Biomedical Letters ISSN 2410-955X DOI: https://doi.org/10.47262/BL/12.1.20260116

Research article
2026 | Volume 12 | Issue 1 | Pages 14-24

ARTICLEINFO

Received
January 06, 2026
Revised
March 02, 2026
Accepted
April 09, 2026

***Corresponding Author**
Md. Tobibul Islam

E-mail
mdtobibulislamthoha@gmail.com

Keywords
Near Field Communication
Electronic Medical Records
Healthcare
Real-time database
Security

How to Cite
Nehal A, Muhammad IA, Islam R, Tarannuma N, Raad TZ, Islam MT. An NFC-based patient identification and access-controlled healthcare management system. Biomedical Letters 2026; 12(1): 14-24.

SCAN ME

Open Access

An NFC-based patient identification and access-controlled healthcare management system

Aparajita Nehal, Ismail Abdullah Muhammad, Raisul Islam, Nushin Tarannum, Tahmid Zaman Raad, Md. Tobibul Islam*

Department of Biomedical Engineering, Military Institute of Science and Technology (MIST), Mirpur, DOHS, Dhaka, 1216, Bangladesh

Abstract

Due to a lack of standardized patient record management, Bangladesh's healthcare system faces significant vulnerabilities. Most hospitals in Bangladesh still use traditional paper-based methods for tracking medical records. This paper presents Med-Sync, a lightweight, web-based healthcare management system that leverages the NFC-based Smart Health Card System. The Med-Sync system is designed to securely provide access to Electronic Medical Records (EMR) for a large number of patients. It uses the Chrome Web NFC API to enable users to interact directly with the browser, making it accessible without the need for using a dedicated application or hardware. The system also makes use of NFC-enabled smart cards with a client–server architecture to support role-based access control and real-time retrieval of patient records. The platform uses both structured and unstructured data storage for quick data retrieval and a user-friendly experience. A functional prototype has been developed and evaluated through system-level testing, showing its feasibility as a practical solution for resource-constrained healthcare settings.

Introduction

Healthcare systems in general struggle with managing patient information on a large scale, and even more so in densely populated developing countries. As Bangladesh is a nation of over 170 million people, it encounters challenges in both rural and urban-level hospitals. Physicians go through extreme burdens to keep track of a vast amount of medical information. Manually preserving documents leads to complications like losing records, unauthorized prescriptions and major setbacks in the treatment schedule, which in turn affect patient safety. The linguistic diversification at the regional level and overreliance on storing data in a paper-based medium give rise to serious medical errors. Across healthcare facilities, the lack of standardized and interconnected medical records creates data silos, hindering the exchange of data among providers. Near Field Communication (NFC) technology offers a profound way of dealing with these challenges in data management. NFC operates within the Radio Frequency Identification (RFID) family and ensures the safe exchange of any kind of data in a close range of 4–10 cm by using 13.56 MHz radio waves. This need for proximity automatically adds an innate security by confining data exchange only to close intentional interactions. In the medical field, NFC facilitates contactless and accurate patient identification as well as retrieving any medical data at the simple touch of an NFC card to an NFC-enabled device. This system eradicates manual searching of records, decreases errors in transcription, and also reduces duration in clinical workflows. As smartphones become more accessible, an NFC-enabled medical card system is a flexible way to modernize Bangladesh's healthcare system.

Recent studies have shown how NFC technology can replace paper-based documentation in the storage of medical data. Marcus et al. [1] developed a smartphone-based NFC system for disease tracking, but it faced operational and compatibility challenges. Still, manual card scanning introduced operational challenges and cross-device compatibility constraints. Doctors can get access to patient reports with a single tap on their mobile phones in the Electronic Medical Report (EMR) system implemented in [2]. Even though this NFC tag-based system allows systematic retrieval of data, the scarcity of NFC-enabled devices poses a drawback to this system. Sethia [3] implemented an Android-based healthcare system that securely exchanges data over Bluetooth using MIFARE Classic tags. But its reliability was uncertain due to its vulnerability to cloning attacks. Singh et al. [4] introduced an NFC-based system to replace paper records with a centralized data system. However, the number of tags and reliance on the internet limit its effectiveness. Despite the challenges in managing security codes, the monitoring system designed by Supriya et al. [3] uses NFC tags for real-time access to EMRs and reducing the risk of a security breach, as it is password-protected. Yu et al. [6] improved hospital workflow by combining NFC and QR codes, but their availability and high deployment cost limited their effectiveness. NFC-based healthcare systems require substantial attention to security measures to address vulnerabilities. Another study by Kumar Polu [4] highlighted a comprehensive analysis of security in NFC cards to identify the attack vectors while suggesting countermeasures, but it relies on encryption and short-range communication. The dual-tag system developed by Ayman et al. [5] transmitted biometric health data securely. But the hardware complexity made it difficult to deploy in the real world. The study by Al Jaafari Hamza et al. [6] compared the encryption methods like Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA) and reached the conclusion that AES and DES offer swifter symmetric encryption that is suitable for larger quantities of medical data. Aldughayfiq and Sampalli [7] demonstrated medication errors in pharmacies. They have integrated NFC tag authentication with fingerprint verification to identify patients. However, implementation challenges hinder the adoption of NFC. Patient-controlled EMR systems prioritize privacy and security [11], but implementing them is challenging because emergency access needs can conflict with privacy policies. In [8], a mobile application for oncology patient management was developed and tested on 100 patients across two clinics over a 60-day trial. This NFC and Firebase integrated model has reduced the waiting period and optimized clinical workflow. However, this system fails to show efficiency for less tech-savvy and elderly people due to their lower proficiency with smartphones. Çobanoğlu and Akalın [13] designed an NFC-based mobile system for emergency response and real-time monitoring, but integration, standardization, and adoption in low-resource settings remain challenging.

