STM JOURNALS

Journal of
Microcontroller Engineering
and Applications

ISSN: 2455-197X
Volume 12, Issue 2, 2025
May–August
DOI (Journal): 10.37591/JoMEA

https://journals.stmjournals.com/jomea

Review JoMEA

Digilocker Based E-Health Card System

Dere Ekata Santosh[1], Gaikwad Neha Ajay[1], Gajbhiye Sahil Hansraj[1,*], Ankita Sudam More[1]

Abstract

Health care system is one of the critical issues for developing countries and thus information technology is becoming progressively more important nowadays. The deployment of smart health cards simplifies the prescription process, improves the standard of care given, and facilitates electronic healthcare records management through a coordinated health service process. Using the smart health card patient's data, doctor's prescription, patient's present and former health history is accessible. When an infant is born, a record is formed with details like blood group, vaccination dates, complications involved, allergies and other important details. This card plays a crucial role during unexpected incidents like accidents and reduces child trafficking problems. The cloud computed system enrolled within helps to secure data of patients and prevent data intrusion. For authentication and security purposes the hospital's unique code, Aadhaar card number and Doctor's access code is provided which could be accessed only within the Hospitals. The e-health card facilitates privacy protection by filtering access to sensitive data which is accessible only to authorized people like Doctors and Cardholders.

Keywords: Smart health cards, healthcare system, electronic health records (EHR), cloud computing, data security

INTRODUCTION

Inadequate infrastructure, unreliable medical record-keeping, and restricted patient information access are some of the difficulties facing healthcare systems in developing nations. Information technology (IT) has emerged as a key enabler in the transformation of healthcare, with innovations such as the smart health card system offering a viable means of accelerating and improving services. A smart health card is a portable, digital health identification device that contains a patient's whole medical history, including personal information, prescription medications, past and current illnesses, allergies, and immunization records. Authorized users get real-time access to a comprehensive and up-to-date health profile thanks to this data, which is updated continuously during an individual's life. Using smart health cards has several benefits, especially in situations where several healthcare providers usually have different medical records. By centralizing patient data and simplifying the retrieval and updating of medical information, smart health cards improve the standard of care provided to patients (Figure 1). Additionally, by enhancing cooperation between different medical facilities, the technology reduces treatment errors and gets rid of unnecessary diagnostic tests.

One of the main elements of the smart health card system is the integration of cloud computing, which ensures scalable data storage and enhances the security and accessibility of patient records. Thanks to cloud-based technology, healthcare professionals

***Author for Correspondence**
Gajbhiye Sahil Hansraj
E-mail: sahilgajbhiye.2829@gmail.com

Research Scholar, Department. of Computer Science Engineering, Rajgad Dnyanpeeth's Shri Chhatrapati Shivaji College of Engineering (SCSCOE), Pune, Maharashtra, India

Received Date: March 28, 2025
Accepted Date: April 07, 2025
Published Date: May 12, 2025

Citation: Dere Ekata Santosh, Gaikwad Neha Ajay, Gajbhiye Sahil Hansraj, Ankita Sudam More. Digilocker Based E-Health Card System. Journal of Microcontroller Engineering and Applications. 2025; 12(2): 10–16p.

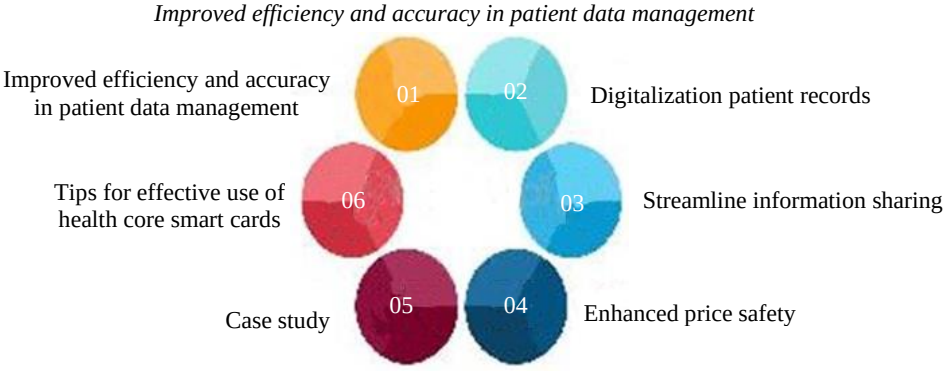

Figure 1. Improving patient data management.

