Volume 11, Issue 3, March – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1553

A Secure and Intelligent IoT-AI Framework for Real-Time Medical Diagnosis and Smart Pharmaceutical Dispensing with Cloud-Based Mobile and Web Access

R. Anandhi, M. E.[1]; Bhuvaneswari M.[2]; Dharshini S.[3]; Dhansika R.[4]

[1]Assistant Professor; Department of Information Technology Panimalar Engineering College Chennai, India
[2]Department of Information Technology Panimalar Engineering College Chennai, India
[3]Department of Information Technology Panimalar Engineering College Chennai, India
[4]Department of Information Technology Panimalar Engineering College, Chennai, India

Publication Date: 2026/03/31

Abstract: In order to facilitate real-time medical diagnosis, ongoing patient monitoring, and automated medication dispensation via mobile and web platforms, this study proposes a safe and intelligent IoT-AI-cloud-based healthcare system. The device's IoT-enabled clinical sensors capture vital health signs, such as body temperature, oxygen saturation levels, and cardiovascular activity (SpO_2). The data is safely transferred to the cloud's storage and processing environment. In order to detect abnormal trends, produce early warning alarms, and provide personalized diagnostic results, sophisticated neural networks and machine learning techniques are used to evaluate both historical and current health data. A smart pharmaceutical dispensing machine improves treatment adherence while reducing manual supervision and dosage errors by automatically delivering precise medicine dosages at predetermined intervals based on the analytical results. Mobile and web applications that show real-time health indicators, diagnostic results, prescription regimens, and alert notifications allow healthcare providers and caregivers to remotely monitor patient status. The framework uses identity, secure role-based surveillance methods, and encrypted communication to guarantee privacy and secure processing of sensitive medical data. The proposal offers a flexible and intelligent healthcare solution that improves diagnostic precision, permits proactive medical intervention, and fosters the development of next- generation linked healthcare services.

Keywords: *Cloud-Based Health Analytics, Automated Medication Dispensing, Biomedical Sensor Networks, Internet of Things (IoT), Artificial Intelligence, Remote Patient Monitoring, Smart Healthcare Systems, and Healthcare Data Security.*

How to Cite: R. Anandhi, M. E.; Bhuvaneswari M.; Dharshini S.; Dhansika R. (2026) A Secure and Intelligent IoT-AI Framework for Real-Time Medical Diagnosis and Smart Pharmaceutical Dispensing with Cloud-Based Mobile and Web Access. *International Journal of Innovative Science and Research Technology,* 11(3), 2632-2641. https://doi.org/10.38124/ijisrt/26mar1553

I. INTRODUCTION

Conventional healthcare systems are being transformed into data-driven, smart, and linked environments by the rapid expansion of virtualization, artificial intelligence (AI), and the Internet of Medical Things (IoMT).Ongoing monitoring, early disease identification, and prompt medical action are essential components of modern healthcare, particularly for patients with chronic illnesses, the elderly, and those in need of long-term care. However, the cornerstones of traditional healthcare models—physical supervision and few hospital stays—can result in medication non-adherence, delayed diagnosis, and higher healthcare expenses.

Recent developments in wearable and Internet of Things-enabled biomedical sensors have made it possible to assess blood oxygen saturation (SpO_2), body temperature, and heart rate in real time.These technologies generate vast amounts of health data, but the real issue lies in transforming this raw data into practical therapeutic ideas.In this situation, machine learning and artificial intelligence (AI) methods are essential for spotting anomalies, anticipating possible health hazards, and assisting with early diagnosis.

High processing power, scalable storage, and universal access to medical data are other benefits of cloud-based healthcare solutions. Integrating IoMT devices with cloud and AI technology enables smart decision-making and remote patient monitoring outside of hospital boundaries. Healthcare providers and caregivers can access patient data at any time using mobile and online applications, facilitating faster emergency response times and better treatment.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1553

Medication management is another important topic in healthcare. Inadequate scheduling, skipped doses, and dosage issues can all have a significant negative influence on treatment outcomes. Smart pharmaceutical distribution systems may automate prescription scheduling and dispensing, ensuring accurate dosages and improving patient adherence while reducing human error, when paired with AI-driven diagnostic insights.

This paper proposes a Safe and Intelligent IoT-AI Framework for Smart Pharmaceutical Dispensing and Real-Time Medical Diagnosis with Cloud-Based Mobile and Web Access in response to these challenges. The proposed system includes a smart automated medication dispenser for treatment compliance, IoMT sensors for continuous health monitoring, AI models for intelligent diagnosis and early warning, and a secure cloud platform for data storage and remote accessible. By combining sensing, intelligence, automation, and security into a single framework, the system aims to enhance treatment accuracy, enable proactive healthcare, and support next- generation linked medical services.

