Biometrics Authentication Implementation Using Raspberry Pi

Shivani Kumawat
[1, 2] Dept of Electronics and Communication Engineering
[1, 2] Poornima College of Engineering, Jaipur, Rajasthan, India

Abstract- *The term Biometrics is a mix of two words-bio i.e. life and measurements i.e. estimation. It alludes to the measurements identified with the human qualities, especially the physical and behavioral perspectives. The innovation is actualized to measure and factually analyse individuals' biological data predominantly for their ID, access control and surveillance. Each individual is one of a kind and conveys a different character in traits like fingerprints, hand geometry, iris acknowledgment, voice, and so on. Advancements in the field of Information Technology additionally make Information Security an important part of it. So as to manage security, Authentication assumes a basic part. In this paper, Biometrics is utilized for validation. This paper likewise portrays how biometrics can use cloud's limitless computational assets and striking properties of adaptability, versatility, and cost lessening keeping in mind the end goal to decrease the cost of the biometrics framework necessities of various computational assets (i.e. handling force or information stockpiling) and to improve the execution of biometrics frameworks' procedures (i.e. biometric coordinating). Here, Raspberry Pi is utilized to manufacture a minimal effort biometric framework. Raspberry Pi (RPi) is acknowledged as an estimated little PC for extraordinary capacities like a PC.*

Keywords *- Internet-of-Things (IoT), Raspberry Pi (RPi), Cloud, Biometrics, Biometric Security*

I. INTRODUCTION

A reliable identity authentication and verification administration system framework is required keeping in mind the end goal to check the widespread development in data fraud and to meet the expanded security prerequisites in an assortment of uses like crime scene investigation, government, transportation, human services, accounts, security, open equity and wellbeing, and instruction[1][2]. Information security is concerned with the guarantee of confidentiality, integrity and availability of information in all forms. Biometric authentication bolsters the part of recognizable proof, verification and non-repudiation in data security. Surrogate portrayals of character, for example, passwords and ID cards are not adequate for dependable identity determination since they can be effectively lost, shared, or stolen. Biometric recognition is the art of building up the personality of people in view of their measurable biological (anatomical or physiological) or behavioral attributes [3].

Biometrics can be classified in two groups:

1) Biological biometrics: Examples of biological biometrics modalities include fingerprint, hand geometry, iris, face, and ear.

2) Behavioural biometrics: Examples of behavioural biometrics modalities comprise gait, signature, and keystroke dynamics.

Biometric authentication has to have a high level of accuracy (i.e. Genuine Accept Rate (GAR) and False Accept Rate (FAR)) to be secure and practical for widespread adoption in different applications [4]. The problem in the adoption of biometrics is the lack of accessibility and scalability of existing biometric technology and also the high cost of implementing biometric systems. It is important to define exceedingly adaptable biometric innovation, equipped for working on colossal measures of information, which, thusly, initiates the requirement for adequate capacity limit and huge handling power. The primary arrangement that rings a bell as for the characterized issues is moving the current biometric innovation to a cloud stage that affirms suitable adaptability of the innovation, adequate measures of capacity, parallel handling abilities and cost decrease. Additionally cost of the biometric can be lessened by the utilization of an ease IoT gadget, Raspberry Pi. The appeal of the Raspberry Pi originates from a blend of the PC's little size and moderate cost. Raspberry Pi, a charge card measured minimal effort Linux PC can be utilized to build up a biometric engineering as it has arrangement of associating with cameras, unique mark scanners and so forth through USB ports. It has an Ethernet port for Internet availability or can be associated with a Wi-Fi hotspot through USB Wi-Fi connectors.

Security of biometric data is another worry to manage. Since, the biometric qualities are utilizing the cloud for capacity, execution and adaptability highlights, it is

imperative to exchange them safely from the customer machine to the remote server. Henceforth, in this paper end-to-end encryption process is proposed. Encryption is finished utilizing upgraded AES-256 with Round structure and dynamic S-box age utilizing pseudo-commotion succession generator. The proposed encryption calculation will fortify the security and many-sided quality of the proposed IoT based biometrics framework [5].