may securely store vast amounts of data while yet having quick access to patient records when needed. Multi-layered authentication techniques, such as the hospital's unique identification code, the patient's Aadhar card number, and the doctor's access code, further enhance the system's security and privacy. Additionally, smart health cards are crucial for facilitating preventive healthcare, such as reminders for routine checkups or vaccinations. They can help reduce the issues related to child trafficking because every child's complete medical history is securely preserved from birth by making it simpler to monitor and identify kids.

LITERATURE REVIEW

Bhardwaj *et al.* [1]

An Io T-based smart health monitoring system created especially for tracking COVID-19 patients is presented by Bhardwaj *et al*. The authors outline a method that uses wearable technology to continuously monitor critical health indicators including oxygen saturation and temperature. In order to improve patient outcomes, the data is sent to medical professionals for prompt intervention. In order to improve the management of health emergencies like pandemics, the study also addresses the system's scalability and possible interaction with current healthcare infrastructures.

Gupta *et al.* [2]

They investigate how IoT and RFID technology can be combined to create a smart card system that serves a variety of industries, such as banking, healthcare, and electricity. The study highlights the ways in which this multi-sector integration can improve service delivery, strengthen data security, and streamline procedures.

Fulong *et al.* [3]

The authors offer a thorough examination of the system's design and features, demonstrating how it has the potential to completely transform the way services are accessed and administered in a variety of fields. The idea of medical cyber-physical systems (MCPS) as a transformative strategy for attaining smart healthcare is covered in this work. In their overview of the state of the art in MCPS, the authors emphasize how computational systems and physical health devices can be integrated for real-time monitoring and decision-making. In order to fully reap the benefits of MCPS, the study highlights the necessity of standardized protocols and interoperability across various healthcare systems, highlighting important research issues and future initiatives.

Senthilkumar *et al.* [4]

This study present a privacy protection approach for smart card-based healthcare systems that makes use of secure cloud storage. To improve user privacy and data security, the authors use symmetric and asymmetric cryptography algorithms. The architecture of the suggested system is described in the study, and simulations are used to assess its efficacy. The results show a notable improvement in data protection against breaches and illegal access, which is essential for preserving patient confidentiality.

Al-Rawashdeh *et al*. [5]

The authors of this systematic review examine a number of papers on the usage of IoT in smart healthcare. They list the main forces behind, difficulties with, and uses of IoT technologies in healthcare environments. The review highlights how crucial IoT is to improving data collecting, patient monitoring, and real-time healthcare delivery. The authors also offer suggestions for future lines of inquiry, such as the necessity of improving data security protocols in IoT healthcare applications and resolving interoperability problems.

Jeong *et al*. [6]

This study explores how blockchain technology and the Internet of Things can be combined to provide intelligent healthcare monitoring [6]. In order to guarantee the confidentiality and integrity of health data gathered by IoT devices, the authors suggest a framework that makes use of blockchain's security properties. The advantages of this integration are described in the study, including increased stakeholder trust and better patient data management. Potential issues with scalability and regulatory compliance in the deployment of such systems are also covered by the writers.

Yuanbing *et al*. [7]

An enhanced authentication protocol for smart healthcare systems that make use of wireless medical sensor networks is presented in this research. To safeguard patient data sent across these networks, the authors stress the necessity of strong security measures. The security is suggested by adding several levels of authentication, the protocol improves security and lowers the possibility of data breaches and illegal access. Through simulations, the authors assess the protocol's efficacy and highlight its benefits in terms of performance and security.

