Machine Learning-Based Security Enhancements in Wireless Sensor Network Routing for Reliable Patient Data Transmission in Healthcare Systems

1. Introduction

Today's healthcare systems depend on Wireless Sensor Networks (WSNs) for efficient data transfer and real-time patient vital monitoring, all of which help make crucial medical choices on time. Because the healthcare sector depends heavily on timely and sensitive data transfer, it is imperative that patient data be sent in a secure and reliable manner. Devastating consequences, including incorrect diagnoses, delayed treatments, and violations of patient confidentiality, might arise from compromises in the safety or integrity of such data. The problem in healthcare settings is to safeguard enormous sensor data generated by IoT-enabled equipment from attacks while maintaining operational flow and communication.

Unfortunately, several kinds of obstacles impede the safe and dependable routing of patient data within WSN, including the presence of noise and artifacts in sensor data that reduce machine learning accuracy, which may lead to less-than-reliable routing decisions; increased security vulnerabilities; lack of strong encryption mechanisms; overfitting, complexity, and long training times of the current techniques spoil the robustness of intrusion detection systems (IDS); lack of classification accuracy; and problems with link failure and network congestion related to WSN routing protocols almost always result in energy inefficiency and delays, particularly in healthcare applications where monitoring must be carried out continuously.

In order to overcome these obstacles, this study incorporates cutting-edge machine learning-based algorithms to improve WSN security and guarantee dependable data transmission, such as the multi-sensor fusion and joint estimation algorithm for pre-processing sensor data to reduce noise and artifacts and enhance model input quality. For example, the Random Forest-RA model prevents overfitting by automatically modifying the fraction of decision tree contributions and combining model complexity with accuracy, while a hybrid encryption method based on ECC with ChaCha20-Poly1305 offers optimal data security. After all, the DT-PBD algorithm produces dependable routing by adjusting routing paths in accordance with network conditions, optimizing energy consumption, and prioritizing crucial data transmission. We also use the SVM (Support Vector Machine) classifier to improve detection accuracy, close anomaly detection gaps, and strengthen data integrity. Thus, these techniques together provide a complete solution for the safe and effective transfer of patient data in healthcare-focused WSNs.

1.1 Research aim and scope:

The objective is to deploy WSNs to improve patient data transmission security and reliability in healthcare systems. This work mainly employs a robust encryption system, machine learning algorithms, and effective routing approaches to handle critical data links and convey critical information about patients in a timely manner. Developing and putting into practice a state-of-the-art technique for creating a dependable, secure framework for patient data transmission in healthcare systems is one of the study's goals..

1.2 Research Objective:

The study paper's primary goal is listed below,

- Improve WSN security by creating a robust encryption system to protect patient data while it is being sent.
- To provide more dependable transmission in healthcare systems by enhancing patient data quality, lowering noise, and increasing accuracy.
- Greater security and accuracy for routing in healthcare-oriented WSNs may be ensured by using machine learning approaches that might reduce overfitting with more effective training.
- To improve the integrity and reliability of data transmission and enable threat detection and classification by employing a classifier to help accurately identify and classify security risks and abnormalities inside WSNs.
- Developing the best routing algorithm for patient data and resolving network issues like congestion and connection failure while guaranteeing prompt and dependable delivery of vital patient data.

2. Problem Statement

2.1 Specific problem statement

Reference 1

Title: “Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications”

Concept:

An ideal routing protocol-based framework for the secure and convenient transport of medical data in the Internet of Things is proposed by this study. Initially, health data is collected via a range of IoT devices, including wearables and sensors. The new data is pre-processed using techniques for analysis and cleansing. "K-nearest neighbor (KNN)" imputation and "principal component analysis (PCA)" are used to reduce the dimensionality of the data. "Modified Local Binary Patterns (MLBP)" are used to extract features from the processed data. By combining the fuzzy dynamic trust-based RPL algorithm with the "Butter Ant Optimization (BAO)" approach for lightweight and losing networks, the proposed "fuzzy dynamic trust-based RPL (FDT-RPL)" method improves the overall privacy of data transmission.

Problem defined:

- The quality of machine-learning models is compromised by noise and abnormalities in sensor data, which can result in inaccurate routing and security flaws.

