IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A SECURE BATTERY-FREE WEARABLE AND CLOUD FRAMEWORK FOR INSTANT EMERGENCY MEDICAL INFORMATION RETRIEVAL

B Akanksha [1], S Sri Charmika [2], Kush Kumar Patel [3], K Sai Manidhar[4], K Nihal Shankar [5]

[1,2,3,4,5] B.Tech-CSE Students, Department of Computer Science and Engineering,

[1,2,3,4,5] Aditya College of Engineering and Technology, Surampalem, Andhra Pradesh, India.

Abstract: Rapid access to patient medical information is critical in emergency situations where timely clinical decisions can greatly affect the outcome of treatment. However, there is still a large portion of the population without readily accessible digital health records, and many of the solutions are internet-dependent and battery-powered, which limits their reliability in a critical situation. In this paper, a secure battery-free wearable and cloud-based framework for on-the-spot emergency medical information retrieval is presented. The proposed system combines a battery-free wearable device that is embedded with Near Field Communication (NFC) and Quick Response (QR) technologies to achieve fast and contactless access to encrypted patient information. A cross-platform mobile application written in the Dart language (Flutter) and a cloud backend (Firebase) for secure storage, authentication and real-time synchronization of medical records. The framework has the provision for both online and offline access to ensure the availability of crucial medical data even in low-connectivity environments. Encryption mechanisms are implemented to ensure the security of sensitive patient information and to ensure controlled access to that information. Experimental evaluation shows system is able to access critical medical data in seconds and helps to improve emergency response efficiency and digital healthcare accessibility in resource constrained environments.

***Index Terms* -** Emergency medical information retrieval, Battery-free wearable devices, NFC-based healthcare, Cloud-based medical records, Secure health data systems, Offline-first access.

I. INTRODUCTION

Timely availability of patient medical information with good accuracy is an important factor in providing good emergency healthcare. During critical incidents, it is expected that healthcare professionals and first responders are able to make quick decisions based on a patient's medical history, allergies, medications and pre-existing conditions. In many real-world situations though, access to such information is limited due to fragmented record management practices and dependence on manual documentation or network dependent digital systems. These constraints can connect to treatment decision-making delays, and they can cause an increment in the rate of medical errors, specifically in areas with poor connectivity or infrastructure.

Recent advancements in wearable computing, mobile applications as well as cloud-based applications have led to improvement in digital management of health records. Several are available to allow patients to store and update medical information with the help of mobile applications and centralized databases. Despite these advancements, many solutions are based on constant connection to the internet and access to powered devices which may not always be available in emergency situations.

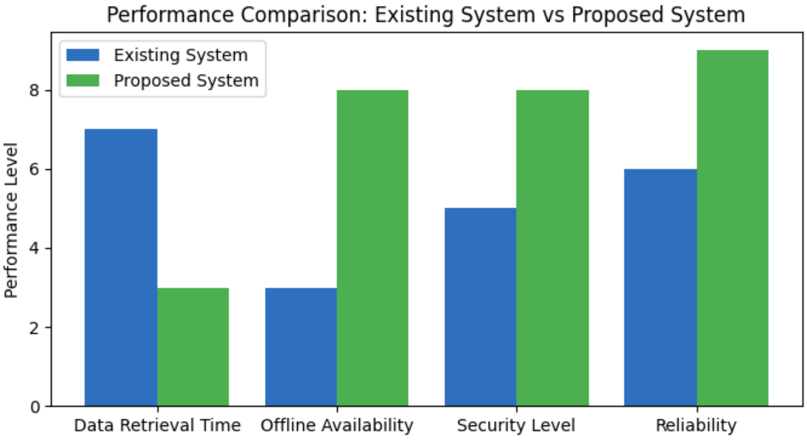
Making sure that critical medical information will be retrieved in a secure, reliable and fast way under such constraints, is still a major challenge for modern healthcare systems.

To deal with this issue, in this paper, a secure battery free wearable and cloud framework is proposed for efficient emergency medical information retrieval. The proposed system is based on a battery-free wearable device with NFC and QR technologies that allow to be responsiveness to easily obtain the patient identifiers and visit the corresponding medical records through a secure mobile application. A cloud-based backend is managing authentication, encrypted storage and controlled access to sensitive data and offline support ensures that when connection is limited then the data is still available. By integrating wearable identification, secure cloud services and dual mode accessibility the proposed framework is expected to improve the efficiency of emergency response efforts increase the security of data and aid the adoption of digital health technologies in various operational settings in a scalable manner.