Abdulbaqi *et al*. [8]

In order to facilitate the delivery of tele-health care, this research presents a smart system designed for healthcare caretakers that makes use of the Internet of Medical Things (Io-MT). The authors talk about how this approach could improve patient-caregiver communication, enabling remote monitoring and prompt actions. The design of the suggested system is described in the paper, along with an assessment of how well it works to enhance patient care and caregiver productivity. According to the results, Io-MT has the potential to drastically alter conventional caregiving methods.

Yang *et al*. [9]

This paper suggests a secure key agreement and authentication protocol designed for cloud-based smart healthcare settings. Given the sensitive nature of health data, the authors stress the vital requirement for cloud system security. In order to prevent unwanted access and data breaches, the suggested protocol is made to guarantee secure communication between patients, healthcare providers, and cloud servers. Through formal proofs, the authors confirm the protocol's security and demonstrate its resilience in safeguarding medical records.

Amintoosi *et al*. [10]

The authors present a simple authentication method created especially for intelligent medical services [10]. They draw attention to the difficulties in putting strong security measures in place in situations with limited resources, which are common in healthcare settings. The suggested method provides efficient authentication while reducing computational overhead by striking a balance between security and performance. Through trials, the authors assess the scheme's effectiveness and show that it may be used in real-world smart healthcare scenarios where efficiency is crucial.

THE RESEARCH GAP

Among the research gaps in IoT-based smart healthcare systems are the challenges of scalability and seamless integration with existing healthcare infrastructures, as well as achieving interoperability between different IoT devices and healthcare systems. Real-time data protection and straightforward

authentication methods that balance security and user convenience are still necessary, even though privacy and security standards have been studied. Furthermore, little is known about how to manage regulatory compliance, overcome ethical conundrums, and combine cutting-edge technology like artificial intelligence (AI) and big data with Internet of Things healthcare systems. The long-term efficacy of telehealth and remote monitoring systems, enhancing real-time health data processing for actionable insights, and enhancing user experience are further topics that need more study.

PROBLEM STATEMENT

Healthcare systems in underdeveloped countries have difficulty managing, accessing, and securing patient data because of a lack of infrastructure, fragmented medical records, and other issues. Processes that are ineffective as tests are repeated, data are scattered, and treatment regimens are faulty as a result. The lack of a centralized, secure infrastructure increases the likelihood of data breaches and exacerbates privacy concerns.

Despite advancements in healthcare technology, many regions still rely on paper-based or disjointed electronic systems, which hinders real-time access to critical patient data and complicates the prescription process. In an emergency, a lack of comprehensive patient data could delay life-saving treatment. A solution that integrates cloud computing, smart health cards, and enhanced security measures might revolutionize patient data management. This would meet the needs of modern healthcare and enhance the quality of therapy.

PROPOSED SYSTEM

The following methodology outlines the systematic approach for developing and implementing the smart health card system (Figure 2).

Login and User Registration User Registration

Patients and healthcare providers must fill out a user registration form with their personal data, which is securely stored in the database, in order to use the system. Each user is given distinct login credentials after successfully registering, guaranteeing that only those with permission can access the system. Data integrity and sensitive information are protected by this controlled access technique. By putting in place such a registration and login procedure, the system guarantees that patients and healthcare providers can communicate in a safe setting, encouraging confidence and privacy in the management of private health data.

