Mobile Continuous Authentication in eHealth: A case study for the ProTego project

Luis de-Marcos, Carlos Cilleruelo, Javier Junquera-Sánchez
Universidad de Alcalá
Departamento de Ciencias de la Computación
Edificio Politécnico. Campus Universitario. Ctra Barcelona km 33.6.
(luis.demarcos, carlos.cilleruelo, javier.junquera)@uah.es

***Abstract**. Health care information is an attractive target for cybercriminals. Nowadays, with the significant diffusion of Internet of Things (IoT) and Bring Your Own Device (BYOD), patients and medical staff use smart devices to generate and access medical data in hospitals and healthcare practice, so protecting them is a critical security domain. Continuous Authentication (CA) is an access control mechanism that monitors user activity to determine if access is legitimate. This paper presents a case study of CA in eHealth that was implemented as part of the ProTego Project. We present the initial results of implementing a keystroke mobile agent with machine learning classifiers to build user models.*

Keywords. Continuous authentication, eHealth, Cybersecurity, Mobile device

1 Introduction

Health care information is an attractive target for cybercriminals. In terms of data acquisition, it has a high black market value, which is around 20-50 times more valuable than financial data for ID theft purposes, with an increase traffic in darknets (Cilleruelo et al., 2020). Moreover, health care information is a critical resource making it an attractive target for denial of access attacks using ransomware. However, health care networks are complex (Malby & Anderson-Wallace, 2016), health management being decentralized to a certain degree in 20 out of 28 member states (European Union, 2012). As a result, data stored in the patient's Electronic Health (eHealth) Record can be challenging to defend.

Moreover, nowadays, with the significant diffusion of Internet of Things (IoT) and the introduction of fifth generation (5G) of cellular networks to support massive Machine Type Communication (mMTC) and third-party services directly on operator's cloud for vertical markets (5G-PPP, 2016), patients and medical staff use smart devices to generate and access medical data in hospitals and healthcare practices. There are several available devices, ranging from consumer ones (including the concept of Bring Your Own Device – BYOD – smartphones, laptops and tablets, often brought by the hospital staff) to medical ones (cardiac pacemakers and defibrillators, drug administration devices, infusion pumps and glucometers, blood pressure measurement devices, wearable heart rate devices).

These devices are used to help clinicians in handling all those emergency situations in which a prompt treatment is required, responding readily and responsively to any health concern. With a mobile device, physicians can access patient data and clinical trial data on the go and share information with colleagues when needed. However, this often depends on exchanging data between the devices and the hospital network. In the case of chronic disorders (e.g., diabetes), for instance, clinicians may ask patients to come to the hospital with their devices (e.g., glucose meters and Continuous Glucose Monitors), so that they can be connected via a doctor's (or nurse's) computer, and data transferred. The transferring is usually performed via proprietary software (e.g., the Diasend platform 5 for diabetes data management).

Prevention measures consider access control and authorization. Since a mobile device is easy to take and use by unauthorized third parties, continuous authentication (CA) provides a means to monitor user activity and determine whether he is the legitimate user of the device. CA systems are those that do not require the active participation of the user to determine her identity.

CA is particularly relevant in healthcare because healthcare providers can deploy BYOD policies for their employees. Also, they can enable patients to access their medical information and records or provide data to feed these medical records through mobile apps or IoT devices, like fit bands. The ProTego project is an EU-funded project that aims to provide a toolkit for health care organizations to assess better and reduce cybersecurity risks related to remote devices' access to healthcare data. CA for BYOD is one of these tools.

Current literature on CA provides various methods that can be applied to BYOD mobile healthcare environments, like physical and behavioral biometrics (Giuffrida et al., 2014). The ProTego project includes an architecture for integrating CA into a wider context (de-Marcos et al., 2020). This is particularly important in healthcare where CA must be integrated into heterogeneous ecosystems that include a variety of hardware and software by multiple providers, as well as data coming from multiple sources including devices and sensors (Shuwandy et al., 2019).

This paper presents the initial results of the ProTego holistic approach for CA in eHealth environments. It includes the implementation and deployment of CA mobile agents, the training of machine learning models to continuously authenticate users, and testing in a real use case scenario.

The rest of the paper is structured as follows: Section 2 briefly presents the ProTego project. Section 3 presents the use case for CA in an eHealth scenario. The framework for CA is presented in section 4. Section 5 presents the method for building and testing CA agents. Results are presented in section 6. Section 7 discusses findings. Conclusions and future work are outlined in section 8.

