RESEARCH ARTICLE OPEN ACCESS

Biometrics security and Its Implementation in Linux PC Systems

Md. Yasir Shaukat [1], Mr. Tabrej Ahamad Khan [2]
[1] Department of Computer Science and Engineering, Jamia Hamdard University, New Delhi
[2] Department of Computer Science and Engineering, Jamia Hamdard University, New Delhi

ABSTRACT
In growing days, increase in threats to safety and security to personal computers data has given rise to introduction of Multifactor Authentication techniques to authenticate into a system which are predominantly of biometric nature. Although biometrics authentication is a complex process and needs specific hardware and software capabilities, more and more PC systems are getting equipped with it. Due to multiplicity of Linux Operating System distributions most of the distributions don't have inbuilt biometrics authentication system. This work focuses on working and function of biometrics authentication and how biometrics authentication can be instated in a Linux OS, its software/hardware architecture, its end results and limitations in real world use.

Keywords: - Biometrics, Authentication, Linux.

I. INTRODUCTION

The global Linux user base, estimated at 33 million users, represents roughly 2.66% of the worldwide PC market. While Linux offers numerous advantages, including flexibility, customization, and robustness, its widespread adoption also presents security challenges. Among these challenges is the vulnerability of traditional authentication methods, such as passcodes, which can be easily compromised, posing significant risks to system security. To address these vulnerabilities, there is a growing emphasis on leveraging biometric authentication methods. Biometrics offer a promising solution, as they not only mitigate security risks but also provide convenience to users. Unlike traditional methods, biometric authentication eliminates the need for additional tokens, such as RFID cards, and reduces concerns about password disclosure or cracking.

Although biometric authentication is prevalent in Windows and MacOS environments, its integration into Linux-powered operating systems is relatively limited. This disparity can be attributed to several factors, including the diverse array of Linux distributions, limited hardware support, and the scarcity of PC manufacturers pre-installing Linux OS by default. In response to this challenge, various libraries and repositories have been developed to facilitate biometric authentication across different Linux distributions. These resources offer a pathway for implementing biometric authentication, provided that the necessary hardware and software requirements are met.

By leveraging these libraries and repositories, Linux users can enhance the security of their systems while benefiting from the convenience of biometric authentication. However, it is essential to recognize the limitations and challenges associated with implementing biometric authentication in Linux environments, including compatibility issues and the need for ongoing support and maintenance.

Overall, the integration of biometric authentication represents a significant step forward in enhancing the security posture of Linux-powered systems, offering users a robust and user-friendly authentication solution in an increasingly digitized world.

II. BIOMETRICS SECURITY: AN OUTLINE

The term biometrics is derived from combination oof two Greek words 'bios' and 'metrikos' meaning 'life' and 'measuring' respectively.

Each individual has different and distinct set of characteristics which makes us differentiate among them, the characteristics are either behavioural or psychological. Over the growing period of time the population has risen drastically and over the time it has been become very important to differentiate or identify individuals. Identification of an individual among various test inputs in very necessary because it is necessary in saving one's individuality and saving an individual from various identity thefts and other security related concerns.

To differentiate among human individuals, we consider parts of their physical features which are distinct to other individuals. Humans take features like facial structures, skin complexion, pitch of voice, eye colour, height, geographical location of the subject and various other factors of differentiation to individualise a subject. When a computer system has to differentiate among individuals or confirm someone's identity it compares factors like pattern of ridges on the tip of the finger, pattern of ridges on the palm, facial structural geometry, unique pattern of retinal blood vessel, segments of frequencies from one's speech, and few other factors. All the listed method of recognition of a human individual by a computer system is called authentication. Authentication is when a computer system recognises and grants or denies access to a person based on matching of biometric parameters provided by the user against the already enrolled dataset.

The computer system authentication is based on 3 major common methods:

1. Something that person knows i.e. passwords, passphrases, Personal I dentification Numbers etc.
2. Something that user is i.e. identity based on fingerprints, pattern of retinal blood vessel etc.
3. Something that the user has i.e. passkeys, RFID cards etc.

III. HOW THE AUTHENTICATION IS PERFORMED

In a biometrics system the system authenticates by comparing the test input (biometrics input from the user that requests access) with the already stored data of that has to granted the access to. In this whole process 'one-to-many' type of comparison is performed by the system.