II. LITERATURE SURVEY

The integration of Internet of Things (IoT), Artificial Intelligence (AI), and cloud computing has attracted considerable attention in modern healthcare systems for enabling intelligent monitoring and remote diagnosis. Various researchers have contributed to multiple aspects of smart healthcare, including data acquisition, analytical processing, security, and medication management. Souri et al. [1] proposed a machine learning-based healthcare monitoring model that utilizes IoT-generated data for diagnosing patient conditions. Their study highlights the importance of combining sensor data with intelligent algorithms to improve diagnostic accuracy. However, the work mainly focuses on predictive models and does not emphasize real-time system integration.Alamsyah et al. [2] developed an IoT-based vital sign monitoring system that captures physiological parameters such as heart rate and body temperature. The system supports continuous monitoring, but it primarily deals with data collection without incorporating advanced decision-making capabilities. Similarly, Swaroop et al. [3] introduced a health monitoring system using IoT devices for real-time tracking of vital signs. Their research demonstrates the effectiveness of IoT in healthcare applications; however, the system lacks integration with intelligent analytics for automated diagnosis.In another study, Raj [4] explored real-time healthcare monitoring using IoT-based information processing techniques. The research emphasizes efficient data handling but provides limited discussion on integrating AI-driven analysis for proactive healthcare. Parisi et al. [5] proposed a hybrid algorithm for predicting disease prognosis using medical datasets. Their approach shows the potential of AI in healthcare analytics, although it is not directly integrated with IoT-based real-time monitoring systems.Further, Mostafa et al. [6] and Jenifer et al. [7] designed IoT-based healthcare monitoring systems capable of continuously collecting patient data. These systems improve accessibility and remote care; however, they rely largely on predefined thresholds and lack adaptive intelligence. A detailed review by Kshirsagar et al. [8] examined various IoT-based healthcare monitoring systems and highlighted challenges related to scalability, efficiency, and security. Similarly, Khan et al. [9] developed and evaluated an IoT-based health monitoring framework, focusing on system performance but with limited emphasis on intelligent automation. Hamim et al.

[10] introduced a remote monitoring system for elderly patients, demonstrating the usefulness of IoT in telemedicine. However, the system mainly functions as a monitoring tool rather than an intelligent decision-support solution.Cloud-based healthcare solutions have been explored by Al-Sheikh et al. [11], who designed a mobile healthcare monitoring system integrating IoT and cloud computing. Their work highlights improved accessibility and storage capabilities but lacks real-time intelligent processing. Similarly, Islam et al.

[12] developed a smart healthcare monitoring system using IoT, focusing on continuous patient monitoring. While effective, the system does not fully utilize AI for predictive analysis.Wearable sensor-based healthcare systems have been proposed by Wu et al. [13], demonstrating the potential of IoT-enabled devices in continuous health tracking. Additionally, Cao et al. [14] introduced emergency healthcare systems for elderly patients, emphasizing remote assistance but lacking automation in treatment processes.

Philip et al. [15] provided a comprehensive review of IoT- based in-home healthcare systems, discussing current advancements and future challenges. Their study identifies issues such as data security, interoperability, and scalability.Gera et al. [16] proposed an IoT-based automated healthcare monitoring system for smart city environments, focusing on urban healthcare applications. However, the integration of AI for intelligent decision-making remains limited.From a security perspective, Lauter et al. [17] and Gentry et al. [18] explored homomorphic encryption techniques for secure data processing. These approaches enable computation on encrypted data, ensuring privacy but increasing computational overhead.Further, Kushala [19] proposed a privacy-preserving healthcare monitoring system using advanced machine learning techniques, emphasizing secure data handling. Similarly, Shivaprakasha et al. [20] implemented secure healthcare data processing using encryption-based approaches. Energy efficiency and IoT network optimization were discussed by Farhan et al. [21], while Alekya et al. [22] presented a review of IoT-based healthcare monitoring systems, identifying gaps in system integration.Sharma et al. [23] developed a secure IoT-based healthcare system focusing on communication security, whereas Rathi et al. [24] proposed an edge AI-enabled healthcare monitoring system to enhance real-time processing.Finally, Alshamrani [25] provided a detailed survey on the integration of AI and IoT in remote healthcare systems, highlighting the need for intelligent, secure, and scalable solutions.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1553

III. EXISTING METHODOLOGY

A multi-layer design comprising sensing, communication, processing, and user interaction is commonly used in current IoT, AI, and cloud-based smart healthcare systems. However, instead of providing a fully automated and integrated healthcare system, most implementations focus on certain characteristics.

- *IoT-Based Patient Monitoring*

These days, vital health data including blood pressure, body temperature, heart rate, ECG, and oxygen levels (SpO_2) are collected via wearable technology and biomedical IoT sensors. These sensors are typically linked to gadgets such as Raspberry Pi, Arduino, or ESP-based modules that facilitate the transmission of the gathered data via Bluetooth or Wi-Fi to a local server or cloud. These systems' primary function is to track a patient's vital signs in real time so that physicians and other medical professionals can readily access the data via dashboards or mobile apps. Nevertheless, the majority of these systems are only capable of gathering and presenting data; they are unable to make wise choices or offer automated medical support.

- *Cloud-Based Health Data Management*

Most existing frameworks use cloud services to store and manage patient health records. Cloud infrastructure enables centralized historical data storage, scalability, and distant accessible. Some systems use cloud services to generate reports and do basic trend analysis of patient vitals over time.Despite these benefits, storing data is the main function of many cloud-based systems.

- *AI/ML for Medical Diagnosis*

Numerous studies use AI and machine learning models to evaluate health data. Among the techniques used to spot anomalies, classify diseases, and predict health risks are neural networks, logistic regression, and support vector machines. These models were trained on past data and can assist medical professionals in diagnosing patients.Nevertheless, realtime IoT streams are not always connected to AI modules in many systems. Medical practitioners frequently have to manually assess the findings rather than initiating automated processes, and the analysis may not be completed right away.

- *Smart Medication Reminder and Dispensing Systems*

Digital pill containers and smart injectors are examples of modern medication devices that use alarms, cellphone notifications, or SMS alerts to remind patients to take their medications on time. Additionally, some sophisticated systems can monitor whether patients are taking their medications as prescribed and provide feedback to caretakers. Nevertheless, the majority of these gadgets operate according to set schedules and do not adapt based on the patient's present state of health or AI-based diagnosis. This restriction prevents them from offering completely automated or tailored care.