Solution:

- To reduce noise and artifacts and provide higher-quality input for safe and dependable routing decisions, we propose a multi-sensor fusion and joint estimation technique.

Reference 2

Title: “WOGRU-IDS — An Intelligent Intrusion Detection System for IoT assisted Wireless Sensor Networks”

Concept:

In order to effectively identify a range of attacks, the presented research proposes the novel "Whale Optimized Gate Recurrent Unit (WOGRU) Intrusion Detection System (IDS)" for WSN-IoT networks. To obtain great performance at minimal processing cost, the deep short-term memory's hyperparameters were adjusted using the whale technique in the suggested framework.

Problem defined:

- Despite achieving a good classification rate against several threats, the model does not have a robust encryption strategy to completely safeguard the transfer of patient data in healthcare systems.

Solution:

- To address the issue, we propose a hybrid encryption technique that combines Elliptic Curve Cryptography (ECC) with ChaCha20-Poly1305.

Reference 3

Title: “Enhancing Cybersecurity in Healthcare: Evaluating Ensemble Learning Models for Intrusion Detection in the Internet of Medical Things”

Concept:

This research investigates intrusion detection using machine learning models in the "Internet of Medical Things" in an attempt to strengthen cybersecurity defenses and protect sensitive medical information. On the "WUSTL-EHMS-2020 dataset," the unpredictability of "Random Forest and Support Vector Machines" serves as the foundation structure for evaluating the packing, organizing, and strengthening ensemble learning procedures.

Problem defined:

- This study's primary drawback is its tendency toward overfitting, which can lower the system's robustness and dependability.

Solution:

- By averaging predictions from many decision trees, we propose a Random Forest-RA method that combines Random Forest with Regularization-Based Adaptive Factor (RA) to reduce overfitting.

Reference 4

Title: “Improved Wireless Medical Cyber-Physical System (IWMCPS) Based on Machine Learning”

Concept:

The IWMCPS architecture's development is presented using a scenario that incorporates medical applications. Because the healthcare industry relies on cyber-physical systems, context-aware and vital medical data are vulnerable to both data theft and cyberattacks. Openness, security, confidence, and dependability are some of the issues that need to be addressed in the growing field of MCPS research. To address the aforementioned issues, researchers provide a "Improved wireless medical cyber-physical system (IWMCPS)" based on machine learning techniques. Because of the variety of devices that make up these systems, such as mobile devices and body node sensors, they are vulnerable to various attacks.

Problem defined:

- This study's classification accuracy of 93% indicates that detection accuracy is still lacking.

Solution:

- In order to improve accuracy, we provide an SVM classifier method that outperforms the IWMCPS design with 99% detection accuracy.

Reference 5

Title: “A Cluster-Based Energy-Efficient Secure Optimal Path-Routing Protocol for Wireless Body-Area Sensor Networks”

Concept:

This paper proposes a unique cluster-based safe routing system called "Safe Optimal Path-Routing (SOPR)" to solve the reliability, energy efficiency, and safety issues in WBAN. This proposed method recognizes and sends data packets in an encrypted fashion while simultaneously preventing black-hole attacks to enhance communication security in WBANs.

Problem defined:

- One drawback of WSN routing for healthcare is that delays and reduced energy efficiency might result from the routing protocol's inability to determine the optimal path due to connection failures and network congestion.

Solution:

- We have employed the PBDR-DT technique, which combines priority-based data routing algorithms with decision trees, to get around this restriction.

2.2 Overall problem statement:

- **Noise and abnormal data:** The sensor data can damage machine learning models, leading to incorrect routing and security concerns in healthcare.
- **Inadequate Encryption Strength:** The insufficient encryption scheme can compromise data security during transmission.
- **Data overload and difficult:** Noisy or outlier-laden data might hinder effective generalization. Furthermore, larger ensemble complexity and increased training duration reduce the overall strength of the IDS.
- **Insufficient Classification Accuracy:** This worsen classified accuracy can impacts the robustness and dependability of the model.
- **Network Routing obstacles:** The protocol cannot locate the best pathways due to network congestion and connection failure, which reduces energy efficiency and causes delays in the transfer of healthcare data.

3. Proposed Methodology:

The suggested approach relies on the integration of machine learning techniques for safe patient data transfer in a wireless sensor network.

