ISSN 2277-2685
IJESR/April-June. 2026/ Vol-16/Issue-2/749-757
A. Kavya Sri *et. al.*, / International Journal of Engineering & Science Research

Full Length Article

Obtain Patient Health Data Priority Classification In A Remote E-Healthcare System While Maintaining Privacy

Dr. Md. Asif[1], A. Kavya Sri[2], B. Tarun Yadav[3], K. Laxmi Prasanna[4], T. Anji[5]
[1]Asst. Prof; Department Of Electronics And Computer Engineering Accredited By Naac J.B. Institute Of Engineering & Technology Hyderabad India
[2,3,4,5]B.Tech Student's; Department Of Electronics And Computer Engineering Accredited By Naac J.B. Institute Of Engineering & Technology Hyderabad India

Accepted 23-04-2026

Abstract
Wireless Body Area Networks (WBANs) have emerged as a key technology for enabling continuous, real-time healthcare monitoring. Despite their potential, significant concerns remain regarding the protection of sensitive patient information and the confidentiality of diagnostic models used by healthcare providers. Although several privacy-preserving approaches have been introduced, many suffer from limitations in computational efficiency and classification accuracy.To address these challenges, this paper presents an efficient privacy-preserving priority classification scheme (PPC) designed for remote e-healthcare environments. The proposed approach enables the WBAN gateway to classify encrypted patient data based on priority levels without requiring interaction with external entities. This non-interactive mechanism reduces processing delays and allows timely forwarding of medical data according to its urgency.Security analysis demonstrates that the proposed scheme safeguards both patient privacy and the confidentiality of medical decision models while performing accurate classification. Furthermore, experimental evaluation, conducted using an Android-based application and Java server implementations, shows that the PPC scheme achieves low computational overhead and reduced communication costs, making it suitable for real-time healthcare applications.

Keywords
WBAN, E-Healthcare, Privacy Preservation, Priority Classification, Encrypted Data, Data Security, Low Latency, Efficiency

Introduction

The rapid growth of smartphone technology, along with the advancement of Wireless Body Area Networks (WBANs), has significantly accelerated the development of remote e-healthcare systems. These systems enable continuous monitoring of patients by collecting physiological signals through wearable sensors, thereby supporting timely medical intervention and improving overall healthcare quality. In recent years, several WBAN-based solutions have been proposed, including energy-efficient communication protocols, adaptive resource allocation strategies, and robust data transmission mechanisms that address challenges such as body shadowing and signal disruption.In a typical remote healthcare architecture, wearable sensors deployed on a patient's body periodically capture physiological parameters such as heart rate, temperature, and blood pressure. Due to the limited computational and energy capabilities of these sensors, the collected raw data is transmitted to a smartphone for preprocessing. The smartphone aggregates and formats the processed data into structured medical packets, which are then forwarded to a nearby WBAN gateway. These gateways collect packets from multiple users and relay them to a centralized healthcare server for further analysis and decision-making.Despite its advantages, this architecture introduces critical concerns related to data privacy and system security. Patients are required to share highly sensitive information, including personal identity details and medical history, which increases the risk of unauthorized access and data misuse. At the same time, healthcare providers rely on proprietary diagnostic models that must remain confidential to protect their intellectual property. The possibility of cyberattacks targeting smartphones or WBAN gateways further intensifies these risks, potentially exposing both patient data and clinical models.To mitigate these issues, various privacy-preserving mechanisms have been developed, particularly those that operate on encrypted data. However, these approaches often encounter trade-offs between security, computational accuracy, and system efficiency. From a security perspective, the system must ensure that encrypted data cannot be deciphered by adversaries, even under ciphertext-only or known-plaintext attack scenarios. In terms of accuracy, certain techniques such as data normalization and noise addition may degrade the reliability of medical analysis, which is unacceptable in critical healthcare applications. Furthermore, many existing solutions introduce significant computational and communication overhead, especially those relying on multi-party

interactions or complex encryption schemes like fully homomorphic encryption. Consequently, achieving a balance between privacy protection, accuracy, and efficiency remains a major challenge in remote e-healthcare systems.

