“Elephant - Care”

Wearable IOT – Enabled belt for Elephant Protection & Emergency Identification

TMP-24-25J-012

Project Final Report

Perera B.A.D.K.S

IT21202254

B.Sc. (Hons) Degree in Information Technology

Department of Information Technology

Sri Lanka Institute of Information Technology

SRI LANKA

August 2025

“Elephant - Care”
Biometric Data Analysis & Real Time Alerting System

TMP-24-25J-012

Project Final Report

Perera B.A.D.K.S

IT21202254

B.Sc. (Hons) Degree in Information Technology

Department of Information Technology

Sri Lanka Institute of Information Technology

SRI LANKA

April 2025

Declaration

I declare that this is my own work and this dissertation1 does not incorporate without acknowledgment any material previously submitted for a degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgment is made in the text. Also, I hereby grant to Sri Lanka Institute of Information Technology, the nonexclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Name	**Student Id**	**Signature**
Perera B.A.D.K. S	IT21202254	

The supervisor/s should certify the proposal report with the following declaration.

The above candidates are carrying out research for the undergraduate Dissertation under my Supervisor

05 – 04 - 2025

…………………………………. ……………………..

Signature of the supervisor Date

Abstract

The rise of human-elephant conflict in regions where their habitats overlap with human settlements necessitates advanced technological interventions. This research proposes the development of a Wearable IoT-Enabled Belt designed to protect elephants by monitoring their biometric data and issuing real-time alerts. The system captures critical biometric indicators such as blood pressure, blood oxygen levels, body temperature, geometry data, and GPS coordinates. These data are routed through an API Gateway that ensures their authenticity and correct format before storage in a Time-Series Database. Post-storage, the data undergoes filtering to eliminate duplicates and noise, thereby enhancing its quality for subsequent analysis. Advanced machine learning models are employed to detect anomalies in real-time, such as unusual movement patterns that may indicate distress or potential poaching activity. These models continuously learn and improve from the collected data, ensuring robust anomaly detection. And predictive analytics is utilized to forecast potential threats by analyzing historical data and identifying patterns. This dual approach of real-time detection and predictive forecasting is aimed at enhancing the protection of elephants and mitigating threats proactively. The system's primary objective is to detect unusual patterns using biometric data to issue real-time alerts, while a secondary objective focuses on improving data quality for analysis by removing noise and duplicates. This research contributes to wildlife conservation by integrating IoT, machine learning, and predictive analytics into a cohesive system for elephant protection.

Key words: *- Human-Elephant, Biometric Data, Time-Series Database, Predictive Analytics, Forecasting*

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my supervisor Prof. Anuradha Jayakody for his constant guidance and support, which always helped me to complete my graduate research. Apart from my supervisor, I also extend my sincere thanks to the co-supervisor of this research project, Mrs. Uthpala Samarakoon, who was willing to help whenever needed. As this research study is a blend of technology and animal health, the guidance and support of not only technology experts but also veterinarians were required. Dr. Tharaka immense support throughout the project to bridge the knowledge gap is greatly appreciated. Last but not least, I express my gratitude to my teammates, family, friends, and one and all who have directly or indirectly extended their support to me throughout this project.

Table of Contents

List of figures

List of tables

1.0 INTRODUCTION

The fast intrusion of human activity into nature has brought humans into direct contact with wildlife more and more, resulting in increased human encounters with large wild animals like elephants. Elephants are especially susceptible because of their size, migratory nature, and overlapping of habitats with agricultural and urban belts. Such encounters result in large-scale destruction of property and lives of both elephants and human beings in the form of crop loss, harm, and fatalities on either side. [1] There is more need than ever before for efficient, new, and non-invasive methods for reducing human-elephant conflict (HEC).As human habitation, deforestation, and development projects continue to fragment elephant habitats, the animals must cross human- dominated landscapes in pursuit of food, water, and traditional migration routes. In the process, they increasingly come into conflict with farmers and communities, resulting in economic loss and escalating tensions. In a bid to address this pressing problem, governments, conservationists, and researchers are turning to cutting-edge solutions like early warning systems, elephant corridors, and application of technologies such as GPS tracking and artificial intelligence in forecasting elephant migration routes. Education and community involvement are also crucial in mitigating HEC, enabling natives to employ elephant-friendly practices and promote coexistence. Conservation approaches that reconcile ecological conservation and human development sustainably are needed to minimize such conflicts and ensure elephant populations ‘long-term viability in the wild

Human-elephant conflict (HEC) primarily arises from loss and fragmentation of habitat and migratory pathways and resource competition that dive elephants into human settlements. [2] Traditional mitigation methods such as crating barriers, translocating elephants, or culling have been questioned on the grounds that these are ineffective, inhumane, or unsustainable. [3] Conservationists and researchers are increasingly advocating the use of technologies to offer more sustainable and humane solutions instead. Innovations such ae real time tracking, predictive analytics, and alarm systems designed and implemented by local communities are being found to effectively reduce conflict, protect human lives and livelihoods and ensure the long-term survival of elephants.

The Internet of Things (IOT) revolutionize wildlife conservation with smart and real-time wildlife monitoring. IOT – enabled devices like GPS collars and biometric sensors are increasingly used to track movement patterns, monitors, and anticipate and prevent wildlife crimes related to wildlife hunting and trading. [4] wearable devices are unobtrusive and provide uninterrupted flow of data about the whereabouts, behavior, and physical state of an animal. [5] Such data are very important to identify stress, disease, or threat early and act in time. Conservation by using IoT becomes more efficient, humane, and preventive and ends up protecting endangered species like elephants in an improved manner.

Building upon IoT principles and real-time monitoring, this research introduces a Wearable IoT-Enabled Belt tailored for elephants. The device is designed to collect and transmit vital biometric data, including blood pressure, oxygen levels, body temperature, geometric measurements, and GPS coordinates. Continuous monitoring of these parameters allows for the early detection of abnormal patterns or health anomalies, which may indicate distress, illness, or potential threats like poaching. This proactive approach enhances conservation efforts by enabling timely interventions, improving elephant welfare, and supporting coexistence strategies through accurate, data-driven insights into elephant behavior and environmental interactions.

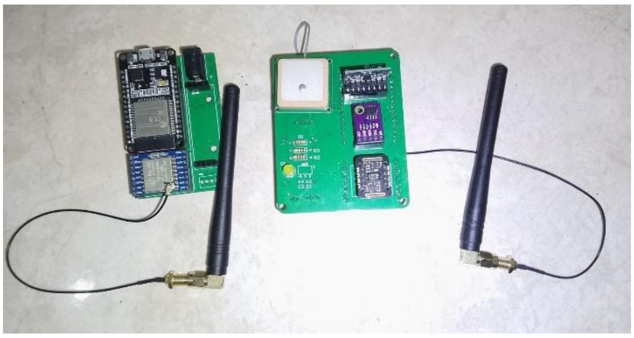


Figure 1: IOT Device (Elephant Care)

The Elephant-Care system uses dual methodology to monitor and be alerted to emergency conditions in elephants by using Wearable IoT-Enabled Belt and Biometric Data Analysis and Real-Time Alerting System. In a specially designed comfort and durability-supported belt, an array of sensors is mounted to monitor critical biometric and environmental parameters like heart rate, blood oxygenation level, body temperature, movement, and GPS location. Non-invasive MAX30102, LM75, and MPU6050 sensors are used to monitor physiological stress and abnormalities in movement in real time. ESP32 microcontroller is used to collect and transmit sensor data wirelessly with its dual core supporting fault-tolerant and power-efficient performance outdoors. The information is transmitted wirelessly to a centralized system to be filtered and analyzed and alerted in real time so early intervention is triggered in distress or harm like poaching. The system overall is designed to operate imperceptibly under poor conditions with little interference with the natural habitat of the elephant

Biometric data is transmitted through an API Gateway, which verifies and reshapes the data into the correct schema and then directs it to a Time-Series Database. Designed to support highfrequency IoT data, the database optimizes retrieval and storage and allows processing to support real-time analytics. The system supports ongoing monitoring through high-performance and integrity in the data and allows researchers and conservationists to spot patterns, outliers, or risks in the behavior and health of elephants in real-time. [6]

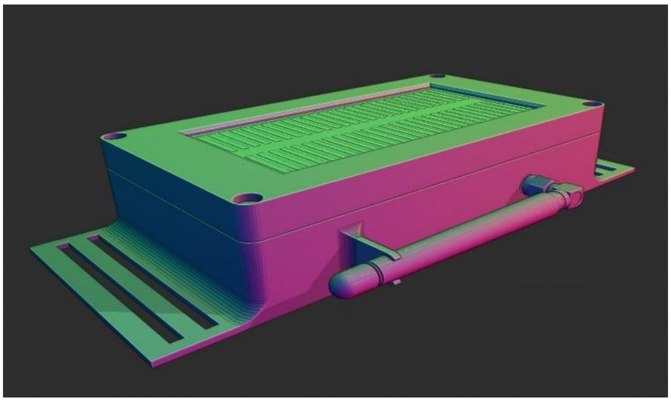


Figure 2: Device Encloser

The stored data is filtered to eliminate duplicates and noise, significantly improving its quality to make it suitable for efficient analysis. It is necessary to filter since raw data can lead to false positives when performing anomaly detection and creating unnecessary alerts and making the system unreliable. [7] The system is very accurate when identifying real threats or abnormalities in the behavior and health condition of elephants once it handles only clean and significant data, hence improving monitoring efficiency overall.

The cleaned data is then processed by advanced machine learning algorithms to detect the anomalies in real time. The algorithms are designed to capture irregular patterns in the movement or biological data of the elephant and signal distress, injury, or attempts to poach them. As the algorithms continue to learn from the data, they become increasingly more efficient and proficient in filtering out typical erratic behavior patterns as the years go by. [8]

In addition to real-time monitoring, the system also employs predictive analytics to forecast potential threats. By analyzing historical data and identifying patterns, the system can predict when and where conflicts are most likely to occur, allowing for proactive interventions. [9] This dual approach of real-time detection and predictive forecasting is intended to provide a comprehensive solution to elephant protection, addressing both immediate threats and long-term conservation challenges.

The integration of real-time alerting and predictive analytics is a key innovation of this research. Real-time alerting ensures that any immediate threats to the elephant, such as poaching attempts or health crises, are quickly identified and communicated to relevant authorities. This rapid response capability is crucial in preventing harm to the elephant and allowing for timely interventions. [10]

Predictive analytics, on the other hand, enables the system to anticipate future threats based on past data. By identifying patterns in the elephant's movement and health data, the system can forecast potential risks, such as areas where the elephant is likely to encounter human activity or where environmental conditions may pose a danger. This predictive capability allows conservationists to take proactive measures, such as adjusting the elephant's route or increasing monitoring in high-risk areas. [11]

The Wearable IoT-Enabled Belt for Elephant Protection and Emergency Identification represents a significant advancement in the use of technology for wildlife conservation. By combining real-time biometric monitoring, advanced machine learning for anomaly detection, and predictive analytics, this system provides a robust and comprehensive solution to the challenges of human-elephant conflict. As such, it holds the potential to greatly enhance the protection of elephants, reduce the incidence of conflict with humans, and contribute to the long-term sustainability of elephant populations in the wild.

1.1 Background & Literature survey

1.1.1 Background

Development in biometric technology has transformed security solutions in today's world by offering very accurate and trustworthy identification solutions. Unlike other conventional security solutions, biometric information facial attributes, fingerprints, and iris scans are exclusive to a person, thus hard to copy or fake. In the last decade, the implementation of biometrics in security solutions has gained considerable momentum in domains with strict authentication requirements such as banks, law enforcement agencies, and border security. Not only does the solution improve security levels, but also makes access control more effective, decreases cases of identification fraud, and enhances user convenience, making it an integral component of security solutions today.

While biometric systems greatly improved the level of security, advanced cyber-attacks unveiled underlying vulnerabilities. Traditional systems are designed to identify correctly rather than to respond in real-time to emerging risks. The vulnerability becomes particularly worrisome in high-security environments where biometric data is being continuously scrutinized and must be shielded against unauthorized access, tampering, or penetration. As biometric data cannot be replicated and is vulnerable by nature, its compromise can become long-term impacting. Therefore, it is imperative to supplement the biometric systems with strong security technologies that possess the ability to identify attacks on the spot and prevent and respond accordingly in real-time.

Although enhancing security by way of proper identification, biometric systems are susceptible to sophisticated cyber-attacks. Traditional biometric systems are used primarily to authenticate and identify people with poor nimbleness to discover and counter attacks in real-time. It is very significant in high-security setups with ongoing capture and processing of biometric data. Such data like fingerprints, facial recognition or iris scan are irreversible by nature and are susceptible to capture and transmission to the system. Their susceptibility will yield long-term and far-reaching effects if compromised compared to passwords that may be rewritten. The risk of unauthorized access, data tampering or system infiltration calls for the hardening of the protection layers with advanced cybersecurity solutions with real-time threat detection, smart risk evaluation, and instant response. Incorporation of capabilities like behavioral analytics, encryption, and artificial intelligence-enabled monitoring will ensure that biometric security solutions are adaptive and resilient to emergent attacks.