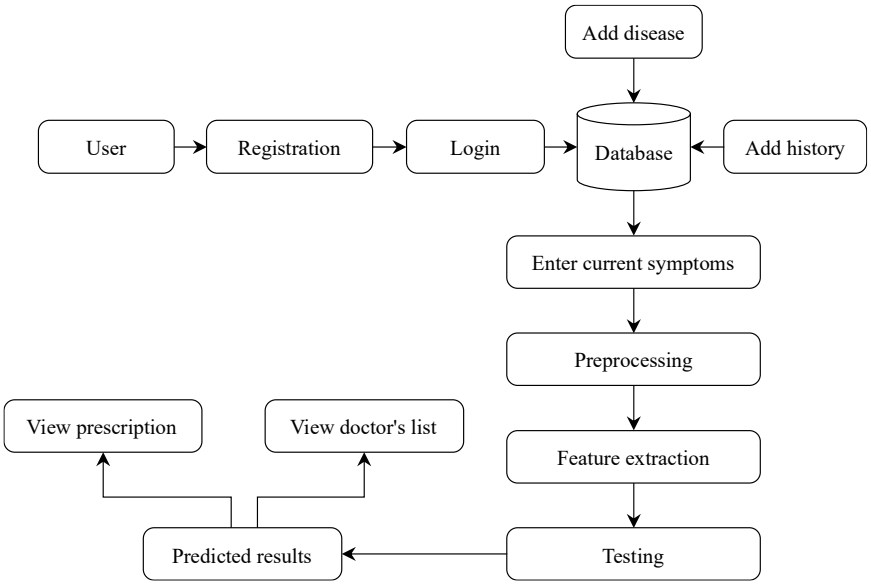

Figure 2. System architecture.

Data Management

Through smooth database integration and a safe cloud-based storage solution, the system effectively handles patient data. Important data, such as personal information, previous medical records, present health conditions, and prescription drugs, are stored in this database. To ensure thorough and current patient information, medical personnel have immediate access to update and input data pertaining to new illnesses or prior medical conditions. Better continuity of care is made possible by this capacity, which makes medical records from the past and present easily accessible for review. The technology improves patient care, expedites data administration, and facilitates well-informed medical decision-making by keeping a clean and safe database.

Entry of Symptoms and Pre-Processing the Symptoms

In order to aid in a precise diagnosis, patients or physicians enter their current symptoms into the system, which are subsequently contrasted with the stored medical history. To guarantee quality and consistency, the given data goes through a pre-processing step prior to analysis. In this stage, any flaws or inconsistencies that can compromise the diagnosis are removed from the input data in order to prepare it for the machine learning model. The system's dependability is increased by this methodical technique that allows for more precise medical evaluations based on both recent and previous health data. The system guarantees effective and precise diagnostic results by simplifying data entry and preparation.

Feature Extraction

To improve diagnostic accuracy, the system collects pertinent features from the dataset following the pre-processing phase. Symptoms, patient demographics, prior diagnoses, and environmental elements that influence health results are some examples of these crucial attributes. The technology guarantees a more accurate and thorough assessment of a patient's status by locating and examining these important data elements. By combining past and current health data, this feature extraction approach helps improve medical evaluations and empowers medical professionals to make informed judgments.

Training and Machine Learning Testing Predicting health disorders and potential therapies involves training a deep learning model, such as a Convolutional Neural Network (CNN), using the pre-processed characteristics. The model finds patterns in the input and gains knowledge from past data.

Testing: The trained model is tested using new data to evaluate its performance. This step ensures that the model can accurately predict health outcomes and treatment recommendations.

1. *Prediction and results*
    a. *Predicted results*: After the model processes the input symptoms and extracted features, it generates a predicted diagnosis. These results are displayed to the healthcare provider or patient.
    b. *Recommendation system*: Based on the predicted diagnosis, the system recommends potential prescriptions (medication) and shows a list of qualified doctors.
    c. *View doctor's list*: The system provides a list of specialists or general practitioners based on the patient’s predicted diagnosis, enabling easy access to healthcare services.
2. *Prescription and follow-up*
    a. *View prescription:* Once the system generates a predicted diagnosis, it offers a set of prescribed medications that the patient should follow, as confirmed by the doctor.
    b. The system maintains a history of prescriptions for future reference and follow-up consultations.
3. *Cloud security and data protection*
    a. *Cloud security*: The system employs cloud computing to store patient information securely. Multi-layer authentication methods (such as Aadhaar, hospital code, and doctor’s access codes) make sure that sensitive data can only be accessed by authorized persons.
    b. *Privacy protection:* The e-health card ensures privacy by filtering sensitive data to prevent unauthorized access. Only doctors and patients have access to specific medical information.