Problem Statement

Modern healthcare systems often rely on locally stored patient records, which limits their accessibility across different locations and healthcare providers. This lack of interoperability becomes particularly problematic in emergency situations, where immediate access to patient information is essential for timely diagnosis and treatment. Delays in retrieving critical medical data can directly impact patient outcomes.In addition to accessibility issues, patient records contain highly sensitive personal and clinical information that must be securely protected. Without robust privacy-preserving mechanisms, there is a significant risk of unauthorized access, data breaches, and misuse of confidential information. Furthermore, many existing systems lack intelligent mechanisms to prioritize patients based on the severity of their medical conditions. As a result, critical cases may not be identified promptly, leading to delays in urgent care. Therefore, there is a strong need for a secure, efficient, and privacy-aware system capable of both protecting sensitive data and enabling rapid prioritization of patients in remote healthcare environments.

Literature Review

Recent advancements in remote healthcare systems have led to the integration of Wireless Body Area Networks (WBANs) and machine learning techniques for continuous patient monitoring and intelligent decision-making. A study by C. Ambika Bhuvaneswari et al. (2022) introduced a remote patient monitoring framework that focuses on identifying critical health conditions using supervised learning methods. The system collects vital parameters such as oxygen saturation, body temperature, and heart rate, and applies classification algorithms to determine the urgency level of patient data. Among the evaluated models, Support Vector Machine (SVM) demonstrated superior performance with an accuracy of 93.5%, outperforming other approaches like Multilayer Perceptron, Bayesian Networks, and Logistic Regression. This work highlights the importance of prioritizing medical data to ensure faster response for critical cases.Another important contribution by Antonio J. Rodriguez-Almeida et al. (2022) addressed the challenge of limited and sensitive medical datasets by introducing synthetic data generation techniques. Their approach creates artificial datasets that closely resemble real patient data while preserving privacy. The study evaluated multiple datasets using statistical metrics and assessed the effectiveness of synthetic data in training machine learning models. The results indicated that synthetic data can maintain model performance while protecting sensitive information, making it a promising solution for privacy-preserving healthcare analytics.In a related study, Taiwo Olubunmi Adetiloye et al. (2022) explored the classification of COVID-19 patients based on hospitalization requirements. By applying machine learning models such as Decision Trees and Random Forest, along with mathematical modeling techniques, the study categorized patients according to disease severity. This approach enabled healthcare providers to identify high-risk patients quickly and allocate resources efficiently. The research also demonstrated improvements in treatment planning and cost management, emphasizing the role of predictive analytics in healthcare systems.More recently, Farha Masroor et al. (2024) proposed an AI-driven framework for patient scheduling and resource allocation with a focus on fairness. Their work compared traditional queuing models with Reinforcement Learning (RL) and Deep Reinforcement Learning (Deep RL) techniques. While RL reduced waiting times, it sometimes compromised fairness, whereas Deep RL provided a better balance between efficiency and equitable resource distribution. This study underlines the growing importance of intelligent automation in managing healthcare services effectively.Despite these advancements, existing systems still face limitations in ensuring data privacy, maintaining classification accuracy, and reducing computational overhead. These challenges motivate the need for more efficient and secure solutions in remote e-healthcare environments.

Existing System

Wireless Body Area Networks have become a widely adopted solution for continuous health monitoring due to their ability to support real-time data collection and transmission. However, current WBAN-based healthcare systems encounter significant challenges related to data privacy and security. Sensitive patient information, including physiological data and personal details, is vulnerable to unauthorized access if not properly protected. Additionally, healthcare providers rely on confidential disease models, which must remain secure to prevent misuse or intellectual property loss. Although several privacy-preserving techniques have been proposed, many of them introduce high computational complexity or reduce the accuracy of medical analysis. These limitations make existing systems less suitable for real-time and large-scale healthcare applications.

