Secure Remote Patient Monitoring System Using Blockchain and Elliptic Curve Cryptography

Biswaranjan Dash

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Secure Remote Patient Monitoring System Using Blockchain and Elliptic Curve Cryptography

Progress Report - October 2025

submitted in partial fulfillment

of the requirements for the degree of

Bachelor of Technology

in

Computer Science and Engineering

by

Biswaranjan Dash

(Roll Number: 122cs0557)

based on research carried out

under the supervision of

Prof. Sujata Mohanty

October, 2025

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Prof. Sujata Mohanty
Professor

October 21, 2025

Supervisors' Certificate

This is to certify that the work presented in the progress report entitled *Secure Remote Patient Monitoring System Using Blockchain and Elliptic Curve Cryptography* submitted by *Biswaranjan Dash*, Roll Number 122cs0557, is a record of original research carried out by him under our supervision and guidance in partial fulfillment of the requirements of the degree of *Bachelor of Technology* in *Computer Science and Engineering* . Neither this project report nor any part of it has been submitted earlier for any degree or diploma to any institute or university in India or abroad.

_____
Sujata Mohanty
Professor

Dedication

I dedicate this project to my cherished family and friends, whose steadfast love and unwavering support have been my guiding force throughout this B.Tech journey. Your encouragement, understanding and patience have fueled my determination, and your belief in me has been my greatest motivation.

To my family, for being my constant pillars of strength, for the sacrifices made, and for the boundless love that knows no bounds, I owe you the world. Thank you also for providing me with a computer early in my life, igniting my passion for technology.

To my friends, the invaluable gems in my life, for the laughter, the late night discussions, and for standing by me in both the highs and lows. Thank you for being the uplifting force that makes this journey memorable.

This project stands as a testament to the collective efforts and sacrifices of my family and friends. Your love has been the driving force behind every achievement, and I am grateful beyond words for the privilege of having you all in my life.

With heartfelt gratitude,
Biswaranjan Dash

Declaration of Originality

I, *Biswaranjan Dash*, Roll Number *122cs0557* hereby declare that this project report entitled *Secure Remote Patient Monitoring System Using Blockchain and Elliptic Curve Cryptography* presents my original work carried out as a student of NIT Rourkela and, to the best of my knowledge, contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of NIT Rourkela or any other institution. Any contribution made to this research by others, with whom I have worked at NIT Rourkela or elsewhere, is explicitly acknowledged in the thesis. Works of other authors cited in this thesis have been duly acknowledged under the sections ‘‘Reference’’ or ‘‘Bibliography’’. I have also submitted my original research records to the scrutiny committee for evaluation of my thesis.

I am fully aware that in case of any non-compliance detected in future, the Senate of NIT Rourkela may withdraw the degree awarded to me on the basis of the present thesis.

Oct 21, 2025
NIT Rourkela

Biswaranjan Dash

Acknowledgement

I would like to express my sincere gratitude to all those who have supported me in my ongoing efforts on this project. I am particularly indebted to our project supervisor for the final year, ***Professor Sujata Mohanty***, whose invaluable suggestions and unwavering support have played a pivotal role in guiding me through the process of conducting this research. His encouragement has continually inspired me to work diligently and push boundaries.

In addition, I wish to extend my heartfelt appreciation to the dedicated personnel of the ***Department of Computer Science and Engineering*** for granting me access to the essential equipment and materials necessary for this project.

Lastly, I would like to convey my profound gratitude to my parents and friends for their continuous encouragement throughout my academic journey and during this project. I am also deeply thankful to the **National Institute of Technology, Rourkela** for their backing and for awarding me the opportunity to undertake this project, along with the provision of essential facilities.