2 The ProTego Project

The ProTego project aims to deliver a toolkit which is an end-to-end cybersecurity solution that delivers the following functionality:

- Risk assessment tools delivering a knowledge base, in design time, of multisource threat intelligence strategically based on Risk Analysis Tools and tactically based on monitoring and situational awareness tools, including context, mechanisms, indicators, implications, and action-oriented advice about an existing or emerging menace or hazard to assets. At first stage, ProTego develops a knowledge base of security threats and measures to address IoT and BYOD scenarios, then extends existing technology to provide design-time machine reasoning.
- Risk mitigation and protection tools to gather the supporting information about security state from a broader range of sources, but automate the process from beginning to end, including data protection and identity management.
- Application integration extends monitoring and situational awareness tool, which provides reliable log ingestion and storage at scale, as well as normalization and correlation of events for real-time monitoring and the automated detection of security incidents, for gathering and analysing various security data for the purpose of making them available and consumable by different stakeholders and enable informed decision making and formalize and automate responsive actions.

The components of the ProTego toolkit are presented in figure 1. A standard Security Information and Event Management (SIEM) centralizes security events. Events can be raised by CA agents responsible of mobile device security or by the Data Gateway responsible of protecting other medical data via Access Control component. End-user applications will communicate with these two components. Network slicing technology is used in hospital premises to provide additional security in wireless networks.

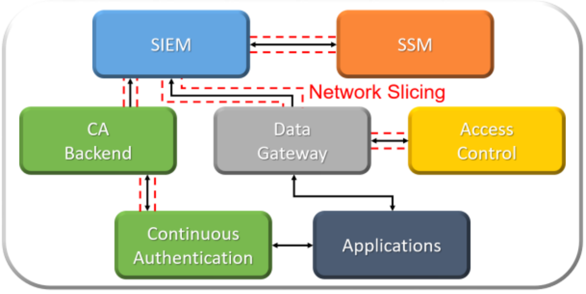

Figure 1. ProTego Integrated Toolkit

3 Use Case for eHealth Continuous Authentication

The specificities of BYOD and mobile devices were addressed using a reference use case involving staff devices and the use a smartphone in the office. It can be stated as follows:

"Bob is employed in the administrative department of the hospital. His daily practice is performed via his Windows desktop computer, provided directly by the hospital. The computer is plugged into the hospital LAN network (which allows Bob to access all the services available on the intranet of the hospital), and it does not move from Bob's desk.

Bob has a family, and he lives far away from the hospital. Bob uses his smartphone in order to stay in touch with his family. They communicate via instant messaging whenever one of his children need a lift or simply to exchange some information during the day. His smartphone is quite old, and so to be sure to have enough battery for the return trip, Bob commonly recharges it by plugging it into his desktop computer.

Once the phone is plugged, it is possible to download (upload) data from (to) it. When he sees the popup suggesting to him all the operations he can do with his smartphone, Bob remembers that he stored a file on the smartphone to be given to his colleague Carl. Bob downloads the file from his smartphone to the computer, collects a USB key from one of the desks in his office, uploads the file onto it, and delivers the USB key to Carl, who visualizes the file with his desktop computer."

4 Continuous Authentication Framework

To meet the project's requirements and address the use case presented in the previous section, we proposed a scalable CA architecture (Fig. 2) (Junquera-Sánchez et al., 2020). The central component of the CA architecture is an API that supports multiple Endpoint Detection and Response (EDR) agents. It stores user information in the form of logs or in a relational database. An AI model in the API generates and updates user models periodically. The API can also return the trustworthiness values of users as requested by third parties. A trustworthiness value represents the probability of the user being who she says she is. Values are generated in the API using one or more user models. Finally, the API agent can also raise alarms to SIEM (Security Information and Event Management) systems if needed.

The API was implemented as a Java REST API server. The communication between the agent and the API takes the form of Data Transfer Objects (DTO) that the client posts to the server. Agents can be implemented in any form and technology as long as they communicate with the API using the REST operations that it provides. For this study, an EDR agent that captures the soft-keyboard events of the mobile phone was developed. It took the form of an Android app, but it was also embedded as a WebView component that could be used in any device that supports it. As an EDR agent, the mobile component also provides response functionalities, like the capacity to lock the mobile phone if unauthorized use is detected.

