IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

TWO WAY AUTHENTICATION USING RASPBERRY PI

M.MANMADHA RAO
AIT-CSE
CHANDIGARH UNIVERSITY
MOHALI, PUNJAB

P. SRI PRANEETH
AIT- CSE
CHANDIGARH UNIVERSIRTY
MOHALI, PUNJAB

ARNAV GUPTA
AIT- CSE
CHANDIGARH UNIVERSITY
MOHALI, PUNJAB

VIJAY BHARDWAJ
AIT-CSE
CHANDIGARH UNIVERSITY
MOHALI, PUNJAB

Abstract: -Authentication is a key component of access control systems to verify users and prevent unauthorized access. Traditional one-way authentication systems only authenticate users but not vice versa. This leads to potential risks of impersonation attacks. This project presents a prototype two-way authentication system using an inexpensive Raspberry Pi single board computer.

The system utilizes the Raspberry Pi to act as an authentication server. It is connected to door locks, cameras and other sensors to control physical access. Users authenticate to the Pi over a wireless network using a mobile app. When authentication is successful, the Pi will grant door access. Additionally, the Pi uses cameras and sensors to capture and verify the user's presence. This provides two-way authentication by verifying not only the user to the system, but also authenticating the system to the user.

Initial testing shows the Raspberry Pi is capable of handling the authentication workload and integrating with common access control devices. The two-way authentication approach helps address risks of impersonation and provides better access security assurance than traditional one-way systems. The low-cost Raspberry Pi makes this kind of advanced access control more accessible. Future work will focus on expanding system functionality and testing real-world deployment scenarios.

Key-Words: - Two-way authentication, Raspberry-Pi, One time password, Authentication server, Multi factor authentication, Cyber Security.

1. INTRODUCTIONAuthentication plays a crucial role in controlling access and ensuring security. Traditionally, many access control systems have utilized one-way authentication methods that only verify the identity of a user attempting to access a restricted area or resource. However, these one-way schemes do not also authenticate the system to confirm it is legitimate to the user. This asymmetry leaves gaps that could potentially be exploited by impersonation attacks.

Two-way, or mutual, authentication aims to establish trust in both directions between user and system. It provides a more robust form of access control by requiring confirmation of both identities - not just the user to the system, but also the system to the user. This helps prevent against man-in-the-middle attacks where an unauthorized party may be able to intercept communications and gain access by posing as either side. Two-way authentication techniques offer stronger protection and have seen wider deployment for network-based access. However, physical access control scenarios have been slower to adopt two-way methods. Traditional embedded authentication controllers for doors, gates and other physical points of entry often have limitations that make robust mutual verification difficult. They generally have limited processing capability, memory constraints and a lack of suitable interfaces for integrating cameras, sensors and other devices needed for two-way schemes. This has made advanced two-way techniques cost- prohibitive or functionally infeasible on many existing physical access control platforms. This project aims to develop a prototype two-way authentication system for physical access using an inexpensive Raspberry Pi single-board computer. The Raspberry Pi provides sufficient computational resources and versatile interfacing options to control doors and readers while running authentication software. It can potentially authenticate users via mobile applications over Wi-Fi

networks, while also verifying their presence using integrated camera feeds - establishing trust in both directions. Initial

experiments explore the Raspberry Pi's capability for performing two-way authentication at a much lower overall system cost than proprietary controllers. The results have implications for making this stronger form of access control economically viable for deployment in practical physical security applications.

2. LITERATURE SURVEY

Advancements in Information Technology have led to Information security is incorporated as a fundamental element. In order to solve security problems, authentication is essential. The use of biometrics for authentication is the main topic of this article. It looks at how biometrics may use the cloud's enormous processing power to suit the many needs of biometric systems while providing flexibility, scalability, and cost savings. The study uses a Raspberry Pi to build a biometric system at a reasonable price. This study uses a Raspberry Pi, a credit-sized minicomputer with features similar to a PC, as a remote enrollment node. The Internet of Things (IoT) has expanded into new areas thanks to the Raspberry Pi and cloud computing combination. systems for biometric authentication, employing fingerprint, iris, and other unique identifiers, are highlighted for their effectiveness in ensuring security and attendance tracking. Fingerprint-based biometric systems are emphasized for their balance between low cost and high accuracy.