October 21, 2025 *Biswaranjan Dash*
NIT Rourkela Roll Number: 122CS0557

Abstract

This project proposes a secure remote patient monitoring system design and its subsequent implementation employing a lightweight blockchain-enabled authentication approach. The described system keeps on recording patients' health parameters like body temperature, oxygen saturation, and so on, through biomedical sensors connected to an Arduino UNO and an ESP Wi-Fi module. After the data collection, it is stored in a cloud platform (ThingSpeak) securely for the purpose of real-time storage and analysis. The use of a blockchain-based authentication scheme along with the use of Elliptic Curve Cryptography (ECC) is a method that guarantees the fact that only the devices that have been verified and hospital servers have the capability to access or transmit sensitive medical data. To this end, the integrity of the data, its confidentiality, and the privacy of the user are improved while simultaneously, the computational costs are kept low which is very important for resource-constrained IoT devices. After that the hospital server fetches the legitimate data from the cloud, thus the doctors will be able to monitor the patients remotely and make the necessary clinical decisions timely.

The proposed system demonstrates an efficient, scalable, and secure solution for healthcare IoT applications, effectively preventing common network attacks such as replay, impersonation, and man-in-the-middle attacks.

Keywords: Remote Patient Monitoring, Internet of Medical Things (IoMT), Blockchain, Lightweight Authentication, Elliptic Curve Cryptography (ECC), Secure Healthcare System.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview

Remote patient monitoring (RPM) is a direct consequence of the increasing usage of technology in healthcare. It is the most effective means for a patient's health to be tracked without a need for frequent hospital visits. The doctors by using IoT (Internet of Things) devices such as sensors and microcontrollers are able to gather live data such as temperature, oxygen levels or heart rate of the patients who are at home or in far-off places. This is extremely valuable because it leads to the prevention of health issues as well as the provision of medical support on time by doctors.

On the other hand, when medical data is sent through the internet, it becomes necessary to guarantee security and privacy of such data. If there is any kind of unauthorized access or data leakage, the result would be the risk of the patient's safety. Thus, the security subsystem in the system should be not only strong in terms of protection but also be efficient enough to work on small, low-power IoT devices.

Our work is to introduce a secure remote patient monitoring system implementation that would support safety and efficiency of the communication process through the use of blockchain technology and Elliptic Curve Cryptography (ECC). The Arduino UNO and the ESP Wi-Fi module that are connected with sensors make up the first part of the system, which is used to collect patient data that is then uploaded to a cloud platform (ThingSpeak). After that, the cloud sends the data to the hospital server, which is the doctor's place, and they are able to remotely monitor the patient's condition through

the data received. The usage of blockchain guarantees that only authorized users and devices have access to the data, whereas ECC is the reason for quick and simple data encryption in an IoT environment.

1.2 Objectives

The primary goals envisaged through this undertaking are:

- To conceive and implement a remote patient monitoring system that gathers real-time health information through IoT sensors.
- To maintain data security and confidentiality by implementing a blockchain-enabled authentication method and using light cryptography (ECC).
- To establish good communication pathways between patient equipment, cloud and hospital server.
- To offer doctors an opportunity to remotely access patient medical records via a safe and user-friendly system.
- To trim down the computational load thereby making it possible for the system to function efficiently on hardware capable of limited resources such as Arduino and ESP modules.

Chapter 2

Literature Review

2.1 Overview

Remote Patient Monitoring (RPM) is the vital element of the Internet of Medical Things (IoMT), a concept in which intelligent devices keep track of a patient's health continuously and the updated information is sent to the respective doctors or hospitals [2]. Different researchers throughout the years have come up with a variety of methods to ensure that such systems are not only secure but also dependable.

The first generation of systems were mainly concerned with gathering and transferring patients' data done through Wi-Fi or Bluetooth while the aspects of privacy and security were only partially taken care of [5]. Consequently, healthcare data being highly sensitive even the slightest negligence of it would lead to a situation where data leakage, impersonation, or unauthorized access would occur.

2.2 Review of Previous Works

2.2.1 Initial IoT-based Healthcare Systems

Ancestor systems were implemented on basic IoT schematics consisting of sensors and cloud platforms (example: ThingSpeak or Blynk) [5]. These frameworks were effective in monitoring vital signs; however, due to the absence of strict authentication and encryption measures, they were susceptible to hacking.

2.2.2 Password-Based Authentication Schemes

A number of later projects incorporated password-protected authentication to secure communications [8]. That said, the security provided by such methods was very weak because passwords can be easily guessed or stolen, thus leading to scenarios where the perpetrator can impersonate the victim or record/replay the communication.