Proposed System

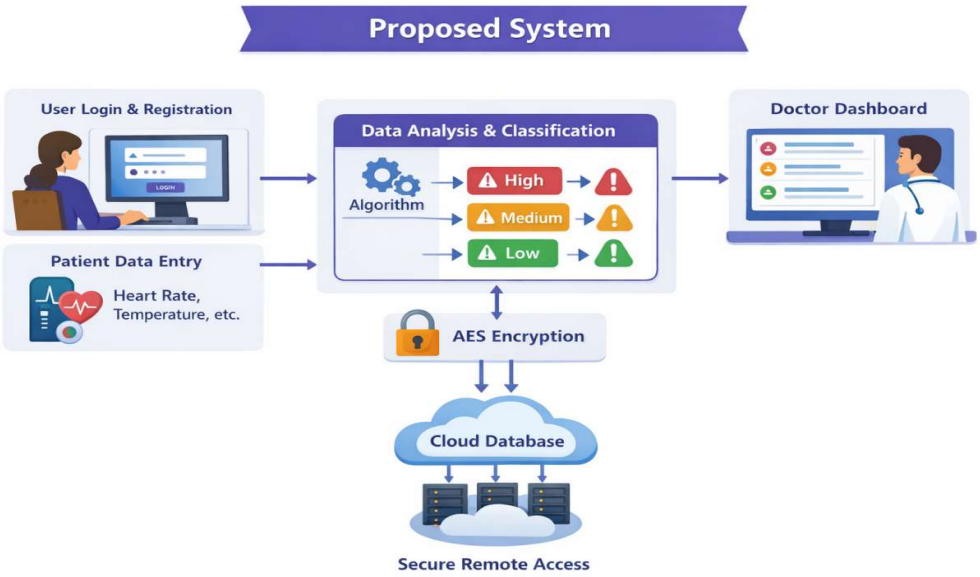


Fig 1: Proposed system

To overcome the limitations of existing approaches, this work introduces a Privacy-Preserving Priority Classification (PPC) scheme for remote e-healthcare systems. The proposed method enables the classification of encrypted patient data directly at the WBAN gateway without requiring interaction with external entities. By adopting a non-interactive approach, the system significantly reduces latency and allows faster decision-making.

The PPC scheme ensures that medical data packets are categorized based on their urgency levels and transmitted accordingly, prioritizing critical cases. At the same time, it preserves the confidentiality of both patient information and healthcare diagnostic models. Security analysis confirms that the system prevents unauthorized disclosure of sensitive data while maintaining accurate classification. Experimental validation using an Android application and Java-based servers demonstrates that the proposed solution achieves low computational cost and minimal communication overhead, making it practical for real-world deployment.

System Description

System Architecture

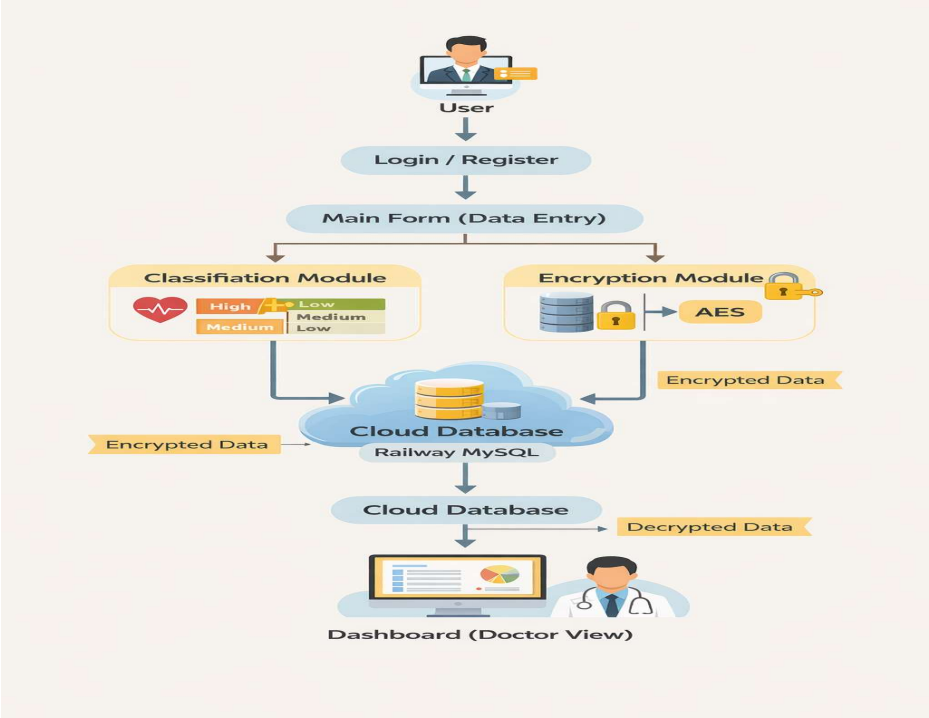


Fig 2: System architecture

The overall system is structured into three logical layers to improve modularity and maintainability. The presentation layer provides the user interface, allowing users to interact with the system through features such as login, registration, and patient data entry. The application layer handles core functionalities, including data processing, encryption, and classification of patient conditions. The data layer consists of a cloud-based database that securely stores user credentials and medical records, enabling remote access and efficient data management.