- *Security Mechanisms in Existing Systems*

To address privacy concerns, current systems employ password-based authentication for user access and simple encryption techniques (such as SSL/TLS) for data transmission. Some advanced frameworks use multi-factor authentication or blockchain technology for secure record keeping.Despite these efforts, security is sometimes added as a feature rather than a basic component of the design, which may lead to vulnerabilities in device-level communication and access control.

IV. PROPOSED METHODOLOGY

The proposed system introduces a secure and intelligent IoT– AI-based healthcare framework designed for real-time monitoring, analysis, and automated medication dispensing. The architecture integrates IoT-enabled sensors, cloud computing, artificial intelligence, and advanced cryptographic techniques to ensure efficient and privacy-preserving healthcare services.As illustrated in Fig. 1, the system is organized into multiple layers including data acquisition, secure encryption, cloud-based processing, and user interaction. Each layer performs a distinct function while maintaining seamless communication with other components of the system. The data acquisition layer is responsible for capturing real-time physiological signals from patients using sensor devices. The encryption layer ensures that sensitive health information is protected before transmission to the cloud environment. The processing layer applies intelligent algorithms to analyze the data and generate meaningful insights. Finally, the user interaction layer enables healthcare professionals and caregivers to access patient information and receive alerts through mobile and web interfaces.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1553