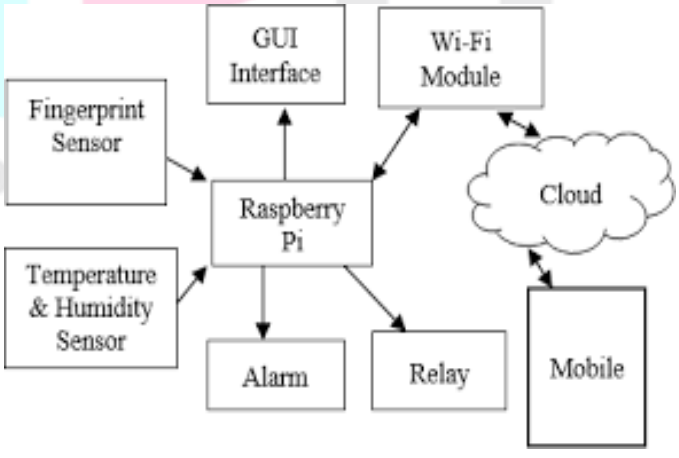
The study emphasizes that in the rapidly changing field of biometric authentication, low-cost, scalable systems with high availability are essential. The utilization of Raspberry Pi adds to the system's cost and portability, while the suggested architecture makes use of the cloud's capacity to improve scalability. The widespread availability of the internet has enabled a multitude of uses, with the Internet of Things developing as a paradigm-shifting idea. Biometric authentication, encompassing technologies such as fingerprint, iris, and face recognition, is recognized for its popularity and applicability. The project aims to implement biometric authentication using the affordable IoT device, Raspberry Pi, connected to the cloud platform, aligning with the emerging trend of low-cost IoT adoption.

The paper distinguishes between two types of systems for establishing a person's identity: verification (authentication) systems and identification systems.
Verification involves submitting an identity claim to the system, whereas identification proves the identity of a subject in the absence of a claim. In the contemporary technological era, personal authentication solutions must be dependable and reasonably priced for everyday applications where privacy and information security are critical. A strong response to this need is offered by combining embedded systems technology with biometric authentication techniques. The usage of reconfigurable architectures for an Automatic Fingerprint Authentication System is suggested, and the study goes into detail on the hardware-software co-design that matches fingerprint minutiae sets.

3. SYSTEM ARCHITECTURE

The fingerprint sensor in our suggested model is the GT511-C3, which has its own database. After enrollment and verification, it promptly notifies the Raspberry Pi. The DHT22, employed as the temperature and humidity sensor, transmits readings to the cloud every second. A buzzer functions as an alarm, activating when the current readings exceed predefined threshold values. Simultaneously, the relay is switched off, turning off the LED to indicate system deactivation. The Raspberry Pi acts as the central hub, facilitating communication with all system components. Equipped with its Wi-Fi module, it continuously uploads temperature and humidity values to the cloud. The Raspberry Pi creates a graphical user interface (GUI) for user interaction The fingerprint sensor in our suggested model is the GT511-C3, which has its own database.
After enrollment and verification, and, if surpassed, triggers the LED while deactivating the relay.

- Fingerprint Sensor (Biometric Factor): Utilizes a high-quality fingerprint sensor such as GT511C3 with a 32-bit CPU and storage capacity for fingerprint templates.
The sensor interfaces with Raspberry Pi, which supports Python for effective integration.
Responsible for capturing and authenticating user fingerprints.
- DHT22 Sensor (Environmental Factor): Incorporates a DHT22 sensor to measure and provide accurate digital outputs for both temperature and humidity.
Offers superior precision compared to alternatives like DHT11. Enhances the overall security of the system by



incorporating environmental data as an additional authentication factor.