Methodology

The system is divided into three primary modules: user management, data collection, and classification with relay functionality. The user module manages authentication and registration, ensuring secure access to the system. The data collection module allows users to input and retrieve encrypted medical data while maintaining access control. The classification and relay module is responsible for processing patient data, assigning priority levels, and ensuring that critical information is transmitted with minimal delay.Patient classification is performed using a rule-based approach that categorizes health conditions into high, medium, and low priority based on physiological parameters such as heart rate and temperature. To ensure data security, the Advanced Encryption Standard (AES) is used to encrypt sensitive information before storage. Database operations are handled using Java Database Connectivity (JDBC), enabling efficient interaction with the cloud-hosted MySQL database. The use of a cloud platform enhances scalability, availability, and real-time accessibility of the system.

Requirements Engineering

Hardware and Software Requirements

The system can operate on standard computing devices with moderate processing capabilities. A minimum configuration includes an Intel Core i3 processor, 4 GB RAM, and adequate storage, while higher configurations improve performance. The software environment supports multiple operating systems, including Windows, Linux, and macOS. The application is developed in Java using NetBeans IDE, with MySQL as the backend database hosted on a cloud platform. JDBC is used for database connectivity, ensuring efficient data operations.

Software Requirement Specification

The functional requirements define the primary operations of the system, including user authentication, registration, patient data entry, classification, secure storage, and dashboard visualization. The system must validate inputs, prevent duplicate accounts, and ensure that encrypted data is securely stored and correctly displayed after decryption.Non-functional requirements focus on system quality attributes. Security is ensured through encryption and controlled access mechanisms. Performance requirements demand fast response times during data processing and retrieval. Scalability is supported through cloud infrastructure, allowing the system to handle increasing workloads. Reliability

ensures consistent system operation without data loss, while usability emphasizes a simple and user-friendly interface accessible to non-technical users.

DEVELOPMENT TOOLS AND IMPLEMENTATION

Features of Java

Java is a widely adopted programming language developed by James Gosling and introduced by Sun Microsystems in 1995. It is designed as a class-based, object-oriented language that supports portability and security. One of its key advantages is the ability to compile code into bytecode, which can run on any system equipped with a Java Virtual Machine (JVM). This feature enables the principle of "write once, run anywhere," making Java highly suitable for cross-platform applications.The language incorporates essential object-oriented concepts such as inheritance, encapsulation, polymorphism, and dynamic binding. These features promote code reusability, modular design, and flexibility in application development. Java also supports multithreading, allowing multiple processes to execute concurrently, which improves system responsiveness and performance. Due to its reliability and extensive library support, Java is widely used in web applications, enterprise systems, and mobile computing environments.

Java Swing Overview

Java Swing is used in this project to design the graphical user interface (GUI). It provides a rich set of components such as buttons, frames, labels, and tables that enable developers to create interactive and user-friendly applications. Unlike traditional Abstract Window Toolkit (AWT), Swing uses lightweight components that are rendered using Java code rather than relying entirely on the operating system. This approach ensures consistent appearance and behavior across different platforms.Swing applications are structured around top-level containers such as JFrame and JDialog, which serve as the main windows of the application. The framework allows flexible customization of UI components and supports event-driven programming, enabling efficient handling of user actions such as button clicks and form submissions. As a result, Swing plays a vital role in building the presentation layer of the healthcare system.