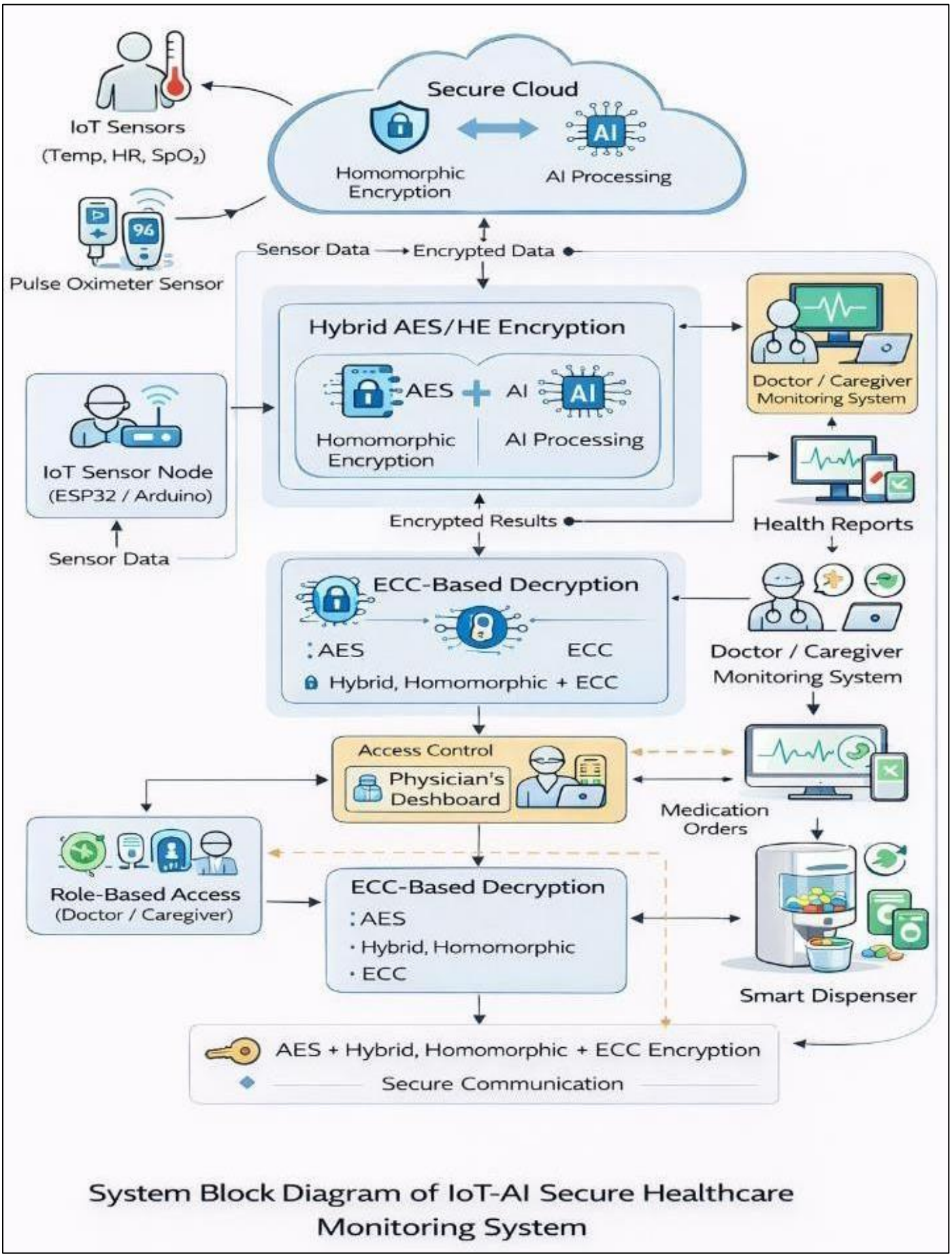

Fig 1 Proposed IoT-AI Smart Healthcare System Architecture

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1553

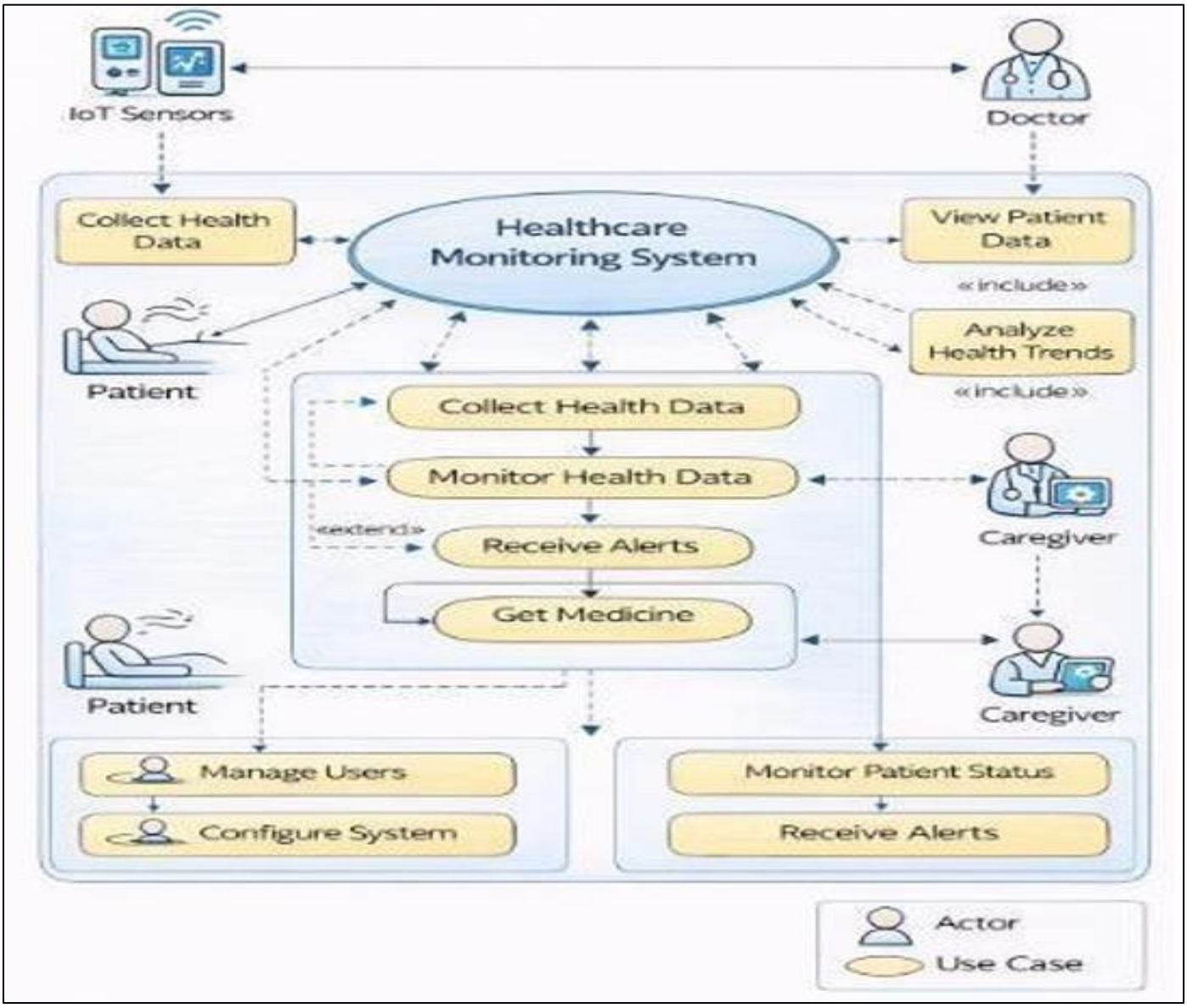

Fig 2 An Illustration of the Proposed Healthcare Monitoring System's use Case

➢ *Data Acquisition and Hybrid Encryption*

The system uses IoT-based biomedical sensors to continuously monitor vital health factors like body temperature, heart rate, and oxygen levels. To protect patient privacy and data, the gathered data is first analyzed and then safely encrypted before being sent. A hybrid encryption technique is employed to preserve both effectiveness and security. AES (symmetric encryption) is used to encrypt vast volumes of health data, and sophisticated cryptographic methods are used to secure the encryption keys.

The encryption process can be represented as: AES_Enc(K,Data)=CiphertextAES_Enc (K, Data) = CiphertextAES_Enc(K,Data)=Ciphertext where:

- KKK represents the session key
- DataDataData denotes the collected health parameters

This approach ensures fast encryption while maintaining strong security.

➢ *Post-Quantum Secure Key Encapsulation (NTRU–Kyber)*

NTRU-Kyber is a secure key exchange technique that guards against hypothetical future risks, such as quantum attacks. Due to its foundation in the intricate mathematical problem known as Ring Learning With Errors (R-LWE), this method is extremely resilient. This technique makes it possible for IoT devices and the cloud server to securely generate and exchange encryption keys. Real-time healthcare applications benefit greatly from the Kyber algorithm's exceptional security and efficiency.