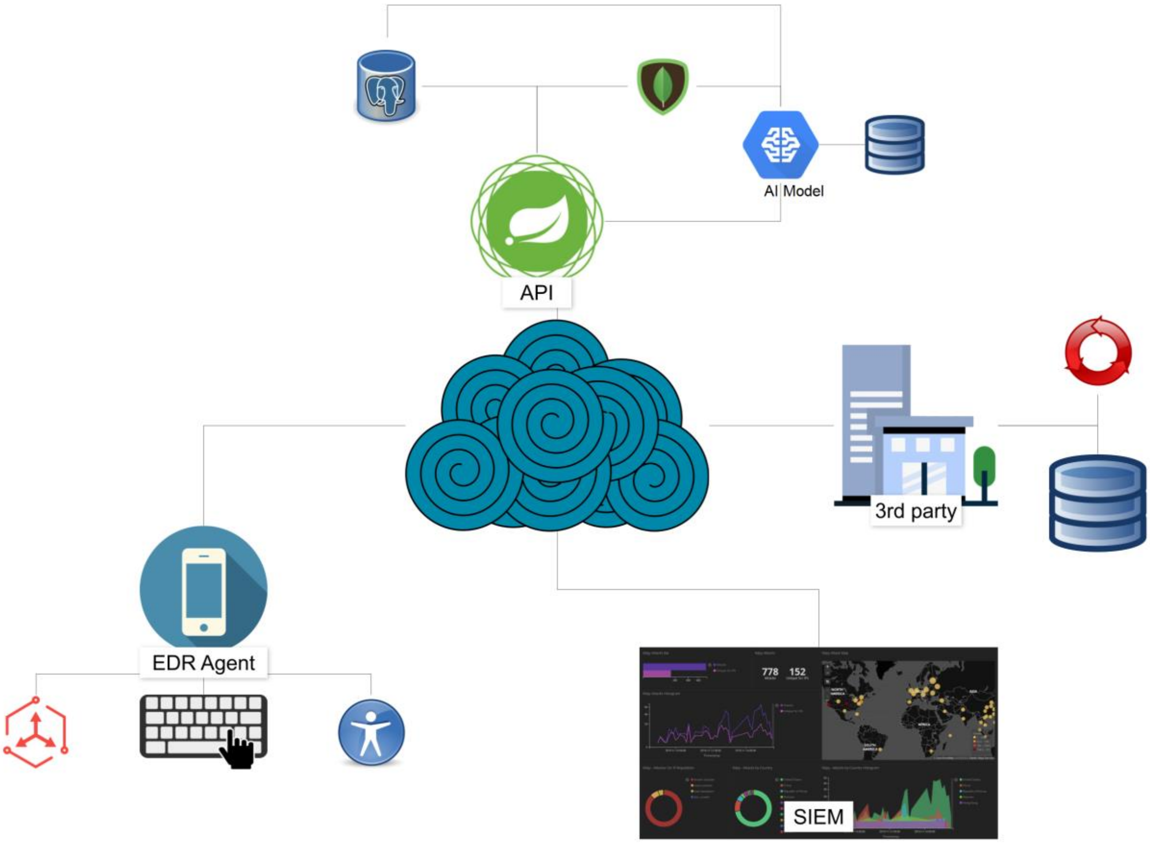

Figure 2. Continuous Authentication Architecture

5 Method

For this research, we implemented a proof of concept mobile agent and several AI models.

5.1 EDR agent and measurements

The EDR mobile agent captured the keystroke mechanics of users. Keystroke mechanics determine unique digital fingerprints based on personal typing patterns. They have proven to be a successful method to continuously authenticate users in desktop computers (Banerjee & Woodard, 2012). There is also a substantial body of research for mobile devices (Abdulhak & Abdulaziz, 2018). The EDR agent captured the standard keystroke measurements, which included the pressing time of each key, the time between the press of two consecutive keys, and the time between the release of each key and the press of the next one.

5.2 AI models and metrics

The measurements gathered for each key pressed by the EDR agent were used to feed Machine Learning (ML) models that would represent users' interaction. Datasets were built for each user containing 2500 legitimate events and 7500 illegitimate events. Legitimate events were captured on typing session in which participants were asked to type a text in their mobile phones. Illegitimate events represented the actions of other users, so a random sample of all the events of other participants was taken.