4. *Continuous learning and model updates*
   a. The system continuously updates its machine learning model as new data is entered into the database This iterative learning process improves prediction accuracy over time, ensuring that the system remains effective in delivering high-quality healthcare.
5. *System evaluation*
   a. Periodically, the system's performance is evaluated to measure the precision and dependability of forecasts and suggestions. This guarantees that patients receive the best care possible, grounded in the most recent medical knowledge and recommendations based on data.
   b. This methodology demonstrates a complete, automated process for integrating smart health cards into healthcare systems, offering a comprehensive approach to managing patient data and predicting diagnoses through advanced machine learning techniques.

ALGORITHM: BIDIRECTIONAL LSTM

A Bidirectional, an improved version of the classic LSTM neural network design is called Long Short-Term Memory (LSTM) (Figure 3). Text, speech, and time series are examples of sequences that are ideally suited for processing using LSTM, a form of recurrent neural network (RNN) that is made to recognize long-range dependencies and patterns in sequential data. By adding two distinct layers of LSTM cells: one that processes the sequence from start to finish (forward LSTM) and another that processes the sequence in reverse (backward LSTM), the bidirectional LSTM improves upon the fundamental LSTM structure. A more thorough understanding of the data is produced by the model's ability to include contextual information from both future and previous sequence parts thanks to this bidirectional approach. The Bidirectional LSTM may identify complex patterns and dependencies in sequential data by integrating the data from the forward and backward LSTMs. For jobs like natural language processing, where a word's meaning frequently depends on the words that come before and after it in a sentence, this is very helpful. In order to detect fake news, bidirectional LSTMs can be used to assess the textual content of news items while accounting for the context of words that come before and after them. This enhances the model's comprehension of linguistic subtleties and increases its precision in differentiating between authentic and fraudulent news items. An effective tool in the deep learning toolbox, the bidirectional LSTM helps create more reliable and accurate models for a range of sequential data analysis applications.

One popular recurrent neural network architecture for natural language processing tasks is the bidirectional Long Short-Term Memory (LSTM). It differs from a traditional LSTM, which solely takes historical data into account, by being able to utilize data from both preceding and succeeding aspects. The model's comprehension of contextual linkages within sequential data is improved by its bidirectional

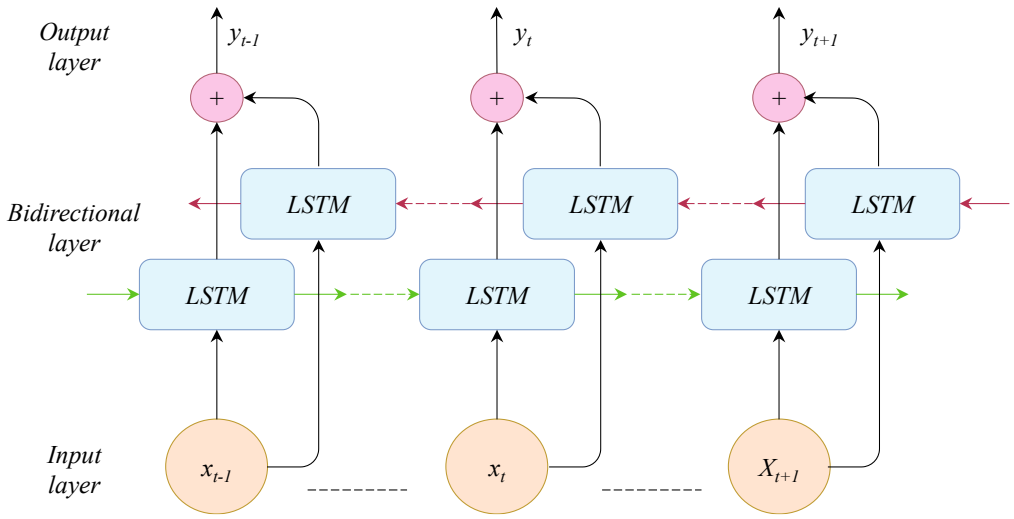

Figure 3. Architect of LSTM.