- Data Acquisition & Preprocessing
- Security Implementation
- Intelligent Threat Detection

- Patient Data Verification
- Secure & Reliable Data Routing

A. Data Acquisition & Preprocessing

In this study, we use Kaggle's IoT Healthcare Security Dataset to implement security improvements in Wireless Sensor Networks (WSNs) that facilitate dependable patient data transfer in healthcare systems. This dataset includes an extensive collection of data produced by IoT devices frequently utilized in medical applications. This dataset includes sensor readings, time stamping, and labels that suggest potential security risks or anomalous activities such data manipulation, illegal access, and network abnormalities. Therefore, this dataset may be used to train machine learning algorithms that can detect and stop security breaches in real-time, guaranteeing the accuracy of patient data provided.

After gathering the data, we proceed with the pre-processing. A **multi-sensor fusion and joint estimation technique** may do this. When collecting data from several sensors, the method is highly helpful in reducing noise and correcting inaccurate readings. In this manner, it uses redundant sensor data to provide the system an even more accurate and consistent depiction of the patient data. In essence, its goal is to synchronize data streams and coordinate sensor inputs. Later on, sophisticated filtering methods are used to help improve the data input into machine learning models, which makes it easier to make security and routing decisions in response to improved input data for the trustworthy transmission of patient data. This paper's strategy aims to reduce the impact of inconsistent data while strengthening the underlying WSN security and performance in a healthcare system while being reliable and effective for data transfer.

B. Security Implementation

To increase security, a hybrid encryption technique that combines **ECC and ChaCha20-Poly1305** is suggested. ECC is used for key exchange to effectively and securely distribute cryptographic keys in the WSN nodes because it offers lightweight processing and a high level of security. The ChaCha20-Poly1305 symmetric encryption system ensures secrecy and integrity during transmission by combining high-speed encryption with the authorized encryption mode. The combination makes use of both the strong key management of ECC and the data encryption efficiency of ChaCha20-Poly1305 to create a powerful security mechanism. Through integration, this suggested solution successfully avoids and prevents a number of attack weaknesses, including tampering and eavesdropping, making the whole data transmission process in healthcare apps safe, reliable, and sensitive.

C. ML based training

Next, we offer a method called **Random Forest-RA**, which combines **Random Forest with the Regularization-Based Adaptive Factor (RA)** to prevent overfitting and lengthen training periods in WSNs for healthcare systems. Without overfitting, this method improves the security of data transfer. In order to lessen the impact of noisy or outlier data, the RA technique dynamically modifies the decision trees' contribution inside the random forest. Consequently, our model provides better generalization and, consequently, dependable and secure patient data routing by averaging predictions from several decision trees. As a dependable solution for intrusion detection systems (IDS) in healthcare-focused WSNs, adaptive regularization also maximizes model training efficiency by successfully balancing complexity and accuracy. This machine learning-based system guarantees the secure, accurate, and effective transfer of data that is crucial for patient monitoring and healthcare delivery.

D. Data classification

Following data training, we used the **Support Vector Machine (SVM)** classifier classification approach. The SVM classifier has shown to be a highly effective tool for increasing detection accuracy, and current methods show a significant improvement. This enhancement further ensures that the system can recognize the suggested security risks in WSN with more accuracy and dependability. In health settings, this is a crucial component for consistently accurate and efficient patient data transfer. The process of SVM is suitable for safeguarding patient data due to its high classification accuracy, which enables swift and accurate detection of irregularities or unauthorized access. This prevents sensitive healthcare data from being compromised by a potential breach or malevolent assault. As a result, it increases detection, which in turn improves the integrity and reliability of the data transmission infrastructure of the healthcare system.

E. Secure & Reliable Data Routing

Lastly, a **PBDR-DT algorithm** that combines the strengths of **Decision trees and Priority-based data routing** is utilized in the dependable transfer of patient data in health care systems employing WSNs to address problems that may arise from link failures and network congestion. It implies that even in crowded or unstable networks, high-priority data, such as patient vital signs or emergency calls, must be transferred with the least amount of delay possible if one packet is crucial. Based on current network conditions, the decision tree mechanism's dynamic routing path modification makes intelligent choices about avoiding malfunctioning links and maximizing energy use. This creates a mix of data transmission dependability and energy efficiency, which is critical in health care because patient monitoring must be constant. By combining these techniques, patient data is sent safely and dependably, supporting prompt medical treatments and improving the efficiency of healthcare systems.