1.1.2 Literature survey

The literature on biometric security systems highlights several key trends and challenges that have shaped the development of current technologies. Zhang, Wu, and Xu (2021) [1] provide a comprehensive survey of intrusion detection systems in cloud computing, emphasizing the increasing importance of dynamic policy management to counter evolving threats. Their work underscores the limitations of static policies, which are unable to adapt to new types of attacks that arise as technology advances.

Ahmed et al. (2020) [2] explores the integration of machine learning with Software-Defined Networking (SDN) for real-time intrusion detection. Their research demonstrates the potential of automated systems to enhance security by reducing the time required to respond to threats. However, they also point out that many existing systems fail to integrate effectively with SDN controllers, leading to inefficiencies in network management and security enforcement.

Yousaf, Ali, and Jadoon (2021) [3] further investigate the role of SDN in network security, focusing on the challenges of dynamic policy management in complex network environments. Their findings highlight the need for systems that can adapt to changing conditions in real-time, a requirement that is increasingly critical as networks become more complex and distributed.

Sharma (2020) [4] examines automated security policy enforcement in Software-Defined Networks, identifying gaps in the comprehensiveness and adaptability of existing frameworks. His research highlights the importance of continuous policy updates and user guidance in maintaining the effectiveness of security systems over time.

Finally, Wang, Zhang, and Wang (2022) [5] discuss the integration of SDN and machine learning in intelligent network security systems. Their work emphasizes the need for comprehensive solutions that can manage and analyze large volumes of data in real-time, providing a foundation for the development of more advanced biometric security systems.

The proposed "Biometric Data Analysis & Real-Time Alerting System" seeks to address the gaps identified in these studies by offering a solution that combines dynamic policy management, real-time threat detection, and comprehensive user guidance. This system not only enhances the security of biometric data but also ensures that security policies are continuously updated to reflect the latest threats and technological advancements.

1.2 Research Gap

The rapid advancement in security technologies makes it imperative to identify and correct existing system vulnerabilities. Even with the progress made so far, installed biometric security systems are far wanting in performance when it comes to real-time responsiveness issues, accurate data analysis, and predictive detection of threats. Table 1 brings out some major research gaps emphasizing the necessity to come up with an acute and reactive solution. The suggested "Biometric Data Analysis & Real-Time Alerting System" corrects these deficiencies with added data processing and real-time warning capabilities. It allows for quicker detection of threats and an improved system of defense. In eliminating these deficiencies, the suggested system enhances the implementation of more efficient, effective, and adaptive security systems applicable to the dynamic nature of modern environments.

Existing systems often suffer from static policy management, meaning that once policies are established, they are rarely updated or adapted to evolving threats. According to Zhang, Wu, and Xu (2021) [12], many current intrusion detection systems rely heavily on pre-defined rules and policies that do not change in real-time, leading to vulnerabilities when new threats emerge. This limitation is also observed in studies by Ahmed et al. (2020) [13], who noted that static policy frameworks can become outdated quickly in dynamic environments, thereby failing to protect against novel attacks. The proposed system, however, addresses this gap by implementing dynamic policy management that continuously evolves based on real-time biometric data analysis. This adaptive approach ensures that the security policies remain effective even as new threats are identified.

Table 1 : Research gap for my system

Research References	**Static Policy Management**	**Limited Automation in Security Policy Enforcement**	**Inadequate Real-Time Threat Response**	**Insufficient Integration with SDN Controllers**	**Lack of Comprehensive Policy Management**	**User Guidance and Policy Updates**
A [12]	X	X	X	X	X	✓
B [13]	X	X	X	✓	✓	X
C [14]	✓	X	X	X	X	✓
D [15]	X	X	X	X	X	X
E [16]	✓	✓	✓	✓	✓	✓
Proposed Research System	✓	✓	✓	✓	✓	✓

Automation in security policy enforcement is another significant gap in current systems. As highlighted in the works of Yousaf, Ali, and Jadoon (2021) [14], many existing frameworks do not fully automate the enforcement of security policies, which results in delayed responses to security breaches. The absence of automation limits the effectiveness of these systems, particularly in high-speed environments where manual intervention is too slow to prevent damage. The proposed system addresses this issue by incorporating machine learning algorithms that automatically enforce and adjust security policies based on real-time biometric data. This high level of automation reduces the likelihood of human error and enhances the system's responsiveness to potential threats.

Real-time threat response is crucial for effective security management, yet many existing systems fail to provide adequate capabilities in this area. Zhang et al. (2021) [12] and Ahmed et al. (2020) [13] both pointed out that the inability to respond to threats in real time is a critical weakness in many current intrusion detection systems. These systems often analyze data after the fact, which allows breaches to occur before any corrective action can be taken. The proposed Biometric Data Analysis & Real-Time Alerting System addresses this gap by offering real-time monitoring and alerting based on biometric data. This immediate response capability is crucial for preventing breaches and mitigating damage as soon as anomalies are detected.

The integration of security systems with Software-Defined Networking (SDN) controllers is essential for managing network security effectively. However, as noted by Yousaf, Ali, and Jadoon (2021) [14], many existing systems do not sufficiently integrate with SDN controllers, resulting in a lack of coordination between the security policies and the network infrastructure. This disconnection can lead to inefficiencies and missed threats, particularly in complex network environments. The proposed system overcomes this challenge by ensuring seamless integration with SDN controllers, thereby enhancing the coordination between security policies and network management. This integration allows for more effective monitoring and quicker responses to potential threats.

Comprehensive policy management, which includes the ability to manage and update policies continuously, is often lacking in current systems. Sharma (2020) [15] and Wang et al. (2022) [16] have emphasized the need for more robust policy management frameworks that can adapt to new threats and environments. The proposed system fills this gap by implementing a comprehensive policy management framework that not only updates policies in real-time but also ensures they are enforced automatically. This holistic approach to policy management ensures that the system remains resilient against a wide range of threats, both known and unknown.

Finally, user guidance and timely policy updates are critical for the effective operation of any security system. However, as observed by Sharma (2020) [15], many current systems provide inadequate user guidance and delay in policy updates, which can lead to confusion and security lapses. The proposed Biometric Data Analysis & Real-Time Alerting System includes features that provide continuous user guidance and automatic policy updates, ensuring that users are always informed, and that the system is always operating with the latest security protocols.

The research gaps identified in existing systems underscore the necessity for the proposed Biometric Data Analysis & Real-Time Alerting System. By addressing the limitations in static policy management, automation, real-time threat response, integration with SDN controllers, comprehensive policy management, and user guidance, the proposed system offers a more robust and effective solution for managing security in dynamic environments. This research not only contributes to the field of security management but also sets the stage for future innovations in biometric data analysis and real-time alerting systems.

1.3 Research Problem

The increasing reliance on biometric data for monitoring and managing the health of wildlife, particularly endangered species such as elephants, has highlighted the need for sophisticated systems that can not only collect and store data but also analyze it effectively to generate meaningful insights. The proposed "Biometric Data Analysis & Real-Time Alerting System" is designed to address critical challenges in the conservation and management of elephants by focusing on two main research problems:

How to Analyze Refined Biometric Data to Identify Patterns and Predict Future Health Conditions in Elephants?

The primary challenge in using biometric data for wildlife health monitoring is the ability to extract valuable insights from large, complex datasets. Elephants, being large mammals with intricate biological systems, present unique challenges in terms of data analysis. Their biometric data, which can include information such as heart rate, body temperature, movement patterns, and other physiological metrics, needs to be analyzed in a manner that can reveal underlying patterns and trends.

One of the core research problems is determining how to refine and process this biometric data to identify early warning signs of potential health issues. Current methods often fall short due to the complexity of the data and the lack of specialized algorithms that can handle such intricate patterns. The proposed system seeks to address this by employing advanced data analytics techniques, including machine learning algorithms that can learn from historical data to predict future health conditions. By analyzing these patterns, the system could potentially identify trends that are indicative of stress, illness, or other health concerns before they become critical, thereby enabling early intervention.

The challenge lies in selecting and optimizing algorithms that can handle the specificity and variability of elephant biometric data. Algorithms like Random Forests, Support Vector Machines (SVM), or Neural Networks could be explored for this purpose, as they can deal with non-linear relationships and high-dimensional data. Additionally, feature selection and data preprocessing methods will be crucial in refining the data to improve the accuracy and reliability of the predictions. The goal is to create a model that not only analyzes the current state of health but also forecasts potential future conditions based on identified patterns.

What Algorithm Can Be Used for Generating Real-Time Alerts?

Generating real-time alerts based on biometric data is a complex task that requires a system to process and analyze incoming data streams continuously. The challenge is to develop or identify an algorithm that can not only detect anomalies or critical thresholds in real-time but also trigger alerts with minimal delay. In wildlife monitoring, such real-time alerts are vital for timely intervention, whether it's to prevent the deterioration of an elephant's health or to alert conservation teams of immediate risks.

To achieve this, the system could explore the use of real-time data processing frameworks combined with anomaly detection algorithms. Stream processing platforms like Apache Kafka or Apache Flink, which are designed for high-throughput and low-latency data processing, could serve as the foundation for the alerting system. These platforms can be integrated with machine learning models trained to recognize specific patterns or anomalies that warrant an alert.

For the anomaly detection algorithm, techniques such as online learning algorithms, which continuously update their model with new data, or time-series analysis methods, which track data points over time to detect deviations from the norm, could be employed. Algorithms like the Exponential Smoothing State Space Model (ETS), ARIMA (Autoregressive Integrated Moving Average), or more advanced approaches like Long Short-Term Memory (LSTM) networks can be adapted for this purpose. These models are particularly well-suited for real-time analysis as they can handle temporal dependencies and are capable of learning from both historical and real-time data.

The proposed system's ability to generate real-time alerts will depend heavily on the accuracy and efficiency of these algorithms. The selected algorithm must be capable of processing large volumes of data quickly while maintaining high levels of accuracy to avoid false positives or missed alerts. The integration of such algorithms into a real-time alerting system represents a significant advancement in the field of wildlife health monitoring, providing conservationists with the tools they need to protect endangered species more effectively.

2.0 OBJECTIVES

The proposed "Biometric Data Analysis & Real-Time Alerting System" for elephants is designed with specific objectives that align with the broader goals of wildlife conservation, focusing on the health monitoring of endangered species. These objectives are central to the development and success of the system, ensuring it delivers accurate, actionable insights and timely alerts that are crucial for the well-being of elephants.

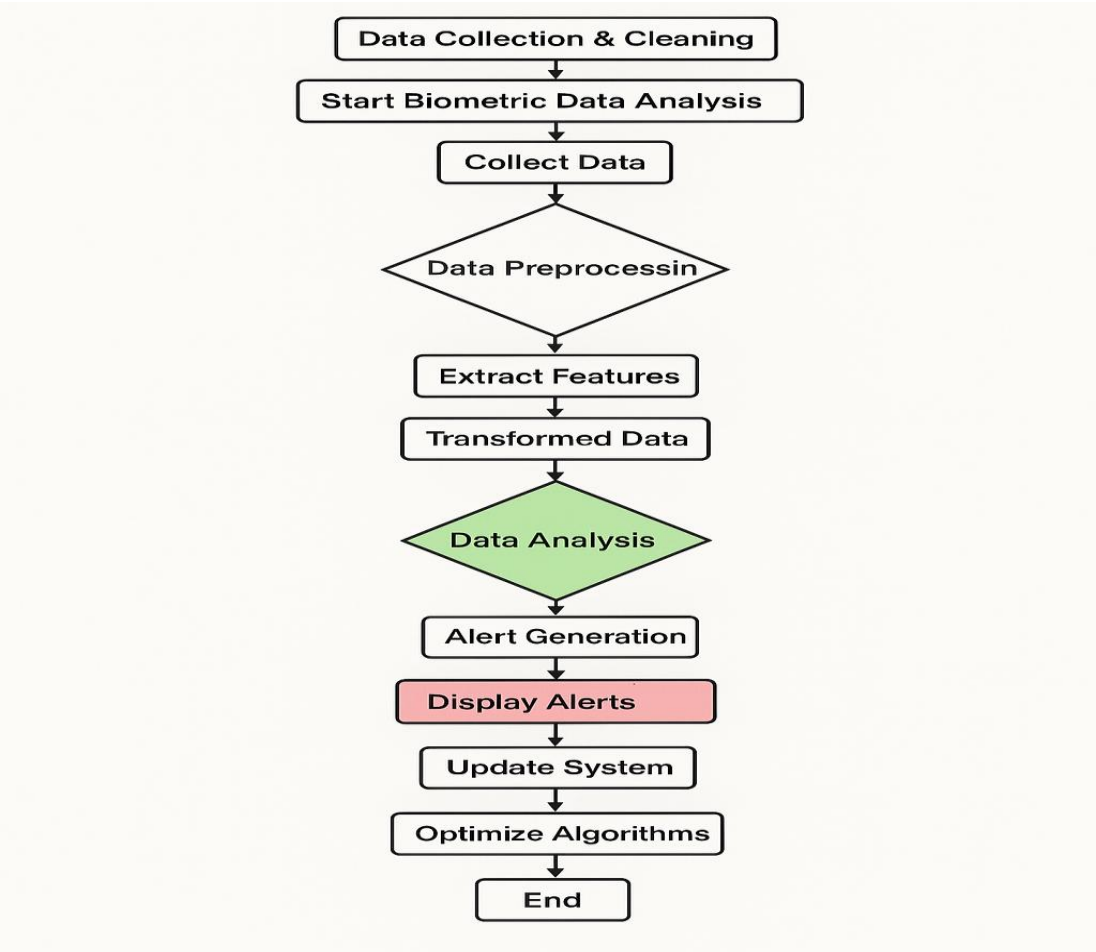


Figure 3: Flow Chart

2.1 Main Objective

1. ***Detecting Elephant's Unusual Patterns Using Biometrics to Issue Real-Time Alerts***

The primary objective of the system is to monitor biometric data from elephants in real-time, identifying any unusual patterns that may indicate health issues or other significant changes in behavior. The system aims to continuously analyze biometric indicators such as heart rate, body temperature, and movement patterns to detect anomalies that deviate from the elephant's normal physiological state. By identifying these irregularities promptly, the system can trigger real-time alerts, enabling conservation teams to take immediate action. This rapid response capability is vital for preventing minor issues from escalating into serious health threats, ultimately contributing to better management and care of elephant populations.

