Aysha Salim, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Medishield IDS- Protecting medical WSNs like a shield

Aysha Salim, Athul S, Abdul Rahman, Alex Abraham
Dept. of Computer Science and Engineering Toc H Institute of Science and Technology City, India

Abstract- MediShield IDS is an IoT-based smart health mon- itoring and security system designed to provide continuous, secure, and intelligent patient care in hospitals. The system includes a wearable smart health band that monitors vital signs like heart rate, body temperature, oxygen saturation (SpO), and patient movement in real time. The band uses biomedical sensors and an ESP32 microcontroller for efficient data collection and wireless communication. The collected health data is securely sent to a cloud-based platform or mobile app, allowing doctors and caregivers to monitor patient health remotely and respond quickly to critical situations. Besides health monitoring, the system provides indoor navigation and real-time patient tracking with Bluetooth Low Energy (BLE) beacons and motion analysis using an accelerometer. This feature helps elderly and disabled patients navigate hospital areas safely with turn-by-turn guidance through vibrations or display alerts on the wearable device. At the same time, healthcare staff can track patient locations via a web-based interface, improving emergency response, patient management, and operational effectiveness. To tackle growing cybersecurity issues in medical Wireless Sensor Networks (WSNs), MediShield IDS includes strong security measures like end-to-end data encryption, device authentication, and anomaly detection to block cyberattacks, data spoofing, and unauthorized access. By combining health monitoring, indoor navigation, real-time tracking, and intrusion detection into one wearable solution, the system improves patient safety, privacy, independence, and hos- pital efficiency. MediShield IDS offers a secure smart healthcare solution that meets the needs of modern digital hospitals.

Index Terms—component, formatting, style, styling, insert.

I. INTRODUCTION

The rapid growth of Internet of Things (IoT) technologies has greatly changed modern healthcare systems. These tech- nologies allow continuous, real-time monitoring of patients using wearable and wireless devices. Hospitals are adopting smart monitoring solutions to enhance patient care, cut down on manual observation, and ensure quicker medical responses during emergencies. Tracking vital signs like heart rate, oxygen saturation (SpO), and body temperature is key
Identify applicable funding agency here. If none, delete this.

to spotting serious health issues early. However, many tradi- tional hospital monitoring systems depend on wired devices and manual oversight, which limit patient movement and delay urgent medical intervention. Identify applicable funding agency here. If none, delete this. Patients also face challenges when navigating large hospital buildings. Elderly, disabled, and newly admitted patients often struggle to find departments, labs, and wards in multi-floor hospitals where GPS signals do not work well. This confusion slows down treatment and increases reliance on hospital staff for help. At the same time, adding IoT to healthcare has raised significant cybersecurity concerns. Medical Wireless Sensor Networks (WSNs) send sensitive physiological data through wireless channels, making them targets for attacks like spoofing, replay, data injection, and tampering. If attackers manipulate patient data, it can lead to wrong diagnoses, breaches of privacy, and serious health

risks. Therefore, maintaining secure communication and data integrity in wearable healthcare devices is as crucial as monitoring health. To tackle these issues, MediShield IDS has been proposed as an IoT-enabled smart wearable band that combines real-time health monitoring, indoor navigation, and intrusion detection into one system. The device utilizes biomedical sensors linked to an ESP32 microcontroller for continuous measurement of vital signs. Bluetooth Low En- ergy (BLE) beacons help with indoor positioning, guiding patients safely within the hospital. Secure data transmission relies on encryption, device authentication, and the MQTT protocol. Additionally, a Django-based cloud dashboard allows healthcare professionals to monitor patient vitals and locations remotely. MediShield IDS not only boosts patient safety and mobility but also protects sensitive medical data from cyber threats. By integrating wearable sensors, navigation support, and cybersecurity features into one system, it offers a scalable and effective solution for today's smart healthcare environ- ments.

II. MEDICAL WSN AND IOT ECOSYSTEM

Medical Wireless Sensor Networks (WSNs) are essential for IoT-based healthcare monitoring systems. These networks include various biomedical sensors that are placed on or around a patient's body to continuously collect physiological data. In MediShield IDS, sensors like MAX30100 for heart rate and SpO, DS18B20 for body temperature, and MPU6050 for motion tracking gather critical health information. These sensors produce real-time data that needs to be processed, transmitted, and stored securely.

