure. In: 2017 Dynamics of Systems, Mechanisms and Machines (Dynamics); 2017. p. 1–7.

[61] KOH PM, LAI WK. Keystroke Dynamics Identification System using ABC Algorithm. In: 2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS); 2019. p. 108–113.

[62] Salem A. Enhanced Authentication System Performance Based on Keystroke Dynamics using Classification algorithms. Korean Society for Internet Information; 2019. Available from: https://www.koreascience.or.kr/article/JAKO201926358473620.page.

[63] Çeker H, Upadhyaya S. User authentication with keystroke dynamics in long-text data. In: 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE; 2016. p. 1–6.

[64] Amigud A, Arnedo-Moreno J, Daradoumis T, Guerrero-Roldan AE. A behavioral biometrics based and machine learning aided framework for academic integrity in e-assessment. In: 2016 International conference on intelligent networking and collaborative systems (INCoS). IEEE; 2016. p. 255–262.

[65] Karim ME, Balagani KS, Elliott A, Irakiza D, O'Neal M, Phoha VV. Active Authentication of Keyboard Users: Performance Evaluation on 736 Subjects. CoRR. 2018;abs/1804.08180. Available from: http://arxiv.org/abs/1804.08180.

[66] Lee K, Lee J, Choi C, Yim K. Offensive Security of Keyboard Data Using Machine Learning for Password Authentication in IoT. IEEE Access. 2021;9:10925–10939.

[67] Kochegurova E, Luneva E, Gorokhova E. On Continuous User Authentication via Hidden Free-Text Based Monitoring. In: Abraham A, Kovalev S, Tarassov V, Snasel V, Sukhanov A, editors. Proceedings of the Third International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'18). Cham: Springer International Publishing; 2019. p. 66–75.

[68] Voris J, Song Y, Salem MB, Hershkop S, Stolfo S. Active authentication using file system decoys and user behavior modeling: results of a large scale study. Computers & Security. 2019;87:101412.

[69] Nguyen T, Memon N. Tap-based user authentication for smartwatches. Computers & Security. 2018;78:174–186.

[70] Ivannikova E, David G, Hämäläinen T. Anomaly detection approach to keystroke dynamics based user authentication. In: 2017 IEEE Symposium on Computers and Communications (ISCC); 2017. p. 885–889.

[71] Maheshwary S, Ganguly S, Pudi V. Deep Secure: A Fast and Simple Neural Network based approach for User Authentication and Identification via Keystroke Dynamics; 2017. .

[72] Kostyuchenko EY, Viktorovich I, Renko B, Shelupanov AA. User Identification by the Free-Text Keystroke Dynamics. In: 2018 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC); 2018. p. 1–4.

[73] Alshehri A, Coenen F, Bollegala D. Iterative Keystroke Continuous Authentication: A Time Series Based Approach. KI - Künstliche Intelligenz. 2018 Nov;32(4):231–243.

[74] Wu C, He K, Chen J, Zhao Z, Du R. Liveness is Not Enough: Enhancing Fingerprint Authentication with Behavioral Biometrics to Defeat Puppet Attacks. In: 29th {USENIX} Security Symposium ({USENIX} Security 20); 2020. p. 2219–2236.

[75] Weiss GM, Yoneda K, Hayajneh T. Smartphone and smartwatch-based biometrics using activities of daily living. IEEE Access. 2019;7:133190–133202.

[76] Buriro A, Gupta S, Crispo B. Evaluation of Motion-based Touch-typing Biometrics for online Banking. In: 2017 international conference of the biometrics special interest group (BIOSIG). IEEE; 2017. p. 1–5.

[77] Buriro A, Crispo B, Conti M. AnswerAuth: A bimodal behavioral biometric-based user authentication scheme for smartphones. Journal of information security and applications. 2019;44:89–103.

[78] Pleva M, Bours P, Ondáš S, Juhár J. Improving static audio keystroke analysis by score fusion of acoustic and timing data. Multimedia Tools and Applications. 2017;76(24):25749–25766.

[79] Yan Sun, Ceker H, Upadhyaya S. Anatomy of secondary features in keystroke dynamics - achieving more with less. In: 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA); 2017. p. 1–6.

[80] Solano J, Tengana L, Castelblanco A, Rivera E, Lopez C, Ochoa M. A few-shot practical behavioral biometrics model for login authentication in web applications. In: NDSS Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb'20); 2020. .

[81] Buschek D, De Luca A, Alt F. Evaluating the influence of targets and hand postures on touch-based behavioural biometrics. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems; 2016. p. 1349–1361.

[82] Lu X, Zhang S, Hui P, Lio P. Continuous authentication by free-text keystroke based on CNN and RNN. Computers & Security. 2020;96:101861.

[83] Ku Y, Park LH, Shin S, Kwon T. Draw it as shown: Behavioral pattern lock for mobile user authentication. IEEE Access. 2019;7:69363–69378.

[84] Sun Y, Ceker H, Upadhyaya S. Shared keystroke dataset for continuous authentication. In: 2016 IEEE International Workshop on Information Forensics and Security (WIFS); 2016. p. 1–6.

[85] Kim J, Kim H, Kang P. Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection. Applied Soft Computing. 2018;62:1077–1087. Available from: https://www.sciencedirect.com/science/article/pii/S1568494617305847.

[86] Kolakowska A. In: Hippe ZS, Kulikowski JL, Mroczek T, editors. Usefulness of Keystroke Dynamics Features in User Authentication and Emotion Recognition. Cham: Springer International Publishing; 2018. p. 42–52. Available from: https://doi.org/10.1007/978-3-319-62120-3_4.

[87] Neha, Chatterjee K. An Efficient Biometric Based Remote User Authentication Technique for Multi-server Environment. Wireless Personal Communications. 2017 Dec;97(3):4729–4745.