Further the biometrics is broken into two types: 1. Static biometrics. 2. Dynamic Biometrics. Static biometrics are the ones that are not based on the behavioural pattern of what the user does but only the fixed characteristics of the person like fingerprint, retinal vein pattern, palm geometry. Whereas Dynamic Biometrics refers to the biometrics where the authentication is performed by noticing pattern of what/how user does/behaves i.e. voice pattern, gait (walking pattern) etc.

IV. GENERIC BIOMETRICS

A generic biometric system is based on the subsequent building blocks discussed in the subsequent sections. Fig.1[2]

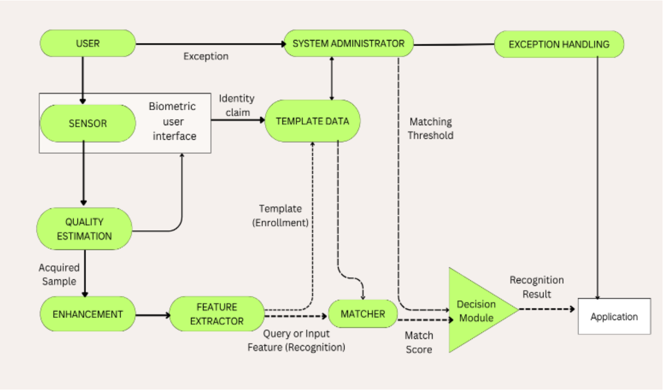

Fig 1. A generic biometrics system

A. Enrolment and Recognition Phase

Enrolment and Recognition phase is itself broken into two parts- 1. enrolment and 2. Recognition[2]. During enrolment phase, the user successfully enrols his/her biometrics data along with his identity and the system extracts the data provided by the user. Normally the extracted data is processed and only outstanding distinguishable features are stored and the rest of the un useful part isn't stored.

During the recognition phase the system tries to recognise the test input by comparing the enrolled data with the test data provided.

The pattern recognition system consists of 4 modules.

1. Sensor Module

It is the hardware part of the biometric system. It may be an optical fingerprint sensor or retinal scanner etc. Data is entered into the system by the sensor module, for fast, efficient, highly readable data it is preferred that the sensor module is of good quality and higher capabilities so that it could read even the minute details of the input provided.

2. Feature Extraction Module

The data entered into the hardware module is raw data and it has to be pre-processed before comparing it with the stored value or storing it.

First step of the feature extraction module is to assess the quality and degree of readability of the entered raw data. Further process of segmentation, noise reduction, smoothing image for readability are initiated only when the entered data is assessed to be of good quality of readability otherwise a request is raised regarding the same.

3. Database Modules

Database module has two types, centralised database or decentralised database. In centralised database the data is stored into one central server and in decentralised database data isn't stored on single server but multiple servers which is beneficial in data recovery if the stored biometrics data is deleted or destroyed from one location by any possible cause. In database module all the biometrics data that is enrolled and processed in Feature Extraction Module is stored with some identifier relating to the registrant of the biometric data. It can be a password, a PIN, a question phrase, etc.

4. Matching Module

The matching module compares the biometric data provided by the query subject with the already stored data in the Database module. A match score is generated which tells about the degree of simulation between the stored data template and the query provided. A lower score means a lower chance of successful authentication and a higher score leads to higher chance of successful authentication.

A. Verification

After enrolment and recognition comes the verification stage. It is basically the verification or confirmation of weather the query subject is to be given access or not. Sometimes the system asks for confirmation by asking the user to provide his identification which has already store during the time of enrolment along with his biometric data, which is stored in the Database Module.

The decision of authentication[6] is given by

$$(I, \mathbf{x}^A) \in \begin{cases} \text{genuine}, & \text{if } s \geq \eta, \\ \text{impostor}, & \text{if } s < \eta, \end{cases}$$

Where x^A is the input query, and I is the identity stored in the database module. S is the match score and η is predefined threshold.

B. Identification

Identification is the final stage; the result is either positive/true or negative/false which is whether the query feature is implicitly or explicitly hiding his true identity or not.