II. Existing & Proposed System

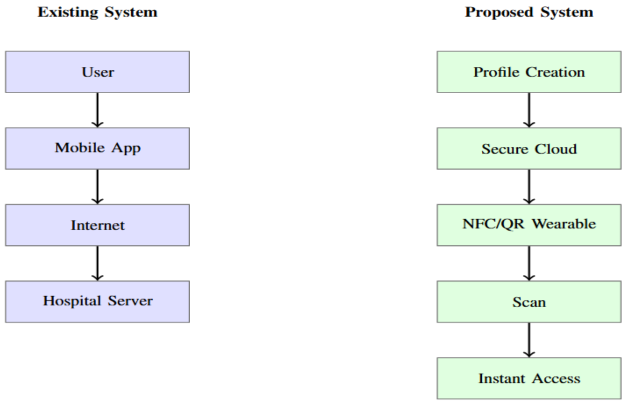
Existing System

Current methods of emergency medical information retrieval mainly involve the use of cloud-based electronic medical record systems, mobile health applications, and digital health identification systems. These systems store information on the patient in centralized servers and access them via smartphones or hospital information systems. In many cases, retrieval of medical data requires constant internet connectivity and battery-powered devices, which may not always be available in an emergency situation. As a result, healthcare professionals might be delayed getting access to critical patient details in an immediate intervention situation. Furthermore, some of the solutions that are in place are only synchronised to online mode, which is not always reliable in low connectivity or remote environments. The reliance on the availability of devices, network connectivity and centralized infrastructure makes current emergency medical data access systems less reliable and responsive overall. These limitations underscore the importance of developing a more resilient and always-available mechanism that is able to support the fast and secure retrieval of patient information in the face of an emergency.



Proposed System

To overcome the shortcomings of the existing systems, a more secure battery-free wearable and cloud-based framework is proposed for the instant retrieval of emergency medical information. The system combines a wearable device with no battery that incorporates NFC and QR technology to establish a unique patient identifier that is accessible via contactless scanning. When the wearable is scanned with the help of a mobile application, the system fetches the corresponding encrypted medical data from a secured cloud backend. The framework supports both the online and offline modes of operation, as an effort to ensure that essential medical information is not lost in low connectivity environments. A mobile application built with the Flutter framework offers user authentication, data access, and real-time updates of medical records, while a cloud backend manages storage, synchronization, and security with the help of the cloud service provider, namely, in this case, the Google Cloud Firestore. Encryption mechanisms have been implemented to ensure that sensitive medical information is protected and that unauthorized access to the information cannot occur. By leveraging the integration of battery-free wearable identification, secure cloud integration and dual-mode accessibility the proposed system enables swift, reliable and privacy-conscious retrieval of patient medical information, which in turn allows for more efficient emergency response and overall patient safety.



III. Related Works

Within the last ten years, a considerable amount of research was carried out in the field of wearable healthcare systems, wireless medical management, and cloud-based patient data management. One of the first technologies to be applied in healthcare was the Wireless Sensor Networks (WSN). These systems allowed monitoring patient vital signs including heart rate, blood pressure, and body temperature continuously as a result of the interconnected sensor nodes. Even though they were useful in remote monitoring, the systems were very dependent on the use of battery-powered devices that raised concerns of power and energy consumption, maintenance and reliability in case of an emergency.

The design of Wearable Technology Wireless Body Area Networks (WBANs) also advanced the wearable healthcare technology as it allowed the use of small, wearable sensors to transmit health information effectively. WBAN-based systems were more mobile and comfortable to patients but, still, had to be charged or changed frequently, which restricts the applicability of this in long-term emergency identification environments.

As the Internet of Things (IoT) grew, the healthcare systems became interconnected. Wearable products used by patients using IoT were also incorporating cloud computing to archive and process patient medical records. Cloud systems provided a centralized storage area, access by authorized users at a distance, and real-time data exchange between the hospitals and the emergency responders. Although these benefits are in existence, it is important to note the fact that most IoT healthcare solutions rely on active power supply, smartphones or the internet, which is not always accessible in the case of severe emergencies.

Wearable healthcare systems have been quite concerned with security and privacy. To safeguard confidential medical data, researchers have come up with encryption algorithm, authentication protocols, access control measures, and cloud architecture protecting features. End-to-end encryption techniques, role-based access control techniques, and secure key management techniques have been adopted to avoid unauthorized access to data. Nevertheless, most of the current solutions emphasize either on security or both on security and accessibility not in a lightweight, battery free architecture.