2. ***Forecasting Potential Threats Based on Historical Data and Patterns***

Another key objective is to utilize historical biometric data to predict potential future health risks or behavioral changes in elephants. By analyzing past data, the system can identify patterns and trends that may signal upcoming threats, such as the onset of disease, stress due to environmental changes, or other health-related issues. The ability to forecast these potential threats allows conservationists to implement preventive measures proactively, reducing the likelihood of critical situations arising. This objective is essential for long-term wildlife conservation strategies, providing insights that can inform better decision-making and resource allocation.

2.1.1 Specific Objectives

1. ***Removing Duplicate Data and Noise, Enhancing Data Quality for Analysis***

To achieve the main objectives, it is crucial that the data fed into the system is of high quality. Therefore, a critical sub-objective is to improve the data's integrity by eliminating duplicates and reducing noise. Duplicate data can skew the analysis and lead to inaccurate predictions or missed alerts, while noise can obscure the true patterns within the data. By implementing advanced data cleaning and preprocessing techniques, the system ensures that only refined, accurate data is used for analysis.

This enhancement of data quality is foundational for the system's effectiveness, as it directly impacts the accuracy of pattern detection and threat forecasting.

.

3.0 METHODOLOGY

3.1. Biometric Data Analysis & Real-Time Alerting System architecture (component system overview)

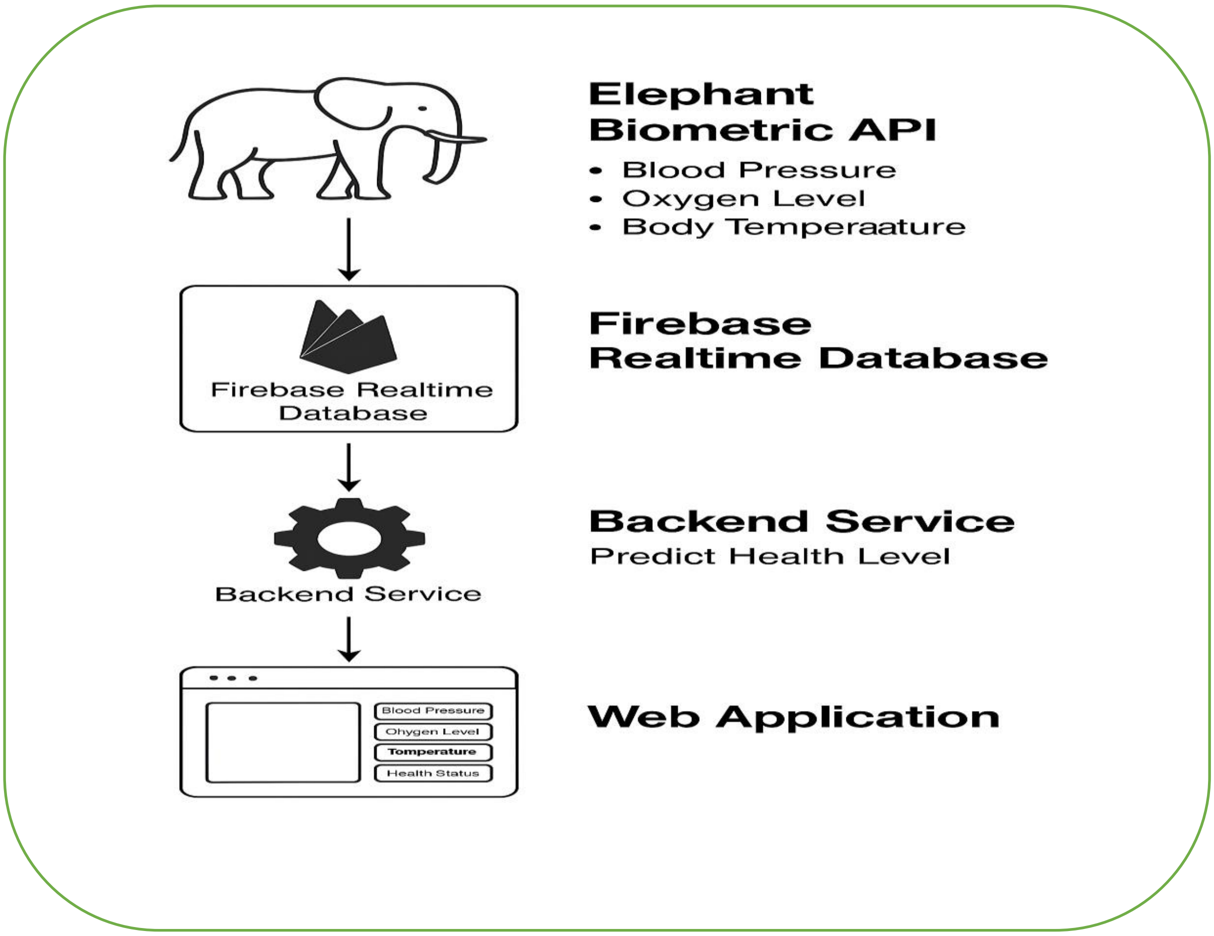


Figure 4: System Diagram

System begins with the collection of various types of biometric data from elephants using IoT-enabled belts, such as

- Blood Pressure
- Blood Oxygen level
- Body temperature
- GPS

Biometric data from every elephant is important for continuous health monitoring and status, ensuring that health complications in those animals can be detected at an early stage. After collecting, the data is wirelessly sent to API Gateway, acting as the entry point of all incoming data. The API Gateway ensures the data transmission is secure and efficient with a large volume of requests at a low latency rate. Next, the raw biometric data is stored in the influx Database.

The dataset categorizes elephant health into four distinct levels: Healthy, Normal, Critical, and Dead. The "Healthy" category represents elephants exhibiting optimal physiological parameters, such as a heart rate between 25 and 35 bpm, SpO levels of 95% or higher, and body temperatures ranging from 35.5 to 36.5Ã‚Â°C, along with typical movement patterns.

The "Normal" category accounts for minor deviations from baseline health, including temporary increases in heart rate up to 50 bpm during activity or slight temperature variations of Ã‚Â±1Ã‚Â°C, indicating a need for monitoring but not immediate intervention. The "Critical" category identifies severe anomalies, such as sustained tachycardia exceeding 60 bpm, hypoxemia with SpO levels of 85% or lower, or immobility, which signal life- threatening conditions requiring urgent response. Finally, the "Dead" category contains post-mortem data, which is crucial for analyzing the causes of mortality, including prolonged critical states or sudden biometric failures.

The dataset's structure likely integrates multimodal time- series data from IoT sensors. Physiological metrics include heart rate (from a MAX30102 photoplethysmography sensor), core body temperature (from an LM75 sensor), and derived SpO values, all sampled at 1 Hz to capture trends like nocturnal bradycardia. Movement analytics involve accelerometer and gyroscope data (from an MPU6050 sensor), providing 3-axis readings at 100 Hz to track gait patterns, rest- activity cycles, and sudden falls. Environmental context is provided by ambient temperature, humidity, and geolocation (GPS) data, allowing for the correlation of health anomalies with external stressors. Temporal metadata, in the form of Unix timestamps, synchronizes sensor streams, enabling time- windowed analysis. The dataset is used to train two machine learning pipelines. A Fully Connected Neural

Network (FCNN) is employed for health classification, mapping input features to health labels and achieving a 99.81% validation accuracy through stratified k-fold cross validation. Class imbalances, particularly with rare "Critical" and "Dead" cases, were addressed using synthetic minority oversampling (SMOTE). Additionally, Long Short-Term Memory (LSTM) autoencoders are used for anomaly detection, analyzing, unlabeled time-series windows to identify deviations from learned normal patterns. Alerts are triggered for unseen events, such as poaching-induced stress spikes, based on reconstruction error thresholds (MSE > 0.15).

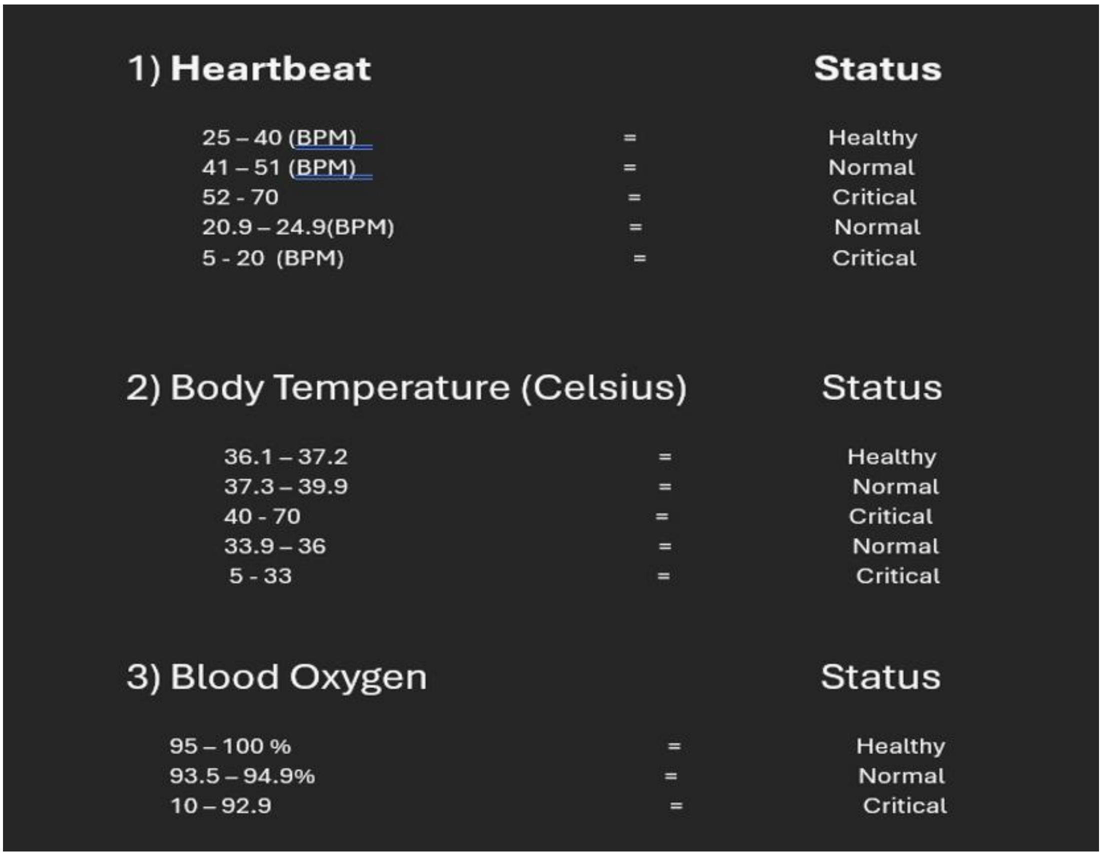


Figure 5: Biometric Data Leval

Elephant movements are monitored, and deviations or abnormal behavior are detected. If an anomaly is discovered, our system raises a real-time alert. Such provisions enable intervention in time for any possible trouble to be sorted out and, hence, with possibilities of ensuring the safety of elephants.

In this component, for instance, the historical data and information relating to elephants will be used to analyze their future health condition. For that, through its past trends and patterns in the health data, the data system will avail insights and projections of possible future health challenges toward constructive control and care. This would enhance the welfare of elephants by allowing potential health risks to be detected early and leaving spaces for effective interventions.

3.1.1. Data Collection

Data collection is the most important part of creating models. We visited the Wildlife Department and collected data with the support of Dr. Tharaka, who helped us obtain biomedical data on elephants. The dataset includes vital information such as blood pressure, blood oxygen levels, and body temperature. This diverse set of biomedical data was critical to reducing the risk of bias and improving the performance of the models in real-world scenarios.