➢ *Secure Cloud Storage and Homomorphic Computation (BGV)*

After encryption, the data is securely transmitted to the cloud, where it is safely stored and processed. To ensure that privacy is maintained even during computation, the system uses the Brakerski–Gentry–Vaikuntanathan (BGV) homomorphic encryption scheme. This technique allows operations to be performed directly on encrypted data without

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1553

revealing the actual information. In this approach, the encrypted data (ciphertext) is represented in the form of a pair, typically written as c=(c0,c1)c = (c_0, c_1)c=(c0,c1) and decryption follows the relation:
Where:

- mmm represents the plaintext data
- sss is the secret key
- qqq is a large modulus

This enables secure operations such as average computation, anomaly detection, and trend analysis directly on encrypted healthcare data without exposing sensitive information.

➢ *AI-Based Health Analysis*

The process for analyzing encrypted health data using AI-based models is illustrated in Fig. 3. In order to identify odd trends and forecast potential health hazards, the system examines both historical data and current data.

A threshold-based condition for alert generation can be expressed as:

Alert={1,if D>T0,otherwiseAlert = begin{cases} 1, & text{if } D>T

0, & text{otherwise} end{cases}Alert={1,0,if D>Totherwise

Where:

- DDD represents the measured health parameter
- TTT denotes the predefined threshold

The AI model enhances this process by detecting complex patterns beyond simple threshold conditions.

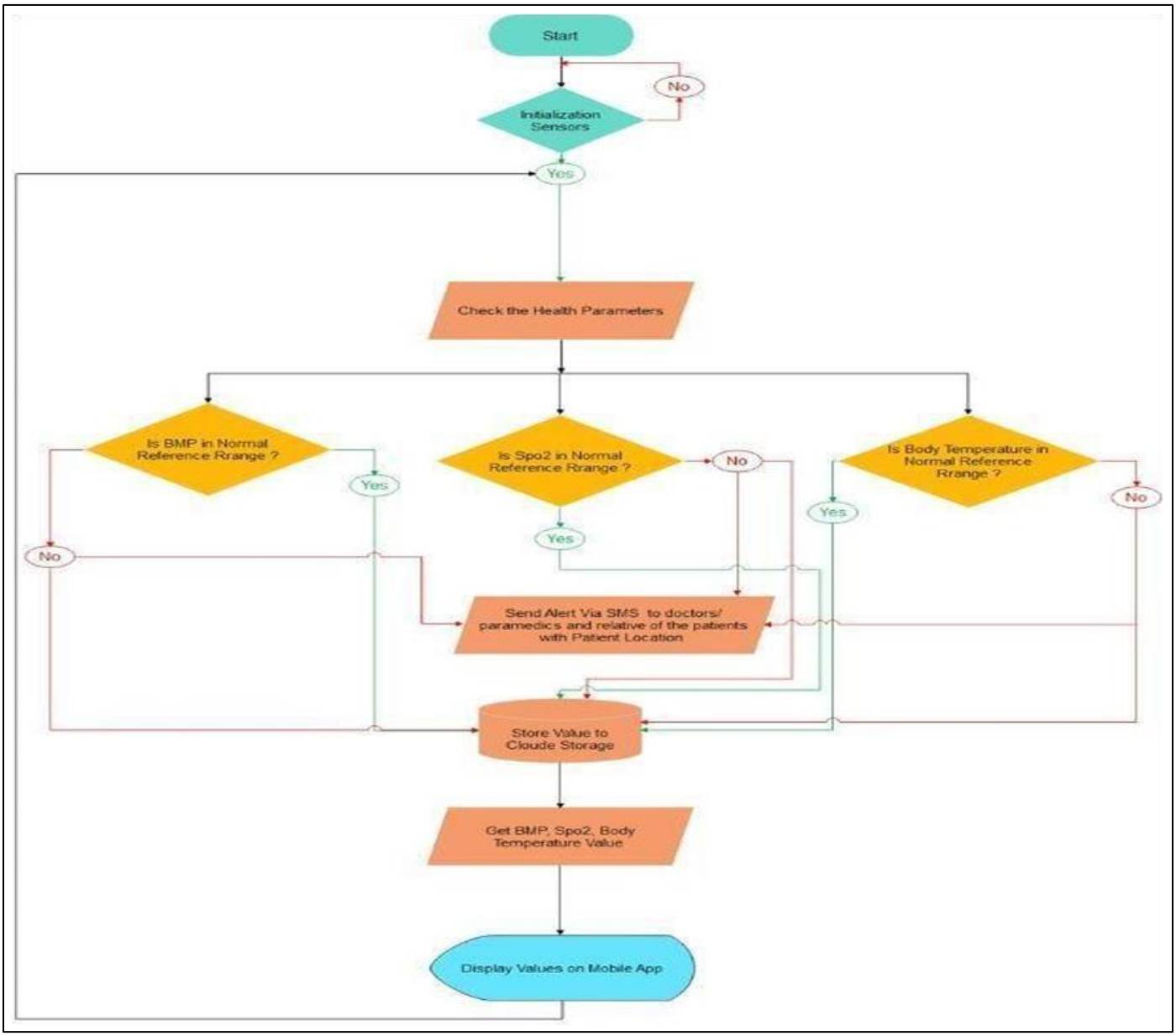

Fig 3 Workflow of the Proposed IoT-AI Healthcare Monitoring System

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1553

➢ *Elliptic Curve Cryptography for Key Management*

Elliptic Curve Cryptography (ECC) is used by the system to regulate access according to user responsibilities and provide safe key sharing. This approach uses a private key and a generator point to create the public key. In this case, d stands for the private key, G for the generator point, and Q for the final public key. ECC is a great option for healthcare devices with limited resources since it provides robust security with lower key sizes.

➢ *Automated Medication Dispensing*

Based on the AI analysis, the system activates a smart pharmaceutical dispensing unit. As shown in Fig. 4, the analyzed results trigger automated medication delivery.