character. There are two separate layers in the bidirectional LSTM design. The input sequence is supplied as usual in the first layer. Nevertheless, a duplicate and inverted copy of the input sequence is added in the second layer. Two parallel layers are essentially created side by side by this repeated first recurrent layer. Two different LSTM networks show each training sequence both forward and backward. A shared output layer is then connected to these networks. Because of this design, the bidirectional LSTM can absorb comprehensive sequential information from every point in a sequence that comes before and after it. The bidirectional LSTM essentially encapsulates a thorough comprehension of the entire sequence by synthesizing the outputs of the forward and backward LSTM networks at each time step. This is not the same as just encoding the sequence in one way. The model's ability to capture complex relationships and dependencies is improved by this bidirectional approach, which makes it a powerful tool for jobs like identifying false information in textual content.

CONCLUSION

Smart health cards are a revolutionary approach to patient data management and care quality in healthcare systems, particularly in developing countries. They centralize and digitize patient information, improving accessibility and accuracy of medical records. Sensitive health data is protected by cloud computing and cutting-edge security techniques, which also address privacy and data security issues. By sending out timely reminders for immunizations and regular exams, the cards also encourage proactive health management and assist preventative healthcare campaigns. Immediate access to thorough patient data can greatly enhance results in emergency situations. The smart health card system is a scalable way to enhance patient experiences, health provider coordination, and healthcare delivery, as the industry changes. To fully reap its benefits, however, issues like compatibility, implementation costs, and patient accessibility need to be resolved.

REFERENCES

1. Bhardwaj Vaneeta, Rajat Joshi, Anshu Mli Gaur. IoT-based smart health monitoring system for COVID-19. SN Comput Sci. 2022; 3(2): 137.
2. Gupta A, Asad A, Meena L, Anand R. IoT and RFID-based smart card system integrated with health care, electricity, QR and banking sectors. In Artificial Intelligence on Medical Data: Proceedings of International Symposium, ISCMM 2021. Singapore: Springer Nature Singapore; 2022 Jul 24; 253–265.
3. Chen Fulong, *et al*. Medical cyber–physical systems: A solution to smart health and the state of the art. IEEE Trans Computat Social Syst. 2021; 9(5): 1359–1386.
4. Senthilkumar Sudha, *et al*. SCB-HC-ECC–based privacy safeguard protocol for secure cloud storage of smart card–based health care system. Front Public Health. 2021; 9: 688399.
5. Al-Rawashdeh Manal, Pantea Keikhosrokiani, Bahari Belaton, Moatsum Alawida, Abdalwhab Zwiri. IoT adoption and application for smart healthcare: a systematic review. Sensors. 2022; 22(14): 5377.
6. Jeong Soon Hyeong, Jun-Hong Shen, Byeongtae Ahn. A study on smart healthcare monitoring using IoT based on blockchain. Wirel Commun Mob Comput. 2021; 2021(1): 9932091.
7. Yuanbing Wang, Liu Wanrong, Li Bin. An improved authentication protocol for smart healthcare system using wireless medical sensor network. IEEE Access. 2021; 9: 105101–105117.
8. Abdulbaqi Azmi Shawkat, Obaid Ahmed J, Sundos Abdulameer Hmeed Alazawi. A Smart System for Health Caregiver Based on IoMT: Toward Tele-Health Caregiving. Int J Online Biomed Eng. 2021; 17(7): 70–87.
9. Wu Tsu-Yang, *et al*. A Provably Secure Authentication and Key Agreement Protocol in Cloud-Based Smart Healthcare Environments. Secur Commun Netw. 2021; 2021(1): 2299632.
10. Amintoosi Haleh, *et al*. Slight: A lightweight authentication scheme for smart healthcare services. Comput Electr Eng. 2022; 99: 107803.