Although NFC technology shows promise for managing healthcare data, several critical limitations remain, especially in resource-constrained settings like Bangladesh. Most proposed systems have not

been tested in real-world environments and remain confined to theoretical or controlled laboratory setups. Dependence on NFC-enabled smartphones limits accessibility in rural areas and among elderly or less tech-savvy populations. Security is a concern, as many systems rely on single-layer encryption or basic authentication, making them vulnerable to sophisticated attacks. Models of patient-controlled access have trouble finding the right balance between privacy and the need for emergency care. Furthermore, existing systems often operate in isolation, lacking integration with older hospital information systems, which perpetuates data silos. Cloud-based architectures commonly lack offline functionality, restricting use in areas with unstable internet connectivity.

This study addresses these limitations by proposing an in-depth medical data management system based on NFC. The system was designed with both the urban and rural contexts of Bangladesh in mind. The system uses multi-layer authentication using JWT and Role-Based Access Control (RBAC) for security. The system is designed to work with offline extensions, using local data caching to ensure it still works even without internet access. For accessibility, the system features a universal compatibility layer that supports both NFC-enabled and non-NFC devices with a QR code-based fallback. For resource-constrained mobile devices, a standard web security mechanism using Hypertext Transfer Protocol Secure (HTTPS) and JWT is implemented for computational efficiency. The system uses Health Level Seven (HL7) and Fast Healthcare Interoperability Resources (FHIR) standards to connect hospital management and stop data silos. The system integrates hospital management using Health Level Seven (HL7) and Fast Healthcare Interoperability Resources (FHIR) standards to prevent data silos. The system's effectiveness was validated with functional and system-level testing.

Materials and Methods

The Med-Sync NFC Medical Web App enables instant access to EMR using NFC-enabled devices, which eliminates paper-based patient records with a digital solution. This technology solves major emergency scenarios where patients are unable to share their medical records, overcomes language barriers, and reduces the hassle of handling paperwork.

The system, as shown in **Fig. 1**, integrates modern web technology and NFC technology to develop an end-to-end healthcare data management solution that balances security, accessibility, and real-time data synchronization. NFC card scanning, user login authentication, role-based access control (RBAC), and automatic logout after a certain period of inactivity are some of its primary functional requirements. Only authenticated physicians have read and write permissions, and RBAC ensures that patients can only access their records for viewing purposes. All changes are automatically stored in the database. The technical solution uses a React-based frontend that interacts with a MongoDB database through a Node.js and Express.js server. JSON Web Tokens (JWTs) are used for user authentication and keep users logged in across different browser sessions. The system's deployment uses a dual-hosting approach, with cPanel handling frontend hosting and Vercel handling backend hosting. This approach guarantees scalability, facilitates recovery from failures, and upholds a secure HTTPS connection.

System architecture

The Med-Sync system uses a modular architecture with four main parts: routes, controllers, models, and middleware. Each NFC card has a unique identifier (UID) that initiates secure API calls to get patient information from the database. HTTPS encrypts all communication between the system's layers to protect against man-in-the-middle (MITM) attacks.

System implementation

The system's backend uses a server architecture based on RESTful API principles to ensure uninterrupted communication between the frontend and the database. Routes are designated API endpoints for fetching patient information from the database using the UIDs of NFC tags, user login, and session handling. Controllers handle incoming requests, database interactions, and response generation. Models are used to set up the data structures for MongoDB and SQL relational databases. This makes sure that all the data is represented the same way across the system. Middleware handles authentication, logging, and data validation before requests are delivered to the controllers. The patient data is retrieved by matching NFC tag UIDs with records in MongoDB and returns the results to the frontend in JSON format.