- No. of nodes vs. Precision (%)
- No. of nodes vs. Classification accuracy (%)
- No. of nodes vs. Recall (%)
- No. of nodes vs. Throughput (Kbps)
- No. of nodes vs. Packet delivery ratio (%)

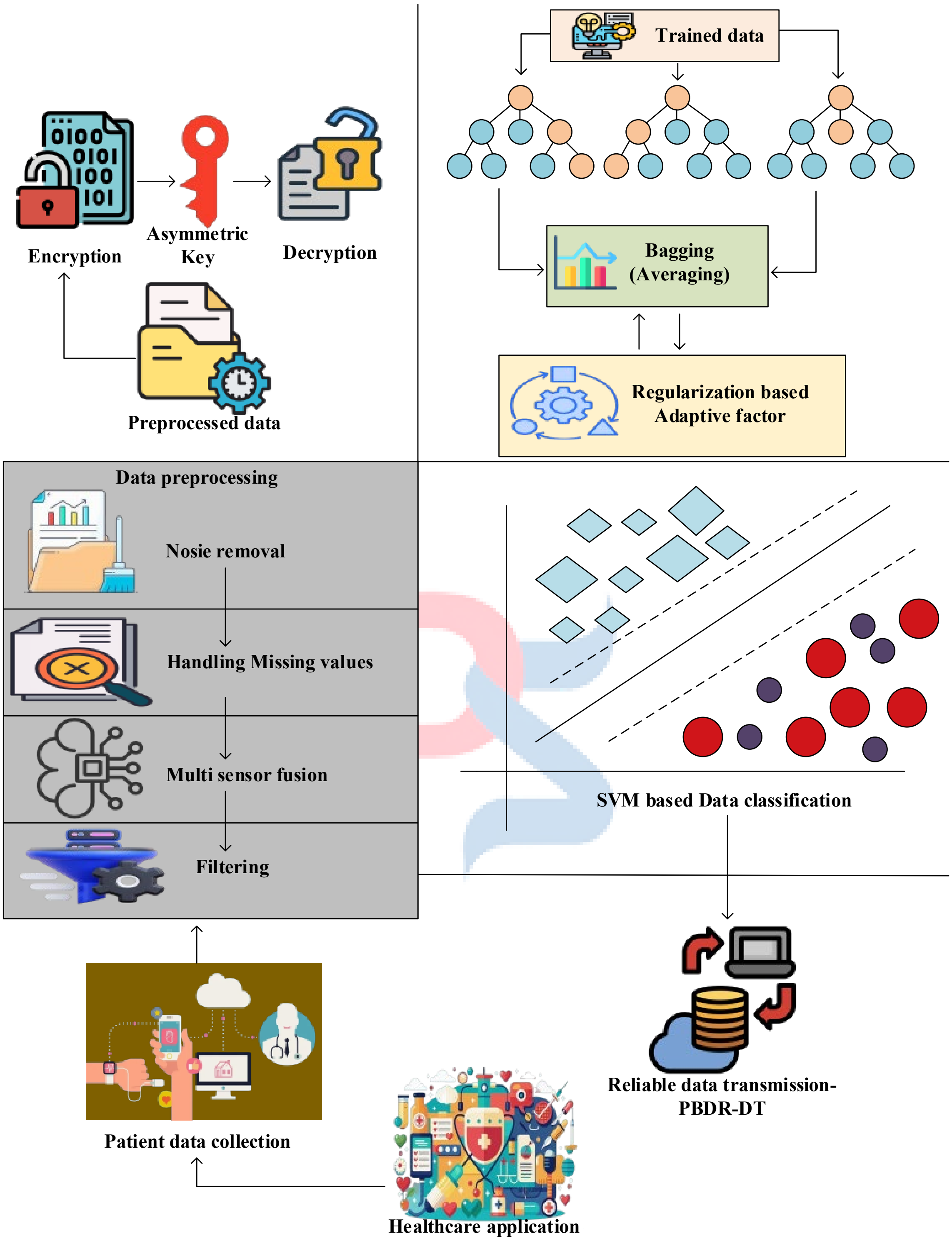

Fig.1 Overall architecture of the proposed model

Research highlights:

