Authentication Using Electrocardiogram Signals

1st Aditi Kumari
Department of Software Engineering
San Jose State University
San Jose, CA
aditi.kumari@sjsu.edu

2nd Anand Kumar
Department of Software Engineering
San Jose State University
San Jose, CA
anand.kumar@sjsu.edu

3rd Maahi Chatterjee
Department of Software Engineering
San Jose State University
San Jose, CA
maahi.chatterjee@sjsu.edu

4th Venkata Kondubhatla
Department of Software Engineering
San Jose State University
San Jose, CA
venkataeshaprajwal.kondubhatla@sjsu.edu

***Index Terms*—ECG, Authentication, Machine Learning**

***Abstract*—ECG or Electrocardiogram is a method used to record activities of the heart by placing diodes on the chest. These activities are displayed in the form of a graph and have been used in the medical industry to monitor the heart for decades. Past experimental results have proved that every individual's ECG has its own unique characteristics. Recently, several researchers have also shown that ECG can be a reliable source for emotion detection as well.**

Passwords comprising of characters are cumbersome, tedious to manage and auto-saving makes them vulnerable to attacks. Biometric authentication in the form of facial recognition and fingerprints have become a popular replacement for passwords in the present-day authentication requirements. However, different ways of stealing and using alternate sources for facial recognition like images, are gradually gaining popularity and therefore, a secure method for authentication which cannot be copied or stolen is an immediate need for all industries.

Our aim with this research project is to explore the possibility of using the electrical signals generated through ECG as a consistent and reliable authentication scheme by implementing complex machine learning algorithms.

I. Introduction

Biometric authentication is an extensively researched and well-deliberated topic amongst researchers concentrated on the expansion of technology in clinical use cases. Several biometrics authentication methods like facial recognition, retina scan and fingerprints are being studied to establish ways via which physiological and behavioral traits of human beings are being used as reliable attributes for authentication.

Character-based passwords are the most commonly used authentication method in the present day. But almost every service available online requires a password which makes it hard for users to memorize them and keep track of them. Research indicates that over 50% of users have the same passwords for different services [1] which makes the data vulnerable to attackers and data breaches. Several other mechanisms are being explored as a replacement for character-based passwords like graphical passwords [2] and trust scores [3]. However, biometrics remains a consistently popular choice because of its ease of use, accuracy, and uniqueness. Through this project, we explore and implement the idea of using the ECG signals from an individual's heart as a metric for authenticating users.

We explore ECG as our choice of biometric because of the following advantages:

- *Uniqueness*: Our heart contracts and relaxes at regular intervals for pumping blood throughout the body. This movement of the heart muscle generates an electrical impulse that is detected by the electrodes in the sensors. The pattern of the signal generated varies according to the dimensions of the heart valve which is unique to every person and hence the waveform generated by the muscles is also unique.
- *Secure*: Capturing an ECG signal requires the use of sensors and hence requires the individual's involvement and consent [4] unlike other biometrics like palm print, hand geometry, etc. This makes ECG data more secure and therefore, harder to replicate.
- *Universality*: Every living being has a heartbeat and hence has an ECG signal generated by their heart muscles. Therefore, it is safe to assume that ECG data can be attainable from any living source unlike other sources like fingerprints which can either get corrupted due to injuries or become unavailable due to amputation.

Although several research papers have been published about the use of ECG in authentication, there is a dearth of firm conclusions about the use of ECG as a biometric over a sustainable period. In this project, we use the data collected in a single session and the conclusions drawn can be expanded to data collected over multiple sessions. Since ECG can vary slightly due to factors like age and health conditions, data collected in multiple sessions over a spread-out time period is one of the most important aspects that are considered in the project. By establishing the mechanism with single-session data, comparison and analysis of conclusions from the multi-session data would become easier and would eventually lead to creating a fully covered stable authentication mechanism.

With the refinement of machine learning algorithms with every passing year, the prospects of ECG authentication look

brighter. In this project, we explore neural networks to train a realistic model for capturing a segment of the waveform and validating it against the data stored in the database. We will also be addressing the limitations with other biometrics against ECG. For instance, external biometrics like facial features are easier to scan and forge, internal biometrics like ECG are a better and safer option for authentication amongst other choices.

REFERENCES

[1] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The tangled web of password reuse. In NDSS, volume 14, pages 23–26, 2014.

[2] Susan Wiedenbeck, Jim Waters, Jean-Camille Birgit, Alex Brodskiy, and Nasir Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. International journal of human-computer studies, 63(1-2):102–127, 2005.

[3] Bjorn Markus Jakobsson, Mark J Grandcolas, Philippe JP Golle, Richard Chow, and Runting Shi. Implicit authentication, November 13, 2012. US Patent 8,312,157.

[4] Karimian, N., Guo, Z., Tehranipoor, M., Forte, D. (2017). Highly Reliable Key Generation From Electrocardiogram (ECG). IEEE Transactions on Biomedical Engineering, 64(6), 1400–1411. DOI: 10.1109/tbme.2016.2607020