- Raspberry Pi:

Serves as the central processing unit and communication hub for the system.

Communicates with the fingerprint sensor, DHT22 sensor, and other system components.

Executes the authentication process by comparing the provided fingerprint data and environmental readings against stored templates and thresholds.

- Firebase (Cloud Storage and Authentication):

Implements Firebase for cloud storage to securely store and retrieve user data, including fingerprint templates. Manages OTP (One-Time Password) generation and validation.

gives a real-time information on the humidity information through the associated mobile app.

- Two-Factor Authentication Process:

User initiates the authentication process by presenting a fingerprint.

Fingerprint data is processed by Raspberry Pi for verification against stored templates.

Simultaneously, DHT22 sensor readings are obtained for environmental authentication.

If both fingerprint and environmental factors pass validation, access is granted.

In the case of a successful authentication, the user is notified through the mobile app.

OTPs may also be used for an additional layer of authentication, with Firebase managing their generation and validation.

4. METHODOLOGY

In the proposed system, we opted for the GT511C3 Fingerprint Sensor, an optical sensor equipped with a 32-bit CPU capable of storing up to 200 templates. The choice of Raspberry Pi was driven by its Python support, facilitating seamless interfacing with the Fingerprint Sensor. Additionally, the system incorporates the DHT22 model, which delivers digital outputs for both temperature and humidity, offering superior accuracy compared to the DHT11.

A. Hardware Implementation:

UART pins are used to create a connection between the Raspberry Pi and the GT511C3 fingerprint sensor. The fingerprint sensor offers alerts for authentication because it has its own memory. Furthermore, GPIO is used to link the DHT22 in order to acquire digital output for humidity and temperature monitoring. The user interface is a monitor screen that has been interfaced. In order to show the system conditions both visually and vocally, a buzzer, relay, and LED are also implemented.

B. Software Implementation:

Firebase stores user information, login credentials that are necessary for the app, and one-time passwords (OTPs) that are generated via the mobile app and used for verification. Temperature and humidity may be tracked in real time because to Firebase's role as a bridge between the hardware and the mobile app. Additionally, the program establishes threshold levels, and when these are exceeded, it will display red warnings. Block coding was used to construct the mobile application with MIT App Inventor. The GUI, or graphical user interface, facilitates user interaction with all components through visual icons and indicators.

When a user wants to enroll, they scan a QR code displayed on the Pi containing the secret key. This registers the Pi as a trusted TOTP generator on their authenticator app.

For authentication, the user enters their username/password on the protected resource.

The Pi acts as the hardware "token" generating OTPs while the client verifies them, providing two-factor authentication for stronger security.

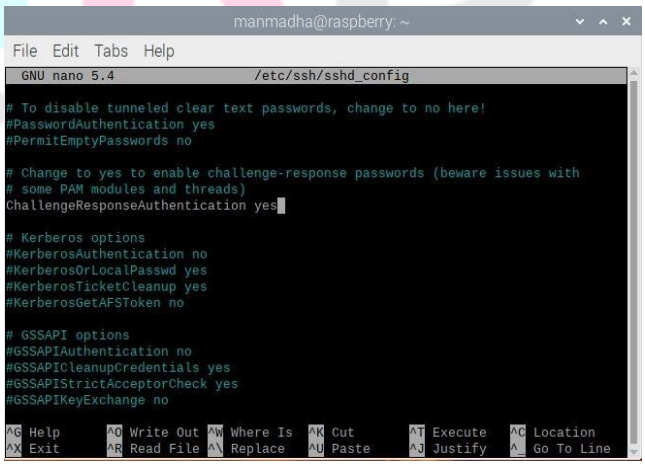
5. EXPERIMENTAL/WORK

Here are some examples of experimental work that could be done to further explore
two-factor authentication using a Raspberry Pi:

•A prototype biometric authentication system that manipulates humidity and temperature levels solely through fingerprint authentication has been developed for industrial use. Enrollment, authentication, and remote authentication are the three processes that make up the authentication system.