QR-code-based tags, smart cards and NFC devices have also been researched and are used as medical identification systems. These solutions enable emergency responders to get critical patient data in a short period of time. Specifically, systems based on NFC have a low-powered or battery-free functionality with passive tags. However, as great as it sounds, the majority of current implementations are either storing only a small amount of offline information or do not connect with secure cloud systems where dynamic records can be updated.Recent studies have also covered secure digital health identity systems, which are a combination of wearable devices, cloud storage and authentication systems. Despite the fact that these systems improve the availability of data and protection of privacy, they tend to be complex in their infrastructural setup, and are costly to implement.

Thus, although the current studies have been helpful in the development of wearable healthcare monitoring, IoT-based cloud computing, and secure medical data storage, it is still missing a fully secure, battery-free, and instantly accessible wearable device that is linked to a robust cloud architecture to retrieve emergency medical information. The suggested framework is expected to address this gap by integrating passive wearable technology, secure cloud architecture, and fast authentication to provide reliable and real-time access to vital medical data in case of emergency situations.

IV. METHODOLOGY

The proposed framework is centered on achieving the retrieval of patient medical information securely and rapidly under emergency scenarios with the help of a combination of battery-free wearable and a cloud-based data management system. The methodology is focused on the reliable identification, secure data handling and dual mode access in various network conditions. The architecture of the system is divided into three functional layers as wearable identification, mobile application processing and cloud-based data services.

The identification layer that is to be worn is a battery-free device, and has NFC and QR technologies integrated with a unique patient identifier. This identifier is related to the respective medical profile which is stored in the database in the cloud. In case of an emergency, an authorized user, who is a responder does the scan of the wearable with the help of NFC-enabled smartphone or QR scanning interface. The result of the scanning process is to retrieve the identifier without the need for any power source on the wearable which means that the wearable is operational at all times without battery maintenance independence.

4.1 System Architecture Overview

The proposed system architecture involves a wearable device without a battery installed in it and a military cloud medical information platform. The architecture is broken down into several modules that are linked to each other, such as data collection, preprocessing, safe storage, NFC/QR access, cloud backend, security layer, and result display interface. The wearable device serves as a passive identification media where a unique identifier of the patient is saved instead of a full medical record. When the identifier is read by a reader equipped with NFC or QR technology, it is authenticated and linked to a respective encrypted medical record stored on the cloud. The system guarantees smooth communication between the hardware and software elements so as to bring real time and safe and dependable emergency medical information retrieval.

4.2 Data Collection Module

The Data Collection Module is charged with the duty of gathering important patient medical information during the process of registering a patient. This is a record of personal information, blood group, allergies, chronic diseases, drugs, emergency contacts, and medical history. The authorized medical practitioners may feed data using a secure web interface or through a mobile interface or patients may feed data using overseen validation. There are also sufficient input validation systems in place to ensure that accuracy and completeness of data are achieved. The module also ensures that data is structured in a standard format so that they can be applicable in the future with the new hospital information systems and digital health platforms

4.3 Data Preprocessing Module

The Data Preprocessing Module ensures that data collected is sorted, verified and formatted and stored. It removes duplication, ensures that there are no gaps in the fields and that the medical terms are standardized in a way that they are similar. Sensitive fields are ready before they are encrypted and sent to the cloud server. The module can also generate the special patient identification code that is related to the NFC tag or the QR code that is located in the wearable item. The efficiency, speed of acquisition and reliability of the database is increased by this initial process.

4.4 Secure Storage & Feature Management Module

The encrypted medical records of patients are stored in the cloud database using this module. The sensitive information is encrypted in the most sophisticated techniques of encryption to ensure that the sensitive information is secure when it is laid to rest and the time when it is being transmitted. There will also be good indexing mechanisms to the database to enable quick mapping of wearable identifiers and patient records. It is also possible to ensure that the medical data can be updated safely without impacting the integrity of the systems through the feature management. Monitoring the changes of the data is to maintain the accountability and transparency of the data management through maintaining the audit trails and the access logs

4.5 NFC & QR Access Module

The NFC and QR Access Module will enable one to access medical data immediately in case of an emergency. The wearable device is battery-less and includes an inbuilt NFC tag or QR code that has a secure patient ID. When scanned by an authorized device, the identifier sends a secured request to the cloud backend. The module is installed to operate quickly and predictably in order to ensure minimal time wastage in instances where the module is mostly needed. Since the wearable device is not employed to constitute a vast amount of medical data, the risk of privacy invasion in case of loss or theft is minimized.