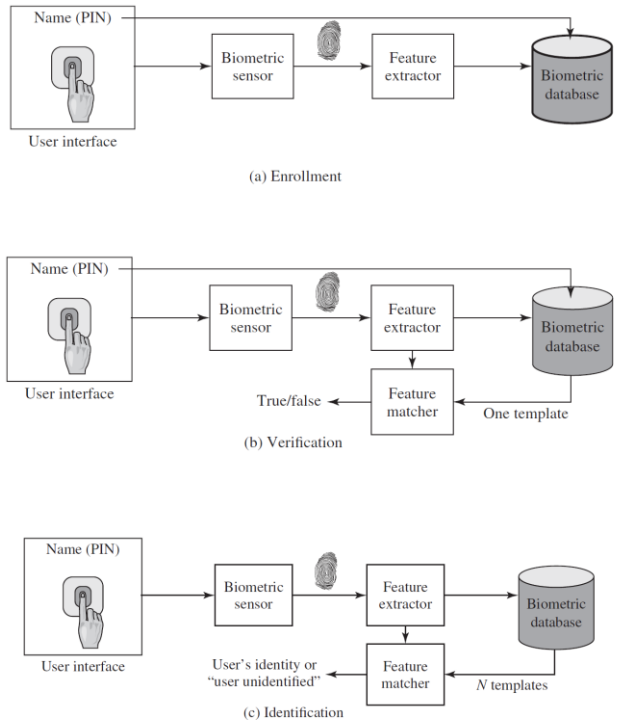

Fig. 2.[1] Biometric System: Enrolment & Recognition, Verification and Identification stages.

V. BIOMETRICS AUTHENTICATION IN LINUX PC SYSTEMS.

Consumer end Linux PC Systems Distributions allows biometric authentication through several ways. Many other means for biometric authentication are still in development for consumer end software distributions. Biometric authentication into Linux Based PC Systems is mainly done by means of fingerprint and facial recognition biometric methods.

A. Authentication Using Fingerprint Recognition

The authentication using fingerprint is done by identifying unique pattern of ridges, arches, lines and loops on one's fingertip. It is one of the most used ways of biometrically authentication in Linux Systems.

The authentication process works in phases as in 2.1.

The phases of enrolment, identification and verification are completed by a hardware and a software unit.
We're using Ubuntu 22.04.03 LTS as our Linux PC distro. The fingerprint sensor module is inbuilt in PC System model K143EA-EB312W.

Hardware Unit: We're using the inbuilt ultrasonic fingerprint reader in our computer system, capable of taking high-quality and precise inputs from the user and live scanning too.

Software Unit: Ubuntu 22.04.03 LTS comes with out of the box fingerprint authentication support in which all the process are controlled in the 'Users' section of the 'Settings' application.

We're We run the command $lsusb in the terminal to get information about the fingerprint reader and manufacturer information.

To enrol fingerprint, user password is required. The in-built fingerprint authentication facility in Ubuntu provides various options like deletion, updation, re-enrolment, adding multiple fingers.

Libfprint

Figures and tables must be centered in the column. Large figures and tables may span across both columns. Any table or figure that takes up more than 1 column width must be positioned either at the top or at the bottom of the page. Libfprint is an open source Linux library under fprint project[3]. It does the job of interacting with the hardware unit i.e. our fingerprint sensor and performs the software process of fingerprint enrolment, verification and identification.

Fprintd

It is a background software component working on D-Bas interface providing fingerprint authentication services. Prerequisites of enrolling a fingerprint is authentication of Pluggable Authentication Module (PAM)[3].

It is installed by command $sudo apt install fprintd libpam-fprintd and later in the process the fingerprint is enrolled by $fprintd enrol command. We edit and save the config file in nano editor and the system is updated and upgraded. We test our authentication by rebooting the system and logging in again by use of fingerprint authentication.

B. Results and Limitations of the fingerprint authentication system

The process of registration and enrolment is a bit slower using the system's inbuilt fingerprint authentication facility than the fprintd software. The efficiency is highly dependent on quality of fingerprint pattern registered on the system which might take few attempts to register a good quality and highly recognisable fingerprint. Authentication capabilities are depended on the finger's physical state as they fail to recognise finger which is soaked in dirt, water or having wrinkles[5].