The dosage decision can be modeled as:

Dose=f(Dhealth)Dose = f(D_{health})Dose=f(Dhealth)

Where:

- DhealthD_{health}Dhealth represents the patient's health condition

This mechanism ensures accurate dosage and improves treatment adherence.

➢ *Role-Based Access Control (RBAC)*

To protect sensitive medical data, the system implements role-based access control. Access decisions are defined as: Access={Granted,if RolegeqRequiredDenied, otherwiseAccess=begin{cases} Granted, & text{if Role geq Required} Denied, & text{otherwise} end{cases} Access={Granted,Denied,if Role geqRequiredotherwise This guarantees that certain data can only be accessed by authorized individuals, such as physicians and caretakers.

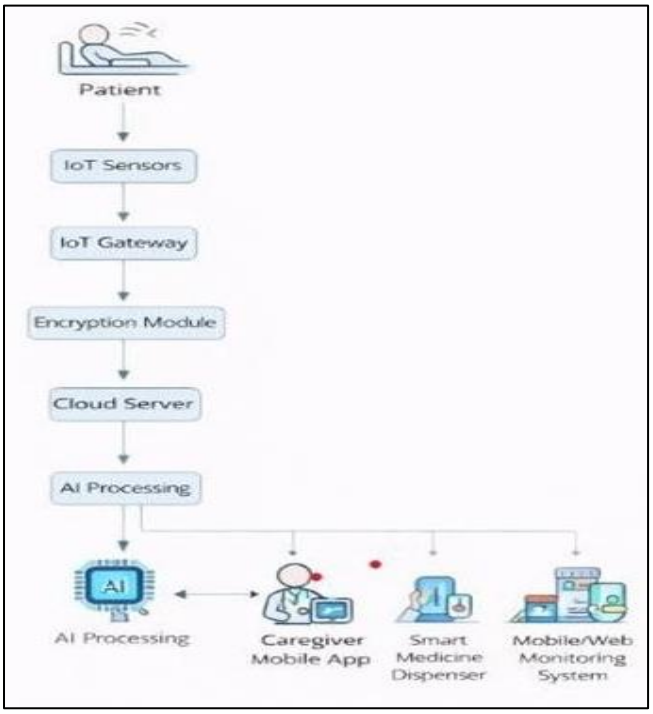

Fig 4 Data Flow Diagram of Proposed Healthcare System

➢ *Overall System Workflow*

Data gathering, safe encryption, cloud-based processing, AI-driven analysis, and automated replies are all included in the proposed system's entire workflow, which is depicted in Figures 3 and 4. The system is intended to facilitate real-time monitoring, facilitate early diagnosis, guarantee safe data management, and raise the general effectiveness of healthcare services.

V. ALGORITHMIC FRAMEWORK

IoT-based data collecting, safe encryption, cloud-based processing, and intelligent analysis are all integrated into the system's organized workflow. The main goal is to enable real-time monitoring and automatic reactions while guaranteeing the safe management of patient data. The data is processed at each step of the workflow and safely moved on to the next without revealing any private information.

- Algorithm: Secure IoT–AI Healthcare Processing Input: Real-timepatient health data
- Output: Alerts, analysis results, and medication actions

➢ *Step 1: Data Collection*

- Start the IoT sensors and begin monitoring.
- Gather vital signs including oxygen saturation, heart rate, and temperature.
- Store the collected values in a structured format:
- D={HR,Temp,SpO2}D = {HR, Temp, SpO_2} D={HR,Temp,SpO2}

➢ *Step 2: Data Encryption*

- Generate a session key KKK.
- Encrypt the collected data using AES:
- Cdata=AES_Enc(K,D)C_{data}=AES_Enc(K, D)Cdata =AES_Enc(K,D)

➢ *Step 3: Key Protection (Kyber)*

Secure the session key using the Kyber algorithm:

- Ckey=Kyber_Enc(PK,K)C_{key}=Kyber_Enc(PK, K)Ckey=Kyber_Enc(PK,K)
- Combine encrypted data and key:
- Packet={Cdata,Ckey}Packet={C_{data}, C_{key}}Packet={Cdata,Ckey}

➢ *Step 4: Data Transmission*

- Send the encrypted packet to the cloud.
- Store it securely for further processing.

➢ *Step 5: Secure Computation (BGV)*

- Convert data into ciphertext form:
- c=(c0,c1)c = (c_0, c_1)c=(c0,c1)
- Perform operations directly on encrypted data:
- Enc(f(D))=f(Enc(D))Enc(f(D))=f(Enc(D))Enc(f(D))
- =f(Enc(D))

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1553

- Compute values such as average and detect unusual patterns.

➢ *Step 6: Analysis*

- Process the results using an AI model.
- Check if values exceed a limit:
- Alert={1,D>T0,otherwiseAlert = begin{cases} 1, & D > T 0, & text{otherwise} end{cases}Alert={1,0, D>Totherwise
- Generate alerts if any abnormal condition is detected.

➢ *Step 7: Access Control*

- Generate ECC keys:
- Q=d·GQ = d cdot GQ=d·G
- Allow access based on user role:
- Access={Granted,Role≥RequiredDenied,otherwiseAcce ss = begin{cases} Granted, & Role geq Required Denied, & text{otherwise} end{cases}Access={Granted,Denied, Role≥Requiredotherwise

➢ *Step 8: Medication Action*

- If alert is generated, calculate required dosage:
- Dose=f(Dhealth)Dose = f(D_{health})Dose=f(Dhealth)
- Activate the dispensing unit and provide medication.