2.2.3 Public Key Cryptography (RSA) Based Approaches

The next step was adoption heavy cryptographic schemes like RSA or alike to secure patient data [1]. The drawback of this approach was that these strong security measures demanded high computational power conflicting with the low-power nature of devices like Arduino or ESP modules.

2.2.4 Lightweight Cryptography & ECC-Based Methods

Researcher solved this problem by switching to Elliptic Curve Cryptography (ECC), an algorithm achieving the same security level as RSA but with smaller key sizes and faster processing speed [7]. Presently, ECC is almost the standard for IoT applications, including healthcare.

2.2.5 Blockchain-Enabled Systems

Recent studies present medical data management with the help of blockchain technology [3]. Blockchain functions as an incorruptible ledger, keeping track of data transactions and making them transparent, thus, trustworthy, and secure against hacker attacks. When combined with ECC, blockchain delivers a decentralized and lightweight authentication solution that suits real-time medical monitoring requirements [4].

2.3 Research Gap

The analyzed papers highlight that while the developed platforms facilitate data gathering and sharing, security is still an open issue and rarely is the trade-off between security and efficiency addressed. Some works call for significant computational

resources, others are vulnerable to certain types of attacks. The key challenges identified include:

- Need to operate under constrained energy of IoT devices,
- Implementation of lightweight cryptographic techniques to ensure security,
- Use of blockchain technology not only for security purposes but also to facilitate user authentication, and
- Being able to guarantee privacy and integrity of data during a continuous patient monitoring scenario.

Table 2.1 presents a comparative analysis of various authentication schemes proposed for IoT-based healthcare systems over recent years. The table highlights the progression from basic password-based methods to more sophisticated approaches incorporating ECC and blockchain technology, culminating in the present work which addresses the limitations of previous approaches.

Table 2.1: Comparative Analysis of Authentication Schemes in IoT-based Healthcare Systems

Year	**Technique Used**	**Focus Area**	**Limitations**
2018	Three-factor authentication using passwords and biometrics	Wireless Sensor Networks in healthcare	High computation time; not suitable for low-power devices
2019	Lightweight ECC-based user authentication	Wearable IoT devices	Lacked decentralized data protection
2020	Password-based DRM authentication	IoT Applications	Weak against replay and impersonation attacks
2021	Three-factor IoT authentication using ECC	Healthcare Systems	Secure but lacked blockchain integration
2022	Secure three-factor authentication for IoT	IoT-based healthcare	Needed more scalability and efficiency
2023	Hyperelliptic curve-based IoD authentication	Internet of Drones	Good security but complex math operations
2024	PUF-based lightweight authentication	Internet of Drones	Focused on drones, not healthcare
Present Work (2025)	**Blockchain + ECC-based lightweight authentication**	**Remote Patient Monitoring System**	**Addresses past issues; provides both efficiency and strong security**

Chapter 3

Proposed Methodology and System Design

3.1 Motivation

Nowadays, healthcare systems are overwhelmed with patients who have to be monitored continuously because of their chronic conditions, postoperative situations, or remote living. Hospitals equipped with conventional monitoring devices are not only time-consuming and costly but also impractical for long-term monitoring. Given the developments in IoT and cloud computing, Remote Patient Monitoring (RPM) offers the possibility of real-time health data acquisition from patients and direct data transfer to doctors or hospitals. On the other hand, the biggest issue that security and privacy concerns regarding the medical data being transmitted.

Most of the present IoT-based solutions have either password-based or RSA-based authentication mechanisms, which can be weak or computationally expensive for small devices such as Arduino or ESP modules. Hence, this project is arisen from the demand for a healthcare data privacy ensuring, third-party access denial preventing, and patient authentication process confidential and secure yet lightweight, resistant to the security threats, and reliable in performance problem.

Therefore, the solution is using the:

- Elliptic Curve Cryptography (ECC) for light encryption,
- Record management via blockchain technology, which is very secure since it is tamper-proof, and

- A cloud-based system to facilitate easy access in real time by the doctors.