Medical sensor data has distinct features compared to other IoT data streams. First, it is time-sensitive; any delays in data transmission can influence medical decisions. Second, the data is continuous and high-frequency, so it requires efficient processing and communication. Third, it is very sensitive to privacy concerns, as unauthorized access to this data breaches patient confidentiality. Finally, this data comes from resource- limited devices like ESP32, which have restricted processing power and memory.

The wireless nature of communication in medical WSNs introduces several security threats. Spoofing attacks occur when harmful devices impersonate real sensor nodes and send false information. Replay attacks happen when previously captured data is resent to trick the system. Injection attacks add fake data packets to the network. Tampering attacks change real data during transmission. These threats can endanger patient safety if not properly managed.

MediShield IDS addresses these threats with multiple se- curity layers. Device authentication ensures that only regis- tered sensors can transmit data. Timestamp validation helps stop replay attacks. MQTT validation and encryption protect against injection and tampering. These measures create a secure environment where sensor data can be trusted for medical decision-making.

A. Role of Biomedical Sensors in Medical WSN

Biomedical sensors are the basic parts of a medical wireless sensor network (WSN). These sensors keep track of important physiological parameters needed to assess patient health. In MediShield IDS:

- MAX30100 measures heart rate and oxygen saturation (SpO) - DS18B20 measures body temperature - MPU6050 detects patient movement and falls

These sensors produce real-time data streams that need efficient processing and secure transmission. Since the data is continuous and time-sensitive, any delay or corruption can result in wrong medical decisions. Therefore, reliable data collection is crucial in the medical WSN.

B. Characteristics of Medical IoT Data

Medical sensor data is quite different from typical IoT data because healthcare applications are critical. Unlike general IoT systems that can handle delays, medical data is very time- sensitive. It needs to be sent quickly for prompt diagnosis and emergency response. A small delay in transmitting abnormal

vital signs, like irregular heart rates or low oxygen levels, can put patient safety at risk.

Additionally, medical data is generated continuously. Wear- able devices monitor vital signs without interruption. This data is also very sensitive because it contains private patient information that needs protection from unauthorized access. Moreover, this data comes from low-power, resource-limited wearable devices, which have limited battery life and process- ing power.

Because of these unique features, medical IoT systems need lightweight communication protocols, efficient data processing methods, and strong security measures to ensure reliability, privacy, and ongoing healthcare monitoring.

C. Security Threats in Medical WSN

Medical wireless sensor networks face many cyber threats because they depend on wireless communication to send sensitive patient data. In hospitals, this allows attackers to take advantage of network weaknesses. For instance, in a spoofing attack, a fake sensor node can send false health readings to the system. In replay attacks, attackers resend previously captured data packets to mislead the monitoring platform. Injection attacks involve adding harmful data to the network, while tampering attacks change real data during transmission.

These attacks can put patient safety at risk, disrupt medical decisions, and breach data privacy. To combat these threats, MediShield IDS includes strong security measures. These measures consist of device authentication, timestamp valida- tion to prevent replay attempts, encrypted communication for safe transmission, and integrity checks to ensure that data stays accurate and unchanged.

D. Integration of IoT, Cloud, and Dashboard

The IoT ecosystem of MediShield IDS connects the wear- able device to a cloud server using the MQTT protocol. The cloud processes and stores data securely and displays it on a Django-based dashboard. Healthcare professionals can monitor patient vitals, receive alerts, and track patient location in real time. This integration creates a complete smart healthcare IoT ecosystem that provides monitoring, mobility, and security.

III. SECURITY AND COMMUNICATION FOUNDATIONS

Security and reliable communication are essential for IoT- based medical wearable systems. Since MediShield IDS op- erates in a medical Wireless Sensor Network (WSN) environ- ment, it must ensure confidentiality, integrity, authentication, and real-time delivery of patient data. The ESP32 wearable device has limited resources, which calls for lightweight and effective security measures. This section explains the commu- nication model and security techniques used in MediShield IDS.

A. Lightweight Cryptographic Techniques for Wearable De- vices

Wearable IoT devices like the ESP32 have limited memory, processing power, and battery life. Because of this, complex encryption methods are not a good fit. MediShield IDS uses lightweight AES, or Advanced Encryption Standard, to secure sensor data before it is sent. AES keeps data private while using few computing resources.

Furthermore, hashing techniques are used to check data integrity. Each data packet created by the ESP32 has a hash value that is checked at the cloud server. If any changes happen during transmission, a difference in hash values shows tampering.