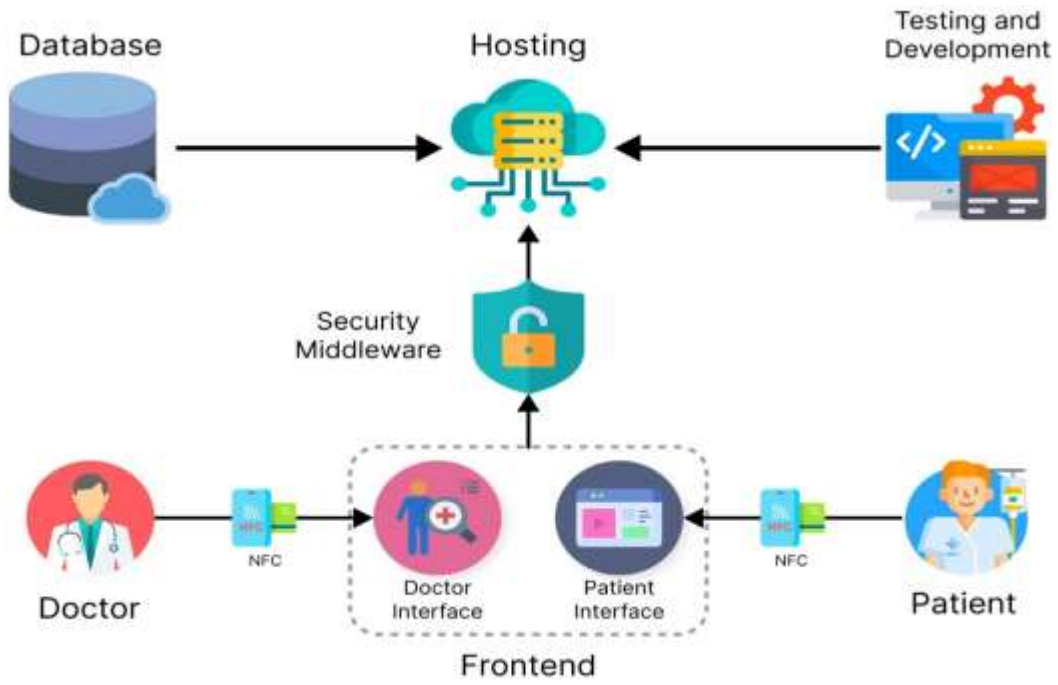

Fig. 1: Represents the overall system architecture of our proposed research work

The frontend uses React.js components to break up the interface into smaller components for later use. This NFC scanner can connect to the Chrome Web NFC API to read NFC tags and retrieve their UIDs. Bilingual support is implemented (Bangla and English), allowing all UI components to dynamically switch language based on user preference. The authentication modal prompts users to log in before accessing sensitive information. The medical records section helps view different health information. Edit and update forms help doctors add, remove, or modify patient records.

Tailwind CSS handles visual elements like colors and layouts, making the app visually appealing on a range of screen sizes. Axios is used to send requests to a server to communicate with the backend. Once an NFC card has been scanned, the server returns patient data in JSON format. There is also local storage for login data, roles, and tokens to keep the user logged in even after the page is refreshed. During loading, the app reads the saved token and displays the interface according to the authorized user's identity.

NFC integration

The system uses the Chrome Web NFC API to allow direct reading of NFC tags in the browser without installing an additional application. When a tag is scanned, the browser reads the UID or the URL from the tag is used to immediately send a request to the backend to locate the corresponding patient record. The displayed information depends on the role. Patients can only consult patient records, but doctors can edit them. The functionality assigned to unsuccessful readings or invalid tags sends a notification with an error description and a request to repeat the scanning procedure.

Database Design

Med-Sync uses both MongoDB and SQL databases. MongoDB stores user credentials, tokens, and session data, which is useful for non-structured data given its document-based nature. SQL uses more specialized tabular data, which simplifies searching for particular details. Role-based data access is another layer of control that ensures people see only the information relevant to their position. The hybrid database approach uses SQL for user data management, authentication, and access control, while MongoDB is used for storing and updating patient records, as it is more compatible with Node.js.

Security

As Med-Sync handles personal health information, security is a primary focus. So, the system integrates

several layers of security to ensure that only authorized personnel can access certain information.

Authentication

Med-Sync uses JWT tokens for logins. After the user logs in, the backend generates a token containing the user's ID, role, and expiry time of the token. The token is then stored on the frontend and is verified every time the user makes a request. The system implements role-based verification at both the frontend and the backend so that the interface shows only the options available based on the user's role. The backend performs additional verifications before servicing any request.