- **Data Pre-Processing with Multi Sensor Fusion:** Cutting-edge methods minimize sensor data mistakes and guarantee that the learning models' decision-making component is more reliable and accurate**.**
- **Advanced Encrypted Protocol:** By enhancing data security and integrity, the suggested combination of **ECC and ChaCha20-Poly1305** makes it more difficult for hackers to alter or listen in on patient data.
- **Improved ML Architecture: Random Forest-RA** has improved the model's ability to safely route patient data without sacrificing performance by minimizing overfitting and wasteful training.
- **Reliable Attack Identification:** By making it simple to identify security risks against malevolent healthcare system intrusions, the **SVM** classifier improves detection accuracy.
- **Highly Effective Path Selection with Decision Trees:** The **PBDR-DT algorithm** makes dynamic, real-time routing decisions in response to shifting network conditions. As a result, it guarantees error-free data transfer across overloaded or malfunctioning networks.

Reference 6

Title: "Hierarchical energy efficient secure routing protocol for optimal route selection in wireless body area networks"

Concept:

Based on threshold values, they proposed "Hierarchical Energy Efficient Secure Routing protocol (HEESR)" separates nodes in distributed bodies into transmit and shortest nodes. Unlike other traditional protocols, the cluster head selection is based on energy consumption and traffic significance data, including critical and non-critical data. Following the identification of the best route for processing the gathered data, the data is encrypted using an asymmetric cryptographic algorithm and compressed using the Huffman encoding technique for secure data transport.

Limitation:

- This model's reliance on network characteristics alone for performance assessment is a drawback. Future developments might improve the analysis of physiological signal data by utilizing cloud platforms, machine learning, and artificial intelligence approaches.

Reference 7

Title: “EEDLABA: Energy-Efficient Distance- and Link-Aware Body Area Routing Protocol Based on Clustering Mechanism for Wireless Body Sensor”

Concept:

In this work, a novel protocol known as "energy-efficient distance- and link-aware body area (EEDLABA) with a clustering mechanism" is compared to the current "Link-Aware and Energy-Efficient Body Area (LAEEBA) and distance-aware relaying energy-efficient (DARE)" routing protocols in a WBSN. The recommended process combines the benefits of both DARE and LAEEBA in an enhanced form. The grouping technique has been introduced and applied in "EEDLABA" for better performance.

Limitation:

- The optimization of QoS, energy efficiency, and node scalability under various scenarios are not included in this study. Strong routing strategies are needed to address these problems.

Reference 8

Title: “An Efficient Routing Approach to Maximize the Lifetime of IoT-Based Wireless Sensor Networks in 5G and Beyond”

Concept:

The proposed system, "Optimal Cluster-Based Routing (Optimal-CBR)," uses a hierarchical routing strategy to extend network lifetime and reduce energy consumption for Internet of Things applications in the context of 5G and beyond. A clustering stage is initiated until the bulk of the nodes are dead before beginning the connection stage for the remaining data transmission. The nodes are arranged using the standard k-means approach during the clustering phase, and the cluster head (CH) is selected based on the node closest to the centroid with the maximum energy. The k-means algorithm is used by the Optimal-CBR protocol to cluster the nodes and the multi-hop method for chain routing.

Limitation:

- The framework's lack of concern for security while sharing data via a multi-hop routing approach is a negative.

Reference 9

Title: "A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0"

Concept:

They developed a unique "Elliptic Curve Cryptography-Based Energy-Efficient Routing Protocol (ECC-EERP)" to provide a high level of security and affordable infrastructure for "Healthcare 5.0." The key-based method ECC-EERP can be used to safeguard data. It reduces the total energy consumption of a WSN by encrypting and decrypting web traffic using pairs of public and private keys. The effectiveness of the suggested method was assessed by comparing it with many existing methods.

Limitation:

- Some of the main issues with PSL-RH are its high error level, poor forecast results, and procedure delays, which reduce the overall effectiveness of the security system.

Reference 10

Title: "Wireless Body Sensor Networks with Enhanced Reliability by Data Aggregation Based on Machine Learning Algorithms"

Concept:

To reduce the quantity of data delivered, they recommend employing data aggregation techniques. The network lifetime is also extended by lowering the resource consumption of the sensor nodes. However, it might negatively impact quality of service metrics like data reliability and connection security. A trustworthy data classification model for various health indicators based on several machine learning techniques has been proposed to ensure the reliability of data aggregation.