Java Collection Framework

The Java Collection Framework provides a standardized architecture for storing and managing groups of objects. It includes interfaces such as Collection, List, Set, and Map, along with their implementations. Lists maintain ordered collections and allow duplicate elements, while sets ensure uniqueness of elements without a defined order. Maps store data in key-value pairs, enabling efficient retrieval based on keys.Different implementations such as ArrayList, LinkedList, HashSet, and HashMap offer flexibility in handling data based on application requirements. These data structures are particularly useful in managing patient records, storing user details, and processing healthcare data efficiently within the system.

Multithreading in Java

Multithreading is an important feature used to enhance the performance of modern applications. A thread represents an independent path of execution within a program. Java supports multithreading through built-in classes and interfaces, allowing multiple tasks to run simultaneously. This capability is especially useful in healthcare systems where data processing, user interaction, and database operations may occur concurrently. By enabling parallel execution, multithreading improves system efficiency and reduces response time.

System Implementation

The implementation of the proposed system is modular in nature, ensuring clarity, maintainability, and scalability. Each module is designed to perform a specific function within the healthcare application.The login module verifies user credentials by comparing the entered username and password with the database records. If authentication is successful, access to the main dashboard is granted; otherwise, an error message is displayed. Similarly, the registration module allows new users to create accounts, ensuring that duplicate usernames are not permitted.The patient data entry module is responsible for collecting and validating user input, including parameters such as heart rate and temperature. Once validated, the data is processed through the classification and encryption modules before being stored securely in the database.The classification module applies a rule-based approach to determine the priority level of a patient. Based on predefined thresholds, patient conditions are categorized into high, medium, or low priority. This enables quick identification of critical cases requiring immediate attention.To ensure data security, the system employs the Advanced Encryption Standard (AES) algorithm. Sensitive patient information is encrypted before storage and decrypted only when authorized users request access. This ensures confidentiality and prevents unauthorized data exposure.The database module handles storage and retrieval operations using structured queries. Patient details, encrypted data, and priority levels are stored in a cloud-based database, enabling remote access and efficient data management.Finally, the dashboard module presents the stored information in a structured format. It retrieves encrypted data from the database, decrypts it securely, and displays it in a user-friendly interface for analysis and decision-making.

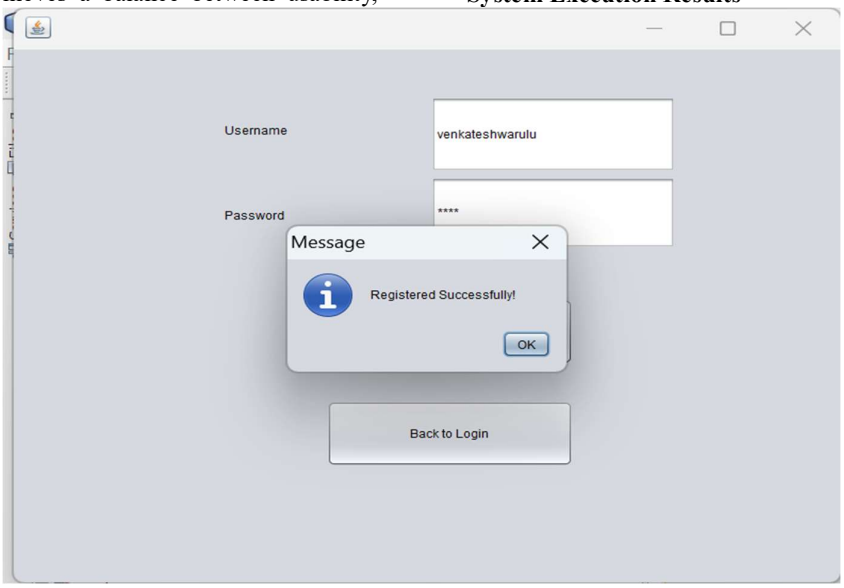
Summary

The development of the proposed system leverages the strengths of Java technologies, including J2EE, Swing, and the Collection Framework, to create a secure and efficient healthcare application. The modular implementation approach ensures that each

component performs its function effectively while maintaining overall system integrity. By integrating classification, encryption, and cloud-based storage, the system achieves a balance between usability, performance, and data security, making it suitable for real-world healthcare environments.

