IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 8, August 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308066|

Secure Authentication in an IoT Based Healthcare Environment with Strong Anonymity and Unclonable Device

S. Sailaja, R. Pavithra

Assistant Professor, Department of Electronics and Communications Engineering, Jaya Engineering College, Thiruninravur, India

PG Student, Department of Applied Electronics, Jaya Engineering College, Thiruninravur, India

ABSTRACT: In the healthcare network, the Internet of Things (IoT) devices are connected to the network for enabling remote monitoring of patient's health. IoT device security, however, is a serious concern because typical security measures might not be appropriate for IoT devices, making them naturally vulnerable to physical and copying attacks. Therefore, device authentication is a very essential security concern for IoT networks. Additionally, the storage and processing power of these devices are constrained. To address all these requirements, Physically Unclonable Functions (PUFs) for device authentication is a potential strategy. An advanced lightweight authentication scheme for IoT devices is proposed by using PUF. This provides robust authentication without storing any sensitive information on the device's memory and establishes the session key exchange process simultaneously. Moreover, this preserves device privacy by including a temporary identity, which is updated at the end of each session. The effectiveness of this model is assessed, and results demonstrate that it is more effective and secure than many existing schemes.

I. INTRODUCTION

The integration of Internet of Things (IoT) technology in healthcare environments has revolutionized patient care, treatment monitoring, and medical data management. The adoption of IoT devices in healthcare introduces significant security and privacy challenges, particularly concerning user authentication and data protection. Subsequently, users are authenticated using a combination of biometric traits and cryptographic credentials, ensuring strong authentication while protecting user privacy. For IoT device authentication, the framework utilizes PUFs, which exploit inherent physical variations in hardware components to generate device-specific cryptographic keys. This approach ensures device uniqueness and prevents unauthorized device cloning or tampering. The integration of Internet of Things (IoT) technology into healthcare environments has revolutionized patient care, monitoring, and management. IoT devices, such as wearable health trackers, smart medical devices, and remote monitoring systems, have enabled real-time data collection, analysis, and communication, leading to improved healthcare outcomes and patient experiences. However, as IoT devices become increasingly interconnected and integral to healthcare infrastructure, ensuring secure authentication and data privacy within these environments has become a paramount concern. Healthcare data is highly sensitive and subject to stringent privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. Moreover, the proliferation of IoT devices in healthcare introduces unique security challenges, including device authentication, data integrity, and protection against unauthorized access and tampering. Traditional authentication methods, such as username-password combinations, are often insufficient to address these challenges, as they are vulnerable to various security threats, including brute-force attacks, phishing, and credential theft. To address these concerns and ensure robust security in IoT-based healthcare environments, innovative approaches leveraging strong anonymity and unclonable device authentication mechanisms are essential. Strong anonymity ensures that users' identities remain confidential while accessing healthcare services and data, protecting their privacy and confidentiality. Unclonable device authentication utilizes unique physical characteristics or cryptographic keys inherent to each IoT device to verify its identity and integrity, mitigating the risk of device cloning and impersonation. In this paper, we propose a comprehensive framework for secure authentication in an IoT-based healthcare environment, incorporating strong anonymity and unclonable device authentication mechanisms. We discuss the challenges associated with traditional authentication methods and highlight the importance of adopting advanced security measures to safeguard

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308066|

patient data and privacy. Furthermore, we present a detailed analysis of existing authentication techniques and explore the feasibility and effectiveness of integrating strong anonymity and unclonable device authentication into IoT-based healthcare systems. By leveraging these innovative security measures, healthcare organizations can enhance patient trust, comply with regulatory requirements, and mitigate the risk of data breaches and unauthorized access. Our proposed framework aims to establish a secure and privacy-preserving authentication mechanism that fosters the widespread adoption of IoT technology in healthcare while ensuring the confidentiality and integrity of patient data.