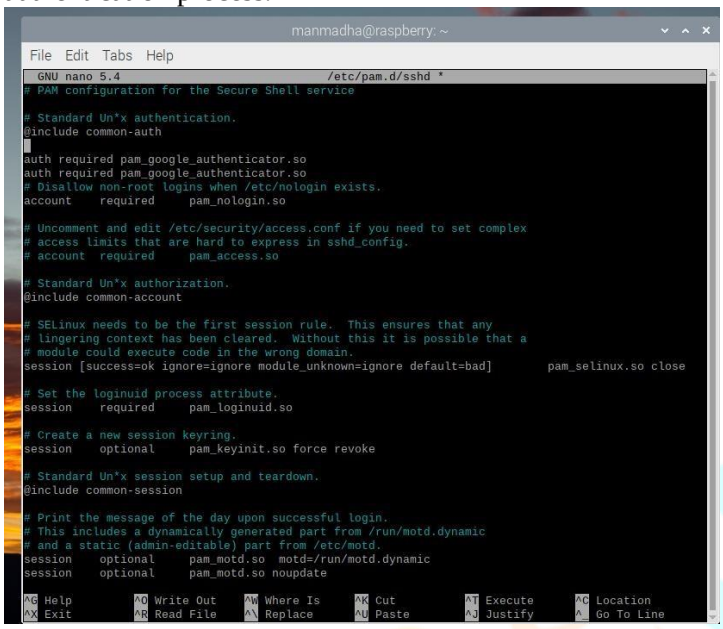
A. Enrolment process:

The enrollment process involves the administ ration granting authorization for others to be registered in the system.



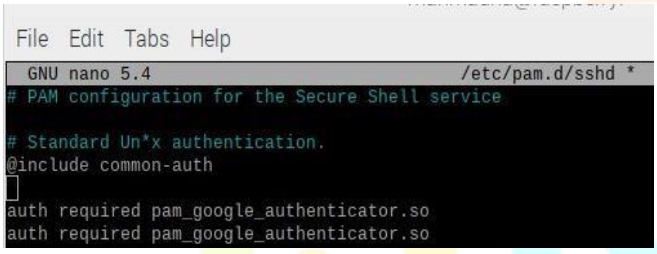
B. Authentication Process:

By using fingerprint authentication, the system administrator can immediately modify threshold values during the authentication process.



C. Remote Authentication Process:

The remote authentication process allows the administra tor, when not physically present, to grant access to another individual with a registered fingerprint. This is achieved by sending a randomly generated 10-digit OTP code through the administrator's mobile app. The code is transmitted as an SMS is sent to the cloud for verification at the same time as it is delivered to the authorized individual for access. In our project, this code is valid for a brief period of time (30 seconds), after which random values take its place.



6. RESULTS

The Enrollment Window serves as the graphical user interface (GUI) for enrolling new users under the administration's authentication. The Authentication Window, on the other hand, is the GUI, where theadministrator can use their fingerprint to change threshold values. Last but not least, another individual can modify threshold values using their fingerprint and the obtained OTP via the Remote Authentication GUIpanel.

7. Conclusion

The Raspberry Pi provides a low-cost, customizable platform for delivering hardware-backed two-factor authentication to both on-premise and remote services. By acting as the shared secret TOTP generator, it adds a physical security token beyond just pa sswords or software authenticators.

Implementing the TOTP generator on the Pi adds an extra layer of assurance that one-time passwords are only generated from authorize d hardware in possession of the legitimate user. Software-only solutions are vulnerable to spoofing or interception of secrets. Pairing the Pi with client-side verification modules allows strong two-factor authentication to be applied across multiple different types ofservices, from SSH access to VPN logins toweb applications. The modular design makes the solution adaptable.