B. Device Authentication and Identity Verification

One major threat in medical WSN is spoofing. In this case, harmful devices pretend to be real sensors. To stop this, MediShield IDS gives each wearable unit a unique device ID and authentication key. The cloud server checks the device's legitimacy before accepting any data pack- ets. This process ensures that only authorized wearable devices can communicate with the server. As a result, it eliminates attacks from fake sensor nodes.

C. Secure MQTT Communication Protocol

MQTT (Message Queuing Telemetry Transport) is the com- munication protocol between the ESP32 wearable device and the cloud server in the MediShield IDS system. MQTT is ideal for IoT applications because it uses a simple publish and subscribe model. The device publishes sensor data,

and the cloud server subscribes to receive it. This method allows for smooth and real-time data exchange, even with limited network bandwidth.

In MediShield IDS, the patient's vital signs are formatted in JSON and sent through encrypted MQTT channels for security and privacy. The protocol ensures reliable message delivery, meaning important medical data does not get lost during transmission. It is also made for low power use, which is crucial for wearable devices that run on batteries. Additionally, MQTT reduces network overhead, making communication quick and efficient.

By using MQTT, the system provides secure, lightweight, and continuous health monitoring. This ensures timely medical updates and better patient care.

D. BLE-Based Secure Indoor Communication

Bluetooth Low Energy (BLE) beacons are commonly used for indoor positioning systems, especially in complex places like hospitals, where reliable location tracking is crucial. BLE technology allows for low-power wireless communication. This enables beacon devices to run for long periods on small batteries without needing frequent maintenance. This feature makes them very suitable for continuous indoor monitoring, including patient tracking, asset management, and navigation assistance.

In a typical setup, BLE beacons are installed at fixed spots throughout the building. An ESP32 microcontroller scans for nearby beacon signals and measures their Received Signal Strength Indicator (RSSI) values. By comparing signal strengths from several beacons, the system can estimate a patient's location using methods like proximity detection or trilateration. This allows for real-time tracking and helps hospital staff quickly find patients, equipment, or restricted areas.

BLE communication typically works over short distances, usually from a few meters to several tens of meters indoors. This limited range reduces the chance of external interception or unauthorized access. Additionally, BLE includes basic security features such as device addressing and encrypted com- munication, which improves data protection. As a result, BLE beacons offer a safe, energy-efficient, and effective solution for indoor navigation and positioning in healthcare settings.

E. Cloud Security and Data Protection

The cloud server uses the Django framework, which provides a strong and scalable platform for managing sensitive healthcare data. Django includes built-in secu- rity features to protect against SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). This makes it a good choice for medical applications. Patient data is kept in a secure database with appropriate access controls to prevent unauthorized use. Access to the cloud-based dashboard is tightly controlled through authentication and authorization processes. Only verified doctors and authorized hospital staff can log in with secure credentials. This ensures that patient information is only available to approved personnel. Role-based access control can also restrict users to viewing or modifying only the data relevant to their duties. All incoming data packets from monitoring devices are checked for integrity and authenticity before being saved in the database. This process helps stop data tampering, duplication, or the injection of false information. Encryption techniques can protect data during transmission and storage to improve confidentiality. Historical patient data is securely archived for long-term medical analysis, trend evaluation, and diagnostic support, while following privacy regulations and maintaining strict patient confidentiality.

F. Intrusion Detection and Alert Mechanism

MediShield IDS is built with an intelligent system that detects anomalies by constantly monitoring sensor data and communication behavior within the medical wireless sensor network. Normally, patient data and device communication follow predictable patterns. Any sudden change, like unusual sensor readings, unexpected traffic, or data mismatches, is seen as a potential threat or abnormal event.

When the system detects these irregularities, it immediately generates alerts and shows them on the

monitoring dashboard. This helps doctors and hospital staff respond quickly, whether

the issue involves a possible cyber intrusion, device malfunc- tion, or a critical change in a patient's health. Real-time alerts cut down response time and improve overall patient safety.

As an Intrusion Detection System (IDS), MediShield IDS adds an important layer of security to the medical wireless sensor network. It protects sensitive medical data from cyber threats, such as data tampering or unauthorized access, while also aiding in the early detection of abnormal patient con- ditions. This dual-purpose approach improves both network security and healthcare reliability.

G. Protection Against Common Medical WSN Attacks

MediShield IDS protects medical wireless sensor networks (WSNs) used in smart healthcare environments from common security threats. The system continuously transmits sensitive patient data and actively monitors communication patterns to detect attacks like data spoofing, packet modification, replay attacks, and unauthorized access. It identifies any abnormal be- havior or integrity mismatch in real-time and immediately flags them on the dashboard. By combining device authentication, encrypted communication, and anomaly detection, MediShield IDS ensures reliable data transmission and prevents malicious interference. This protection is crucial for maintaining accu- rate health monitoring, patient safety, and trust in wearable healthcare systems.