Data protection

All communication between the frontend and backend is encrypted using HTTPS and SSL certificates, preventing anyone from attempting to snoop on the data. The frontend is hosted on cPanel, and the backend is hosted on Vercel, both of which have the HTTPS protocol. Information that needs to be guarded, such as passwords and medical information, is only stored on MongoDB and never on the user's device. Only JWT tokens and expiry times are stored in local storage to maintain the session, and nothing critical is kept on the client side. Tokens are set to expire quickly to narrow down the window of token misuse. There are various other things that are logged (e.g., a failed NFC scan or where someone tried to access when they didn't have access) and all input is checked and scrubbed to prevent typical attacks.

Implementation and validation

The Med-Sync workflow starts when a patient scans their NFC card that has a unique URL or UID against any NFC-enabled device. The URL is then automatically opened in the device browser that shows the data in the user's selected language. The frontend issues an API call to the backend with the data received, and the backend fetches corresponding patient records from MongoDB and returns a response for frontend presentation. The interface lets the user see the personal details, the medical history, allergy information, test reports, and emergency contact numbers for patients, properly gated by the user access level and current authentication state. Patients can only view their information after a password-protected login, while authenticated doctors are given both read and write access for updating medical prescriptions, test reports, and any other clinical information, with all updates synchronized to the database in real time. Timely session expiration expires the current user session and forces a re-login, with the timeout period calibrated to maintain security without degrading user experience.

System validation used a multiphase testing mechanism. System validation was done using a multiphase testing approach. The JWT authentication mechanisms were also validated to ensure that only authorized users with the correct roles could access the system and use the appropriate UI elements. Session timeout calibration is performed iteratively to define the optimal expiration periods that balance security and user convenience. To ensure uniform rendering and consistent system operation, the responsiveness of the design was tested with two device types. Performance optimization focused on API response time, efficient MongoDB queries, and appropriate caching strategies to reduce high latency for operations involving patient data retrieval. Finally, load testing was conducted for the system's performance under concurrent, multi-user access.

Deployment

The deployment phase was tailored to provide secure accessibility, operational stability, and maintainability in the real healthcare settings. The system uses a dual-hosting setup that separates the frontend from the backend for independent scaling and uninterrupted updates. To provide secure client access, CPanel deployed the frontend application with HTTPS protocols, SSL certificates, and DNS configurations. Backend services were deployed to Vercel. A git-based continuous deployment workflow was implemented to enable swift updates, bug fixes, and versioning without interrupting services. Post-deployment iterations significantly improved usability, system responsiveness, and customization, such as providing clear, succinct error messages, indicating loading states, and resetting navigation flows based on early-stage user interactions. Finally, the system was tracked in real-world clinical use cases where healthcare experts and patients used the platform in real operational contexts. Post-deployment security assessments were conducted that validated authentication and data protection mechanisms, including JWT handling procedures, session timeout enforcement, and secure communication practices. Vulnerabilities identified during penetration tests were immediately mitigated

through configuration changes and more permanent code-based remedies. A post-deployment assessment revealed that the system effectively combined NFC identification technology with a web-based healthcare data management scheme, ensuring dependability, security, and convenience in clinical use.

Results

Access Control

Fig. 2A and **Fig. 2B** demonstrate that the Med-Sync system uses a custom design, which consists of the platform name, along with the unique patient identifier in the patient care workflow for a smooth coupling of NFC technology.

These NFC cards serve as the electronic key to access the NFC-based EMR. This enables the user to fetch data instantly by scanning it against any NFC-embedded device. Upon scanning, a role-based interface pops up, and authentication credentials are required.

While the system protects classified medical information behind authentication, it displays a small portion of the patients' personal information. For patients to retrieve their classified data, they must enter a unique password that authenticates them and provides access to verified information. In contrast, doctors must authenticate themselves by entering verification numbers that validate their BMDC number to access the patient's classified information. This bi-level authentication method ensures protection of the medical data of the patients from any unauthorized access, as well as maintains accessibility to legitimate users.

Patients have been given access to update their own passwords in case any risk of password exposure occurs. However, the patients' medical information update is restricted to prevent any unauthorized and inadvertent alteration. Doctors have the authority to read and write, allowing them to modify both patients' personal and confidential medical information, including allergies, diseases, checkup schedules, prescriptions, and diagnostic reports in various formats (PNG, JPG, and PDF). All the changes performed by the authorized doctor synchronize with the database instantly to ensure that the most recent information remains throughout all the access points.

Medical data management

The Med-Sync system uses its dashboard, which contains authentication-based detail levels to manage EMR through its categorized system. The first verification step provides a summary overview, which appears in **Fig. 3A**. Authenticated users access three categories: allergies and sensitivities, disease information, and diagnostic reports, as shown in **Fig. 3B**, documenting food and drug allergies with severity, symptoms, medications, and emergency protocols to prevent adverse reactions; disease information, shown in **Fig. 3C**, which provides condition details, severity, history, prescriptions, appointments, and physician contacts. The diagnostic reports shown in **Fig. 3D** store CT scans, MRIs, and lab results in multiple formats, which include download functionality for sharing and archival purposes.

