Authentication of Smartphone users Using Touch Based Data and Decision Tree Algorithms

Russell Mcilwain
Advisor: Dr. Kaushik Roy
Center for Cyber Defense (CCD)

North Carolina Agricultural and Technical State University

Cyber Identity & Biometric Lab
North Carolina A&T State University

Abstract

Currently around half of the of the world's population own smartphones or some type of touchscreen smart devices. Smartphone are responsible for most of the data being generated across the globe from messaging to web browsing, to instore purchasing. By using analytical features smartphones can tailor their settings based on the users' interactions with their applications. The user interaction can be sued to create a profile of the smartphone user. This in turn makes smartphones high risk items for theft and intrusion due their ability to connect to internet. In this research, we apply a randomized decision tree on touch analytics dataset [Frank et al.] to identify the users. In this effort, we were able to achieve 99%-100% testing accuracy through this algorithm.

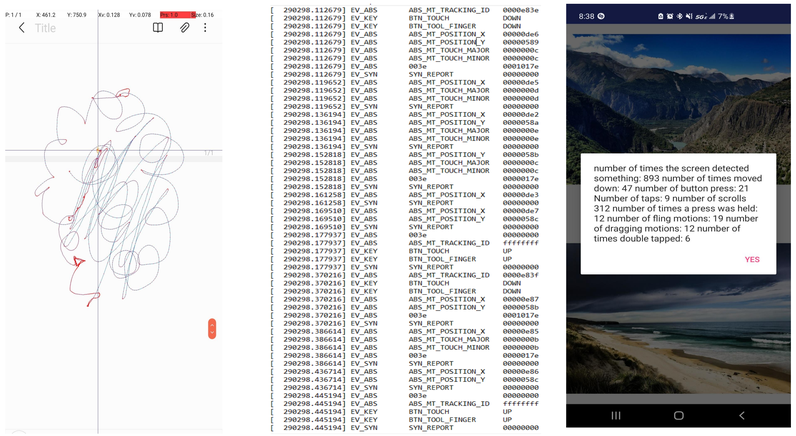
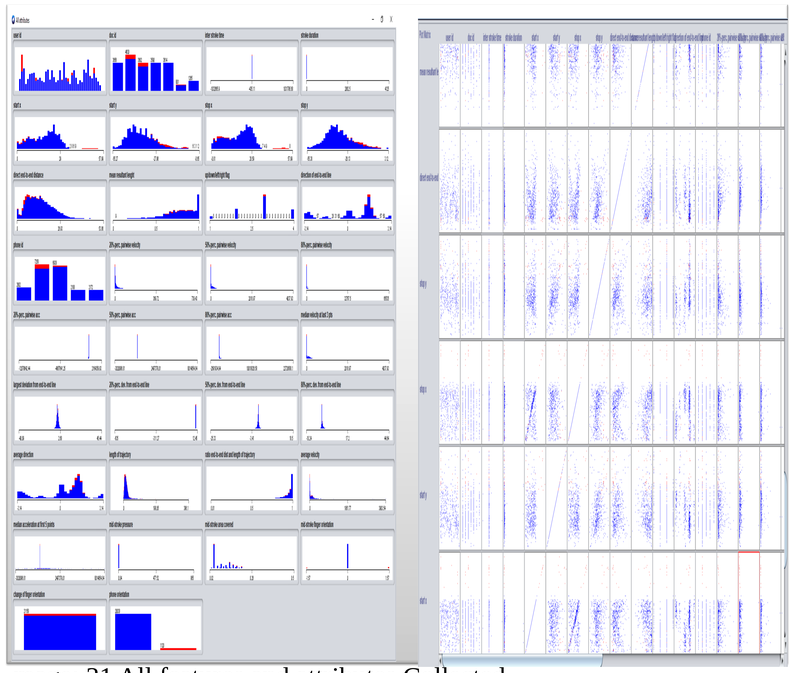


Image from the raw data visuals from the data set [Frank et al.].