H. Figures

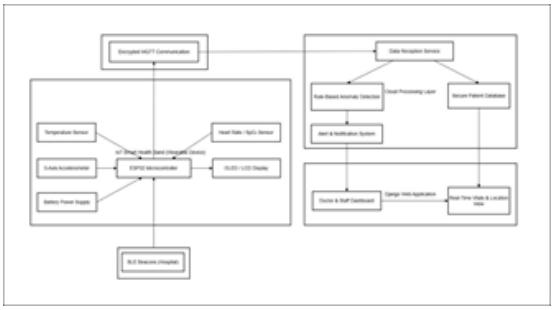

Fig. 1. Proposed MEDISHIELD I Architecture

IV. PROPOSED MEDISHIELD IDS ARCHITECTURE

The MediShield IDS architecture is structured as a layered IoT healthcare framework. It combines wearable sensing, secure communication, indoor navigation, cloud processing, and real-time visualization into one system. This setup ensures continuous monitoring of patient vitals and tackles significant cybersecurity issues in medical Wireless Sensor Networks (WSNs). Its modular design allows for scalability and straight- forward deployment in large hospital settings, enabling the monitoring of multiple patients at the same time.

A. Sensor Layer – Biomedical Data Collection

The Sensor Layer collects real-time physiological data from the patient using biomedical sensors built into the wearable band. In MediShield IDS, multiple sensors work together to monitor different health parameters. The MAX30100 sensor measures heart rate and blood oxygen saturation (SpO). This provides vital information about cardiovascular and respira- tory health. The DS18B20 sensor tracks body temperature accurately, which helps detect fever or unusual temperature changes. Additionally, the MPU6050 accelerometer and gy- roscope module monitors body movement and aids in fall detection. This feature is especially important for elderly or high-risk patients.

These sensors continuously observe the patient's condition and generate time-sensitive data that must be sent immediately. Since the system works in real time, even small abnormalities can be detected early. The collected sensor data is then sent to the ESP32 microcontroller. There, it gets processed, formatted, and prepared for secure transmission to the cloud server for further monitoring and analysis.

B. ESP32 Processing Layer – Local Data Processing

The ESP32 microcontroller serves as the central processing unit of the MediShield IDS wearable device. It acts as a link between the sensor layer and the cloud communication layer, making sure that all collected physiological data is handled properly before being sent. Once the biomedical sensors capture the patient's vital signs, the ESP32 reads the

raw sensor values and checks them to confirm they are within acceptable ranges.

To improve accuracy, the microcontroller filters out noise and unwanted fluctuations from the raw data. This step is cru- cial because biomedical sensors can sometimes produce small variations due to movement or environmental factors. After cleaning the data, the ESP32 organizes it into a structured JSON format, which makes it easy to send and understand on the cloud server.

Finally, the microcontroller prepares secure data packets for encrypted transmission using MQTT. By processing in- formation efficiently at the device level, the ESP32 reduces communication delays, cuts down on power consumption, and maintains high data accuracy, making sure real-time health monitoring is reliable.

C. Secure Communication Layer – Encryption and MQTT Protocol

In this layer of the MediShield IDS system, strong security measures are applied before any patient data is transmitted to the cloud. Since medical information is highly sensitive, it is first protected using AES encryption, ensuring that even if the data is intercepted, it cannot be read without the proper decryption key. This protects patient privacy during wireless communication.

To further enhance security, a hash value is generated for each data packet. This hash helps verify data integrity, ensuring that the information has not been altered during transmission.

Device authentication credentials are also attached to each packet, allowing the cloud server to confirm that the data is coming from a trusted and registered wearable device.

Finally, the encrypted and verified data is transmitted using the MQTT publish–subscribe protocol. By combining encryp- tion, integrity checks, and authentication, this layer effectively defends against spoofing, replay, injection, and tampering attacks, ensuring secure and reliable health monitoring.

D. BLE Navigation Layer – Indoor Position Tracking

BLE beacons installed in the hospital send out signals that the ESP32 can detect. The system estimates the patient's indoor location based on signal strength (RSSI). This feature helps with navigation in places where GPS signals are not available.

The location data is sent to the cloud for monitoring, along with health data.