Doctors possess complete rights to modify all EMR throughout the day, which the system demonstrates in Fig. 4 through its sequential workflow that shows both image and text-based medical data entry, plus the immediate creation of allergy records and the real-time connection to the database. The system enables immediate updates through its system, which keeps all patient information recent at every point of access because it allows users to enter data without waiting for verification while keeping data secure through role-based access.

The Med-Sync system uses its structured dashboard, which organizes patient information into different authentication-based detail levels to manage complete medical record operations. The system shows a summary of the patient's medical information when users complete their first verification process, which is displayed in **Fig. 4A** as a complete health status summary. Authenticated users have the right to view complete EMR, which the system divides into four main sections. The allergy section in **Fig 4B** shows the complete list of food and drug allergies, which contains essential safety details about all allergens, showing their danger level and associated symptoms and needed medications and emergency response procedures, which function as direct alert systems to protect caregivers from harmful reactions during emergency medical treatment. The disease section in **Fig 4C** shows all necessary information about medical conditions, which includes severity levels, complete medical history, current medication details, the last

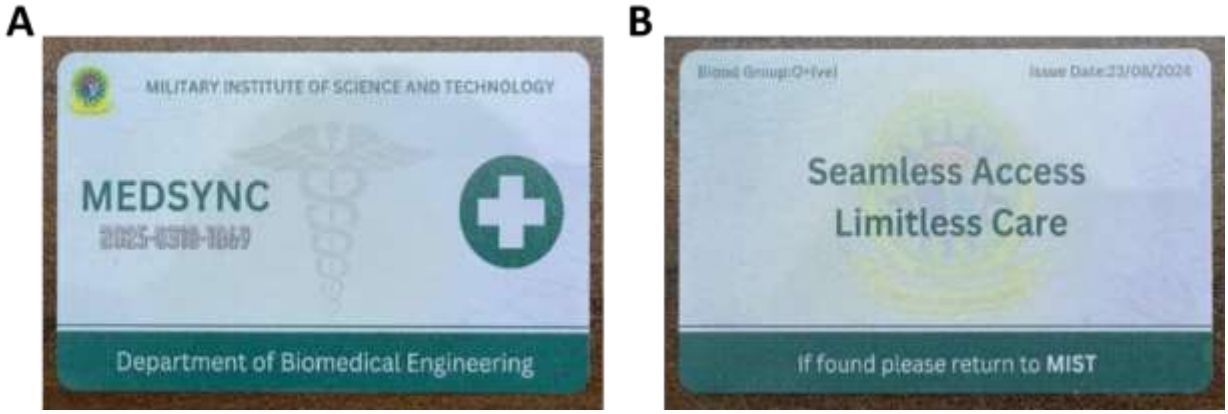

Fig. 2: Design of NFC card: (A) front side, (B) back side

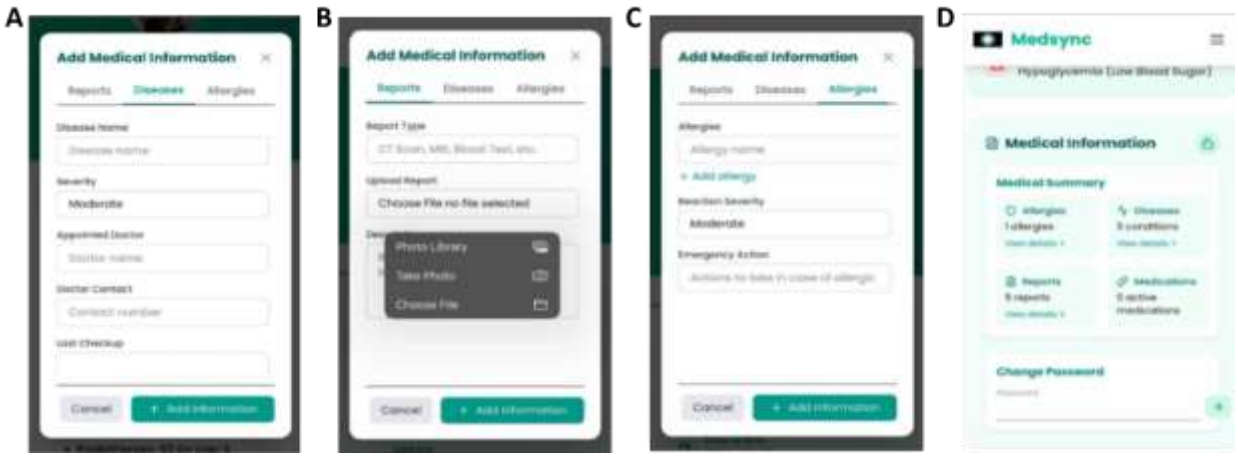

Fig. 3: Med-Sync medical record interface: (A) disease information section, (B) diagnostic report section, (C) allergy and sensitivities section, (D) password update interface