➢ *Step 9: Output*

- Show results in mobile web application.
- Notify doctor and caregiver.
- Store logs for future reference.

VI. RESULT AND DISCUSSION

The accuracy, security, and efficiency of the suggested secure IoT-AI healthcare system were assessed through implementation and evaluation. To guarantee dependable and secure healthcare monitoring, it combines IoT-based data collecting, cloud processing, and AI-driven analysis with cutting-edge encryption techniques.

➢ *Performance Evaluation of Encryption Techniques*

The system incorporates multiple encryption mechanisms, including AES, RSA, BGV, and Kyber, to ensure secure handling of sensitive medical data. A comparative analysis of these algorithms is presented in Table 1.

Table 1 Algorithm Comparison for Encryption

Algorithm	Type	Speed	Security Level
AES	Symmetric	Fast	Medium
RSA	Asymmetric	Moderate	Medium
BGV	Homomorphic	Slow	High
Kyber	Post-Quantum	Moderate	Very High

From Table 1, it can be observed that AES provides faster encryption due to its symmetric nature, making it suitable for bulk data processing. RSA, being an asymmetric algorithm, offers moderate performance but is less efficient for large- scale data encryption. The BGV homomorphic encryption scheme enables computation on encrypted data, ensuring data privacy, although it introduces higher computational overhead.

Kyber, a post-quantum cryptographic algorithm, demonstrates a higher level of security compared to traditional methods. Its resistance to quantum attacks makes it particularly suitable for healthcare systems where long-term data protection is critical. Based on this comparison, the proposed system effectively combines AES for speed and Kyber for secure key exchange, while BGV ensures privacy-preserving computation.

➢ *Accuracy Analysis of the Proposed Model*

The effectiveness of the proposed AI-based healthcare model was evaluated by comparing it with existing machine learning algorithms. The comparison results are illustrated in Fig. 5.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1553

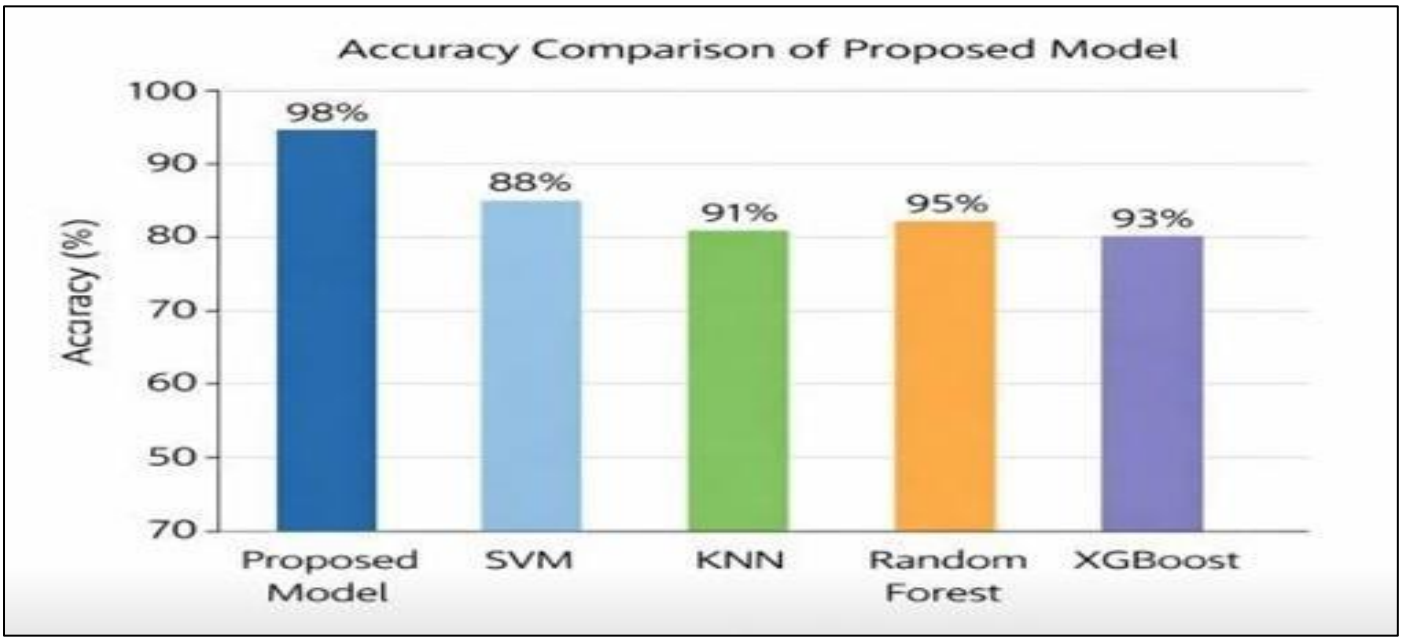

Fig 5 Accuracy Comparison of Proposed Model

As shown in Fig. 5, the proposed model achieves an accuracy of 98%, which is higher than other models such as Support Vector Machine (88%), K-Nearest Neighbors (91%), Random Forest (95%), and XGBoost (93%). This improvement in accuracy is due to the integration of real-time IoT data with intelligent analysis techniques.

The results indicate that the proposed model is more effective in identifying abnormal health conditions and generating early alerts. The combination of continuous monitoring and intelligent processing contributes to improved prediction performance.