E. Cloud Processing Layer – Data Validation and Storage

The cloud layer in MediShield IDS is built using a Django- based server connected to a secure database, forming the backbone of the remote monitoring system. Once data is received from the wearable device, the server first verifies the device's authentication credentials to ensure the information is coming from a trusted source. It then checks the hash values attached to each data packet to confirm that the data has not been altered during transmission.

After successful verification, the patient's sensor readings and location information are securely stored in the database for real-time access and future medical analysis. The system continuously analyzes incoming data by comparing it with predefined medical thresholds. If any vital signs, such as heart rate, temperature, or oxygen levels, fall outside the normal range, the system immediately identifies them as abnormal.

When such conditions are detected, alerts are generated and displayed on the dashboard, enabling doctors and hospital staff to respond quickly. This ensures both patient safety and reliable health monitoring.

F. Visualization Layer – Dashboard and Alert Interface

The Visualization Layer offers an easy-to-use web dash- board for doctors and hospital staff. It shows real-time pa- tient vital signs such as heart rate, body temperature, and oxygen levels, allowing for continuous remote monitoring. The dashboard also alerts medical professionals whenever it detects

abnormal readings, enabling quick responses to potential health emergencies.

Additionally, the system displays the patient's indoor lo- cation within the hospital, making it simpler to track and assist them when needed. Historical health data is available for review, supporting better medical decisions. Overall, this layer helps healthcare professionals monitor patients effectively from a distance and take timely action.

G. Data Flow Mechanism

The overall data flow in MediShield IDS follows this sequence:

Sensors, ESP32, Encryption, MQTT, Cloud, Database, Dashboard, Alerts.

This clear flow ensures reliable, secure, and real-time mon- itoring throughout the system.

V. SECURITY METHODOLOGY

Security is crucial in Medical Wireless Sensor Networks (WSNs) because sensitive physiological data is constantly sent over wireless channels. Any breach of this data can lead to misinterpretation of a patient's condition, privacy violations, and serious safety risks. Unlike general IoT systems, health- care monitoring systems handle real-time data that can affect lives, which requires stronger protection methods.

MediShield IDS uses a multi-layered security approach to ensure confidentiality, integrity, authentication, secure trans- mission, and intrusion detection while working within the hardware limits of the ESP32 wearable device. The security process starts when sensor data is collected and continues until the data is safely stored and displayed on the cloud dashboard. Each step in the system has specific protections against common cyber threats like spoofing, replay attacks, injection, tampering, and unauthorized access.

A. Secure Data Acquisition and Preprocessing

The security process starts with data acquisition. Biomedical sensors continuously generate raw physiological readings. These readings may have noise or inconsistent values because of environmental factors or limitations of the sensors. Before sending this data, the ESP32 conducts preprocessing tasks like filtering out noise, checking sensor values, and formatting the readings into standard JSON.

This preprocessing stage matters because it makes sure that only valid and consistent data goes into the communication channel. By removing irregular readings early on, the system lowers the chances of false alerts and stops attackers from taking advantage of sensor noise to introduce misleading data into the network.

B. Data Confidentiality Using AES Encryption

To protect patient data from eavesdropping and interception, MediShield IDS uses AES (Advanced Encryption Standard) encryption for every data packet before transmission. AES is chosen because it offers strong security with low computa- tional demands, making it ideal for devices like the ESP32 that have limited resources. Once the sensor data is converted to JSON format, it is encrypted with an AES key that is stored securely on the device. Even if an attacker intercepts the wireless transmission, they cannot interpret the encrypted data without the decryption key. This keeps important information such as heart rate, SpO levels, temperature, and motion data private throughout transmission.

C. Data Integrity Verification Through Hashing

Maintaining the integrity of medical data is just as important as keeping it confidential. MediShield IDS creates a hash value for each encrypted data packet before it is sent. This hash serves as a digital fingerprint for the data.

When the cloud server receives the packet, it recalculates the hash and compares it with the one that was sent. If any part of the data has changed during transmission, the difference in hash values quickly shows that tampering has occurred. This system defends against data modification attacks and ensures that healthcare professionals get reliable and accurate information.

D. Device Authentication and Identity Verification

Spoofing is one of the most dangerous attacks in medical wireless sensor networks. An attacker creates a fake device that sends false medical readings. To prevent this, each MediShield wearable device gets a unique device ID and authentication key during startup.

Whenever the ESP32 tries to send data to the cloud server, it checks these credentials. If the authentication fails, the server rejects the data packet. This process ensures that only autho- rized wearable devices can communicate within the network. It eliminates the chance of fake sensor nodes.