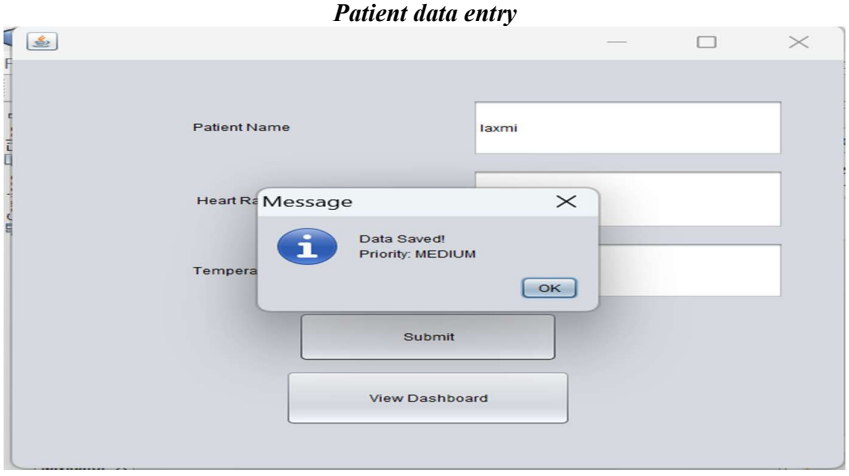
RESULTS AND DISCUSSION

System Execution Results



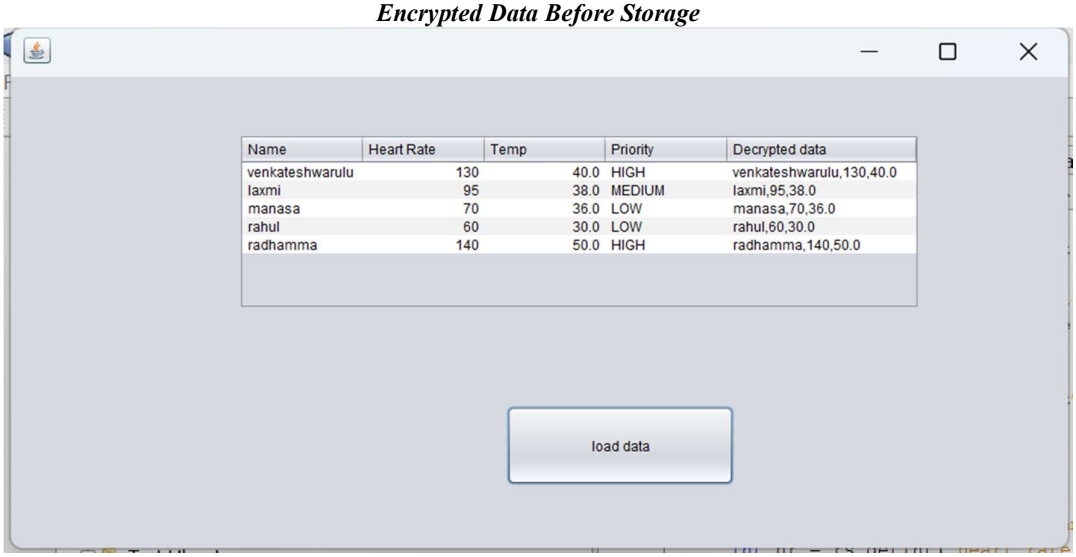
User Registration Form

Patient data entry

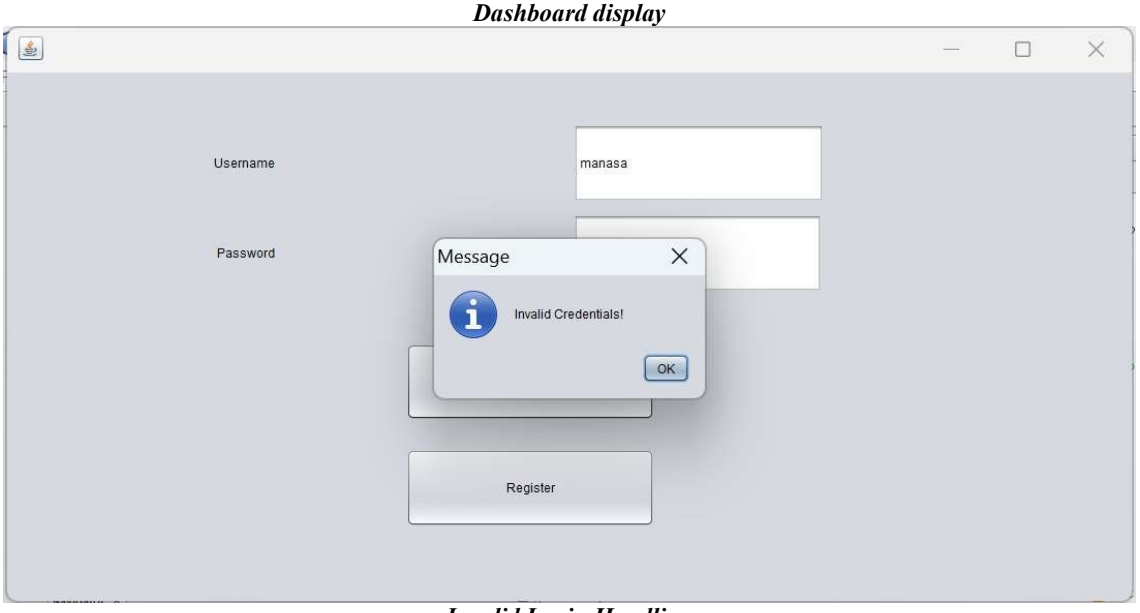


Data saved (priority: medium)

Encrypted Data Before Storage



Dashboard display



Invalid Login Handling

The system was implemented and tested using the NetBeans development environment. All core modules were executed individually and collectively to verify their correctness and integration.The user registration and login functionalities were validated to ensure secure access control. New users were able to create accounts successfully, with the system preventing duplicate entries. During login, only valid credentials were accepted, thereby restricting unauthorized access.The patient data entry module allowed users to input medical parameters such as heart rate and body temperature. The system processed this data efficiently and forwarded it to subsequent modules for classification and encryption. The classification mechanism accurately categorized patient conditions into high, medium, and low priority levels based on predefined thresholds. This enabled rapid identification of critical cases requiring immediate attention.Data security was ensured through encryption, where sensitive patient information was transformed into a secure format before storage. The encrypted data was successfully stored in a cloud-based database, demonstrating reliable remote accessibility and scalability. The dashboard module provided a consolidated view of patient records, where encrypted data was decrypted and displayed in a readable format for authorized users.The system also handled invalid login attempts effectively by displaying appropriate error messages, ensuring robust authentication mechanisms.

Discussion