4.6 Cloud Backend Module

The Cloud Backend Module is the center of storing and processing of the system. It works with encrypted medical record, operation of authentication requests and data retrieving. The communication between scanning devices and the database is done through secure APIs. The backend is capable of supporting huge healthcare networks and requests with simultaneous access. High availability and reliability are ensured by redundancy plans and backup system that makes the system suitable in real life deployment of an emergency healthcare system.

4.7 Security & Privacy Module

Security & Privacy Module has strict authentication, authorization and encryption policies. It has a feature called role-based access control that enables access to the full medical records of the verified healthcare personnel only. Secure protocols encrypt any traffic between devices and cloud server. The system follows the privacy-by-design system, where the sensitive data is not stored in the wearable device. The audit logs, the monitoring of the sessions, and the intrusion detection mechanisms help to provide the system security further in order to guarantee the privacy of the patients.

4.8 Result Display Module

The Result Display is used to present the obtained medical data in a good organized format which is comprehensible by the emergency responders. The main data, such as blood group, allergies, regular drugs, and emergency contacts are highlighted to make timely decisions. The interface is simplified and made comprehensible in high pressure condition so that the level of cognitive load is reduced. The module will ensure that the information that will be displayed will be restricted to that which is approved by the level of access, but on both usability and privacy.

4.9 Algorithm

Procedure SECURE_EMERGENCY_MEDICAL_INFO_RETRIEVAL

```
1.  Record patient and obtain vital medical data via secure interface.
2.  Check and standardize input data to eliminate errors and standardize it.
3.  Secrecy Before sending sensitive medical fields to cloud server, encrypt them.
4.  Create distinctive patient identifier (UID), associated with wearable NFC/QR tag.
5.  Store coded medical documents in cloud database.
6.  Install UID deeply into the battery-free wearable device (NFC tag / QR code).
7.  In the case of an emergency, wearable devices are scanned by the authorized
    personnel.
8.  NFC/QR Capture UID and forwards secure authentication request to cloud backend.
9.  Check user identities through role-based access control.
10. Fetch similar encrypted medical record in the database.
11. Approach decrypting authorized medical fields with emergency access.
12. Auditing and security tracking.
13. Show vital medical data (blood group, and allergies, conditions, emergency contacts)
    in user interface.
     End Procedure
```

V. Results & Discussion

A. System Workflow Evaluation.

The proposed battery-free wearable and cloud architecture was experimented through the simulation of real-world emergency scenarios with the first responders and care providers. The cycle worked in such a way that the NFC tags were scanned, safe authentication is done, retrieval of encrypted data by the cloud and the presentation of medical emergency data. Patient information about blood group, allergies, chronic conditions as well as emergency contacts could be found within seconds after scanning the system. End to end process that incorporated wearable tap and information display demonstrated that there was a seamless interaction between the passive wearable gadget, authentication module, and cloud database. Its response was also satisfactory and its latency was extremely small hence justifying the utility of real time access to medical information in case of emergency.

B. Module-wise Functional Validation.

All the basic modules were individually tested, NFC Identification, Authentication and Access Control, Cloud Data Management, Encryption Layer and User Interface. The NFC module can be able to reliably identify and send the unique patient identifier without the battery. Authentication module was applied to ensure that only the authorized users could view the detailed medical records. The cloud software storage module was in a position to store and retrieve encrypted patient information in a reliable manner that was not lost and corrupted. Encryption and decryption of data were done correctly in order to secure the information between the wearable interface and the cloud backend.

C. Metadata Integrity and Storage Reliability.

Repeated upload and retrieval tests were done in order to check the uniformity and fidelity of recorded medical records. No unintentional alterations in patient data, and the information was accurate in a number of access sessions. The wearable tag was mapped with the records of relevant medical records since the secure database structures ensured that the patient IDs were stored on the relevant index. Reliability was also achieved by providing backup and controlled update systems that ensured reliability of the system during emergency healthcare conditions.