VI. AUTHENTICATION USING FACIAL RECOGNITION

The idea of distinguishing/recognising faces by its various distinct characteristics was first propounded in the year 1888 by Sir Francis Gabon.

The authentication using facial recognition method is performed by scanning the face from forehead to chin and matching the data with the already stored template.

The algorithm of recognising individual faces by distinguishing between geometric pattern of facial structure and its features is called Geometric facial recognition algorithm.

Photometric facial recognition algorithm is applied when only the value of facial images is compared to authenticate.

The facial features read by the system are shape of the face and its features like eyes, eyebrows, nose, lips, structure and depth on points on faces, moles, scars, skin colouration etc.

Hardware Unit: We're using the inbuilt ultrasonic fingerprint For facial recognition and authentication in Linux a hardware component is required which comprises not just of the camera module capable of facial recognition but also an Infrared Emitter as optional for getting enhancement in facial identification and capturing best details about the features of the face. We're using the inbuilt camera module on our computer system with Ubuntu 22.04.03 Linux distribution supporting the software end.

Software Unit: Since the distribution used doesn't have out of the box support for facial authentication, which is only available on Deeping OS 20.5+ Linux distributions, so we're using a freely distributed software howdy to setup facial based authentication on our system.

Howdy

This software allows user to authenticate through the user login on the system. It uses computer's inbuilt camera and IR Emitter to provide Windows Hello^{TM} Style authentication[4].

Implementation of howdy

Initially we add a Personal Package Archive (PPA) for howdy. We update and upgrade our system before installing howdy. Howdy is being installed using Advanced Package Tool or famously apt, after installation of howdy we register the sample face using 'add' option command and a message 'Scan Complete' is prompted on the screen.

By $howdy we're displayed with all the howdy configuration options like adding new face, removing/deleting already registered face models, listing information about all the faces enrolled, enabling and disabling a face model is also provided by howdy.

The system is rebooted and the successful authentication is performed by providing correct face sample at time of user login.

VII. RESULTS AND LIMITATIONS OF FACIAL AUTHENTICATION SYSTEM

The registration of the face model was completed in matter of few seconds and efficiency and speed the unlocking of the device using registered face model depended on the visibility of face template on the various lightning conditions (amount, angle and colour of light falling on the face), angle of presenting face to the camera also affected the accuracy of results.

Due to lack of different sophisticated hardware support the facial authentication on Linux is highly affected by change in lightning conditions (Dim lights especially), higher width and length of the reach of the camera module and most importantly the quality of the facial images taken.

VIII. CONCLUSION

This paper gives an outline of how the authentication based on biometrics techniques works, its components, phases involved, and algorithms performing behind the process performed.

In the context of consumer-end Linux PC systems, the integration of biometric authentication modalities, notably fingerprint and facial recognition methods, has witnessed notable strides. While fingerprint authentication stands out for its inherent reliability and user-friendly interface, facial recognition modalities present distinct challenges stemming from nuanced hardware requisites and environmental variabilities.

Looking ahead, the trajectory of biometric security systems portends a pivotal role in fortifying security frameworks across diverse domains. However, it is incumbent upon ongoing research endeavours and developmental initiatives to address existing limitations and refine the precision and dependability of biometric authentication systems, thereby bolstering their efficacy in real-world deployment scenarios.

Sizable amount of research was performed on the study of the Linux authentication system and previous research done on biometric authentication process and a test environment was developed to conduct the tests of the biometric authentication on the consumer end Linux OS distribution.

The precision results are likely to differ if different conditions are provided or if the number of times the test is performed.

REFERENCES

[1] Williaam Stallings. Lawrie Brown, Computer Security Principles And Practice, Third Edition, 2015.

[2] Introduction to Biometrics, Anil K. Jain, Arun A. Ross, Karthik Nandakumar, 2015

[3] Fingerprint Reader Support- https://fprint.freedesktop.org/

[4] Howdy- https://wiki.archlinux.org/title/Howdy

[5] Study on Biometric Authentication Systems, Challenges and Future Trends: A Review, Krishna Dharavath, F. A. Talukdar, R. H. Laskar.

[6] Embedded System for Biometric Identification, Ahmad Nasir Che Rosli (2010), InTech. doi: 10.5772/9296.