Limitation:

- The absence of real-time execution of the "Random Forest classifier" and improved security communication in WBSN is a serious negative.

Reference 11

Title: "An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks"

Concept:

An effective and efficient "Anomaly-Based Intrusion Detection System (AIDS) for IoMT networks" is presented by the author in this research. Taking into account the computational cost, the suggested AIDS uses host-based and network-based techniques to reliably gather log files from each IoMT device and the gateway itself, as well as information from the IoMT edge of the internet. This proposed AIDS would employ machine learning (ML) techniques to identify dangerous incidents in the IoMT network by identifying abnormalities in the collected data, taking processing overhead into account. The evaluation's findings showed which of six popular machine learning techniques are most suited for the suggested AIDS in anomaly detection.

Limitation:

- The presented approach solely addresses binary classification for attack identification, restricting the AIDS to determine the presence or absence of assaults.
- Multi-class classification, which could enhance the detection engine's capacity to recognize particular attack types that are taken into account in terms of computational overhead, is not supported by AIDS.

- Nevertheless, the hyperparameter selection of ML algorithms has not been thoroughly examined, and further research is required to monitor its impact on both performance and computational cost.

Reference 12

Title: "An Improved AI-Based Secure M-Trust Privacy Protocol for Medical Internet of Things in Smart Healthcare System"

Concept:

The SMP protocol was created in this work to address these issues. The SMP protocol uses machine learning, encryption, and trust mechanisms to provide and safeguard data secrecy during transmission. The SMP protocol is thought to function within the smart healthcare monitoring system; it offers a private and secure means of communication between the system's many parts. The SMP protocol is an improvement over the current security and privacy regulations controlling medical data.

Limitation:

- To improve patient outcomes and save healthcare costs, telemedicine applications and remote monitoring of chronic illnesses need more developments.
- Even if MIoT security is still complicated, simple security measures like the SMP protocol used in medical data need more investigation to ensure that they are enough for protection.

Reference 13

Title: "Certain Investigation on Healthcare Monitoring for Enhancing Data Transmission in WSN"

Concept:

When creating "Wireless Sensor Networks IEEE 802.15.4" standards, which provide the optimal channels for complete communication using the recommended Energy Optimization Algorithm, it is essential to analyze the observed data flow in order to enable effective data transmission. In order to accomplish efficient data transfer for health care monitoring, the suggested solution has increased data packet transmission speed by up to 25% and helps to extend the lifespan of wireless sensor networks.

Limitation:

- The research's focus on safe data transfer in wireless sensor networks for medical surveillance is a constraint.

Reference 14

Title: “Designing a Healthcare-Enabled Software-Defined Wireless Body Area Network Architecture for Secure Medical Data and Efficient Diagnosis”

Concept:

In order to protect complicated patient data while it is being distributed across public wireless networks, this study first created a framework for "Software-Defined Wireless Body Area Networks (SD-WBANs)" and then suggested "lightweight Schnorr encryption with hyper elliptic Curve Cryptography (HECC)." Additionally, the popular "Examination Based on Distance from Average Solution (EDAS) Multi criteria Decision-Making (MCDM) technique" is used to illustrate the efficacy of the suggested system. According on the performance study, the suggested approach performs better than previous state-of-the-art techniques in terms of energy usage, storage costs, communication overhead, and processing expenses.

Limitation:

- This approach does not use quantum cryptosystems or attribute-based fog-edge-assisted sign encryption when paired with 5G communication technologies.

Reference 15

Title: “An Enhanced Energy Optimization Model for Industrial Wireless Sensor Networks Using Machine Learning”

Concept:

In order to address this set of issues, an advanced energy optimization model for Industrial WSNs was created using machine learning techniques. The approach identifies and optimizes the nodes' energy usage while using a small amount of energy through knowledge-based learning to accomplish the necessary activities in Industrial WSNs. The model estimates the optimal results to be used in industrial WSNs and further assesses the efficacy of feedback control approaches to ensure increased productivity and a longer network lifetime. The model also permits potential trade-offs between electricity consumption and communication efficiency in order to make the solution greener.