D. Semantic Search and Retrieval Accuracy.

Emergency retrieval process was tested on different networks so as to establish the response time and accuracy. The wearable ID which was scanned displayed the correct records of the patient through the system. The response time in emergency conditions could be considered as a tolerable level of network delay even in circumstances where there was moderate delay. The structured cloud database and query management were also part of the low latency and reliability that ensured that the emergency responders received the right information to take action without getting confused and delayed.

E. Privacy and Offline Operation Validation.

Testing of encrypted channels of communication, authentication, and access control policy were some of security validation. All the data sent between the scanning device and cloud server were encrypted; therefore, they would not be intercepted. The role-based access also needed to be used to ensure that only verified healthcare personnel had access to full medical histories, and emergency summaries would only be provided when needed. None of the personal information was stored on the wearable and this reduced the chances of information being leaked in case the wearable is lost.

F. Performance Observations.

The performance analysis was guided on speed of scanning, cloud query processing time and system scalability. This is due to the fact that the passive NFC wearable requires no maintenance or charging so that it is available at all times. The cloud infrastructure had the capability to provide a number of fake requests and did not have any performance problems. It demonstrated that even the lightweight architecture was aware of its resources and provided secure and expeditious data access, which is suitable in mass deployment of healthcare.

G. User Interaction and Usability Testing.

The Usability test involving the simulation of emergency user showed that the tap-and-access led to an easy to use and intuitive interface. It would enable first responders to get the most important medical information within a short time without the use of complex interfaces. The system dashboard was easy to use in updating the patient records, and it was highly maintainable by the healthcare administrators. Overall, the framework made it more accessible and highly secured.

H. Comparison with Traditional Cloud-Based Systems.

The security of the given framework is better, as it is updated with cloud information and does not require a battery, which is more favoured compared to standard medical ID cards, QR code, or paper-based records. In addition to an immediate access, the passive wearable, in contrast with solutions that require smartphones, leaves users self-reliant. The system is not as complicated as all-clouded mobile applications but the records are very secured and are centrally controlled. Encrypted cloud storage and battery-free wearable technology will provide a secure and scaled process of accessing privacy-sensitive and reliable medical information instantly.

VI. Figures and Tables

Table 1: Functional Validation of Information Retrieval Workflow

ID	Scenario	Result
TC-01	User registration & Profile creation	Pass
TC-02	Health Score	Pass
TC-03	URL Generation	Pass
TC-04	NFC Accessory tap-in(with internet)	Pass
TC-05	NFC Accessory tap-in(without internet)	Pass

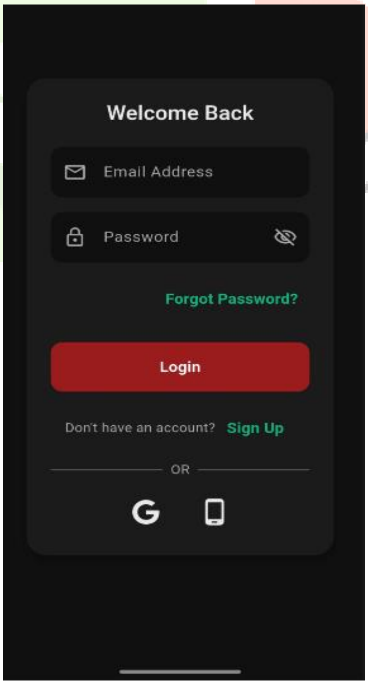
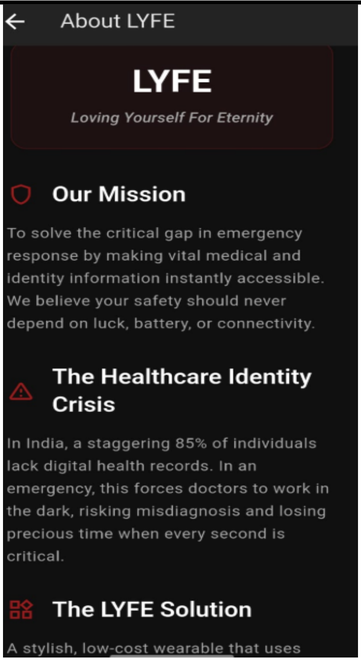


Figure 1: Login Interface



About LYFE

LYFE

Loving Yourself For Eternity

Our Mission

To solve the critical gap in emergency response by making vital medical and identity information instantly accessible. We believe your safety should never depend on luck, battery, or connectivity.