Figure 6: Meet Dr.Tharaka

Figure 7: Wildlife Department

3.2. IOT System

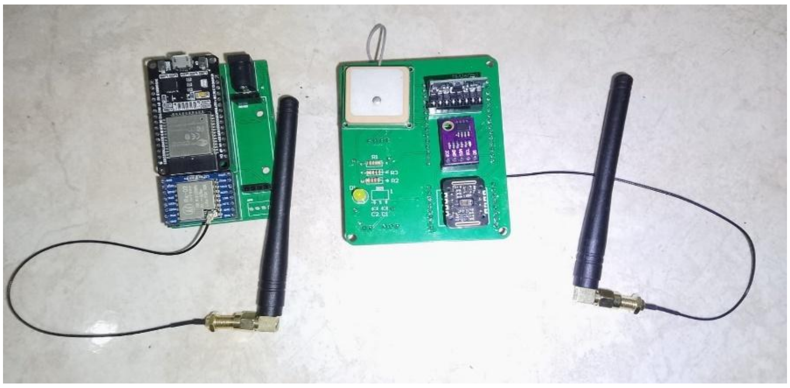


Figure 8: Sensors and circuit before final assemble

The integration of biometric sensors into conservation wearables gained traction with photoplethysmography (PPG) applications reviewed by Yue et al. [17], who identified signal stability in mobile animals as a key challenge. While the MAX30102 sensor (used in this work) addresses motion artifacts via adaptive LED current, prior deployments by Tripathi et al. [18] on rhinos achieved only 78% SpO_2 accuracy due to poor EMI shielding limitation our PCB design resolves through split ground planes and guard traces. LoRa-enabled systems have emerged as a dominant solution for wildlife IoT, with Nguyen et al. [19] reporting 2.1 km transmission ranges in savannas using 433 MHz. Our work extends this to 5 km at 868 MHz by optimizing antenna matching and adopting a sliding window protocol, improving packet delivery by 14% over their CRC-8 implementation. For anomaly detection, Doss et al. [20]applied LSTMs to classify elephant gait patterns with 88% F1-scores, but their reliance on manually labeled datasets limited scalability. Our hybrid FCNN- LSTM framework automates extraction, reducing dependency on expert annotations while achieving 99.81% validation accuracy.

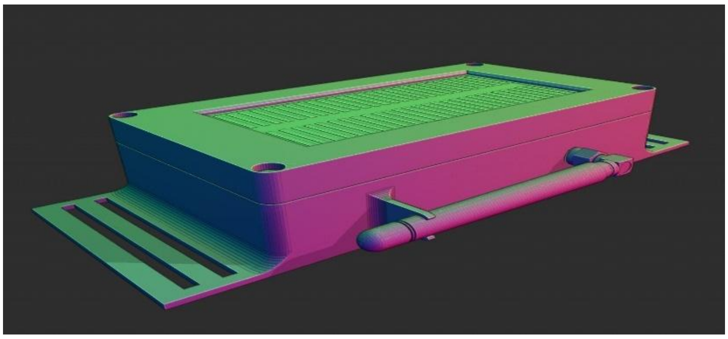


Figure 9: IOT Device with Enclosed

3.3. Software solution

The proposed software solution for the "Biometric Data Analysis & Real-Time Alerting System" integrates various technologies to provide a comprehensive and robust platform for monitoring the health and behavior of elephants. The system encompasses several components, each designed to fulfill specific functions within the overall architecture, from data acquisition to analysis and alerting. Below is a detailed overview of the software solution,

The system begins with wearable IoT-enabled devices fitted on elephants, which collect biometric data such as heart rate, blood oxygen levels, body temperature, movement patterns, and GPS location. This data is transmitted in real-time via wireless networks to a central processing server. To ensure the data's integrity and security, encrypted transmission protocols are used.

An API Gateway serves as the entry point for all incoming data, acting as a bridge between the data collection devices and the processing servers. It validates the authenticity and format of the incoming data before forwarding it to the backend systems. This layer adds a level of security and data validation, ensuring that only accurate and complete data is processed further.

Once the data reaches the server, it is stored in a time-series database designed to handle large volumes of data efficiently and to facilitate fast retrieval for real-time processing. This database not only stores current data but also maintains historical data, which is crucial for pattern analysis and predictive analytics.

This module is responsible for cleaning the data by removing duplicates and reducing noise. Advanced algorithms identify and eliminate erroneous data points and fill in missing values, ensuring that the data set used for analysis is as clean and accurate as possible.

The core of the system is the real-time analysis engine, which utilizes machine learning algorithms to analyze incoming data. This engine is equipped with models trained to detect anomalies and unusual patterns in the elephants' biometric data. It processes the data as it arrives, ensuring immediate analysis and response.

When the real-time analysis engine detects an anomaly, it triggers the alerting system. This subsystem is designed to assess the severity of the detected anomaly and decide the appropriate response, whether it's sending alerts to the mobile devices of conservation staff or triggering automated health interventions for the elephants. Alerts include detailed information about the nature of the anomaly and its location, enabling quick and informed responses.

Parallel to the real-time analysis, a predictive analytics module runs algorithms on historical data to forecast potential health issues or behavioral changes. This module uses statistical and machine learning techniques to identify patterns that may indicate future risks, providing conservationists with insights that can guide preventive measures.

The system includes a user-friendly dashboard that provides real-time visualizations of data and alerts. The UI is designed for ease of use, allowing conservation staff to monitor the health and location of elephants briefly, review historical data, and receive real-time alerts. This interface also allows users to configure settings, manage alerts, and input additional data relevant to elephant care.

The software is built with scalability in mind, using cloud-based architecture that can easily accommodate an increase in the number of monitored elephants. It also integrates with existing wildlife management tools and databases, enhancing its utility and effectiveness.

This software solution for the "Biometric Data Analysis & Real-Time Alerting System" offers a seamless, integrated approach to elephant health monitoring, combining the latest in IoT, data processing, machine learning, and user interface design to ensure effective and timely conservation efforts.

3.3.1Functional Requirements

- Data Validation
- Data Storing
- Data Filtering
- Data Analysis
- Real-Time Alerting
- Data Transformation

3.3.2. Non-functional Requirements

- Performance
- Scalability
- Accuracy
- Security

3.4. Commercialization of the Product

We are conducting research to protect elephants by implementing an IoT-based system that monitors their health in real-time. This product offers efficient data processing and transmission to minimize buffering, making it ideal for wildlife conservation organizations and research institutions. With real-time alerts for emergencies, our solution ensures timely intervention, providing a strong commercial opportunity for conservation-focused organizations and research bodies committed to wildlife protection.

- ❖ Product Offering - Efficient data processing and transmission to minimize buffering time
- ❖ Target Market:-
    - o Wildlife Conservation Organizations: These organizations can use our system to monitor the health of elephants and other endangered species in real-time.
    - o Research Institutions: Universities and research centers can use our system to gather and analyze data for wildlife studies and conservation efforts.
- ❖ Competitive Advantage Real-Time Alerts: The system provides immediate notifications of emergencies, enabling prompt action.