Limitation:

- Improved Energy Efficiency Limitations in energy, bandwidth, and signal intensity have an influence on the model's dependability and efficiency. Additionally, handling dynamic data transfer leads to complexity. Another problem is scalability, which is the inability to adjust to big networks.

Reference 16

Title: "Design of advanced intrusion detection systems based on hybrid machine learning techniques in hierarchically wireless sensor networks"

Concept:

The author of this paper proposes advanced "hybrid machine learning-based intrusion detection systems (AIDS-HML)" to identify and classify intrusions on wireless sensor networks. Hybrid machine learning classifiers are used to identify threats to wireless sensor networks. Using benchmark datasets, the precision, recall, f1-score, and accuracy of the proposed model are compared with baseline models. The technique evaluates and trains prediction models. This shows that detection rate of 99.80% was achieved using the NSL-KDD standard dataset, which is based on "hybrid random forest and extreme gradient boost (RF-XGB)".

Limitation:

The study has some important limitations, which are listed below.

- As the number of nodes and data traffic increases, the performance might decrease, demanding substantial computing and memory resources.
- In nodes with limited resources, hybrid machine learning approaches impair real-time responsiveness and energy efficiency by adding computational overhead.
- Resource limitations and controlled conditions make it difficult to collect diverse and labeled training data for infrequent incursion scenarios.

Reference 17

Title: "Healthcare monitoring of mountaineers by low power Wireless Sensor Networks"

Concept:

Low-power CPUs that can tolerate temperatures as low as -40 °C are used in the proposed electronic design. The system tracks the body's temperature, heart rate, oxygen level, and other characteristics using advancements in satellite modems, LoRa, and WSN. The gathered data is subsequently sent to a central control center. In the event that victims are unintentionally buried, a special function of the electrical system will immediately activate "Op-Mode-5" and relay data to the master node at maximum strength.

Limitation:

- The influence of low temperatures on related energy sources and the viability of power regeneration during movement are not thoroughly discussed in the study. Further hardware design optimization is also required for lower power consumption.

Reference 18

Title: "An Improved Authentication Protocol for Smart Healthcare System Using Wireless Medical Sensor Network"

Concept:

For a smart healthcare system, the researchers provide a sophisticated anonymous identification method based on "Elliptic Curve Cryptography." The "BurrowsAbadi-Needham logic and Automated Validation of Internet Security" Procedures and Applications tools were used to guarantee the required integrity in order to assure the procedure's soundness, and additional schemes of a similar kind were employed to examine its soundness. According to the research, the enhanced protocol would enable efficient computing and communication while offering better security protection.

Limitation:

- Although the low-complexity data compression scheme efficiently reduces data traffic and saves on-board energy, the feasibility of power regeneration during movement and the impact of low temperatures on the involved energy source have not been thoroughly investigated, which could be a limitation of the proposed study.

Reference 19

Title: “An intelligent healthcare monitoring framework using wearable sensors and social networking data”

Concept:

In order to handle and analyze medical data accurately and improve categorization reliability, this study suggests an innovation in a recently built healthcare monitoring system that is based on a cloud-based infrastructure and a big data analysis algorithm. The proposed large data analysis engine is based on ontologies and data mining techniques. Data mining techniques may be used to efficiently pre-process healthcare data and minimize its dimensionality. Semantic knowledge regarding entities, aspects, and connections of such is included in ontologies based on diabetes and blood pressure domains. Bi-LSTM can accurately categorize medical data to predict medication side effects and to depict patients' abnormal circumstances.

Limitation:

- Therefore, fuzzy taxonomy and fuzzy LSTM may be integrated into this framework to improve categorization in the healthcare industry.

Reference 20

Title: "Healthcare security in cloud-based wireless sensor networks: Botnet attack detection via autoencoder-aided goal-based artificial intelligent agent"

Concept:

The suggested plan is based on a novel security strategy for cloud-based wireless sensor networks used in healthcare. Such advancement is achieved by creating an autoencoder-based agent called AE-A by fusing the autoencoder structure with the goal-based artificial intelligence agent called GAIA. The hybrid system's primary goal is to increase the effectiveness of botnet attack detection in light of the increasing security risk connected to cloud computing. Therefore, the objective is to create an all-encompassing, goal-oriented AI agent specifically intended for usage in healthcare settings.