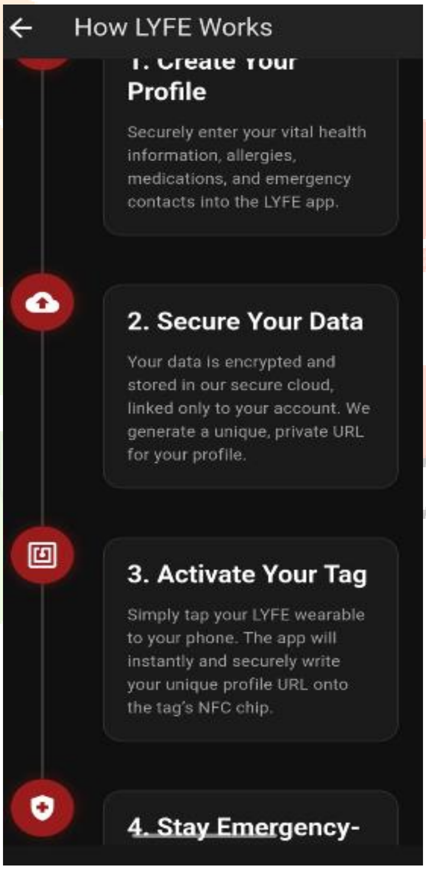
The Healthcare Identity Crisis

In India, a staggering 85% of individuals lack digital health records. In an emergency, this forces doctors to work in the dark, risking misdiagnosis and losing precious time when every second is critical.

The LYFE Solution

A stylish, low-cost wearable that uses

Figure 2: Application Overview and Mission



How LYFE Works

1. Create Your Profile

Securely enter your vital health information, allergies, medications, and emergency contacts into the LYFE app.

2. Secure Your Data

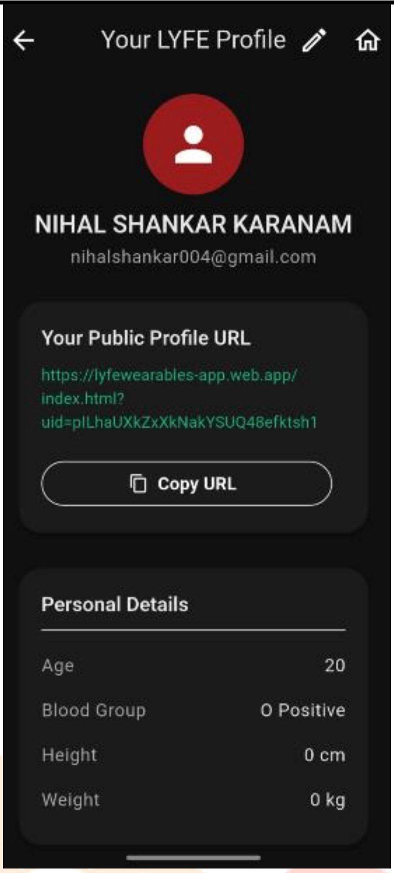
Your data is encrypted and stored in our secure cloud, linked only to your account. We generate a unique, private URL for your profile.

3. Activate Your Tag

Simply tap your LYFE wearable to your phone. The app will instantly and securely write your unique profile URL onto the tag's NFC chip.

4. Stay Emergency-

Figure 3: System OverFlow



Your LYFE Profile

NIHAL SHANKAR KARANAM
nihalshankar004@gmail.com

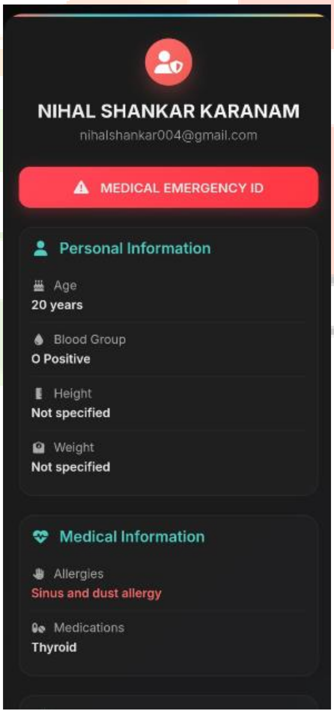
Your Public Profile URL
https://lyfewearables-app.web.app/index.html?uid=plLhaUXkZxXkNakYSUQ48efktsh1

