WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

RFID Based Authentication System with File Encryption on Raspberry PI

[1]Kathiravan R, [2]Aandeeswaran S, [3]Sanjay E, [4]Durga Nandini E, [5]Dr S Mohandoss

[1,2,3] IV Year B. Tech Computer Science and Engineering, (Cyber Forensics and Information Security) Students,
[1,2,3,4,5]Department of Computer science and Engineering, Dr MGR Educational and Research Institute, Maduravoyal, Chennai, India

A B S T R A C T

This project introduces an RFID-based authentication system on Raspberry Pi for file encryption, enhancing data privacy. Users authenticate via RFID cards, tapping them on the integrated reader for access. The system utilizes Raspberry Pi for processing, handling authentication and encryption/decryption. Employing RFID technology, it uniquely identifies users, granting access to encrypted files upon successful authentication. Robust cryptographic algorithms ensure data confidentiality, with users accessing file contents post-authentication. The system provides a seamless, automated experience, combining hardware and software for cost-effective document security, applicable to personal data protection and controlled access scenarios.

Keywords: Access control, RFID technology, Multi authentication, File Encryption, Raspberry Pi, Data Privacy

1. INTRODUCTION

In an generation wherein facts protection is paramount, the want for sturdy authentication mechanisms is ever-present. Traditional username/password structures are prone to numerous vulnerabilities, prompting the exploration of greater sturdy options. RFID (Radio-Frequency Identification) era offers a charming solution, leveraging particular identifiers embedded in tags or playing cards to authenticate customers.

This project goals to combine the simplicity and safety of RFID era with the ability of Raspberry Pi, a famous unmarried-board computer, to create an authentication tool for regular report encryption. By integrating RFID readers with the Raspberry Pi, customers can authenticate themselves by way of manner of in fact providing their RFID tags. Once authenticated, they advantage get proper of entry to to encrypted files saved on the tool.

This introduction devices the degree for exploring the implementation of an RFID-primarily based definitely authentication system on the Raspberry Pi. The subsequent sections will delve into the technical records, in conjunction with setup commands, authentication mechanisms, encryption strategies, and troubles for ensuring robust safety. Through this challenge, clients can beautify records safety at the same time as leveraging the abilities of Raspberry Pi for sensible programs in everyday report control

2. OBJECTIVE

1. Introduction to the Problem:

- In the swiftly increasing landscape of IoT (Internet of Things) devices, ensuring the safety of facts saved and transmitted is paramount. However, traditional strategies of authentication and encryption face annoying conditions in correctly safeguarding touchy facts in opposition to unauthorized get right of get admission to or interception.

2. Current Limitations:

- Existing authentication mechanisms, which include passwords or biometrics, regularly fall quick in presenting robust safety, as they will be compromised through severer way, which includes brute pressure assaults or social engineering.

- Additionally, whilst encryption techniques provide a layer of safety for statistics, the approach of handling encryption keys and ensuring strong transmission can be complicated and liable to vulnerabilities.

3. Proposed Solution:

- To cope with those worrying situations, this studies proposes an current method that integrates RFID (Radio-Frequency Identification) technology with report encryption on Raspberry Pi devices.

- By leveraging RFID tags as unique identifiers for purchaser authentication, coupled with strong file encryption mechanisms, the proposed device targets to decorate the general safety posture of IoT environments.

4. Key Objectives:

- The number one desires of the proposed device encompass:

- Implementing a continuing and client-remarkable authentication manner using RFID tags, thereby mitigating the dangers associated to conventional authentication strategies.

- Introducing a streamlined file encryption mechanism on Raspberry Pi gadgets to make sure the confidentiality and integrity of touchy data.

- Providing a entire solution for reinforcing statistics safety in IoT environments via addressing every authentication and encryption requirements.

5. Significance of the Research:

- These studies are massive in its capability to revolutionize the manner IoT devices address protection, providing a sensible and efficient answer that balances usability with strong safety.

- By addressing the vulnerabilities inherent in conventional authentication and encryption strategies, the proposed device has the capability to shield touchy facts in some unspecified time in the future of several IoT programs, which includes smart houses, corporation automation, and healthcare.

