Finger Print Authentication on Web-Services One Step to Next Security

Prof. Vidhya Dhoke[1], Ombase Abhijeet Suresh[2], Kharade Suraj Satish[3],
Nagane Sahil Sunil[4], Bhondwe Nisha Raju[5]
Guide, Department Of Information Technology[1]
Students, Department Of Information Technology[2,3,4,5]
Zeal College of Engineering and Research, Pune, Maharashtra, India
abhijeet.ombase@gmail.com[1], suraj.kharade99 @gmail.com[2], sahilnagane52@gmail.com[3], nishabhondwe8@gmail.com[4]

Abstract: *The system that automatically identifies the anthropometric fingerprint is one of the systems that interact directly with the user, which every day will be provided with a diverse database. This requires the system to be optimized to handle the process to meet the needs of users such as fast processing time, almost absolute accuracy, no errors in the real process. Therefore, in this paper, we propose the application of machine learning methods to develop fingerprint classification algorithms based on the singularity feature. The goal of the paper is to reduce the number of comparisons in automatic fingerprint recognition systems with large databases. The combination of using computer vision algorithms in the image pre-processing stage increases the calculation time, improves the quality of the input images, making the process of feature extraction highly effective and the classification process fast and accurate. The classification results on 3 datasets with the criteria for Precision, Recall, Accuracy evaluation and ROC analysis of algorithms show that the Random Forest (RF) algorithm has the best accuracy (≥96.75%) on all 3 databases, Support Vector Machine (SVM) has the best results (≥95.5%).*

Keywords: Fingerprint, Web Authentication, Security

I. INTRODUCTION

Reliable person identification is necessary due to the growing importance of the information technology and the necessity of the protection and access restriction. The identification or verification might serve for a purpose of an access grant. Everyone successfully identified and accepted may acquire certain privileges. In the lawsuit, the identification is very important as the best evidence. In this system there is one modules namely User. User can login using biometrics.

II. SCOPE AND OBJECTIVE

Security is an important aspect nowadays. It is safe to say that money and important document and all things related to money need security. Biometrics security as an investment and not an added expense. This technology provides the highest method of authentication ensuring unauthorized personnel cannot access the sensitive website and maintain the privacy.

III. PROBLEM STATEMENT

- Now days many internet accounts have been compromised due to hacking, people use common and similar passwords for all accounts.
- Frauds happening all around the internet.
- For each and every account user need to have Id and password and they might face problem remembering them.
- To hack into someone's account and get their personal information, there are many tools available
- To prevent happening this things like resetting Password, Forgot password & OTP Generation.

IV. METHODOLOGY

SecuGen WebAPI is an application programming interface that enables web applications to access SecuGen fingerprint readers from most modern web browsers. With support for JavaScript access to the readers, SecuGen WebAPI can be used across different browsers for extremely fast capturing and matching of fingerprint data for use in a web application.

SecuGen WebAPI makes it very simple to incorporate fingerprint capturing functionality in your browser based application through JavaScript. Using SecuGen WebAPI eliminates the need for Java runtimes or browser plug-ins on the client machine, so there are no issues involving applet signing and deployment related to different JRE versions and browser versions. This document describes the RESTFUL web service calls that are supported by SecuGen WebAPI.

1. SGIFPCapture
2. SGIEnrollCapture
3. SGIMatchScore

4.1 SGIFPCapture

The SGIFPCapture service returns fingerprint data, details of the fingerprint reader, and the extracted template to the caller as a JSON object. For HTTP requests, this service can be called as URI https://localhost:8000/SGIFPCapture. The port number may change depending on the way the service is configured. The default port for the service is 8000.

4.2 SGIEnrollCapture

The SGIEnrollCapture service is useful for capturing multiple fingerprints from the fingerprint reader. The parameters are the same as those used for SGIFPCapture and can be used to capture one fingerprint as well. For HTTP requests, this service can be called as URI https://localhost:8000/SGIFPEnroll. The port number may change depending on the way the service is configured. The default port for the service is 8000.

The first call to this service creates a unique session and returns the session handle in the returned JSON object. The caller can use this handle for subsequent calls to capture additional fingerprints in the same session. These are accumulated by the service until the session ends. The session ends when the service is called with a null session handle or no session handle.

Every call returns a JSON object containing all the templates captured up until that point. If you wish to capture multiple fingerprints, call this service the first time with the SrvHandle parameter as null (or do not provide it at all). When the call returns, you will receive a session handle as part of the JSON object, which you can keep on passing for as long as you wish the fingerprint scans to be accumulated.

Call this service once for each capture along with the same server handle to accumulate fingerprint scans. The service also ensures that one fingerprint is present only once in the array, i.e. a local duplicate check is performed on the client end. The returned JSON object will contain an array of templates and current scan data.

4.3 SGIMATCHScore

The SGIMatchScore service takes two templates as input, compares them with each other, and returns a matching score back to the calling application. For HTTP requests, this service can be called as URI https://localhost:8000/SGIMatchScore. The port number may change depending on the way the service is configured. The default port for the service is 8000.

V. SYSTEM ARCHITECTURE
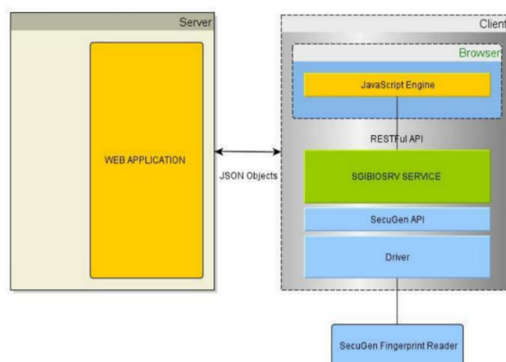
VI. SECUGEN BIOMETRIC DEVICE

SecuGen Hamster Pro 20 Biometric Finger Print Scanner

VII. ADVANTAGES

1. This system is supposed to be extremely reliable.
2. Biometric security systems are highly secure.
3. The protected devices impossible to be misused due to the biometric protection

VIII. ACKNOWLEDGMENT

We are pleased to present "Finger Print Authentication on Web Services" project and take this opportunity to express our profound gratitude to all those people who helped us in completion of this project. We thank our college for providing us with excellent facilities that helped us to complete and present this project also special thanks to our Guide Prof Sneha Vanjari.

IX. CONCLUSION

This was our project of System Design about "Fingerprint Authentication on Web Services" developed as web application based on Asp .Net programming language. The Development of this system takes a lot of efforts from us. We think this system gave a lot of satisfaction to all of us. Though every task is never said to be perfect in this development field even more improvement may be possible in this application. We learned so many things and gained a lot of knowledge about development field. We hope this will prove fruitful to us.

REFERENCES

[1]. Nagar, K. Nandakumar and A. K.Jain, "Multibiometric
[2]. Cryptosystems Based on Feature-Level Fusion," IEEE ,pp. 256-278, Feb 2012.
[3]. Norman Poh and Josef Kittler, "A Unified Framework for Biometric Expert Fusion Incorporating Quality Measures," IEEE , pp. 3-17, Jan 2012.
[4]. J.Dai and J.Zhou, "Multifeature Based High-Resolution palmprint Recognition,", IEEE , pp. 945-957, May 2011.
[5]. E. Maiorana and P. Campisi, "Fuzzy Commitment for Function based Signature Template Protection," IEEE, pp.249–252, Mar 2010