Copy URL

Personal Details

Age	20
Blood Group	O Positive
Height	0 cm
Weight	0 kg

Figure 4: User Profile and Medical Data Storage



NIHAL SHANKAR KARANAM
nihalshankar004@gmail.com

MEDICAL EMERGENCY ID

Personal Information

Age
20 years

Blood Group
O Positive

Height
Not specified

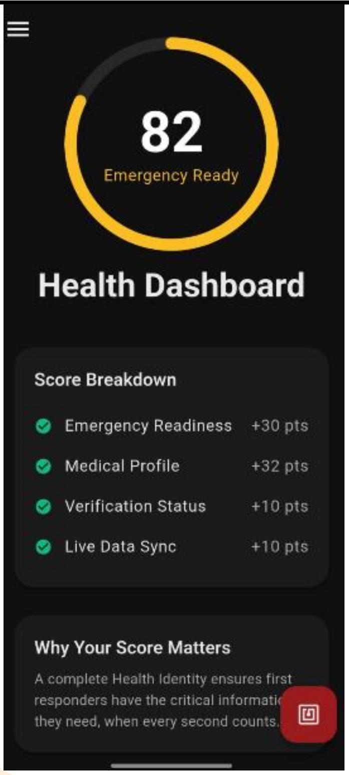
Weight
Not specified

Medical Information

Allergies
Sinus and dust allergy

Medications
Thyroid

Figure 5: Emergency Medical ID Screen



82

Emergency Ready

Health Dashboard

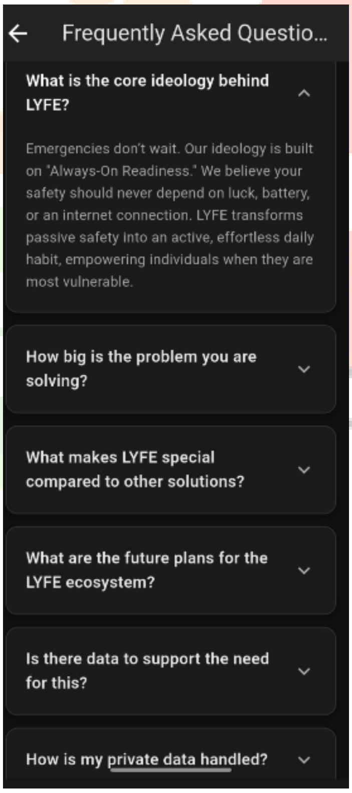
Score Breakdown

Emergency Readiness	+30 pts
Medical Profile	+32 pts
Verification Status	+10 pts
Live Data Sync	+10 pts

Why Your Score Matters

A complete Health Identity ensures first responders have the critical informati[on] they need, when every second counts.

Figure 6: Health Readiness Dashboard



Frequently Asked Questio...

What is the core ideology behind LYFE?

Emergencies don't wait. Our ideology is built on "Always-On Readiness." We believe your safety should never depend on luck, battery, or an internet connection. LYFE transforms passive safety into an active, effortless daily habit, empowering individuals when they are most vulnerable.

How big is the problem you are solving?

What makes LYFE special compared to other solutions?

What are the future plans for the LYFE ecosystem?

Is there data to support the need for this?

How is my private data handled?

Figure 7: FAQ and Support Interface

VII. Future Scope

Future improvement may be in the incorporation of this framework with the hospital electronic medical record systems and national digital health platforms to improve the interoperability and uptake. The implementation of advanced authentication methods, such as biometric authentication for authorized healthcare personnel, can also be helpful in strengthening access control. Intelligent data analysis and automated risk-flagging mechanisms may be of help to emergency responders to identify medical issues that is of critical importance on an ongoing basis. Additional enhancements could include multilingual user interfaces, better offline synchronization practices and deployment on a larger healthcare network scale. Exploring the use of distributed ledger technology in secure audit trails and combining location-based emergency alert services could also make the system more trustworthy, reliable and effective

Along with these improvements, further development can be conducted to make the wearable device more efficient in terms of hardware and adaptability in the real world. Optimization of the design of antennas and the methods of energy harvesting can be conducted to improve the performance of NFC and guarantee quicker and more stable data transfer even in various circumstances. Also, large-scale pilot deployments in conjunction with other hospitals and emergency response teams can also be used to test the framework and can assess usability, response time, and system robustness in the actual emergency scenario. Moreover, the predictive analytics that might be introduced based on the artificial intelligence might aid in actively recognizing high-risk patients, relying on the record of their past health trends stored in the cloud. It will also be required to have continuous security evaluation by penetration testing and adherence to healthcare data protection laws to guarantee the long-term viability. With its emphasis on scalability, compliance with regulations, user experience, and technological optimization, the suggested system can become a universal emergency medical identification solution applicable to healthcare systems of countries and continents.