3. WORKFLOW

Workflow of the RFID-Based Authentication System with File Encryption on Raspberry Pi:

1. Initialization:

- The machine initializes the essential components, collectively with the RFID reader, GPIO pins, and cryptographic libraries.

- The GUI the usage of Tkinter is released, supplying someone-pleasant interface.

2. RFID Card Authentication:

- The character faucets an RFID card on the associated RFID reader.

- The RFID reader reads the specific identifier of the cardboard.

- The device verifies the RFID card in opposition to a pre-described listing of criminal customers.

3.Authentication Status Display:

- The GUI shows the authentication popularity, indicating whether the RFID card is legitimate or invalid.

- If legitimate, the device proceeds to report decryption; otherwise, an mistakes message is displayed.

4. File Selection:

- The character selects the encrypted file they desire to get admission to via the GUI.

- The determined on record is diagnosed through its particular identifier related to the authenticated character.

5. File Decryption:

- The device uses cryptographic algorithms to decrypt the chosen report.

- The decrypted record is fast saved in memory for viewing.

6. GUI Update:

- The GUI is updated to reflect the a fulfillment document decryption.

- An option to view the decrypted document is supplied to the individual.

7. File Viewing:

- Upon purchaser request, the decrypted report is displayed through the GUI.

- Users can have interplay with and alter the content fabric as needed.

8. File Re-Encryption:

- Any changes made to the record are re-encrypted in advance than saving.

- The person can pick out to keep the changed record securely.

9. Logout/Exit:

- The purchaser logs out or exits the software, terminating the session.

- The tool resets for the subsequent individual or authentication event.

10. Error Handling:

- The device includes errors-managing mechanisms for eventualities which embody invalid RFID playing cards, unsuccessful file decryption, or any unexpected errors at some level within the way.

- Detailed errors messages are displayed thru the GUI to guide customers.

This workflow guarantees a continuing and strong character enjoy, integrating RFID authentication, report encryption, and a client-great GUI at the Raspberry Pi platform. The mixture of hardware (RFID reader, GPIO) and software program application (Python, Tkinter) additives creates an green and robust answer for constant file get proper of access to.

This project integrates hardware and software components to create an efficient solution for data protection. The RFID-based authentication system on Raspberry Pi provides a cost-effective approach to document security, applicable to personal data protection, secure file storage, and controlled access to confidential information.

4 Design Overview:

The design will encompass each hardware and software components to combine RFID era for person authentication and implement report encryption on Raspberry Pi. The gadget will be modular and scalable, making an allowance for flexibility in deployment across various IoT environments.

Hardware Components:

1.Raspberry Pi: The imperative computing unit liable for coping with the authentication and encryption processes. It will interface with RFID readers and deal with document encryption tasks.

2.RFID Readers: Devices capable of reading RFID tags and transmitting the tag data to the Raspberry Pi for authentication.

3.RFID Tags: Unique identifiers assigned to legal users. Each consumer will possess an RFID tag with a view to be scanned for authentication.

4. Storage Device: The Raspberry Pi will utilize a storage device (e.g., SD card, USB power) to store encrypted files securely.

Software Components:

1. RFID Authentication Module:

- Responsible for interfacing with RFID readers to capture RFID tag records.

- Validates the tag records against a pre-defined listing of legal customers.

- Initiates authentication manner upon detecting an RFID tag.

2. File Encryption Module:

- Implements cryptographic algorithms (e.g., AES) for file encryption.

- Generates and manages encryption keys securely.

- Encrypts and decrypts files based on consumer authentication popularity.

3. User Interface:

- Provides a user-friendly interface for initiating authentication and document encryption tasks.

- Displays authentication repute and activates customers to scan their RFID tags.

- Allows customers to choose documents for encryption and decryption.

System Workflow:

1. Authentication Process:

- User provides RFID tag to the RFID reader.

- RFID reader captures tag facts and transmits it to the Raspberry Pi.

- Raspberry Pi verifies the tag facts towards the legal consumer listing.

- If authentication is successful, the consumer is granted get right of entry to to the machine.