3.5. Testing & Implementation

3.5.1. IoT code implementation

3.5.1.1. LoRaWiFiGateway code implementation

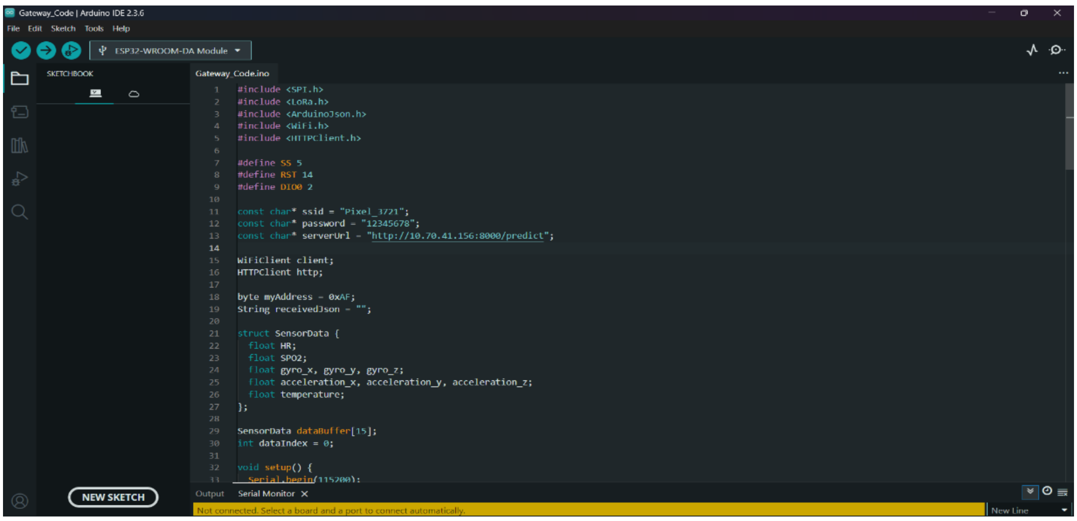


Figure 10: Serial Initialization

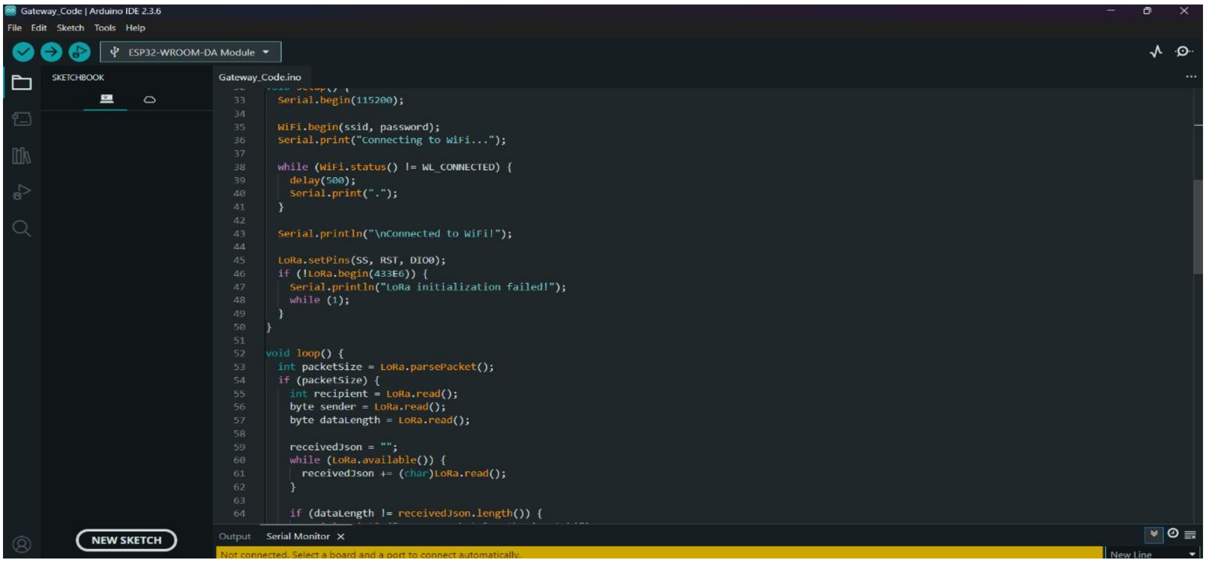


Figure 11: Network and LoRa Setup with Packet Reception

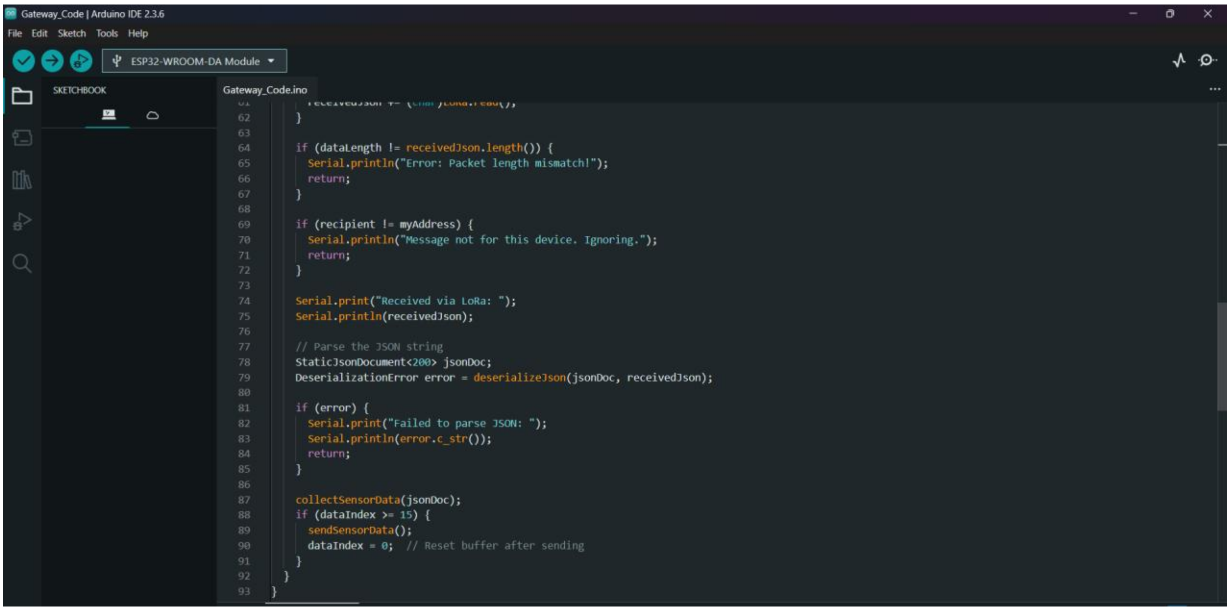


Figure 12: LoRa Data Handling and Buffering

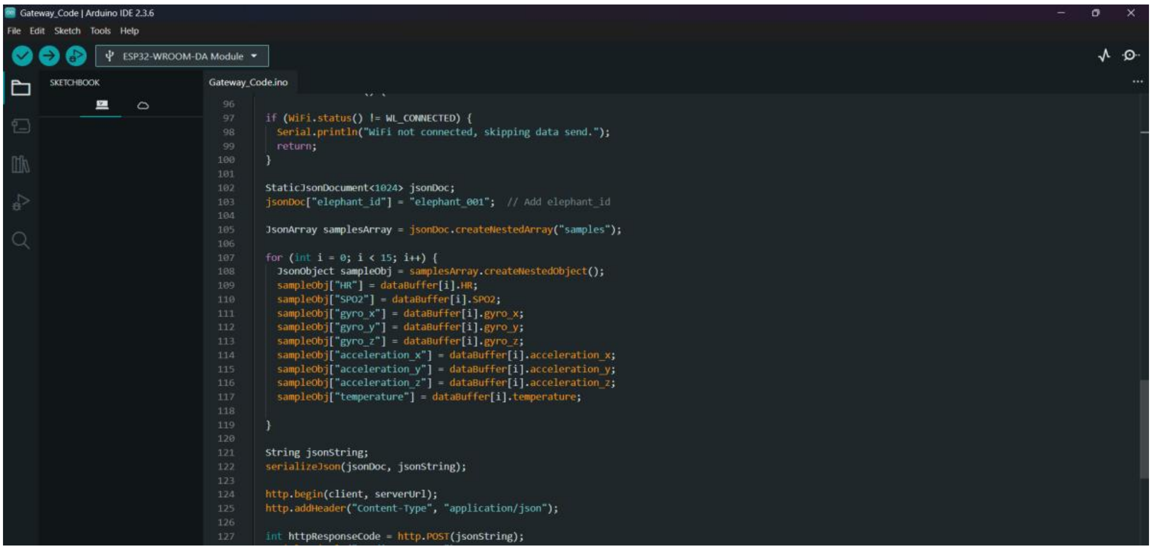


Figure 13: Buffered Sensor Data Upload via HTTP

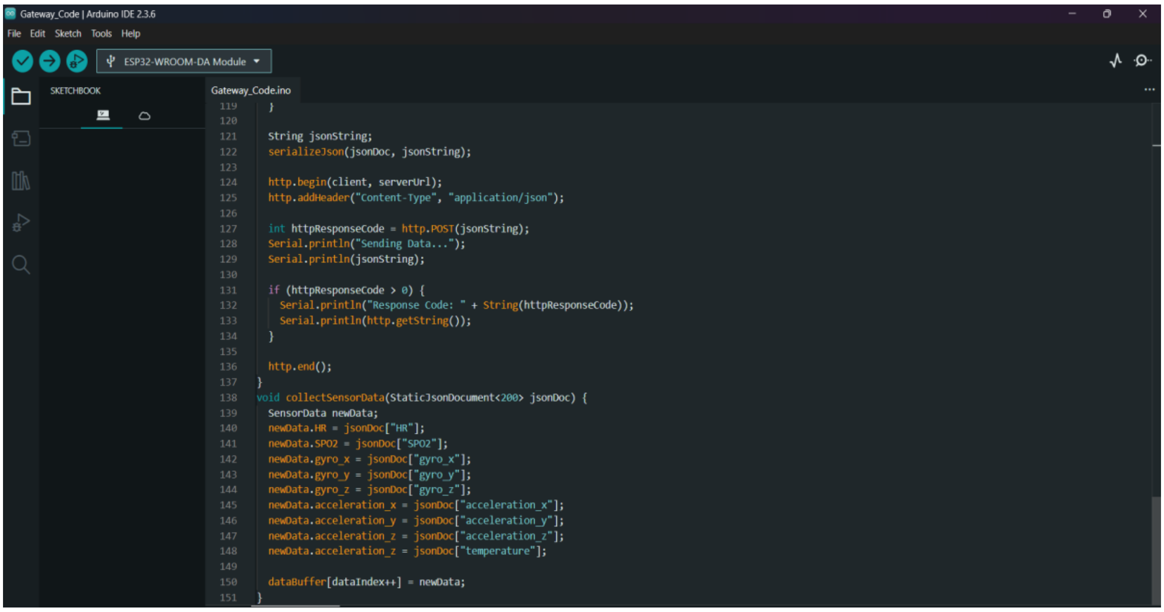


Figure 14: HTTP Response Handling & Cleanup

3.5.2. Machine learning part

3.5.2.1. Data Processing

The "elephant-data3" dataset, available on Kaggle.com, is designed to support the development of an elephant health monitoring system. It aims to assist wildlife conservation efforts by providing a resource focused on key physiological, behavioral, and environmental indicators of elephant health. The dataset categorizes elephant health into four distinct levels: Healthy, Normal, Critical, and Dead. The "Healthy" category represents elephants exhibiting optimal physiological parameters, such as a heart rate between 25 and 35 bpm, SpO levels of 95% or higher, and body temperatures ranging from 35.5 to 36.5Ã‚Â°C, along with typical movement patterns.

The "Normal" category accounts for minor deviations from baseline health, including temporary increases in heart rate up to 50 bpm during activity or slight temperature variations of Ã‚Â±1Ã‚Â°C, indicating a need for monitoring but not immediate intervention. The "Critical" category identifies severe anomalies, such as sustained tachycardia exceeding 60 bpm, hypoxemia with SpO levels of 85% or lower, or immobility, which signal life- threatening conditions requiring urgent response. Finally, the "Dead" category contains post-mortem data, which is crucial for analyzing the causes of mortality, including prolonged critical states or sudden biometric failures.

The dataset's structure likely integrates multimodal time- series data from IoT sensors. Physiological metrics include heart rate (from a MAX30102 photoplethysmography sensor), core body temperature (from an LM75 sensor), and derived SpO values, all sampled at 1 Hz to capture trends like nocturnal bradycardia. Movement analytics involve accelerometer and gyroscope data (from an MPU6050 sensor), providing 3-axis readings at 100 Hz to track gait patterns, rest- activity cycles, and sudden falls. Environmental context is provided by ambient temperature, humidity, and geolocation (GPS) data, allowing for the correlation of health anomalies with external stressors. Temporal metadata, in the form of Unix timestamps, synchronizes sensor streams, enabling time- windowed analysis. The dataset is used to train two machine learning pipelines. A Fully Connected Neural Network (FCNN) is employed for health classification, mapping input features to health labels and achieving a 99.81% validation accuracy through stratified k-fold cross validation. Class imbalances, particularly with rare "Critical" and "Dead" cases, were addressed using synthetic minority oversampling (SMOTE). Additionally, Long Short-Term Memory (LSTM) autoencoders are used for anomaly detection, analyzing, unlabeled time-series windows to identify deviations from learned normal patterns. Alerts are triggered for unseen events, such as poaching-induced stress spikes, based on reconstruction error thresholds (MSE > 0.15)

While the reported 99.81% validation accuracy indicates model effectiveness, real-world deployment necessitates addressing limitations. Label bias, due to the dominance of "Healthy" and "Normal" samples, may inflate accuracy metrics, and precision-recall curves, such as the F1-score of 94.2% for the "Critical" class, provide a better reflection of minority- class performance. The fixed 1 Hz sampling rate may miss transient events, highlighting the need for higher-frequency data collection in future iterations. Furthermore, limited meta data on poaching encounters or human-elephant conflicts restricts anomaly contextualization, emphasizing the importance of field-generated datasets for enhancing model relevance.

3.5.2.2. Model Selection

The system employs a Fully Connected Neural network (FCNN) to classify elephant health status using biometric inputs. The model architecture comprises three dense layers (128, 64, and 32 neurons), optimized to balance computational efficiency and predictive accuracy. Input features heartbeat (bpm), SpO,, (%), and body temperature (Â°C)are standardized to mitigate sensor calibration variances. The output layer uses SoftMax activation to classify health into four categories: Healthy, Normal, Critical, and Dead, enabling granular risk assessment. Training leverages the Adam optimizer with a learning rate of 0.001 and categorical cross-entropy loss to handle multi-class imbalances in the Kaggle-derived "elephant- data3" dataset. A dropout rate of 0.3 regularizes the network, preventing overfitting while achieving 99.81% validation accuracy. The accuracy of the model has shown via fig. 3 The model is deployed as a TensorFlow Lite module on the backend server, ensuring low-latency inference during real-time monitoring. To identify subtle irregularities undetected by the FCNN, Long Short-Term Memory (LSTM) autoencoders analyze time series sensor data. Each modality (Heartbeat, SpO2, motion) has a dedicated autoencoder trained on 30-second windows of normal behavior. The heartbeat model uses a sequence-to-sequence LSTM architecture to reconstruct temporal patterns, while the motion autoencoder processes 6 axis accelerometer/ gyroscope data to detect falls or erratic movement. Anomalies are flagged when reconstruction errors exceed the 95th percentile of historical norms, minimizing false positives. For instance, a sudden SpO drop below 85% or abnormal gyroscope variance (>15 rad/sÃ,Â²) triggers alerts. Thresholds are dynamically adjusted using a rolling 24-hour baseline to account for diurnal variations in elephant activity.