3.2 System Architecture

Proposed system is a combination of IoT devices, cloud storages, and security based on blockchain. It can be divided into four primary layers:

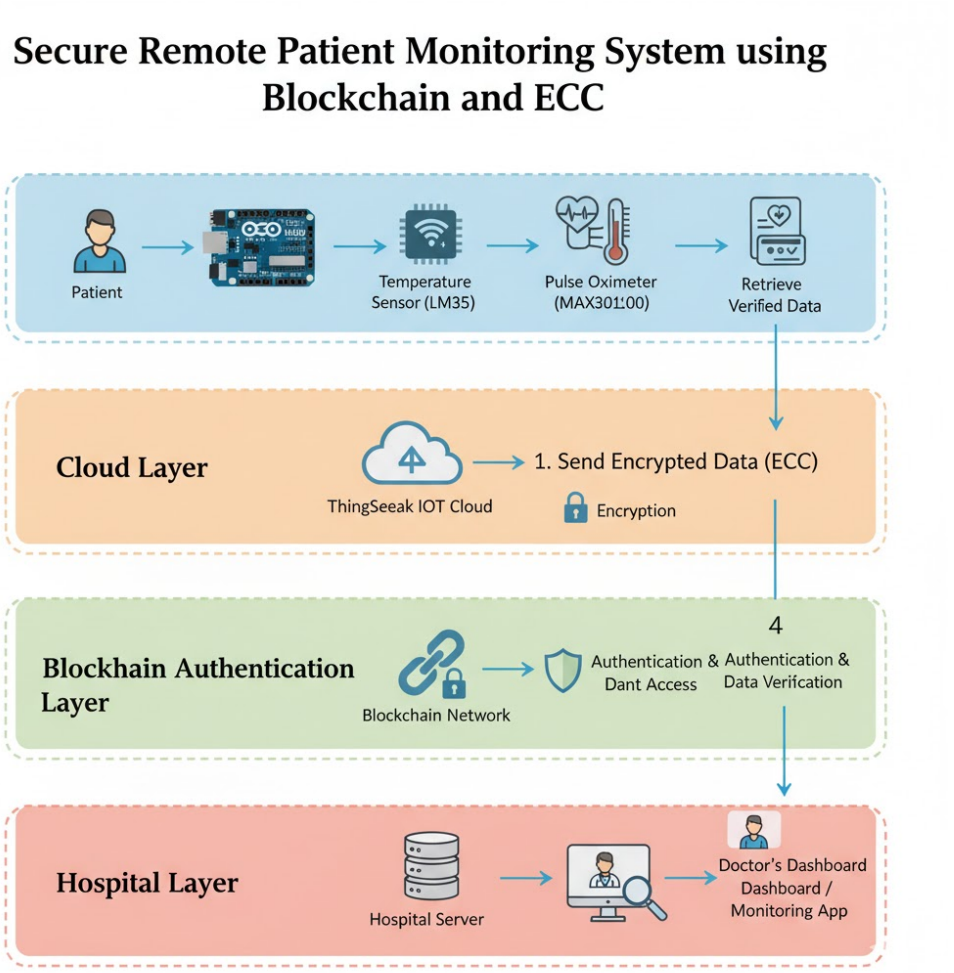

Figure 3.1: System Architecture of Remote Patient Monitoring

3.2.1 Patient Layer (Device Layer)

- Temperature Sensor (LM35) and Pulse Oximeter (MAX30100) are examples of the sensors that might be included in this system.
- These sensors are linked to an Arduino UNO that gathers real-time health data of the patient.
- The encrypted data is sent to the cloud by an ESP8266 Wi-Fi module.

3.2.2 Network / Cloud Layer

- The ThingSpeak IoT Cloud Platform is put to use for storing and receiving data coming from a patient.
- The information is in an encrypted format, which uses the session key created via ECC.

  Before accepting the data, the blockchain verifies the sender (patient's device) to be genuine.

3.2.3 Blockchain Authentication Layer

- Every patient device enrolled is given a digital smart card that contains authentication credentials.
- These smartcards are written in the blockchain ledger, which makes them very secure and cannot be altered easily.
- During each connection, the mutual authentication process occurs between:
  - Patient device,
  - Cloud server, and
  - Hospital server.
- Patient device,

- Cloud server, and
- Hospital server.
- None of the devices will be given their connecting request if the verification is not successful.