Initially, we selected the following ML classifiers:

- Random Forest Classifier (RFC). (Breiman, 2001)
- Extra Trees Classifier (ETC). (Geurts et al., 2006)
- Gradient Boosting Classifier (GBC). (Friedman, 2001)
- K-Nearest Neighbors (KNN) classifier.
- Support Vector Machine (SVM) classifier.

Classifiers selected include a representation of ensemble methods (RFC, ETC, GBC) and instance-based algorithms (KNN and GBC). (Hastie et al., 2009). An AI version of the classifiers was implemented in Python using the Scikit-learn module For each user, the 70% of the dataset was used as the training set. The remaining 30% was the testing set. AI models return a prediction for each key event of the testing set. The following metrics were used to evaluate the performance of the different ML classifiers:

- Accuracy. It measures the proportion of true positives and negatives to the overall tested data. Accuracy is a performance measure of the continuous authentication component. A high accuracy guarantees that the system is able to classify both authorized and unauthorized accesses correctly. However, accuracy shall be used in combination with other metrics, mainly if the data is unbalanced.
- False Positive Rate (FPR). It measures the percentage of identification instances in which unauthorized persons are incorrectly accepted. A low False Acceptance Rate is fundamental to prevent unauthorized access and, therefore, to ensure data protection. This will improve the security of the applications, data, and infrastructure and reduce the risk of data privacy breaches. In CA research, FPR is also called False Acceptance Rate
- False Negative Rate (FNR). It measures the percentage of identification instances in which authorized persons are incorrectly rejected. Reducing the FAR to the lowest possible level, the FRR is likely to rise sharply. However, a low False Rejection Rate is fundamental to ensure that the system is usable. Therefore, it is essential to balance the FAR and FRR to prevent unauthorized access while not falsely rejecting legitimate users. In CA research, FPR is also called False Rejection Rate

6 Results

This section presents the initial results of experimentation with our mobile CA proposal according to the method described in the previous section. Tables 1-3 present the results of the target metrics for all classifiers for three different users.

Table 1. Results of AI models for User 1

Classifier	Accuracy	FPR	FNR
RFC	0.81	0.10	0.37
ETC	0.81	0.11	0.37
GBC	0.82	0.08	0.40
KNN	0.77	0.13	0.43
SVM	0.69	0.01	0.97

Table 2. Results of AI models for User 2

Classifier	Accuracy	FPR	FNR
RFC	0.81	0.16	0.22
ETC	0.78	0.18	0.26
GBC	0.80	0.13	0.28
KNN	0.73	0.27	0.27
SVM	0.64	0.02	0.81

Table 3. Results of AI models for User 3

Classifier	Accuracy	FPR	FNR
RFC	0.81	0.09	0.47
ETC	0.78	0.09	0.54
GBC	0.81	0.09	0.50
KNN	0.75	0.12	0.61
SVM	0.74	0.01	0.96

Results show that all ensemble methods (RFC, ETC, GBC) return similar values for all target metrics, although GBC performs slightly better with accuracy ratings around 0.80, FPR in the range 8%-13%, and FNR between 28% and 50%. Although the values may seem high, they represent the rates for each keypress event. The results of several consecutive predictions can be combined to improve the accuracy. As for the ratio between, they can be fine-tuned but there is a trade-off, since the increase in one usually results in a decrease of the other. Table 4 presents the estimated impact on FPR and FNR when combining several consecutive predictions assuming that each keypress is an independent event.

Table 4. Estimated FPR and FNR when combining several consecutive keypress events

#events	FPR	FNR
1	0.100	0.390
2	0.014	0,004
3	0.004	0.016
4	0.001	0.064

7 Discussion

Our findings can be compared with the existing state-of-the-art research in CA. Best results on desktop CA systems using keystroke mechanics reported a FPR as low as 0.0002 and a FNR of 0.0482 (Ahmed & Traore, 2014). However, there is far more research and experience in the development of CA solutions for desktop computers, with firsts studies dating from the 90s (Shepherd, 1995), and evidence suggests that interaction with desktop keyboard results in more accurate statistical models of user typing patterns (Bours & Mondal, 2015).