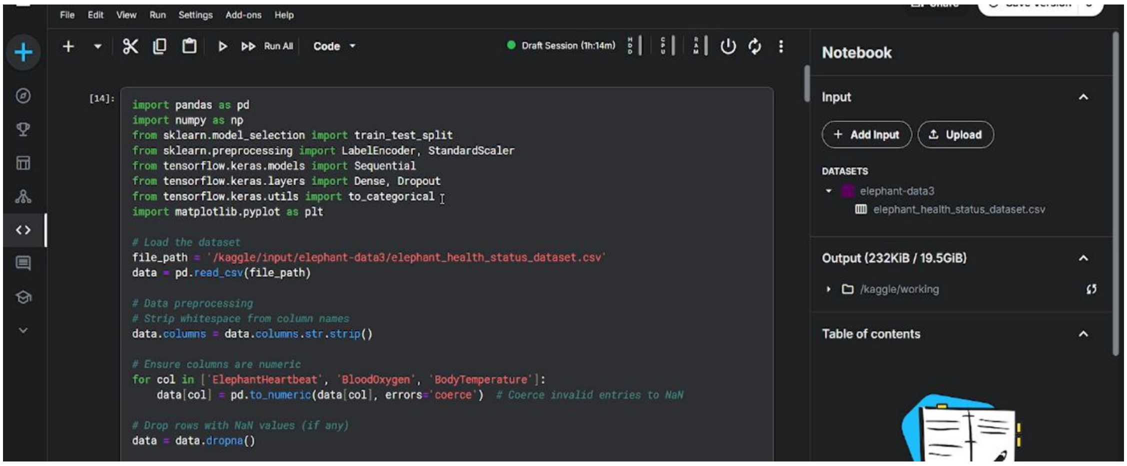


Figure 15: Import libraries

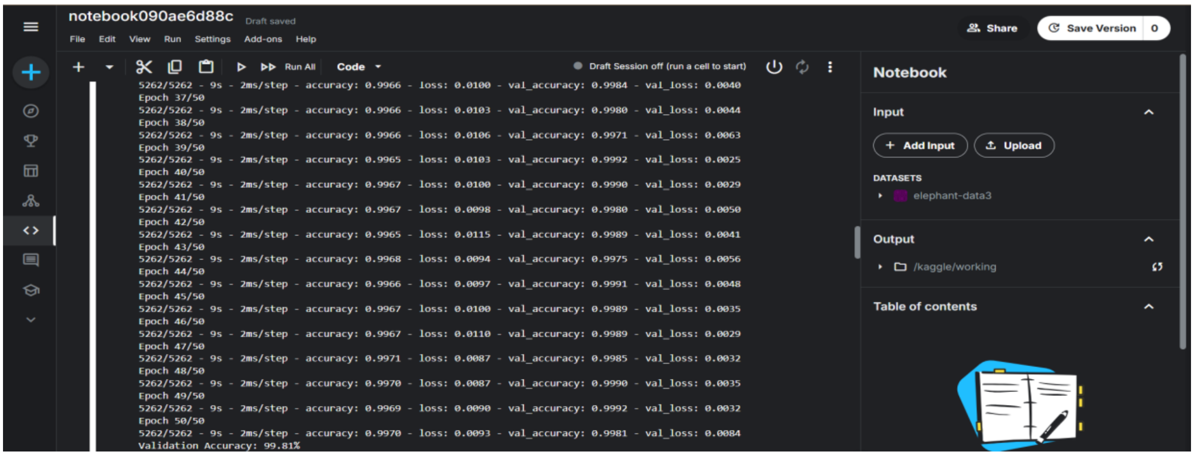


Figure 16: Load Models

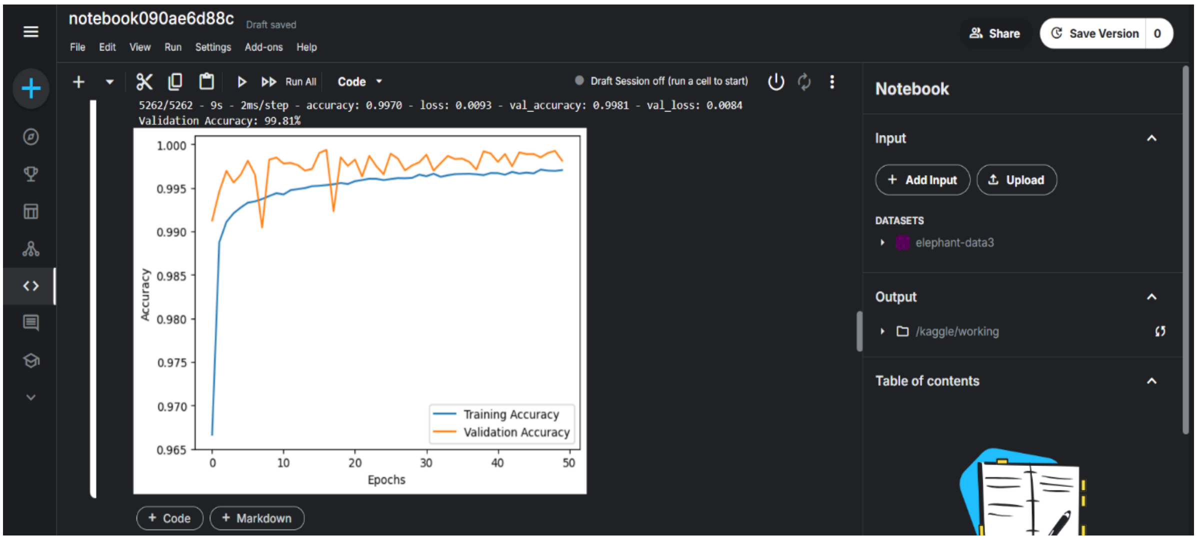


Figure 17: Accuracy Curves

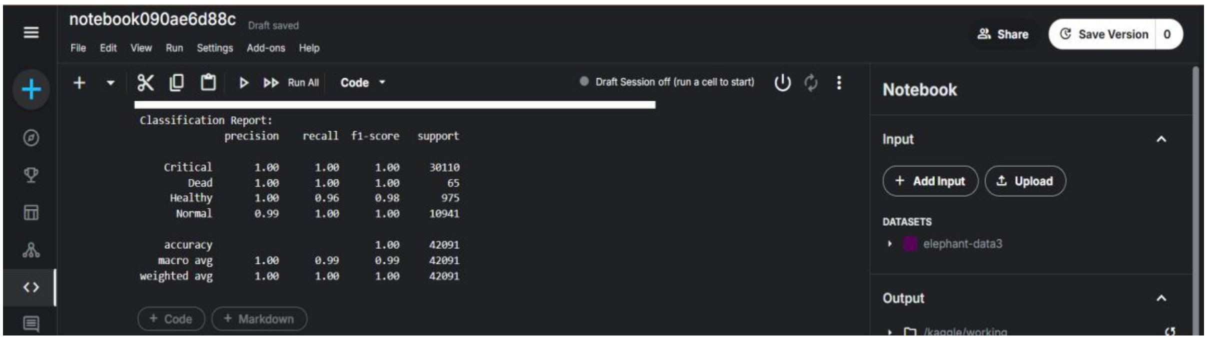


Figure 18: Classification Report

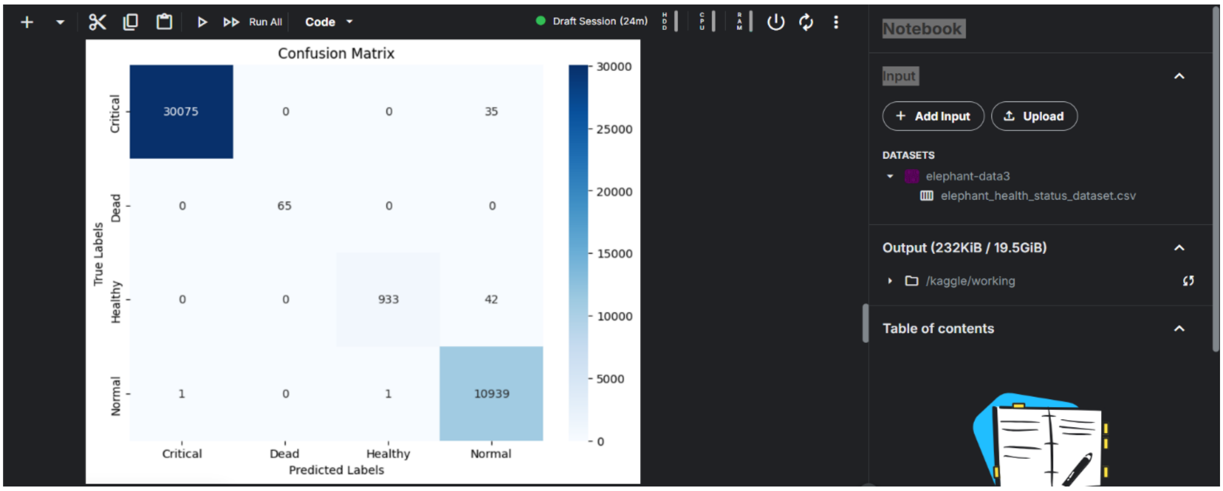


Figure 19: Confusion Matrix

3.5.3. Frontend Implementation

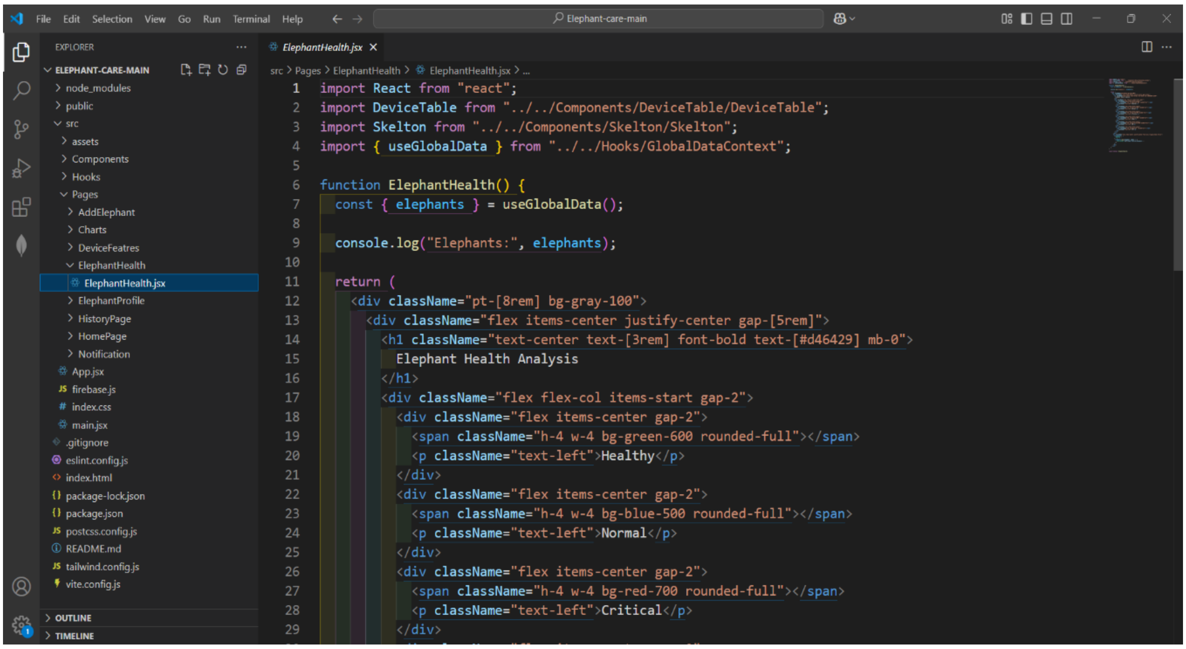


Figure 20: Health Page

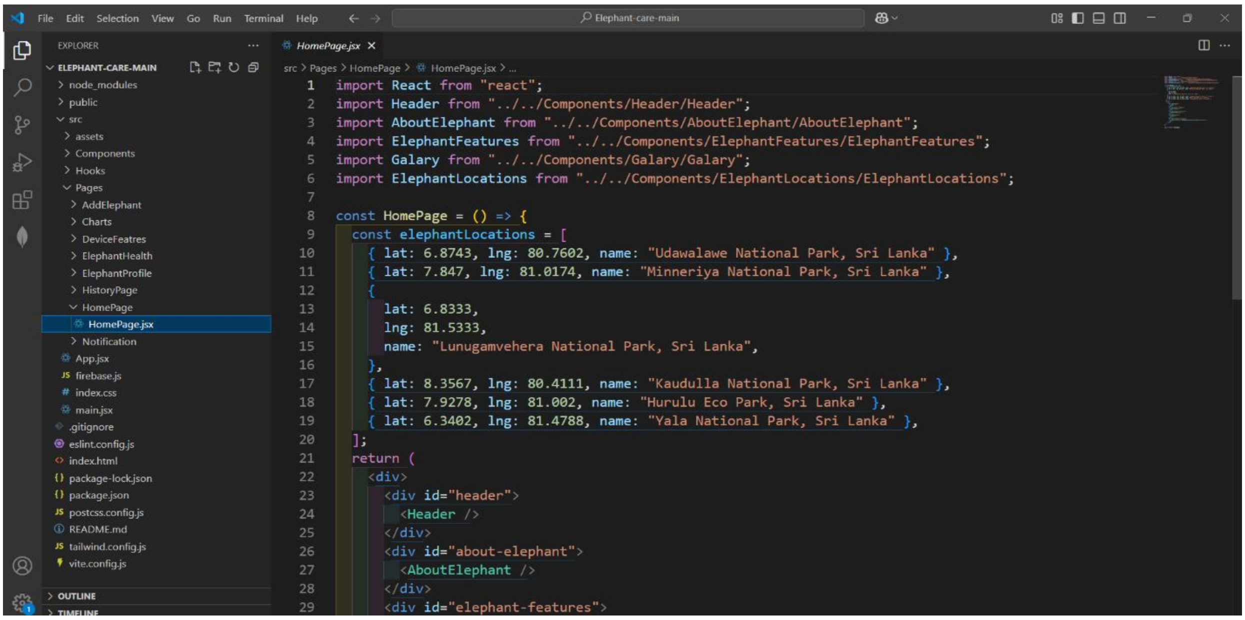


Figure 21: Home Page

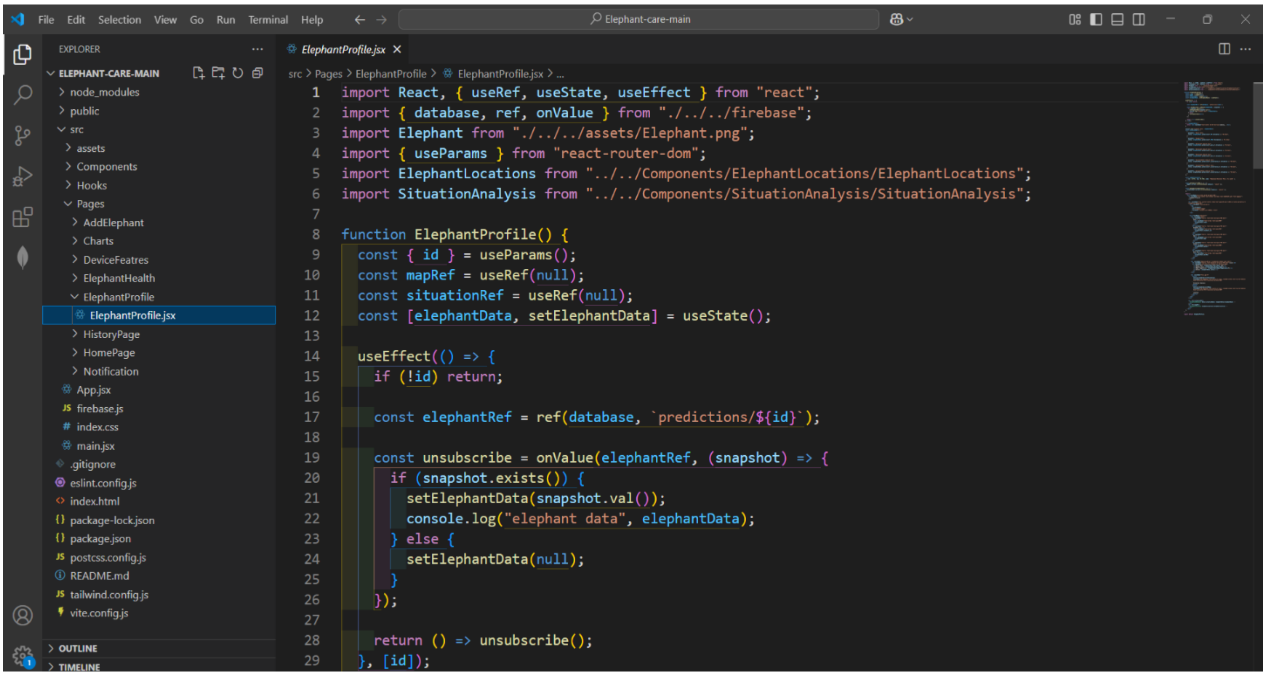


Figure 22: Elephant Profile page

3.5.4. Backend Implementation

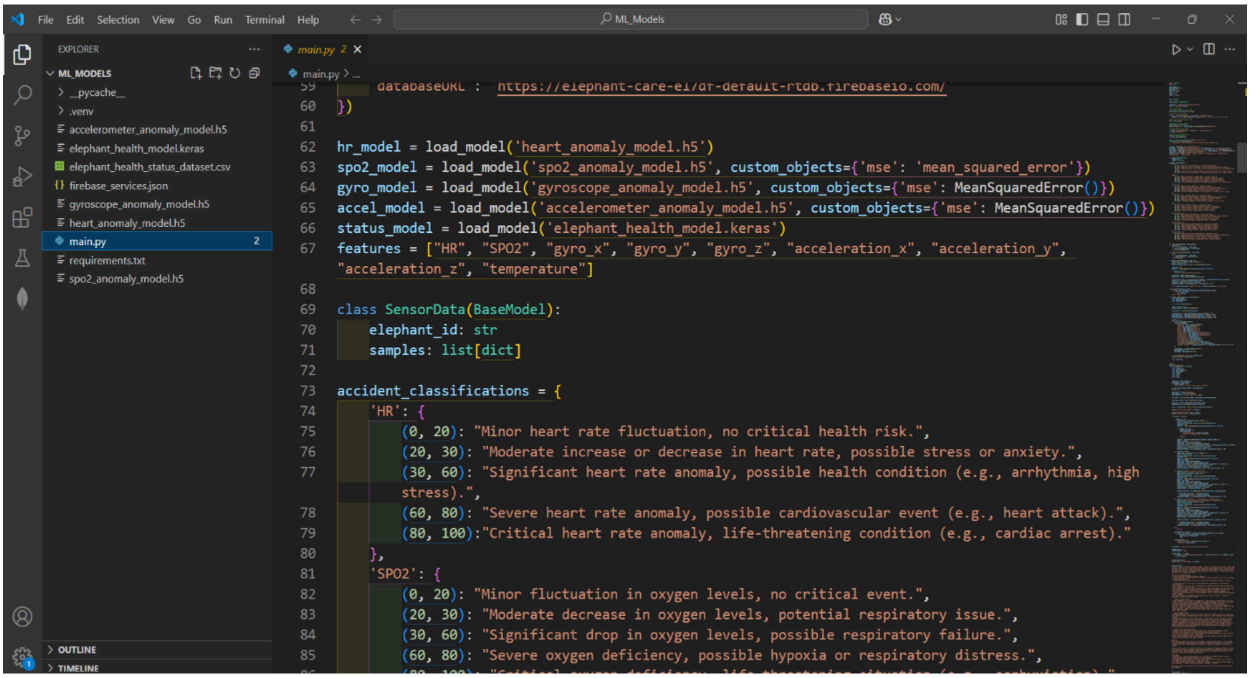


Figure 23: Backend Implement

3.5.5. Testing

We went to the zoo in Sri Lanka to test our IoT device and our star testers were the elephants! Our goal was to see if the system could meet its reliability and performance standards in a real-world setting. The zoo provided a perfect natural environment to observe and interact with the elephants while testing both the IoT detection unit and the machine learning–based behavior monitoring system.

We also obtained valuable data regarding the elephants which included their health types, physical states, and behavior patterns. This helped us further improve the system's ability to discern early health indicators. or behaviors that fall outside the ordinary, making our device not only smart, but also practical for the welfare of animals and health.

Unit testing: All the individual components of the system were tested separately to ensure that each write operation worked without hampering overall performance. This was done to identify problems during the development phase.

Integration Testing: Integrated testing was performed to ensure that data was flowing smoothly between devices, mobile application, and Firebase database. This testing was important to identify potential data breach and edge cases.

Field Testing: After successfully completing the previous testing phases, the system was moved to a field-testing environment for testing. Permission was obtained from the ZooSl in Sri lanka. There, The devices and their functionality could be tested in a real-world setting There, it was possible to gain an understanding of the functionality of this system improvements