checkup date, the next appointment details and doctor contact information, which helps healthcare workers to quickly understand all aspects of a patient's health situation. The report section in **Fig 4D** supports the storage of different diagnostic results through multiple diagnostic outputs, which include CT scans, MRI images, and laboratory test results stored in different file types like PNG and JPG and PDF, while users can download reports to easily share them and store them for future reference. Doctors have complete power to change any medical data section at any moment. The procedure begins with new medical data added through both image and text methods, while allergy data is registered immediately through both image and text methods, while allergy data is being added through both image and text methods while allergy data gets registered immediately, and the system updates its database in real-time. This system enables instant updates to patients from all location can see the latest data. The system maintains data security by using role-based access controls, which stop patients and other users without proper credentials from making unauthorized alterations to the system.

Accessibility innovation

The Med-Sync system now supports bilingual users through its implementation of Google Translate. This enables the uninterrupted translation between Bangla and English as depicted in Figure 5. Both foreign users and native Bengali speakers can easily access patients' information, prescriptions, diagnostic data, and follow-up schedules in their preferred language while breaking down the language barrier. The application translates all interface elements of the web application, which includes allergies and prescriptions and emergency protocol, while maintaining patient care quality and safety through its complete

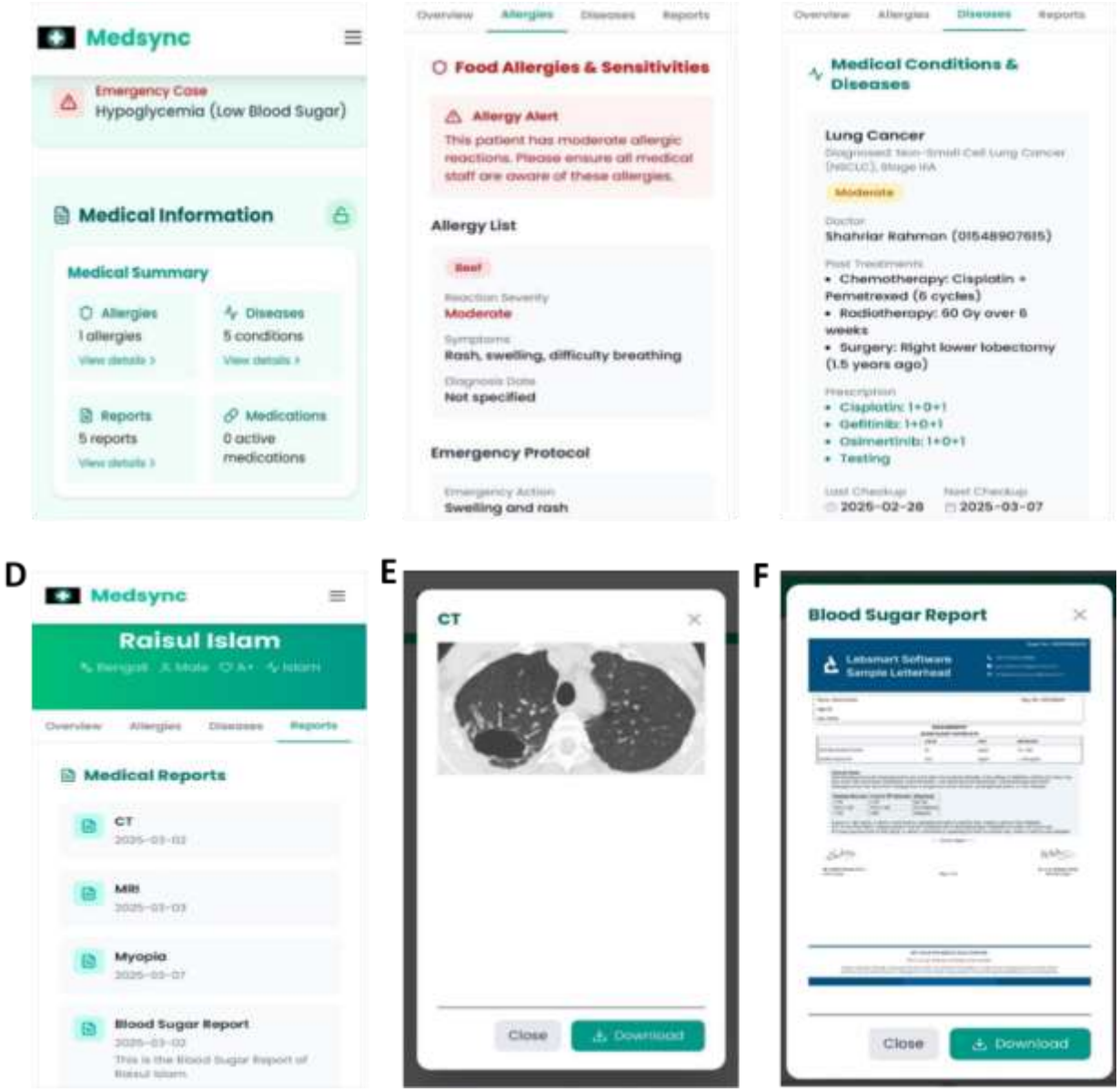

Fig. 4: Medical records display showing (A) summary view, (B) allergy information, (C) reports section, (D) reports list, (E) CT scan (PNG) (F) Blood sugar level (pdf)

translation of the web application interface.