E. Secure MQTT Communication Channel

MediShield IDS uses MQTT for communication between the wearable device and the cloud server. MQTT is lightweight and works well for IoT applications that need real-time data transfer with low bandwidth usage.

Before sending data to MQTT topics, the data is encrypted and includes authentication details. The cloud server sub- scribes to these topics and checks the authenticity of each message. This secure publish and subscribe model stops harm- ful packet injection and ensures reliable data delivery with minimal delay.

F. Timestamp Validation to Prevent Replay Attacks

Replay attacks occur when an attacker captures valid data packets and resends them later to mislead the system. MediShield IDS prevents this by attaching a timestamp to every data packet.

The cloud server checks if the received timestamp is recent. If it detects an old or duplicate packet, it discards it immedi- ately. This ensures that only fresh, real-time data is used for monitoring and analysis.

G. Secure BLE Communication for Indoor Navigation

BLE beacons help with indoor positioning when GPS sig- nals are not available. BLE communication operates over short distances, reducing the risk of long-range attacks. The ESP32 scans only registered beacon IDs and ignores unrecognized signals.

This process of validating beacons prevents attackers from adding fake beacons to alter the patient's location data. As a result, indoor navigation stays accurate and secure.

H. Intrusion Detection Through Anomaly Monitoring

In addition to encryption and authentication methods, MediShield IDS includes an intelligent intrusion detection system (IDS) to improve overall security. This system continu- ously monitors patient health data and network communication patterns to spot any unusual or suspicious activity. It checks if sensor readings go beyond normal medical thresholds, which could indicate a sudden health crisis or possible data manipulation.

The system also tracks sudden irregular transmission pat- terns, like unexpected spikes in data traffic or unusual com- munication frequency. It flags integrity mismatches detected through hashing right away, as these may suggest tampering or unauthorized changes to data. Additionally, any odd device behavior, like an unregistered node trying to communicate, is seen as a possible security threat.

When the system detects such anomalies, it quickly gener- ates alerts on the dashboard for hospital staff. This real-time intrusion detection not only boosts network security but also ensures a quick medical response, safeguarding both patient safety and data integrity.

I. Protection Against Common Cyber Threats

MediShield IDS is specifically made to protect against com- mon attacks in medical WSN environments. It prevents spoof- ing through device authentication. Replay attacks are stopped with timestamp validation. Injection attacks are avoided by using MQTT validation and encryption. Tampering is detected through hash integrity checks. Eavesdropping is blocked with AES

encryption. Unauthorized access to the dashboard is limited by login authentication.

Each security method works together to build strong pro- tection around the wearable healthcare system.

J. Secure Cloud Storage and Dashboard Access Control

The cloud server uses the Django framework and is linked to a secure database. Before it stores data, the server checks authentication credentials, integrity values, and timestamps.

Only authorized doctors and hospital staff can access patient data through login authentication. Historical data is stored securely for future medical analysis while keeping patient privacy intact. This protects sensitive health information even after transmission.

VI. RESULTS AND DISCUSSION

The MediShield IDS prototype was designed and implemented using ESP32, biomedical sensors, BLE beacons, MQTT communication, and a Django-based cloud dashboard. The main goal was to see if a wearable device could monitor health in real-time, securely transmit data, navigate indoors, and detect intrusions in a hospital setting. The results show that combining these components into a single healthcare monitoring system is feasible, reliable, and effective.

During implementation, the biomedical sensors connected to the ESP32 microcontroller to measure heart rate, oxygen saturation (SpO), body temperature, and patient movement.

The sensor readings were collected regularly and processed by the ESP32. Noise filtering and validation techniques made sure the data sent to the cloud was consistent and correct. The system continuously captured vital signs without significant delay, demonstrating that wearable monitoring is practical for real-time healthcare.

Communication between the ESP32 and the cloud server used the MQTT protocol. Sensor data was converted to JSON format, encrypted with AES, and securely published to the MQTT broker. The cloud server subscribed to the MQTT topics and received the data in real-time. The encrypted channel prevented unauthorized interception, and data integrity was checked using hash values. During testing, attempts to alter transmitted data led to integrity mismatches, which the system successfully detected, proving the security mechanisms worked.
BLE beacons were placed at various indoor locations to mimic a hospital environment. The ESP32 continuously scanned for beacon signals and calculated the patient's indoor position based on signal strength. The system successfully de- termined the patient's approximate location within the building and sent this information along with health data to the cloud dashboard. This showed that BLE-based navigation is a good solution for indoor positioning where GPS is not available.