Related Works

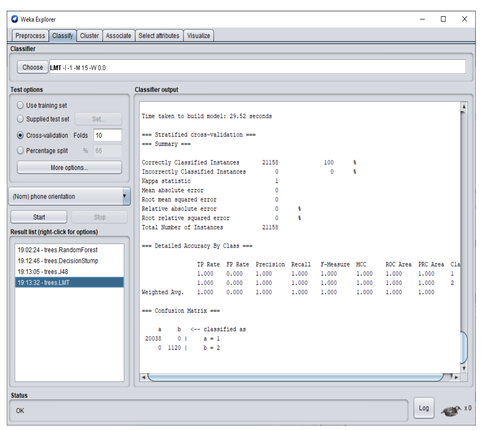
- Aljohani, N., Shelton, J., & Roy, K. (2021), IEEE CICS 2021. In this paper, authors used Artificial Immune System (AIS) to continuously authenticate the users on smartphones.
- Montgomery, M., Chatterjee, P., Roy, K. (2019), SpaCCS 2019. In this paper, an empirical evaluation of machine learning classification algorithms was conducted on touch data.
- Meng, Y., Wong, D. S., & Schlegel, R. (2012), ICISC 2012: Authors propose a user authentication scheme based on touch dynamics that uses a set of behavioral features related to touch dynamics for accurate user authentication. The neural network classifier is optimized by using Particle Swarm Optimization (PSO) to deal with variations in users' usage patterns.

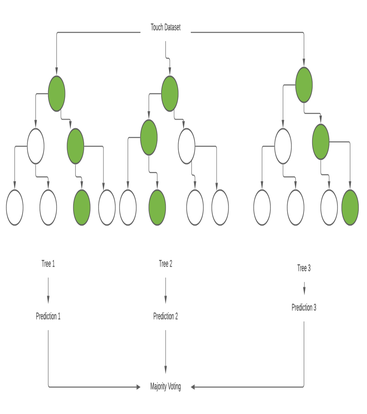


mage: 31 All features and attributes Collected

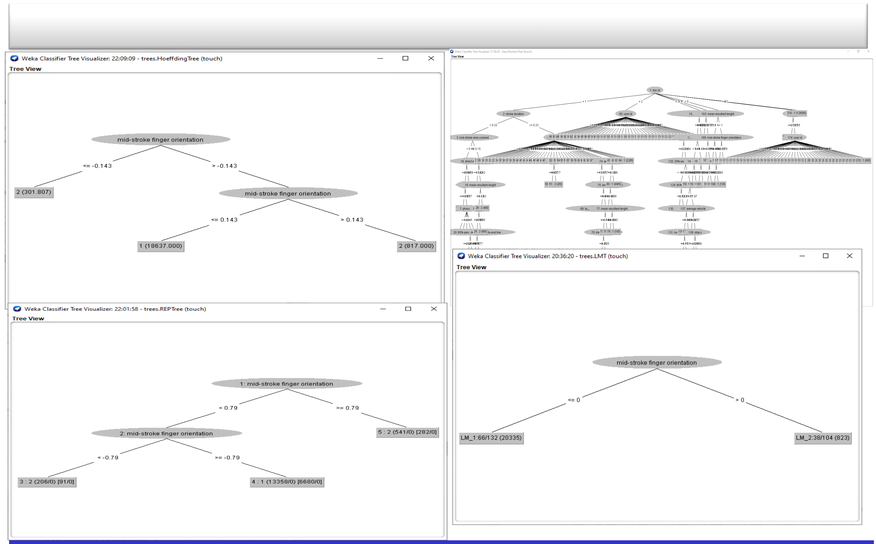
Methodology

- This research proposes Randomized decision tree forest, with 10 cross validation folds and a confusion matrix to help identify multiple attributes and features and perform tasks. This architecture is used to classify between the different users.





Results



Conclusion

- Our solution shows that with a baseline decision tree we can classify users via touch screen data
- In the future we plan to add more features and designs to our tree to create a more stable and through look into the set data.
- We will also be continuing the search for more or create more detailed dataset, looking to find ones with more available features and attributes so that we can used that material to further supplement the accuracy of our accuracy of our algorithms so that we can reach 100% accuracy

Acknowledgements

- NSA
- Center for Cyber Defense, NCAT

References

Frank et al. "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication." IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, 2013, pp. 136–148., https://doi.org/10.1109/tifs.2012.2225048.

Fenget al. "Continuous Mobile Authentication Using Touchscreen Gestures." 2012 IEEE Conference on Technologies for Homeland Security (HST), 2012, https://doi.org/10.1109/ths.2012.6459891.

Jiang, Lijun, and Weizhi Meng. "Smartphone User Authentication Using Touch Dynamics in the Big Data Era: Challenges and Opportunities." Signal Processing for Security Technologies, 2016, pp. 163–178., https://doi.org/10.1007/978-3-319-47301-7_7.

Shankar, Vishnu, and Karan Singh. "An Improved User Authentication Scheme on Smartphone Using Dominating Attribute of Touch Data." Journal of Discrete Mathematical Sciences and Cryptography, vol. 22, no. 8, 2019, pp. 1549–1561., https://doi.org/10.1080/09720529.2019.1695903.