Comparative analysis

The healthcare sector has not adopted NFC technology because of its existing security flaws and accessibility problems, as well as difficulties in real-world implementation. Many of the previous systems were limited to controlled or small-scale implementations. Table 1 offers a summary of current NFC-based healthcare systems, which demonstrate their technical strengths and operational weaknesses according to existing research. This table enables researchers to compare Med-Sync system advantages through its demonstration of essential NFC-based healthcare systems. **Table 1** shows how our proposed research compares to state-of-the-art research. The system solves essential security problems that existed in earlier system designs. The previous studies found security weaknesses. The system protects against unauthorized access through its combination of password authentication, user role identification, and JWT tokens. The system uses HTTPS encryption together with role-based access control, which

Table 1: Represents the comparison of State-of-the-Art research work with our proposed research

Ref	Title	Novelty	Limitations
[2]	Using NFC-enabled Mobile Phones for Public Health in Developing Countries	Real time disease surveillance GPRS based Communication Data can temporarily be stored locally when no internet is available. Data is stored centrally. Real-time database update	No password protection No Security measure No detailed prescription or report No bilingual support No role-base access
[4]	Patient Health Description using NFC-Tag-M-Health	Central data storage Patient info, Health details, diagnosis details, medical details Secured encrypted data transmission	No mention of real-time database updates. No bilingual support No dual role-base access No mention of password protected Security
[9]	Near Field Communication Based System for Health Monitoring	Real-time database update Sensor integration Password protection	Requires expensive reader No role-base access Not compact in size
[13]	NFC based m-Healthcare application focusing on security, privacy and performance	Role-base access Data encryption Two step authentications Real-time database update Central database	No prototype or practical implementation No emergency Protocol No database for doctors
Proposed System	An NFC-Based Patient Identification and Access-Controlled Healthcare Management System	Context-Specific NFC Healthcare Solution Secure Bilateral NFC Authentication Mechanism Real-Time NFC-Triggered Data Retrieval via Secure APIs	User Adaptation and Operational Challenges

operates throughout both the frontend and backend systems. The system is built with security features like access control and authentication to help reduce common threats found in previous studies. The system establishes two access levels, which give patients only read access while doctors can modify medical files, which helps protect patient data and lets patients manage their passwords.

Med-Sync demonstrates practical implementation advantages compared to several existing systems. The system enables organizations to deploy their solutions at lower expenses because it utilizes standard NFC features available on most Android smartphones. The system enables hospitals to produce reports through a single interface that supports multiple document formats, including text and JPG and PNG images and PDF files. The system uses Google Translate to provide bilingual functionality, which enables users to translate English and Bangla text in prescriptions, reports, and emergency protocols. The system provides emergency contacts together with structured emergency information that includes allergy details, severity levels, and treatment response procedures, which provides immediate operational data that previous systems lacked because they focused on retrieving medical history from users [1,2,9].

Discussion

The findings of this study demonstrate that the proposed Med-Sync system effectively addresses several longstanding challenges in healthcare data management, particularly within resource-constrained environments like Bangladesh. The system combines NFC technology with a web-based architecture to offer a practical alternative to traditional paper-based record systems. This greatly improves data accessibility, accuracy, and workflow efficiency. architecture, the system provides a practical alternative to traditional paper-based record systems, significantly improving data accessibility, accuracy, and workflow efficiency. One of the most notable contributions of this work is the successful implementation of a lightweight, browser-based NFC solution using the Chrome Web NFC API. Unlike many existing systems that rely on dedicated mobile applications or specialized hardware, Med-Sync minimizes deployment barriers by using smartphones and web technologies. This design choice directly responds to accessibility issues identified in prior studies, making the system more inclusive, especially

in low-resource and rural settings. Security remains a central concern in digital healthcare systems, and Med-Sync introduces a multi-layered approach to mitigate common vulnerabilities. JWT-based authentication, HTTPS encryption, and role-based access control work together to protect sensitive medical data while ensuring accessibility for authorized users. This system is more secure than earlier systems that relied on single-layer encryption or lacked proper authentication mechanisms. This layered security framework protects the system from unauthorized access and data breaches. The system also has advantages in terms of real-time data management and interoperability. By utilizing RESTful APIs and integrating standards such as HL7 and FHIR, Med-Sync facilitates seamless data exchange and reduces the issue of fragmented medical records. This is particularly significant in the context of Bangladesh, where healthcare systems often operate in data silos. The hybrid database architecture, which uses SQL for structured user data and MongoDB for flexible medical records, makes it easier to handle data and allows for growth. This architectural decision balances performance with flexibility, making it suitable for diverse healthcare scenarios.