The Django-based dashboard displayed real-time patient vitals, alerts, and indoor location clearly. Healthcare staff could monitor multiple parameters at once and get notifications for abnormal readings. Threshold values were set for heart rate, SpO, and temperature. When these values exceeded the limits, the system generated immediate alerts on the dashboard. This indicates that the system can support timely medical intervention during emergencies.

From a security standpoint, MediShield IDS showed strong resistance against common medical WSN attacks. Device authentication ensured that only registered wearable devices could send data to the server. Timestamp validation helped to prevent replay attacks by rejecting old packets. AES encryp- tion safeguarded patient data, while hash verification ensured data integrity. These mechanisms together created a secure communication environment suitable for healthcare.

Integrating health monitoring, indoor navigation, and cy- bersecurity into one system proved to be very effective. The system kept low power consumption, making it suitable for wearables. The MQTT protocol ensured minimal bandwidth usage while providing reliable communication. The modular structure allows for easy expansion to

monitor multiple pa- tients across different hospital wards.

However, some limitations were noted during testing. The accuracy of BLE-based indoor positioning relies on beacon placement and density. Environmental barriers like walls and electronic interference can impact signal strength. Addition- ally, continuous wireless communication needs a stable net- work for real-time dashboard updates.
Overall, the results confirm that MediShield IDS is a feasi- ble and efficient solution for smart healthcare monitoring. The system not only allows continuous monitoring of vital signs

but also ensures data security and patient mobility in hospital environments. The blend of IoT, BLE navigation, and intrusion detection makes the system suitable for modern healthcare infrastructure that requires both reliability and security.

VII. CONCLUSION AND FUTURE WORK

The MediShield IDS system was created to build a secure, wearable healthcare monitoring framework. It performs real- time vital sign monitoring, indoor patient navigation, and intrusion detection within a Medical Wireless Sensor Network (WSN). As the use of IoT devices in healthcare grows, it brings important security and privacy challenges, especially when sensitive physiological data is sent over wireless channels. MediShield IDS tackles these issues by combining biomedical sensing, secure communication methods, BLE-based indoor positioning, and cloud-based visualization into one cohesive system.

The system uses ESP32, MAX30100, DS18B20, MPU6050, BLE beacons, the MQTT protocol, AES encryption, hashing techniques, and a Django-based dashboard. This shows that a lightweight yet secure healthcare monitoring system can be developed for hospitals. The layered architecture protects each step of the data flow—from sensing to visualization—using security measures like encryption, authentication, integrity checks, and anomaly detection.

Prototyping results confirm that MediShield IDS can con- tinuously monitor patient vitals with minimal delay while keeping the transmitted data confidential and intact. The system effectively prevents common cyber threats like spoof- ing, replay attacks, injection, tampering, and unauthorized access. Additionally, using BLE beacons for indoor navigation addresses patient tracking issues in areas where GPS does not work well. The dashboard interface offers healthcare professionals real-time information and alerts, allowing them to respond quickly when abnormal conditions arise.

MediShield IDS has a modular design, making it scalable for monitoring multiple patients across different hospital de- partments. Using MQTT keeps bandwidth usage low, while the ESP32 is an energy-efficient option for wearables. Overall, the system shows that secure IoT-based healthcare monitoring is practical and effective in modern smart hospitals.
Despite its successful deployment, there are limitations. The accuracy of BLE-based positioning relies on beacon placement and environmental conditions. Continuous wireless communication needs stable network connectivity. Also, the current intrusion detection method is based on rules and could be improved with smarter detection techniques.

Future work could extend the system by adding more biomedical sensors, such as ECG and blood pressure monitors, for broader health analysis. Machine learning algorithms could be included in the cloud layer to predict health issues and recognize complex intrusion patterns. The BLE navigation system might benefit from better localization techniques for improved accuracy. Support for mobile applications could enable doctors to monitor patients remotely via smartphones. Moreover, testing on a larger scale in real hospital settings could help assess its performance with multiple wearable devices at the same time.

With these improvements, MediShield IDS could develop into a comprehensive smart healthcare security framework, ensuring safe, reliable, and

intelligent patient monitoring in IoT-enabled medical environments.

Acknowledgment

We want to thank everyone who helped make the MediShield IDS project and this research work successful. This project wouldn't have been possible without the ongoing support, guidance, and encouragement from many people and organizations.