3.2.4 Hospital Server and Doctor Layer

- The Hospital Server through a secure dashboard validates the information arriving from the blockchain.
- Doctors access the patient's condition in real-time through the server and intervene if they find any abnormality.

3.3 Working Flow

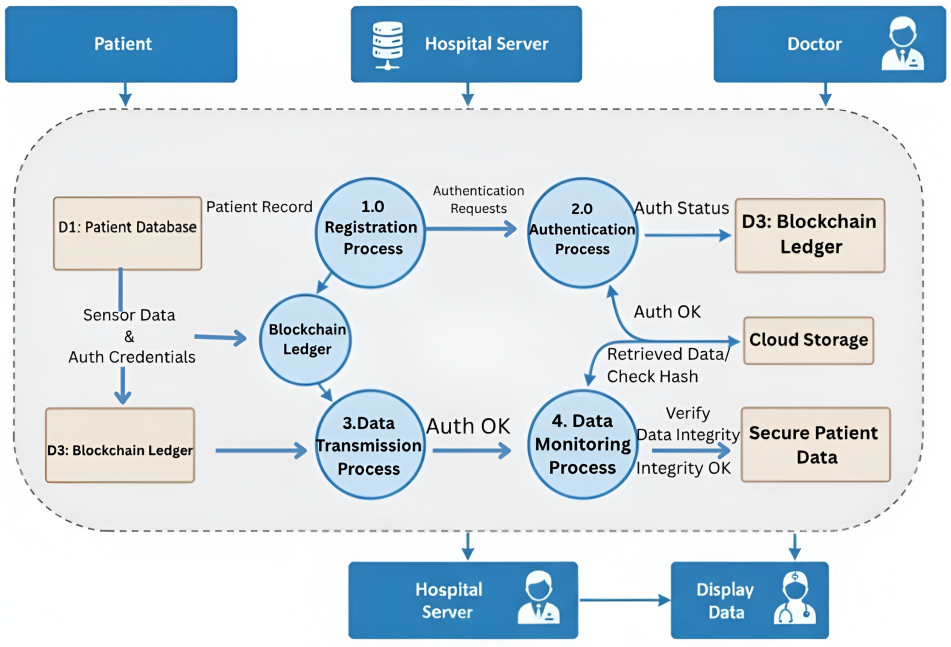

Figure 3.2: System Workflow: Registration, Authentication, Data Transmission, and Monitoring

3.3.1 Patient Registration

The patient's device is registered with the hospital server. A smart card with cryptographic parameters is generated and saved on the blockchain.

3.3.2 Data Collection

The sensors take the vital signs of the patient (temperature, SpO_2) and forward the data to the Arduino.

3.3.3 Data Encryption

ECC is implemented by Arduino to encode the data with the session key (SK).

3.3.4 Data Transmission

Data in encrypted form is being transferred to the ThingSpeak Cloud through Wi-Fi.

3.3.5 Authentication and Verification

A blockchain performs a check between the device credentials and the records. If the verification is positive, the data is allowed.

3.3.6 Data Access by Doctor

The data, after verification, is pulled out by the hospital server, and the doctor is able to follow up with the patient from a distance.

3.4 Algorithm Explanation

The presented scheme is a simplified, lightweight, blockchain-enabled authentication version from the Internet of Drones paper [6], that was the basis for the system.

It has three steps:

3.4.1 Phase 1: Registration

- The hospital server sets up elliptic curve parameters.
- Patient device forwards identity and password to the server.
- Server prepares a smart card and puts its hash on the blockchain.
- The patient gets the smart card that encloses public parameters.

3.4.2 Phase 2: Authentication

- Smart card is used by the patient to log in.
- Nonces are generated on both sides, ECC is performed to get the session key (SK) operation.
- Ethereum smart contracts validate identities and control impersonation.
- If the operation succeeds, the parties get a secure channel.

3.4.3 Phase 3: Data Transmission

- Patient data is encrypted by the Arduino with the session key.
- Data are securely transmitted to the cloud.
- Hospital server gets the data decrypted for doctors' viewing.