Despite these strengths, we must acknowledge certain limitations. The system's dependence on internet connectivity for full functionality may still pose challenges in remote areas with unstable networks, even though local caching partially mitigates this issue. Furthermore, while initial system-level and real-world testing indicate feasibility, large-scale clinical validation across diverse healthcare settings is necessary to fully assess performance, reliability, and user adoption. Training requirements for healthcare professionals and patients, especially those with limited technological literacy, also remain an important consideration for widespread deployment. Overall, this study demonstrates the potential of NFC-enabled, web-based systems to transform healthcare data management in developing countries. By addressing both technical and contextual challenges, Med-Sync provides a scalable foundation for future innovations aimed at improving patient care, reducing medical errors, and enhancing healthcare system efficiency.

Conclusion

The paper offered an NFC-based patient healthcare system, Med-Sync, while addressing the paper-based documentation limitations and fragmented patient records in Bangladesh's healthcare infrastructure. This system utilizes the Chrome-built Web NFC API, eliminating the need for an external NFC reader or any application download. It allows access to the necessary medical information immediately during an emergency. The key features of the system include the display of allergy and contact information without authentication, dual-role access control that differentiates the accessibility of a patient's read-only and doctor's read and write privileges, diverse data format medical record storage, a dual-language interface, and multi-layered security through JWT authentication, HTTPS encryption, and role-based control. The future enhancement may include the Google Map API for locating nearby hospitals and an online payment system. Med-Sync provides a practical and cost-effective NFC implementation in the healthcare system, which can bridge the gap between the real-world clinical deployment and theoretical research in an adverse environment. It can establish a profound base for technological transformation in the healthcare system of Bangladesh.

Acknowledgement

The Department of Biomedical Engineering at the Military Institute of Science and Technology (MIST) is deeply appreciated by the authors for providing the facilities and assistance required to carry out this study. We also acknowledge the academics and staff for their support and direction during the project.

Conflict of interest

The authors declare no conflict of interest.

References

[1] Marcus A, Davidzon G, Law D, Verma N, Fletcher R, Khan A, et al. Using NFC-Enabled Mobile Phones for Public Health in Developing Countries. 2009 First International Workshop on Near Field Communication, IEEE; 2009, p. 30–5. https://doi.org/10.1109/NFC.2009.25.

[2] ALBATTAH A, ALGHOFAILI Y, ELKHEDIRI S. NFC Technology: Assessment Effective of Security towards Protecting NFC Devices & Services. 2020 International Conference on Computing and Information Technology (ICCIT-1441), IEEE; 2020, p. 1–5. https://doi.org/10.1109/ICCIT-144147971.2020.9213758.

[3] Supriya A, Ramgopal S, George SM. Near field communication based system for health monitoring. 2017 2nd IEEE International Conference on Recent Trends in

Electronics, Information & Communication Technology (RTEICT), IEEE; 2017, p. 653–7. https://doi.org/10.1109/RTEICT.2017.8256678.

[4] Kumar Polu S. NFC based Smart Healthcare Services System. IJIRST-International Journal for Innovative Research in Science & Technology| 2018;5.

[5] Ayman M Mansour. NFC Based Android Mobile Healthcare System in Multi-Agent Environment. International Journal of Economics and Management Systems 2017:7.

[6] Hamza A, Kumar B. A Review Paper on DES, AES, RSA Encryption Standards. 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), IEEE; 2020, p. 333–8. https://doi.org/10.1109/SMART50582.2020.9336800.

[7] Aldughayfiq B, Sampalli S. A System to Lower the Risk of Dispensing Medication Errors at Pharmacies Using NFC. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE; 2018, p. 196–202. https://doi.org/10.1109/Cybermatics_2018.2018.00063.

[8] Bedriova N, Smetana M, Gombarska D. Design and Development of Technical Solution for NFC-Based Self-Management Therapy in Actual Oncology Treatment. Applied Sciences 2023;13:2397. https://doi.org/10.3390/app13042397.

[9] Lahtela A, Hassinen M, Jylha V. RFID and NFC in healthcare: Safety of hospitals medication care. 2008 Second International Conference on Pervasive Computing Technologies for Healthcare, IEEE; 2008, p. 241–4. https://doi.org/10.1109/PCTHEALTH.2008.4571079.