II. HEALTH DATA AQUSISATION

Secure authentication in an IoT-based healthcare environment with strong anonymity and unclonable device identity is crucial for ensuring the confidentiality, integrity, and privacy of sensitive health data.

Device Authentication

Each IoT device, such as wearables, medical sensors, or monitoring devices, is equipped with a unique and unclonable identity, often achieved through hardware-based cryptographic mechanisms like physically unclonable functions (PUFs). During the initial setup or registration process, devices authenticate themselves to the healthcare network using their unique identities. Strong authentication protocols, such as mutual authentication, are employed to ensure that both the device and the network verify each other's identities before establishing a connection.

Anonymity and Privacy

Health data transmitted by IoT devices is anonymized to protect patient privacy. Techniques like data aggregation, pseudonymization, and differential privacy are used to mask individual identities while still allowing for meaningful analysis of health trends and patterns. Anonymity measures ensure that even if data is intercepted, the identities of the individuals associated with that data remain protected.

Secure Communication

Communication between IoT devices and the healthcare network is encrypted using robust cryptographic algorithms like AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman). Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) protocols are employed to secure data transmission over the network. Secure communication channels prevent unauthorized access and tampering of health data during transit.

Access Control

Role-based access control (RBAC) mechanisms are implemented to regulate access to health data based on the user's role and privileges within the healthcare system. Fine-grained access control policies are enforced to restrict access to specific data based on the user's authorization level. Multi-factor authentication (MFA) may be required for accessing sensitive health data, adding an extra layer of security.

Data Integrity

Hash functions and digital signatures are used to ensure the integrity of health data transmitted and stored within the IoT healthcare environment. Hashing algorithms generate unique checksums for data packets, allowing recipients to verify the integrity of received data. Digital signatures provide proof of data origin and integrity, preventing unauthorized modifications to health records.

Continuous Monitoring and Intrusion Detection

Anomaly detection systems continuously monitor network traffic and device behaviour to detect any suspicious activities or potential security breaches. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are deployed to identify and mitigate security threats in real-time. By implementing these security measures, an IoT-based healthcare environment can ensure secure authentication, strong anonymity, and unclonable device identity while acquiring and transmitting health data, thereby safeguarding patient privacy and confidentiality.

Advantages

- Strong anonymity ensures that sensitive patient health data remains private and confidential.
- The system protects against unauthorized access and data breaches, maintaining patient trust and compliance with privacy regulations.
- Unclonable device characteristics prevent the cloning or replication of IoT devices used for authentication.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308066|

- This safeguards against identity theft and impersonation, ensuring that only authorized devices can access the healthcare environment and patient data.
- Strong authentication mechanisms, combined with unclonable device features, provide robust security against unauthorized access and cyberattacks.
- This helps prevent malicious actors from infiltrating the IoT healthcare network, protecting patient data and the integrity of medical devices.
- Secure authentication ensures that only authenticated and authorized devices can interact with medical equipment and access patient data.
- This reduces the risk of unauthorized device tampering or malicious activities that could compromise patient safety and treatment outcomes.

Key Features

- Arduino-Based Processing: The Arduino microcontroller serves as the central processing unit, acquiring and processing ECG signals efficiently.
- ECG Sensor Integration: A dedicated ECG sensor is employed to capture accurate analog signals from the user's body, ensuring reliable heart rate monitoring.
- Graphical User Interface (GUI): The system features a user-friendly GUI that displays real-time ECG waveforms and heart rate information, enabling users to observe and analyze their cardiac activity.
- Portability: The design emphasizes portability, allowing users to carry the device for continuous monitoring, making it suitable for personal health tracking and educational purposes.
- Signal Processing: The system incorporates signal processing algorithms to filter and enhance the acquired ECG signals, ensuring accurate and clear representation on the oscilloscope display.