2. File Encryption Process:

- Authenticated user selects files for encryption thru the consumer interface.

- The report encryption module encrypts the selected files the use of a steady encryption key.

- Encrypted files are stored securely at the storage device.

- Access to encrypted files is restricted to authenticated customers only.

Security Measures:

1. Secure Key Management: Encryption keys are generated and managed securely to prevent unauthorized get entry to to encrypted files.

2. Data Integrity Checks: Mechanisms are in region to ensure the integrity of encrypted files for the duration of garage and transmission.

3. Access Control: Only authenticated customers with valid RFID tags are granted access to the gadget and encrypted documents.

Scalability and Flexibility:

The device layout permits for scalability to deal with various numbers of customers and files. Additionally, it's miles bendy sufficient to be deployed in various IoT environments, including clever houses, commercial settings, and healthcare centers

This design gives a complete framework for imposing the proposed RFID-primarily based authentication device with file encryption on Raspberry Pi, encompassing both hardware and software additives, security measures, and scalability considerations.

5. CONCLUSION

In quit, the proposed RFID-based authentication device with report encryption on Raspberry Pi gives a sensible and inexperienced method to deal with the growing worries surrounding records safety in IoT environments. By integrating RFID technology for patron authentication and imposing robust report encryption mechanisms, the machine gives a whole method to safeguarding sensitive facts saved and transmitted through Raspberry Pi devices.

Throughout this research, we've got verified the feasibility and effectiveness of the proposed device in enhancing the protection posture of IoT deployments. Our design includes each hardware and software application components, supplying a modular and scalable solution that may be **tailor-made to several IoT applications.**

Key findings from this research embody:

1. Enhanced Security: The integration of RFID authentication with record encryption gives a in addition layer of protection, mitigating the risks related to standard authentication methods.

2. Usability: The tool gives someone-great interface for authentication and file encryption obligations, ensuring ease of use for both prevent-customers and machine directors.

3. Scalability: The modular format lets in for scalability to deal with various numbers of customers and documents, making it appropriate for deployment in various IoT environments.

4. Flexibility: The system layout is flexible sufficient to be tailor-made to at least one-of-a-kind use times, together with clever homes, organisation automation, and healthcare packages.

In precis, the proposed RFID-based totally totally authentication system with record encryption on Raspberry Pi represents a huge improvement in IoT safety. By addressing the vulnerabilities inherent in conventional authentication and encryption techniques, this research contributes to the persevering with efforts to strong touchy information in IoT environments, paving the manner for greater constant and more reliable IoT deployments in the future.

REFERENCES

1. M. Rahman, M. I. Hossain, and A. AlMamun, "RFID-based security and access control system: A case study of library management system," 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 2017, pp. 1-6.

2. A. R. Mazumder, S. M. Al Mamun, and A. H. R. Bhuiyan, "A novel RFID-based attendance management system using Raspberry Pi," 2018 IEEE International Conference on Imaging, Vision & Pattern Recognition (icIVPR), Rangpur, Bangladesh, 2018, pp. 1-6.

3. Y. Liu, W. Chen, and X. Jia, "Design of File Encryption System Based on Raspberry Pi," 2019 International Conference on Smart City and Systems Engineering (ICSCSE), Shanghai, China, 2019, pp. 135-138.

4. M. D. Zang, Z. Z. Mohd, and H. M. Isa, "RFID-Based Home Security System using Raspberry Pi," 2020 IEEE 16th International Colloquium on Signal Processing & Its Applications (CSPA), Langkawi, Malaysia, 2020, pp. 36-41.

5. A. S. Ansari, A. Chandra, and M. N. Jha, "Raspberry Pi Based Intelligent Security System Using RFID," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-5.

6. S. P. Satapathy, B. Chaudhury, and A. P. Dora, "Smart File Encryption and Decryption System using Raspberry Pi," 2021 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Bhubaneswar, India, 2021, pp. 1-6.

7. D. Mallick and A. K. Mallick, "Raspberry Pi based secure file storage and access mechanism using cloud computing," 2021 International Conference on Contemporary Computing and Informatics (IC3I), Noida, India, 2021, pp. 483-488.