Research on CA for mobile devices usually reports Equal Error Rate (EER). EER is the minimal point at which FPR and FNR intersect. As the model's sensitivity can be adjusted at the expense of the trade-off between FPR and FNR, there is an optimal point where the lines representing them intersect. Although EER helps to report research results and to compare the performance of CA systems, FPR and FNR are preferred for practical applications since they can be fine-tuned for their purpose. For the ProTego project, the aim is to reduce FPR to the minimum possible while keeping a reasonable number of false negatives. A false positive means that an illegitimate user is getting access to medical information. Although this can happen in a particular situation, e.g., smartphone is stolen, and the other security mechanisms of the ProTego toolkit will be in place to prevent or mitigate the breach, it is desirable to keep FPR at a very low rate. A false negative means that a legitimate user is negated access to his medical record. This results in a usability issue since the event raised will result in the user being logged off. Although this can be annoying from the user perspective, he can use his credentials to log in again.

All in all, we can use the ERR values reported in the existing literature to compare our findings with state-of-the-art approaches keeping in mind that it represents the point where FPR and FNR meet. Sitova et. al. presented a new set of metrics called HMOG (hand, movement, orientation, and grasp), and compared different combinations of user interaction for CA in smartphones (Sitová et al., 2016). The best results were obtained when combining their suggested HMOG metrics with keyboard metrics, returning an EER of 0.07. Although we preferred to report FPR and FNR, our results are around 0.09 for EER when combining 2 or 3 keypress events. Smith-Creasey and Rajarajan reported an EER of 0.0081 using gesture typing (Smith-Creasey & Rajarajan, 2019). However, gesture typing is an unusual way to input text in smartphones. When it comes to keyboard interactions in mobile phones, Clarke and Furnell reported an EER of 0.128 in early mobile handsets (Clarke & Furnell, 2007) using keypads.

Furthermore, Kambourakis et al. reported an FPR of 0.237 and an FNR of 0.035 (Kambourakis et al., 2016) for smartphones when including two new metrics. A comprehensive review by Pin Shen et al. surveys existing research and results on authentication for mobile devices (Teh et al., 2016) that can be used to compare ours and other approaches. Although they are limited to a reduced sample, our initial results are then promising, and they represent an initial test with ML classifiers for mobile CA.

8. Conclusion and Future Research Work

This paper presented the ProTego project and the CA approach that is being developed as part of it. A proof of concept of the architecture was developed with a keystroke mobile agent and ML models. The mobile agent captures the typing interactions of the user that are then used to feed ML classifiers that can predict future interactions. Five different ML classifiers were tested. Results suggest that ensemble algorithms can deal with the CA problem efficiently. When several consecutive events are combined to produce a single prediction, results are competitive with current state-of-the-art research on CA for mobile phones.

Future lines of research include increasing the research sample and the scope of the research to get results that have more potential for generalization. Since FNR impacts the usability of the proposed solution, we also suggest further experimentation to find and validate usability guidelines that can be used in mobile CA systems (Garcia-Lopez et al., 2021; Garcia-Lopez et al., 2017). From the IA modeling perspective, we can analyze other methods and classifiers and find new approaches to deal with the high dimensionality of data like feature selection or big data (Palma-Mendoza et al., 2019).

Acknowledgments

This project has received funding from the European Union's Horizon 2020 Research and innovation programme under grant agreement No. 826284.

References

5G-PPP. (2016). *5G Empowering vertical industries (White paper).* Retrieved from https://5g-ppp.eu/wp-content/uploads/2016/02/BROCHURE_5PPP_BAT2_PL.pdf

Abdulhak, S. A., & Abdulaziz, A. A. (2018, 11-14 Feb. 2018). *A systematic review of features identification and extraction for behavioral biometrie authentication in touchscreen mobile devices.* Paper presented at the 2018 20th International Conference on Advanced Communication Technology (ICACT).

Ahmed, A. A., & Traore, I. (2014). Biometric Recognition Based on Free-Text Keystroke Dynamics. *IEEE Transactions on Cybernetics, 44*(4), 458-472. doi:10.1109/TCYB.2013.2257745

Banerjee, S., & Woodard, D. L. (2012). Biometric Authentication and Identification Using Keystroke Dynamics: A Survey. *Journal of Pattern Recognition Research, 7*(1), 116-139. doi:10.13176/11.427

Bours, P., & Mondal, S. (2015). Continuous Authentication with Keystroke Dynamics. In Y. Zhong & Y. Deng (Eds.), *Recent Advances in User Authentication Using Keystroke Dynamics Biometrics* (Vol. 2, pp. 41-58). Thrace, Greece: Science Gate Publishing.