First, we thank our respected institution, Toc H Institute of Science and Technology, for giving us the opportunity, resources, and learning environment we needed to carry out this work. The college provided essential facilities, including laboratory resources and technical support, which were key in implementing and testing our prototype.

We deeply appreciate our project guide and faculty mentors for their valuable guidance, helpful suggestions, and constant motivation throughout this project. Their technical insights, en- couragement, and timely feedback helped us turn our concept into a practical solution. Their support was crucial in helping us understand the challenges in medical IoT security and in refining the MediShield IDS architecture.

We also thank the faculty members of the Computer Science and Engineering department for their support and for providing the academic knowledge needed to grasp concepts related to Wireless Sensor Networks, IoT, cybersecurity, and cloud computing, which form the foundation of this project.

Our sincere thanks go to our friends and classmates who assisted us during the development and testing phases. Their help in testing the wearable prototype, dashboard features, and BLE positioning setup allowed us to validate the system in a real-world setting.

Additionally, we acknowledge the developers and contribu- tors of open-source platforms, tools, and libraries like ESP32 frameworks, MQTT services, Django framework, and sensor libraries, which greatly supported the implementation of this project. Without these resources, creating a complete working prototype within the set timeframe would have been very difficult.

Finally, we thank our families for their constant encourage- ment, patience, and moral support during this project. Their belief in us gave us the confidence to complete this research successfully.

We are grateful to everyone who contributed, directly or indirectly, to the completion of the MediShield IDS project and this research paper.

REFERENCES

1. D. V. Dimitrov, "Medical Internet of Things and Big Data in Healthcare," Healthcare Informatics Research, vol. 22, no. 3, pp. 156–163, Jul. 2016.
2. M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos, and S. Andreescu, "Health Monitoring and Management Using Internet-of-Things Sensing with Cloud-Based Processing," in Proc. IEEE Int. Conf. Services Computing (SCC), 2015, pp. 285–292.
3. S. Hamrioui and P. Lorenz, "Efficient Wireless Mobile Networks Com- munications Applied to E-Health," in Proc. IEEE Int. Conf. Communi- cations (ICC), 2017, pp. 1–7.
4. J. Wan, S. Tang, Z. Yan, D. Li, R. Wang, and S. Wang, "A Manufacturing Big Data Solution for Active Preventive Maintenance," IEEE Trans. Ind. Informat., vol. 13, no. 4, pp. 2039–2047, Aug. 2017.
5. K. Ashton, "That 'Internet of Things' Thing," RFID Journal, vol. 22, no. 7, pp. 97–114, Jun. 2009.
6. A. B. M. Alim Al Islam and M. S. Amin, "A Study on MQTT: A Protocol of Internet of Things (IoT) for Better Quality of Service," in Proc. IEEE SmartTech Con. (SmartTech), 2019, pp. 1–6.
7. S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time Intrusion Detection in the Internet of Things," Ad Hoc Networks, vol. 11, no. 8, pp. 2661–2674, Nov. 2013.
8. H. Ning and H. Liu, "Cybersecurity and Privacy in Cyber-Physical Sys- tems: Challenges and Opportunities," IEEE Trans. Dependable Secure Comput., vol. 15, no. 5, pp. 1070–1080, Sep.–Oct. 2018.

9. M. Z. A. Bhuiyan, M. Atiquzzaman, and S. T. Vuong, "A Survey on Internet of Things Security: Challenges and Solutions," IEEE Commun. Surv. Tuts., vol. 22, no. 1, pp. 616–644, Firstquarter 2020.
10. J. K. Zao, X. Wang, and J. Li, "Indoor Localization Techniques Based on BLE for IoT Applications," IEEE Internet Things J., vol. 7, no. 10, pp. 9715–9725, Oct. 2020.
11. P. N. Pathirana, "Security Issues for MQTT Based IoT Communica- tions," IEEE Internet Technol. Newsl., vol. 22, no. 2, pp. 12–16, Jun. 2020.
12. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The ROADmap," Computer Networks, vol. 76, pp. 146–164, Jan. 2015.
13. F. Al-Turjman and M. Malekloo, "Security and Privacy for IoT Based Smart Systems: Challenges and Opportunities," Future Generation Comp. Syst., vol. 92, pp. 1008–1021, Oct. 2019.
14. J. Pan, R. Jain, S. Paul, and T. Vu, "Anomaly Detection in Medical IoT Networks Using Machine Learning: A Survey," IEEE Access, vol. 8, pp. 103346–103371, 2020.
15. R. Roman, J. Zhou, and J. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.