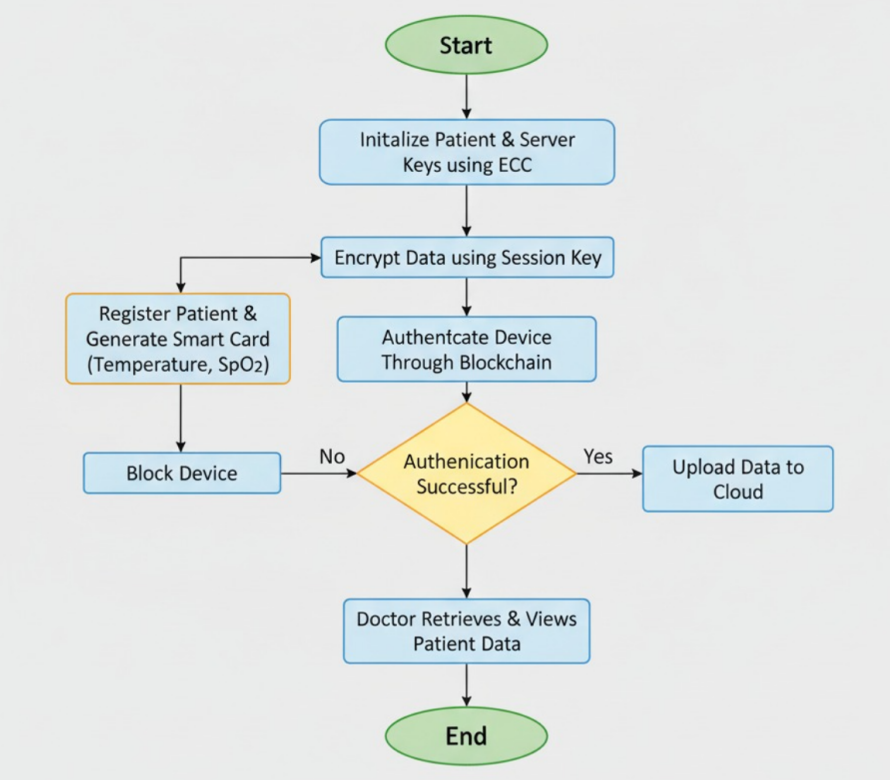

Figure 3.3: Algorithm Flow Diagram

3.5 Mathematical Overview of ECC (Simplified)

The equation for the elliptic curve cryptography (ECC) curve is:

$$y^2 = x^3 + ax + b \pmod{p}$$

Every party has:

- A private key (d)
- A public key (Q = d ×G), where G is a point on the curve.
- A private key (d)
- A public key (Q = d ×G), where G is a point on the curve.

The session key (SK) is generated by:

$$SK = (d_A \times Q_B) = (d_B \times Q_A)$$

which allows both parties to have the same shared key without letting other parties know it.

This is the key that is utilized for encrypting the medical data before the data is sent to the cloud.

Table 3.1: System Stages, Components, and Purpose

Stage	**Component Used**	**Purpose**
Data Collection	Temperature & SpO_2 Sensors, Arduino UNO	Capture real-time health data
Transmission	ESP8266 Wi-Fi Module	Send data to cloud securely
Authentication	Blockchain + ECC	Verify device and user identity
Data Storage	ThingSpeak Cloud	Store encrypted patient data
Data Access	Hospital Server, Doctor Interface	View and monitor health status

Chapter 4

Conclusion and Future Work

4.1 Conclusion

The objective of the present work was to devise a radically secure and a very light in terms of computing remote patient monitoring system that safeguards the data collected through blockchain technology and employing Elliptic Curve Cryptography (ECC). The system topology suggests that any patient health data in real-time, e.g. body temperature and oxygen saturation, IoT-based sensors can collect these details. After that, the data will undergo secure transmission to the cloud for medical review. With the help of blockchain and ECC that are strategically combined, the layout accomplishes a successful equilibrium among safety, effectiveness, and scalability aspects thus it solves the problems to a large extent. These include issues concerning the healthcare IoT sector in general: data tampering, unauthorized access, and privacy breaches. Mutual authentication, data confidentiality, and user anonymity are some of the features implemented deepening on this system, therefore this makes the proposed framework highly compatible with med-tech integration. At the moment, this work is mainly focused on the conceptualization part including the design of the system, the drafting of the algorithm and composition of the architecture which has been well demonstrated by this study as an effective method for securely storing medical data while the overhead is maximum kept at a minimum.