➢ *System Efficiency and Practical Impact*

In addition to accuracy, the system demonstrates efficient real- time performance by processing data with minimal delay. The use of cloud infrastructure allows scalable storage and fast data access, enabling remote monitoring by healthcare professionals.

The automated medication dispensing mechanism further enhances the system by ensuring timely drug delivery based on analytical results. This reduces the chances of human error and improves patient adherence to prescribed treatments.

➢ *Discussion*

The findings show that IoT, AI, and sophisticated encryption methods greatly improve healthcare monitoring systems. The suggested approach increases diagnostic precision while protecting privacy and data security. By integrating sensing, intelligent decision-making, and automation, the suggested system offers a cohesive solution as opposed to conventional systems that mainly concentrate on either monitoring or analysis. The incorporation of post-quantum cryptography enhances resistance to potential security risks. All things considered, the system shows great promise for practical healthcare uses, especially in chronic illness management, elder care, and remote patient monitoring.

VII. CONCLUSION

A smart and safe IoT-AI healthcare system for automated medication support and real-time patient monitoring is presented in this work. To provide a dependable and effective healthcare solution, the framework combines cloud computing, artificial intelligence, IoT-enabled sensors, and cutting-edge encryption methods.

The system continuously gathers physiological data, uses intelligent models to assess it, and produces timely alarms for abnormal circumstances. AES, Kyber, and BGV are examples of hybrid encryption algorithms that are integrated to provide secure data processing, storage, and transmission. By limiting access to just authorized individuals, role-based access control also improves data privacy.

According to the performance evaluation, the suggested model outperforms traditional machine learning techniques in terms of accuracy. Its real-time data processing and automated drug distribution capabilities improve patient care while reducing human error. All things considered, the system offers a thorough framework that combines automation, security, analysis, and monitoring. It can be used successfully in practical situations including managing chronic illnesses, providing care for the elderly, and monitoring patients remotely.

Future improvements might incorporate blockchain-based mechanisms for safe and decentralized data management, better scalability for large-scale deployment, and sophisticated deep learning models.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1553

REFERENCES

[1]. A. Souri et al., "A machine learning-based healthcare monitoring model for student condition diagnosis in IoT environments," Soft Computing, vol. 24, pp. 17111–17121, 2020.

[2]. M. S. Alamsyah et al., "IoT-based vital sign monitoring system," International Journal of Electrical and Computer Engineering, vol. 10, no. 6, pp. 5891–5898, 2020.

[3]. K. N. Swaroop et al., "Health monitoring system for vital signs using IoT," Internet of Things, vol. 5, pp. 116–129, 2019.

[4]. J. S. Raj, "Information processing in IoT-based real-time healthcare monitoring systems," Journal of Electronics, vol. 2, pp. 188–196, 2020.

[5]. L. Parisi et al., "Hybrid algorithm for prognosis prediction in hepatitis patients," Neural Computing and Applications, vol. 32, no. 8, pp. 3839–3852, 2020.

[6]. S. M. G. Mostafa et al., "Design of an IoT-based healthcare monitoring system," in Proc. ICISET, 2022, pp. 362–366.

[7]. M. Jenifer et al., "IoT-based patient healthcare monitoring system," in Proc. ICICCS, 2022, pp. 487–490.

[8]. P. Kshirsagar et al., "Review on IoT-based healthcare monitoring systems," in Proc. ICCCE, 2019, pp. 95–100.

[9]. M. M. Khan et al., "IoT-based health monitoring system development and analysis," Security and Communication Networks, 2022.

[10]. M. Hamim et al., "IoT-based remote health monitoring system for elderly patients," in Proc. ICREST, 2019, pp. 533–538.

[11]. M. A. Al-Sheikh et al., "Mobile healthcare monitoring system using IoT and cloud computing," IOP Conf. Series, 2020.

[12]. M. M. Islam et al., "Development of smart healthcare monitoring system in IoT environment," SN Computer Science, vol. 1, 2020.

[13]. T. Wu et al., "Wearable health monitoring sensor patch for IoT applications," IEEE IoT Journal, vol. 7, pp. 6932– 6945, 2020.

[14]. H.-R. Cao et al., "Emergency healthcare system for elderly communities," Wireless Communications and Mobile Computing, 2018.

[15]. N. Y. Philip et al., "IoT for in-home healthcare monitoring systems," IEEE JSAC, vol. 39, pp. 300–310, 2021.

[16]. S. Gera et al., "IoT-based automated healthcare monitoring system for smart cities," in Proc. ICCMC, 2021.

[17]. K. Lauter et al., "Improved security for homomorphic encryption schemes," IMACC, 2013.

[18]. C. Gentry et al., "Homomorphic encryption from learning with errors," CRYPTO, 2013.

[19]. K. Kushala, "Privacy-preserving cloud-based patient monitoring," 2020.

[20]. K. S. Shivaprakasha et al., "Secure healthcare data processing using homomorphic encryption," ICDCECE, 2025.

[21]. L. Farhan et al., "Energy efficiency in IoT networks," Network, vol. 1, pp. 279–314, 2021.

[22]. R. Alekya et al., "IoT-based smart healthcare monitoring: A review," European Journal of Molecular & Clinical Medicine, 2021.

[23]. N. Sharma et al., "Secure IoT-based healthcare monitoring system," IEEE ICECCT, 2019.

[24]. V. K. Rathi et al., "Edge AI-enabled IoT healthcare system," Computer & Electrical Engineering, 2021.

[25]. M. Alshamrani, "AI and IoT in remote healthcare monitoring systems: A survey," Journal of King Saud University, 2022.