Breiman, L. (2001). Random Forests. *Machine Learning, 45*(1), 5-32. doi:10.1023/A:1010933404324

Cilleruelo, C., De-Marcos, L., Junquera-Sanchez, J., & Martinez-Herraiz, J. J. (2020). Interconnection between darknets. *IEEE Internet Computing*, inPress. doi:10.1109/MIC.2020.3037723

Clarke, N. L., & Furnell, S. M. (2007). Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security, 6*(1), 1-14. doi:10.1007/s10207-006-0006-6

de-Marcos, L., Cilleruelo, C., Junquera-Sánchez, J., & Martínez-Herráiz, J.-J. (2020). A Framework for BYOD Continuous Authentication: Case Study with Soft-Keyboard Metrics for Healthcare Environment. In H. Florez & S. Misra (Eds.), *Applied Informatics* (pp. 347-358). Cham: Springer International Publishing.

European Union, T. (2012). *The management of health systems in the EU Member States - The role of local and regional authorities*. (978-92-895-0717-2). Retrieved from https://cor.europa.eu/en/engage/studies/Documents/health-systems/health-systems-en.pdf

Friedman, J. H. (2001). Greedy Function Approximation: A Gradient Boosting Machine. *The Annals of Statistics, 29*(5), 1189-1232.

Garcia-Lopez, E., Garcia-Cabot, A., de-Marcos, L., & Moreira-Teixeira, A. (2021). An Experiment to Discover Usability Guidelines for Designing Mobile Tourist Apps. *Wireless Communications and Mobile Computing, 2021*, 2824632. doi:10.1155/2021/2824632

Garcia-Lopez, E., Garcia-Cabot, A., Manresa-Yee, C., de-Marcos, L., & Pages-Arevalo, C. (2017). Validation of navigation guidelines for improving usability in the mobile web. *Computer Standards & Interfaces, 52*, 51-62. doi:https://doi.org/10.1016/j.csi.2017.01.011

Geurts, P., Ernst, D., & Wehenkel, L. (2006). Extremely randomized trees. *Machine Learning, 63*(1), 5-32.

Giuffrida, C., Majdanik, K., Conti, M., & Bos, H. (2014). *I Sensed It Was You: Authenticating Mobile Users with Sensor-Enhanced Keystroke Dynamics.* Paper presented at the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Cham.

Junquera-Sánchez, J., Cilleruelo-Rodríguez, C., de-Marcos, L., & Martínez-Herráiz, J. J. (2020). JBCA: Designing an Adaptative Continuous Authentication Architecture. In L. M. Bergasa, M. Ocaña, R. Barea, E. López-Guillén, & P. Revenga (Eds.), *Advances in Physical Agents II* (pp. 194-209). Madrid: Springer International Publishing.

Kambourakis, G., Damopoulos, D., Papamartzivanos, D., & Pavlidakis, E. (2016). Introducing touchstroke: keystroke-based authentication system for smartphones. *9*(6), 542-554. doi:https://doi.org/10.1002/sec.1061

Malby, B., & Anderson-Wallace, M. (2016). *Networks in Healthcare: Managing Complex Relationships*: Emerald.

Palma-Mendoza, R.-J., de-Marcos, L., Rodriguez, D., & Alonso-Betanzos, A. (2019). Distributed correlation-based feature selection in spark. *Information Sciences, 496*, 287-299. doi:https://doi.org/10.1016/j.ins.2018.10.052

Shepherd, S. J. (1995, 16-18 May 1995). *Continuous authentication by analysis of keyboard typing characteristics.* Paper presented at the European Convention on Security and Detection, 1995.

Shuwandy, M. L., Zaidan, B. B., Zaidan, A. A., & Albahri, A. S. (2019). Sensor-Based mHealth Authentication for Real-Time Remote Healthcare Monitoring System: A Multilayer Systematic Review. *J Med Syst, 43*(2), 33. doi:10.1007/s10916-018-1149-5

Sitová, Z., Šeděnka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P., & Balagani, K. S. (2016). HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users. *IEEE Transactions on Information Forensics and Security, 11*(5), 877-892. doi:10.1109/TIFS.2015.2506542

Smith-Creasey, M., & Rajarajan, M. (2019). A novel word-independent gesture-typing continuous authentication scheme for mobile devices. *Computers & Security, 83,* 140-150. doi:https://doi.org/10.1016/j.cose.2019.02.001

Teh, P. S., Zhang, N., Teoh, A. B. J., & Chen, K. (2016). A survey on touch dynamics authentication in mobile devices. *Computers & Security, 59,* 210-235. doi:https://doi.org/10.1016/j.cose.2016.03.003