The experimental results confirm that the system achieves its intended objectives. The authentication module ensures controlled system access, while the classification component enables quick prioritization of patient conditions. The integration of encryption enhances data confidentiality, and cloud storage improves data availability and scalability.Overall, the system demonstrates efficient performance across all modules and maintains stability during multiple operations. Its simplicity and ease of use make it suitable for practical deployment. However, further improvements can enhance its capabilities, such as incorporating advanced analytics, role-based access control, and real-time monitoring features.

Limitations

Despite its effectiveness, the system has certain limitations. The classification approach is based on simple rule-based logic, which may not capture complex medical conditions. The number of input parameters is limited, restricting the depth of analysis. Additionally, reliance on cloud infrastructure requires a stable internet connection. The absence of graphical analytics and reporting features also limits data visualization capabilities. These aspects can be addressed in future enhancements.

SOFTWARE TESTING

Testing Methodology

A structured testing strategy was adopted to validate the system. The process began with designing test plans that covered all functional and non-functional requirements. Each module was tested individually, followed by integration testing to ensure proper interaction between components. Quality control measures were applied throughout the process to confirm that the system met design specifications and user expectations.

Testing Approach

Manual testing was conducted by providing different input scenarios and verifying the corresponding outputs. The testing process included validation of individual modules, evaluation of complete system workflows, verification of database operations, and confirmation of cloud connectivity. Multiple test cases were executed to ensure system stability and correctness.

Test Case Analysis

The executed test cases covered key functionalities such as registration, login, data entry, classification, encryption, and data retrieval. In all scenarios, the actual outputs matched the expected results, indicating that the system performs reliably. Patient data was correctly classified, securely encrypted, and accurately displayed on the dashboard after decryption.