II. IOT BASED BIOMETRICSIMPLEMENTATION ON RASPBERRY PI

The proposed system is a multimodal biometric system; face and unique mark are the biometric qualities under thought. The proposed IoT based biometrics engineering comprises of 3 modules as shown in the figure 1: Raspberry Pi as a remote enrolment hub, improved AES-256 for security and the Azure cloud for capacity, adaptability and execution concerns. The FS88 scanner is interfaced utilizing LibScan API and libusb libraries on the RPi. After the interfacing of webcam the RPi is prepared for enrolment process. When the sensor recognizes movement, a work area application opens up which starts the enlistment/login process. After the picture catching procedure, the biometrics are encoded on the RPi on Mono Developer (C# dialect) utilizing the proposed AES-256 calculation alongside Round structure and dynamic S-box age in light of pseudo clamor arrangement generator as clarified underneath. The last advance is to transfer the scrambled pictures on the Azure cloud where they are put away in blobs inside the enroll/login compartments relying upon whether the client is as of now enlisted or he is another client. After the decoding procedure on the cloud, the first biometric characteristics are recovered.
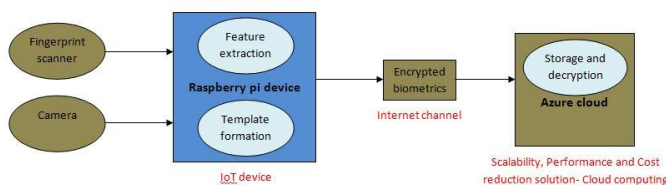

Fig. 1: Biometrics implementation using Raspberry Pi

This section focuses on the results after the implementation of the IoT based system. Results are produced in following way: Raspberry Pi as a remote enrolment node, proposed AES-256 analysis and the uploading of encrypted images to the register/login containers. Figure 2 shows the image capturing application on Raspbian using Mono Develop.

The following part is to scramble biometric characteristics to guarantee security of the normal in-travel to

the Azure. The biometric data is changed over into cipher data utilizing the proposed AES-256 calculation on the RPi customer. Next, on the Linux working framework we have completed a correlation of typical AES-256 and the proposed AES-256 with Round structure of 14 rounds and dynamic S-box. The examination parameters incorporate encryption time, CPU and memory. The contribution to the calculations is the Fingerprint picture whose size is 1228800bits.

III. HARDWARE DESCRIPTION

The proposed system is a multimodal biometric system; face and fingerprint are the biometric traits under consideration. The hardware requirements for the remote enrolment node are listed below:

In this research, Raspberry Pi 2 Model B is used which costs US $35. It has 4 USB ports, a HDMI port for connection with the display, micro SD card slot for booting and data storage as RPi doesn't have on-board storage. Also it has 10/100 Mbit/s Ethernet port for internet connection. To make RPi portable in this paper wireless USB Wi-Fi adapter is used. The OS used is Raspbian (Debian wheezy). RPi needs power supply of 5V-800mA (4.0 W). In order to make the proposed portable, RPi is supplied power through power bank. RPi 2 has 1GB RAM and CPU speed is 900 MHz quad core ARM Cortex-A7. It is a Broadcom2835 System-on-chip hardware. One powerful features of the Raspberry Pi is the row of GPIO pins along the edge of the board as shown in Figure 1. These pins are a physical interface between the Pi and the outside world. Other peripheral include Passive Infrared motion sensor for the sensing the motion, Futronics FS88 fingerprint scanner and the HP-3100 USB webcam for capturing the biometric traits, finger and face respectively.

IV. CONCLUSION

In this examination, an ease of IoT based biometrics engineering is exhibited. Raspberry Pi is effectively executed as a remote enrolment hub. The encoded biometric characteristics are sent to the Azure cloud for decoding. The proposed framework can be utilized for security and access control instruments like opening an entryway, logging points of interest of a man entering and leaving a building, participation administration, getting to a specific administration and so on. This framework can be connected at all spots where validation is required.

V. ACKNOWLWDGMENT

REFERENCES

[1] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, Review Article: Biometric Template Security, Journal on Advances in Signal Processing Volume 2008, Article ID 579416.

[2] Debnath Bhattacharyya, Rahul Ranjan1, Farkhod Alisherov A., and Minkyu Choi, Biometric Authentication: A Review, International Journal of u- and e- Service, Science and Technology, Vol. 2, No. 3, September, 2009.

[3] http://biometrics.gov/Documents/Glossary.pdf, National Science and Technology Council's (NSTC) Subcommittee on Biometrics, Biometrics Glossary, 2006.

[4] Abdullah A. Albahdal and Terrance E. Boult, Problems and Promises of Using the Cloud and Biometrics ResearchGate publications, 17th November 2015.

[5] Peter Peer and Jernej Bule, Jerneja Zganec Gros and Vitomir Struc., Building Cloud-based Biometric Services, Informatica 37 (2013) 115–122 115.