III. EXISTING SYSTEM

In an existing system for secure authentication in an IoT-based healthcare environment with strong anonymity and unclonable device features, several technologies and strategies may be employed. The system may utilize secure communication protocols such as Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) to ensure encrypted communication between IoT devices and the central healthcare system. These protocols help prevent eavesdropping and man-in-the-middle attacks, ensuring the confidentiality and integrity of data transmission. Each IoT device in the healthcare environment is assigned a unique identifier, such as a Universally Unique Identifier (UUID) or a hardware-based identifier.

IV. PROBLEM STATEMENT

A portable digital oscilloscope using Arduino involves addressing several challenges. The realm of electronics, troubleshooting and waveform analysis are fundamental tasks for engineers, hobbyists, and students. The availability of affordable, portable, and user-friendly digital oscilloscopes is limited. The challenge is to design and develop a Portable Digital Oscilloscope using Arduino. A compact and lightweight design that allows users to carry the oscilloscope easily, making it suitable for fieldwork, educational environments, and hobbyist projects. The open-source nature of Arduino to allow users to customize and extend the functionality of the oscilloscope according to their specific needs.

V. PROPOSED SYSTEM

The proposed system aims to provide secure authentication in an IoT-based healthcare environment while ensuring strong anonymity and unclonable device characteristics. The system utilizes RFID (Radio Frequency Identification) and keypad authentication methods, integrated with Arduino and an IoT application. The RFID reader is used to read unique identifiers (RFID tags) associated with patients or staff members. A keypad is integrated with the authentication system to provide an additional layer of security. Users can enter a PIN code for authentication purposes. The Arduino board acts as the central processing unit for the authentication system. It interfaces with the RFID reader, keypad, and IoT module. An IoT module (e.g., ESP8266 or ESP32) is used to establish communication between the Arduino board and the IoT application, enabling remote monitoring and control. The Arduino board runs a sketch (program) that controls the operation of the RFID reader, keypad, and authentication logic. It verifies the RFID tag and/or PIN code entered by the user.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308066|

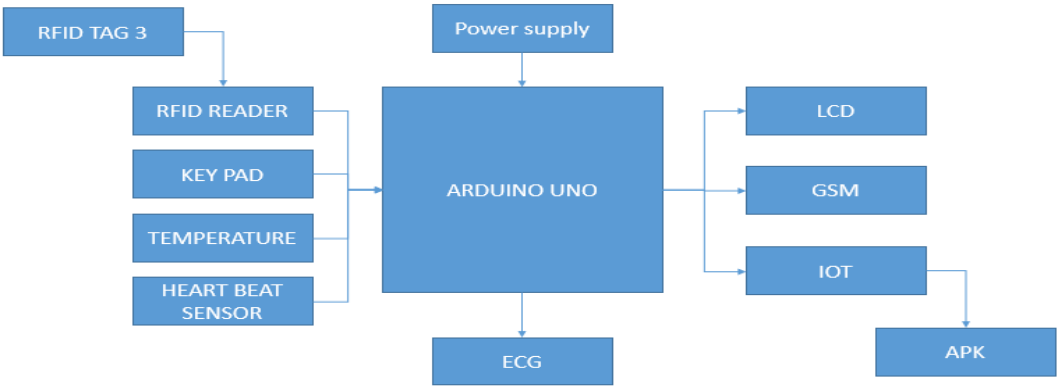

Fig 3: Architecture of proposed system

An IoT application is developed to interface with the Arduino board and provide remote access to the authentication system. The application allows administrators to monitor authentication events, manage user access permissions, and receive alerts for unauthorized access attempts. The authentication algorithm implemented on the Arduino board verifies the authenticity of the RFID tag and/or PIN code entered by the user. It ensures that only authorized individuals are granted access to the healthcare environment. When a user (patient or staff member) approaches the entry point, they are prompted to present their RFID tag. The RFID reader reads the unique identifier from the RFID tag and sends it to the Arduino board for verification. Simultaneously, the user enters their PIN code using the keypad. The Arduino board verifies both the RFID tag and the PIN code against the preconfigured database of authorized users. If the authentication is successful, access is granted, and an event log is sent to the IoT application for monitoring. In case of an authentication failure or unauthorized access attempt, an alert is generated and sent to the IoT application for further action.