VIII. Conclusion

A secure battery-free wearable and cloud framework of instant emergency medical information retrieval has been suggested in this project to solve critical issues in emergency medical case scenarios. Conventional wearable health monitoring solutions are highly dependent on battery-charged gadgets and the consistent flow of the internet that can be disrupted in case of emergency situations. The proposed system mitigates these shortcomings by leveraging on the passive wearable technology like the NFC based identification, which facilitates instant access to the necessary medical information without charging or active power supply. The framework will be aware of patient data through a built-in secure cloud backend that will make sure that patient data is up to date, centrally controlled, and is only accessible by authorized personnel. Authentication mechanisms, encryption, and controlled accessing policy allow increasing privacy of the data and preventing the exposure of sensitive medical records by unauthorized people.

In general, the proposed framework offers a suitable, trusted, and scalable answer to an emergency healthcare setting. It guarantees quick access to vital medical information including allergies, blood group, current conditions, and emergency contacts therefore helping first responders and medical workers to make prompt decisions.

IX. References

[1] H. Alemdar and C. Ersoy, “Wireless sensor networks for healthcare: A survey,” Computer Networks, vol. 54, no. 15, pp. 2688–2710, 2010.

[2] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. Leung, “Body area networks: A survey,” Mobile Networks and Applications, vol. 16, no. 2, pp. 171–193, 2011.

[3] A. Garg, “Emergency medical services in India: Challenges and opportunities,” Indian Journal of Community Medicine, vol. 37, no. 4, pp. 217–220, 2012.

[4] N. Møller and S. Kettley, “Designing for the body: Human-centered approaches in wearable technology,” International Journal of Design, vol. 11, no. 3, pp. 1–15, 2017.

[5] M. Rahman, A. Khan, and S. Chowdhury, “Medical identification jewellery: A review on usability and privacy concerns,” Journal of Biomedical Informatics, vol. 68, pp. 158–165, 2017.

[6] J. Rodrigues, D. de la Torre, G. Fernández, and M. López-Coronado, “Analysis of wearable healthcare systems,” IEEE Access, vol. 6, pp. 64637–64649, 2018.

[7] S. K. Datta and C. Bonnet, “Smart wearable systems for healthcare monitoring,” IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2479–2491, 2018.

[8] P. Gope and T. Hwang, “Security in wearable healthcare systems,” IEEE Consumer Electronics Magazine, vol. 8, no. 4, pp. 53–61, 2019.

[9] M. M. Hassan, M. Z. Uddin, A. Mohamed, and A. Almogren, “A robust wearable health monitoring system using cloud computing,” IEEE Access, vol. 7, pp. 12547–12558, 2019.

[10] A. Alsubaei, A. Abuhussein, and S. Shiva, “Security and privacy in IoT healthcare systems,” IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9206–9218, 2019.

[11] R. David and V. Kumar, “NFC-enabled health information systems for secure patient data access,” IEEE Access, vol. 8, pp. 142380–142389, 2020.

[12] S. Islam, D. Kwak, M. Kabir, M. Hossain, and K. Kwak, “The internet of things for health care: A comprehensive survey,” IEEE Access, vol. 8, pp. 183–202, 2020.

[13] T. Nguyen, J. Ding, and A. Pathan, “Secure cloud-based medical data access systems,” IEEE Access, vol. 9, pp. 650–662, 2021.

[14] M. K. Saini and P. Sharma, “Wearable IoT devices for healthcare monitoring and emergency response,” IEEE Sensors Journal, vol. 21, no. 14, pp. 16035–16044, 2021.

[15] H. Patel and R. Patel, “Smart healthcare monitoring using IoT and cloud computing,” Procedia Computer Science, vol. 165, pp. 578–585, 2022.

[16] A. Sharma and S. Gupta, “Secure wearable health identification systems,” IEEE Access, vol. 10, pp. 22345–22358, 2022.

[17] Y. Chen, X. Liu, and Z. Wang, “Wearable computing for emergency healthcare applications,” IEEE Sensors Journal, vol. 23, no. 5, pp. 4321–4330, 2023.

[18] P. Singh and M. Verma, “Secure digital health identity systems for emergency care,” IEEE Access, vol. 12, pp. 11234–11246, 2024.