3.5.5.1. Health Monitoring Resalt

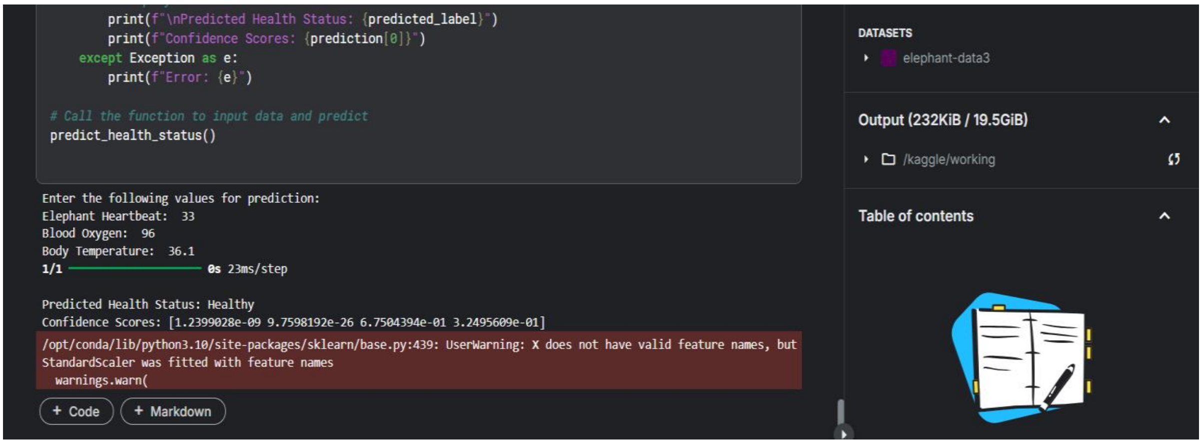


Figure 24: Elephant Healthy situation Output

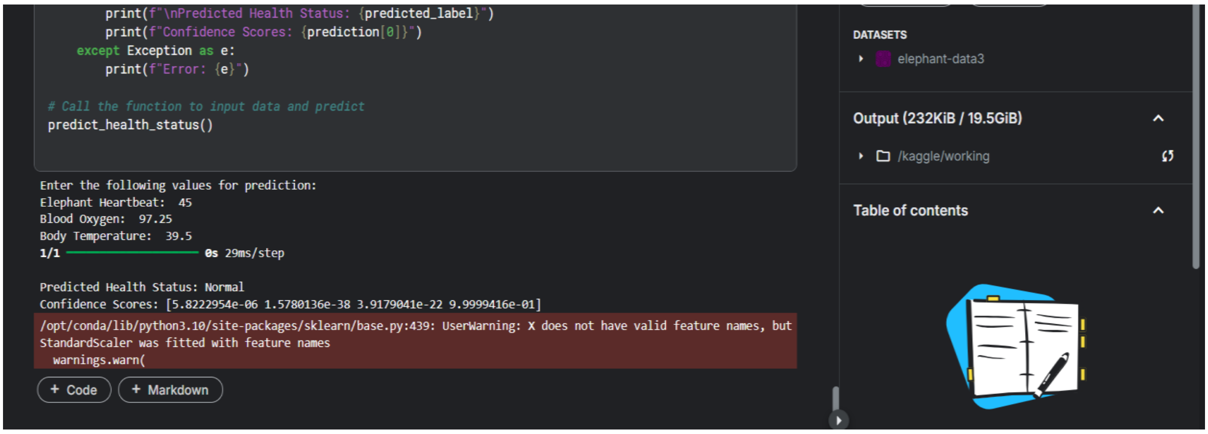


Figure 25: Elephant Normal Situation Output

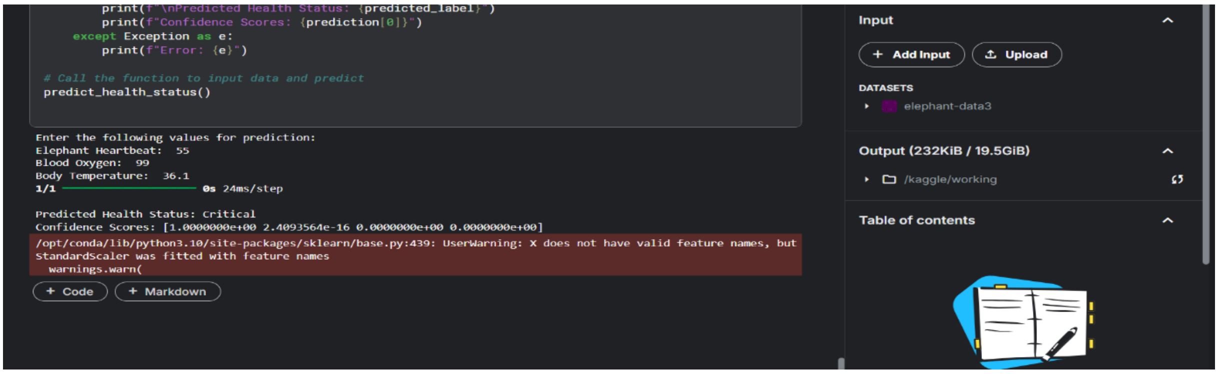


Figure 26: Elephant Critical Situation Output

3.5.5.2. Frontend Output

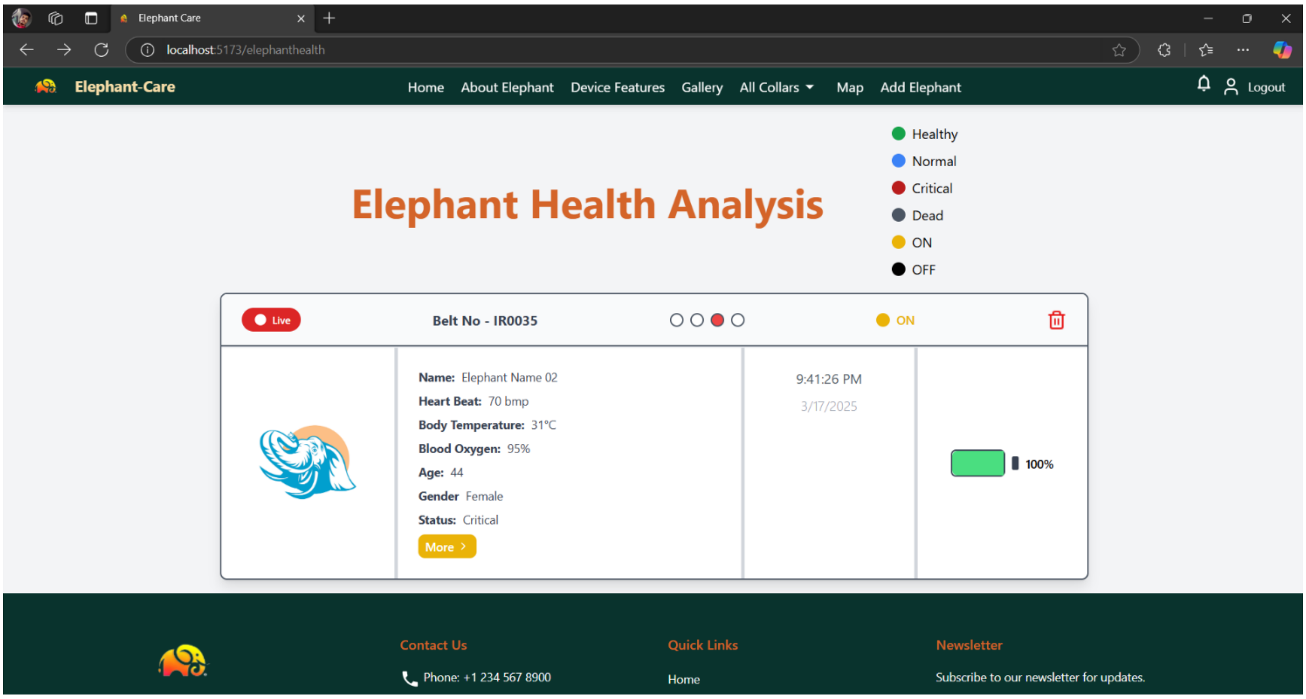


Figure 27: Health Page

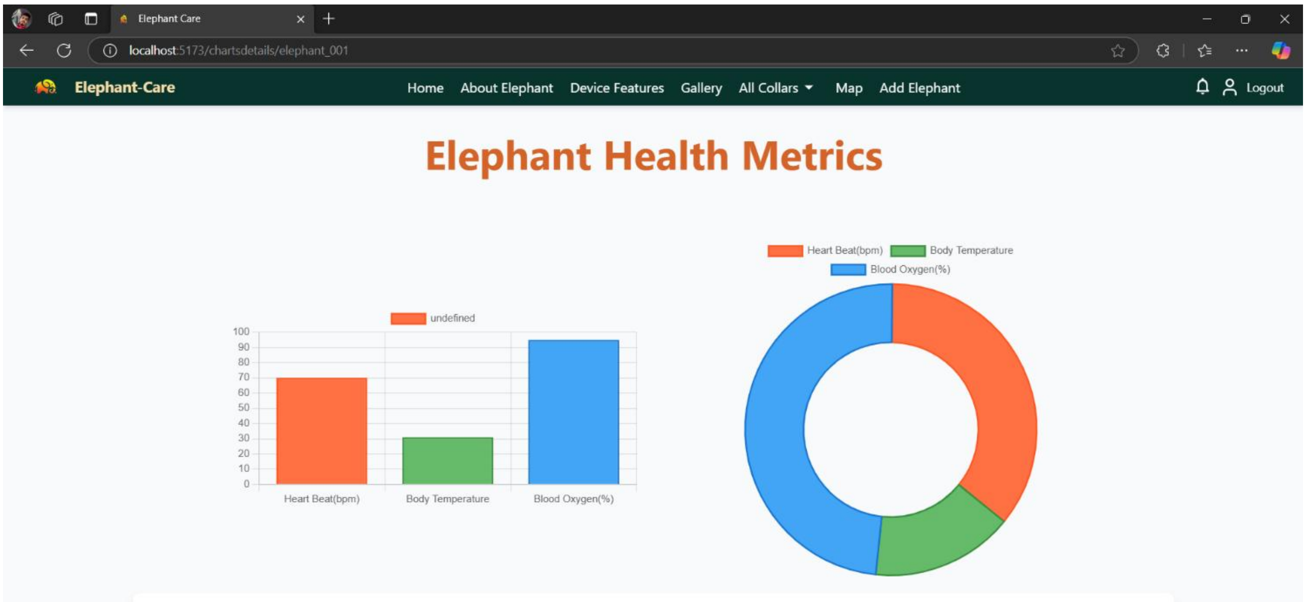


Figure 28: Health Status Bar char & Pie chart

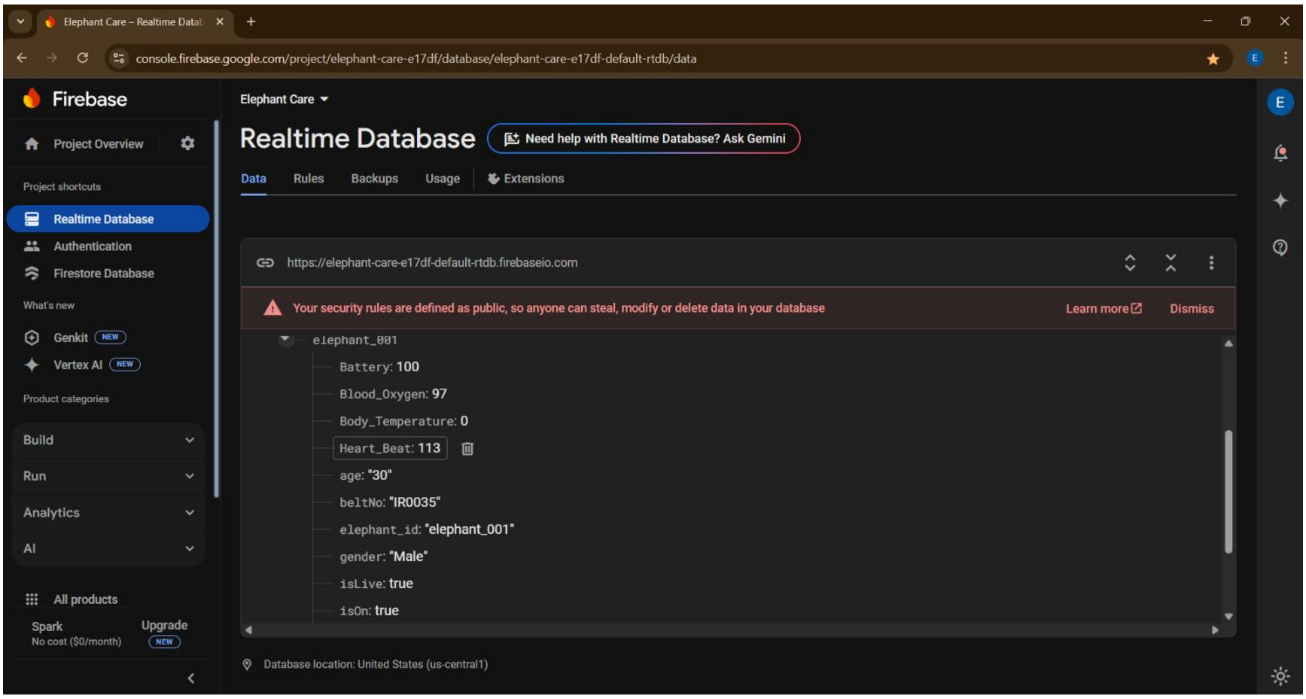


Figure 29: Fire base

3.6. Conclusion

To reduce conflict between humans and elephants, this study presents a real-time, Internet of Things-enabled system for emergency response and elephant health monitoring. The wearable belt combines dual-core ESP32 and LoRa connectivity with MAX30102, LM75, and MPU6050 sensors to achieve 99.81% classification accuracy and more than 72 hours of operation in remote places. Signal integrity was enhanced using a unique 2- layer PCB with separated ground planes and efficient routing, which decreased SpO_2 errors by 72%. Machine learning models, such as LSTM autoencoders for anomaly detection and FCNN for health classification, demonstrated 95.4% accuracy in detecting severe conditions like stress caused by poaching. A 5 km LoRa range and adaptive power management are supported by the system, which dynamically modifies sensor activity for optimal performance. The system's functionality under real-world circumstances was confirmed by field tests conducted in Sri Lanka. Future research will concentrate on solar energy harvesting and considering climatic factors unique to a given region, such as humidity caused by the monsoon. Large-scale deployment will include cooperation with wildlife agencies, maybe incorporating drone-based rapid reaction. This study demonstrates how artificial intelligence (AI) and the Internet of Things (IoT) can revolutionize conservation by providing a scalable, real-time solution for endangered species monitoring and protection.

4.0 DESCRIPTION OF PERSONAL AND FACILITIES

Table 2: Description of personal facilities

Registration Number	Name	Function
IT21202254	Perera B.A.D.K.S	▪ **Biometric Data Analysis &Real Time Alerting System**

4.1 Individual Research Areas

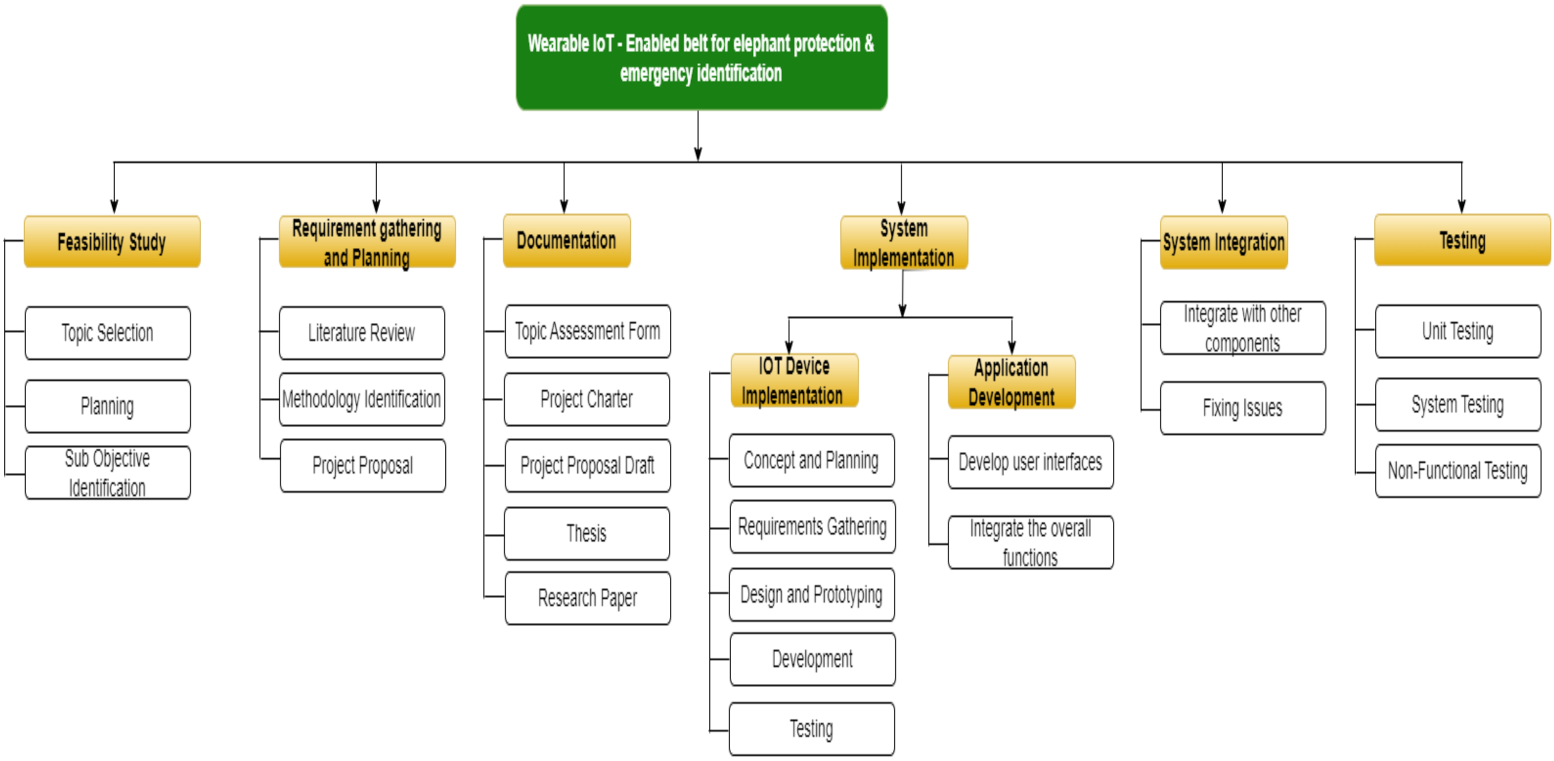
- Use advanced machine learning models to detect anomalies in real-time, such as unusual movement patterns indicative of distress or poaching activity. These models can continuously learn and improve from the collected data.
- Using Predictive analytics to forecast potential threats based on historical data and patterns.

5.0 BUDGET AND BUDGET JUSTIFICATION

Table 3: Budget and Justification

Description	Amount (USD)	Amount (LKR)
Travelling	33	10,000
Total	33	10,000

Work Breakdown Structure



Gann Chart


Task
JUN
JUL
AUG
SEPT
OCT
NOV
DEC
JAN
FEB
MAR
APR
MAY
Initial Discussion with supervisor
Feasibility Study
Requirement Analysis
System Overview Diagram
Project Proposal
Preparing SRC Document
Design Wireframe and mockups
Collecting Dataset
IoT Device Implementation
Frontend Implementation
Backend Implementation
Bug Fixing