Conclusion

This work presents an efficient privacy-preserving priority classification (PPC) scheme for remote e-healthcare systems. The proposed solution enables classification of patient data based on urgency while ensuring the confidentiality of sensitive information and healthcare models. By adopting a non-interactive approach, the system reduces communication overhead and improves efficiency.The implementation, which includes an Android application and Java-based server components, demonstrates that the proposed scheme achieves low computational cost and efficient data processing. The integration of encryption and classification mechanisms ensures both security and timely decision-making, making the system suitable for real-world healthcare applications.

Future Enhancements

The system can be further improved by incorporating advanced technologies and expanding its capabilities. Future work may include the integration of machine learning techniques such as federated learning to enhance classification accuracy while preserving data privacy. Real-time data processing can be introduced to support continuous monitoring and immediate response in critical situations.Scalability can be enhanced through distributed or edge computing frameworks, allowing the system to support a larger number of

users and healthcare providers. Integration with Internet of Things (IoT) devices can enable automated data collection from wearable sensors. Additional security measures, such as blockchain technology, can be implemented to ensure data integrity and transparency.Furthermore, the system can be extended to provide personalized healthcare recommendations based on historical data and priority classification. Compliance with international data protection standards and support for cross-platform access through web and mobile applications will improve its adaptability and usability in diverse healthcare environments.

References

1. C. Otto, E. Jovanov, and A. Milenkovic, "A WBAN-based system for health monitoring at home," in *Proceedings of the IEEE/EMBS International Summer School on Medical Devices and Biosensors*, 2006, pp. 20–23.
2. O. Omeni, A. Wong, A. J. Burdett, and C. Toumazou, "Energy-efficient medium access protocol for wireless medical body area sensor networks," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 2, no. 4, pp. 251–259, 2008.
3. A. Argyriou, A. C. Breva, and M. Aoun, "Optimizing data forwarding from body area networks in the presence of body shadowing with dual wireless technology nodes," *IEEE Transactions on Mobile Computing*, vol. 14, no. 3, pp. 632–645, 2015.
4. S. Rezvani and S. A. Ghorashi, "Context-aware and channel-based resource allocation for wireless body area networks," *IET Wireless Sensor Systems*, vol. 3, no. 1, pp. 16–25, 2013.
5. N. McDonald, D. Atkinson, Y. Khmelevsky, and S. McMillan, "Sport wearable biometric data encrypted emulation and storage in cloud," in *Proceedings of Electrical and Computer Engineering Conference*, 2016, pp. 1–4.
6. M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51–58, 2010.
7. Z. Chen, H. Hu, and J. Yu, "Privacy-preserving large-scale location monitoring using Bluetooth Low Energy," in *International Conference on Mobile Ad-Hoc and Sensor Networks*, 2016, pp. 69–78.
8. C. Y. Chou, E. J. Chang, H. T. Li, and A. Y. Wu, "Low-complexity privacy-preserving compressive analysis for ECG telemonitoring systems," *IEEE Transactions on Biomedical Circuits and Systems*, 2018.
9. Cynthia Dwork and Moni Naor, "On the difficulties of disclosure prevention in statistical databases," *Journal of Privacy and Confidentiality*, 2008.
10. M. Fredrikson, E. Lantz, S. Jha, S. Lin, D. Page, and T. Ristenpart, "Privacy in pharmacogenetics: An end-to-end case study," in *USENIX Security Symposium*, 2014, pp. 17–32.
11. Dan Boneh and Mark Zhandry, "Multiparty key exchange and traitor tracing from indistinguishability obfuscation," in *Advances in Cryptology*, 2014, pp. 480–499.
12. Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan, *Fully Homomorphic Encryption over the Integers*. Springer, 2010.
13. Dan Boneh, Eu-Jin Goh, and Kobbi Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Theory of Cryptography Conference*, 2005, pp. 325–341.
14. D. Harrison, S. Boyce, P. Loughnan, P. Dargaville, H. Storm, and L. Johnston, "Skin conductance as a measure of pain and stress in hospitalized infants," *Early Human Development*, vol. 82, no. 9, pp. 603–608, 2006.
15. G. Wang, R. Lu, and C. Huang, "PGuide: A privacy-preserving smartphone-based pre-clinical guidance scheme," in *IEEE Global Communications Conference*, 2015, pp. 1–6.