VI. CONCLUSION

In conclusion, the implementation of secure authentication in an IoT-based healthcare environment using RFID and keypad authentication, along with Arduino and an IoT app. RFID and keypad authentication methods, the system ensures multiple layers of security, making it more difficult for unauthorized individuals to gain access to sensitive healthcare data or devices. Strong Anonymity: The system prioritizes user privacy by incorporating strong anonymity measures. Through the use of RFID tags and keypad input, sensitive user information can be securely transmitted and authenticated without compromising anonymity. Leveraging Arduino and IoT technology, the system can generate unique device identifiers that are unclonable, enhancing the overall security of the authentication process. This helps prevent unauthorized duplication or tampering of devices within the healthcare environment. The integration of Arduino and an IoT app enables real-time monitoring and control of authentication processes. Healthcare providers can remotely manage access permissions, monitor authentication attempts, and respond to security incidents promptly. The use of a keypad interface and IoT app makes the authentication process user-friendly and accessible to healthcare professionals and patients alike. This enhances usability while maintaining robust security measures. The implementation of RFID and keypad authentication using Arduino and an IoT app in a healthcare environment offers a comprehensive solution for secure authentication with strong anonymity and unclonable device identification. This not only ensures the privacy and security of sensitive healthcare data but also enhances user experience and usability within the healthcare setting.

REFERENCES

[1] Nurkifli, E. H., & Hwang, T. (2023, September). Secure Authentication in an IoT-Based Healthcare Environment with Strong Anonymity and Unclonable Device. In 2023 6th International Conference of Computer and Informatics Engineering (IC2IE) (pp. 13-18). IEEE.

[2] Yanambaka, V. P., Mohanty, S. P., Kougianos, E., & Puthal, D. (2019). Pmsec: Physical unclonable function-based

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308066|

robust and lightweight authentication in the internet of medical things. IEEE Transactions on Consumer Electronics, 65(3), 388-397.

[3] Zhou, X., Wang, S., Wen, K., Hu, B., Tan, X., & Xie, Q. (2023). Security-Enhanced Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare. IEEE Internet of Things Journal.

[4] Masud, M., Gaba, G. S., Kumar, P., & Gurtov, A. (2022). A user-centric privacy-preserving authentication protocol for IoT-AmI environments. Computer Communications, 196, 45-54.

[5] Asassfeh, M., Obeid, N., & Almobaideen, W. (2020). Anonymous authentication protocols for iot based-healthcare systems: a survey. International Journal of Communication Networks and Information Security, 12(3), 302-315.

[6] Subramani, J., Maria, A., Rajasekaran, A. S., & Al-Turjman, F. (2021). Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANs. IEEE Transactions on Industrial Informatics, 18(5), 3484-3491.

[7] Satamraju, K. P., & Malarkodi, B. J. C. C. (2021). A decentralized framework for device authentication and data security in the next generation internet of medical things. Computer Communications, 180, 146-160.

[8] Shao, X., Guo, Y., & Guo, Y. (2022). A PUF-based anonymous authentication protocol for wireless medical sensor networks. Wireless Networks, 28(8), 3753-3770.

[9] Suganthi, S. D., Anitha, R. V. S. S., Sureshkumar, V., Harish, S., & Agalya, S. (2020). End to end light weight mutual authentication scheme in IoT-based healthcare environment. Journal of Reliable Intelligent Environments, 6, 3-13.

[10] Fakroon, M., Gebali, F., & Mamun, M. (2021). Multifactor authentication scheme using physically unclonable functions. Internet of Things, 13, 100343.

[11] Wazid, M., Das, A. K., Khan, M. K., Al-Ghaiheb, A. A. D., Kumar, N., & Vasilakos, A. V. (2017). Secure authentication scheme for medicine anti-counterfeiting system in IoT environment. IEEE Internet of Things Journal, 4(5), 1634-1646.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details