4.2 Future Scope

At a later date, an actual working version of the system envisaged in this proposal will be possible to achieve in this project. The subsequent axe will be:

- Hardware Implementation: Construction of a patient node to record and report data using an Arduino UNO, ESP8266 Wi-Fi module, LM35 temperature sensor, and MAX30100 pulse oximeter.
- Software Development: Executing the authentication algorithm via ECC to achieve encryption and blockchain employed for decentralized confirmation of smartcards and device identification.
- Cloud Integration: Encrypting data uploaded to the ThingSpeak cloud platform facilitating the on-the-fly visualization by medical personnel.
- Performance Testing: Checking parameters like calculation time, network delay, data integrity, and energy consumption in a demo environment consisting of resource-limited hardware to evaluate the prototype.
- Scalability and Deployment: Amplifying the concept so it would cater the medical needs of several patients and doctors at a time, and maybe, merge mHealth (Mobile health) applications or hospital management systems functionality.

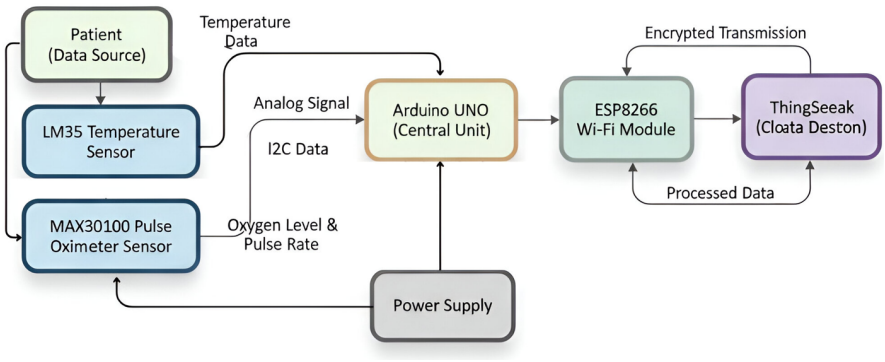

Figure 4.1: Hardware Architecture Diagram

References

[1] Masanobu Katagi and Shiho Moriai. Lightweight cryptography for iot: A comparative analysis. *Sony Corporation*, pages 1–17, 2008.

[2] Pardeep Kumar, Rajesh Kumar, Gautam Srivastava, Gulshan Gupta, Rohit Tripathi, Thippa Reddy Gadekallu, and Naixue Xiong. Internet of medical things (iomt)-based smart healthcare system: Trends and progress. *Computational Intelligence and Neuroscience*, 2021:1–28, 2021.

[3] Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *GigaScience*, 6(10):1–13, 2017.

[4] Vishal Sharma, Ilsun You, and Rajesh Kumar. Blockchain-based authentication and authorization framework for remote patient monitoring in iomt. *IEEE Access*, 8:113659–113675, 2020.

[5] Mahi Singh, Priyanka Sharma, and Jaspreet Kaur. Iot based patient health monitoring system using thingspeak. In *International Conference on Intelligent Computing and Control Systems (ICICCS)*, pages 614–619. IEEE, 2019.

[6] A Vamsi Vardhan, Sujata Mohanty, and Manabhanjan Pradhan. A lightweight blockchain-enabled authentication scheme for securing internet of drones devices. In *IEEE International Conference on Smart Power Control and Renewable Energy (ICSPCRE)*, NIT Rourkela, India, July 2024. IEEE. Virtual mode, 19-21 July 2024.

[7] Ronald Watro, Derrick Kong, Sue-fen Cuti, Charles Gardiner, Charles Lynn, and Peter Kruus. Elliptic curve cryptography for wireless sensor networks. *IEEE Wireless Communications*, 11(1):60–67, 2004.

[8] Thomas Wu and Michael Malkin. Security vulnerabilities in password authentication protocols. *IEEE Security & Privacy*, 3(4):56–61, 2005.