8. FUTURE WORK

Future work in blood banking via cloud computing holds immense potential for further advancements and improvements in the field. Here are some areas that can be explored:

1. Advanced Analytics and Decision Support Integration of advanced analytics cloud-based blood banking systems enable predictive analysis,
trend. identification, and decision support. This canhelp in optimizing blood inventory management, predicting patient 34 needs, and improving resourceallocation.
2. Internet of Things (IoT) Integration: Incorporating IoT devices, such as smart sensorsand wearable devices, into the blood banking ecosystem can provide real- timedata on temperature, storage
conditions, and transportation logistics. This canenhance traceability, ensure quality control, and reduce the risk of blood wastage.
3. Blockchain Technology: Implementing blockchain technology in blood banking can enhance security, transparency, and traceabilityof blood supply chains.
Blockchain can help authenticate donor records,track blood units from collection to transfusion, and ensure the integrity of data across multiple stakeholders.
4. Mobile Applications and Telemedicine: Developing mobile applications and telemedicine platforms integrated with cloud- based blood banking systems can facilitate remote blood donor registration, appointment scheduling, and result notifications. This can improve
accessibility, donor engagement, and overall convenience for both donors andhealthcare professionals.
5. Virsstual Reality (VR) and Augmented Reality (AR): Leveraging VR and AR technologies can enhance training programs for blood bank staff, allowing them to practice complex procedures ina virtual environment. AR can also assist in real-time blood unit identification during transfusions, reducing the risk of errors.
6. Data Sharing and Collaboration:
Establishing standardized protocols and frameworks for secure data sharing and collaboration among blood banks, healthcare providers, and research institutionscan facilitate knowledge
sharing, research collaborations, and the exchangeof best practices.

9. REFEERENCES

[1] Matt Richardson and Shawn Wallace – Abestseller that is great for beginners to get up and running with basic projects using a Pi.

[2] Simon Monk covers a wide varietyof projects with clear explanations of electronics and coding principles.

[3] Divil jain, Dr. P.S Ramkumar, and DR. K.V.S.S.S.S Sairam, “IoT based Biometric Access Control System”, International Journal of Innovative Research Science, Engineering and Technology (IJIRSET), vol. 5 Issue9, pp. 555–559, May 2016.

[4] Dhvani Shah, D.K.Bharadi, V.A.Kaul, V.J.Amrutia, S., “End-to- End Encryption Based Biometric SaaS: Using Raspberry Pi as a Re- mote Authentication Node”, IEEE sponsored 1st International Conference on Computing, Communication, Control and Automation (IC-CUBEA) February2015, pg. 52 59.

[5] Vijayasanthi. R, Radha N, Jayashree M, Sindhuja P Fingerprint Authentication using Raspberry Pi based on IoT, International conferenceon
Algorithm, Methodology, Models andApplications in Emerging Technologies (ICAMMAET).

[6] A. K. Jain, L. Hong, S. Pankanti,
R. Bolle, An identity authentication system using fingerprints, Proceedingsof the IEEE, vol. 85, no. 9, pp. 1365- 1388, September 1997.

[7] Archana S. Shinde, Varsha Bendre, An Embedded Fingerprint Authentication System, 2015 International Conference on ComputingCommunication Control and Automation.

[8] Adventures in Minecraft by DavidWhale and Martin O’Hanlon- Explore coding and engineering concepts withinthe popular games.

[9] Hello Raspberry Pi! By Ryan Heitz, Ben Everard step by step fundamentals of Linux, Python, Hardware interfacing for educators.

[10] Dan Aldred – perfect for younger learners, it holds their hands through creative toy builds.

[11]https://precisebiometrics.com/products/fingerprint-recognition-software/