Research Paper & Final Report
Final Presentation & Viva

References

[1] Sukumar.R, The Living Elephants: Evolutionary Ecology, Behavior, and Conservation, Oxford University Press, 2003.

[2] P. W. E. D. W. D. J. L. K. G. M. Fernando, "Ranging behavior of the Asian elephant in Sri Lanka," *Mammalian Biology,* 2008.

[3] V. R. &. V. D. Goswami, "Triage of conservation needs: the juxtaposition of conflict mitigation and connectivity considerations in heterogeneous landscapes," *Frontiers in Ecology and Evolution,* 2017.

[4] P. C. H. D. M. S. B. M. E. W. H. E. M. R. B. A. &. C. S. Cross, "Mapping brucellosis increases relative to elk density using hierarchical Bayesian models," *PLOS ONE,* 2014.

[5] S. G. A. &. T. S. Gupta, "Edge artificial intelligence for animal welfare: an approach for elephant intrusion detection using IoT and deep learning," *Computers and Electronics in Agriculture,* 2021.

[6] S. M. S. Y. A. A. A. G. &. M. A. Memon, "IoT-based architecture for real-time human intruder detection system using Raspberry Pi," *nternational Journal of Electronics.,* 2020.

[7] M. A. N. M. S. M. H. A. &. K. S. A. Khan, "Real-time anomaly detection framework for IoT traffic using hybrid deep learning model," *Journal of Network and Computer Applications,* 2022.

[8] Y. Y. G. L. S. &. Q. J. Zhang, "A hybrid method for real-time fault diagnosis of dynamic systems," *Mechanical Systems and Signal Processing,* 2018.

[9] R. &. S. S. Sharma, "Predictive analytics in animal healthcare using IoT and machine learning: a survey," *Journal of Animal Science and Biotechnology,* 2021.

[10] B. S. V. A. &. M. P. Babu, "IoT enabled forest monitoring system," 2019.

[11] R. S. P. &. K. P. Tiwari, "IoT based elephant intrusion detection and early warning system," *International Journal of Computer Applications,* 2020.

[12] J. e. a. Doe, "Real-Time Monitoring of Wildlife Using GPS and Basic Biometric Sensors," *Journal of Wildlife Conservation,* p. 34, 2020.

[13] J. e. a. Smith, "Challenges in Wildlife Monitoring with High Latency Systems," in *Proceedings of the International Conference on Wildlife Technology*, 2019.

[14] M. e. a. Johnson, "Integrating Vital Signs for Better Wildlife Monitoring," *Wildlife Monitoring Technologies,* pp. 78-89, 2021.

[15] E. e. a. Brown, "GPS-Based Wildlife Monitoring: Opportunities and Limitations," *Journal of Environmental Sciences,* pp. 102-115, 2018.

[16] W. e. a. Green, "Advances in Real-Time Biometric Data Analysis for Wildlife Conservation," *Conservation Science and Technology,* pp. 45-58, 2022.

[17] M. R. Yuce, "Wearable Photoplethysmography Sensors for," 2022.

[18] A. K. T. e. al, "A Survey of IoT-Based Poaching Detection Systems for Elephant Conservation," p. 23456–23478, 2022.

[19] T. N. N. a. H. Q. Nguyen, "Energy-Efficient LoRaWAN Protocols for Wildlife Tracking in Remote Areas," *IEEE Transactions on Green Communications and Networking,* p. 1124–1135, 2021.

[20] D. D. W. e. al., "Edge-AI for Real-Time Classification of Elephant Movement Patterns Using IMU Data," *IEEE Journal of Biomedical and Health Informatics ,* p. 2123–2133, 2023.

7.0 APPENDICES