Limitation:

- Strong autoencoders or more recent deep-learning architectures might be used in this hybrid model, thus it lacks some power. Furthermore, the system does not have a way to detect and react to more recent botnet assault patterns.

Reference:

1. Zachos, G., Essop, I., Mantas, G., Porfyrakis, K., Ribeiro, J. C., & Rodriguez, J. (2021). An anomaly-based intrusion detection system for Internet of Medical Things networks. *Electronics*, *10*(21), 2562.
2. Sankaran, K. S., Kim, T. H., & Renjith, P. N. (2023). An Improved AI-Based Secure M-Trust Privacy Protocol for Medical Internet of Things in Smart Healthcare System. *IEEE Internet of Things Journal*, *10*(21), 18477-18485
3. Gebremariam, G. G., Panda, J., & Indu, S. (2023). Design of advanced intrusion detection systems based on hybrid machine learning techniques in hierarchically wireless sensor networks. *Connection Science*, *35*(1), 2246703.

4. Garg, R. K., Bhola, J., & Soni, S. K. (2021). Healthcare monitoring of mountaineers by low-power wireless sensor networks. *Informatics in Medicine Unlocked*, *27*, 100775.
5. Belhaj Mohamed, M., Meddeb-Makhlouf, A., Fakhfakh, A., & Kanoun, O. (2021). Wireless body sensor networks with enhanced reliability by data aggregation based on machine learning algorithms. *Advanced Sensors for biomedical applications*, 67-81.
6. Iqbal, J., Adnan, M., Khan, Y., AlSalman, H., Hussain, S., Ullah, S. S., ... & Gumaei, A. (2022). [Retracted] Designing a Healthcare-Enabled Software-Defined Wireless Body Area Network Architecture for Secure Medical Data and Efficient Diagnosis. *Journal of Healthcare Engineering*, *2022*(1), 9210761
7. Ali, F., El-Sappagh, S., Islam, S. R., Ali, A., Attique, M., Imran, M., & Kwak, K. S. (2021). An intelligent healthcare monitoring framework using wearable sensors and social networking data. Future Generation Computer Systems, 114, 23-43.
8. Chellathurai Amirthabai, S., Malhotra, U., Thapasimuthu Rajeswari, S., & Thachankurichy Natesan, S. (2024). Healthcare security in cloud-based wireless sensor networks: Botnet attack detection via an autoencoder-aided goal-based artificial intelligent agent. *Concurrency and Computation: Practice and Experience*, *36*(19), e8152.
9. Roshini, A., & Kiran, K. V. D. (2023). Hierarchical energy efficient secure routing protocol for optimal route selection in wireless body area networks. *International Journal of Intelligent Networks*, *4*, 19-28
10. Alsolami, T., Alsharif, B., & Ilyas, M. (2024). Enhancing Cybersecurity in Healthcare: Evaluating Ensemble Learning Models for Intrusion Detection in the Internet of Medical Things. *Sensors*, *24*(18), 5937.
11. Yuanbing, W., Wanrong, L., & Bin, L. (2021). An improved authentication protocol for smart healthcare systems using wireless medical sensor network. *IEEE Access*, *9*, 105101-105117.
12. Alzahrani, A., Alshehri, M., AlGhamdi, R., & Sharma, S. K. (2023, January). Improved wireless medical cyber-physical system (IWMCPS) based on machine learning. In *Healthcare* (Vol. 11, No. 3, p. 384). MDPI.

13. Refaee, E., Parveen, S., Begum, K. M. J., Parveen, F., Raja, M. C., Gupta, S. K., & Krishnan, S. (2022). Secure and scalable healthcare data transmission in IoT based on optimized routing protocols for mobile computing applications. *Wireless Communications and Mobile Computing*, *2022*(1), 5665408
14. Dass, R., Narayanan, M., Ananthakrishnan, G., Kathirvel Murugan, T., Nallakaruppan, M. K., Somayaji, S. R. K., ... & Almusharraf, A. (2023). A cluster-based energy-efficient secure optimal path-routing protocol for wireless body-area sensor networks. *Sensors*, *23*(14), 6274.
15. Iqbal, J., Adnan, M., Khan, Y., AlSalman, H., Hussain, S., Ullah, S. S., ... & Gumaei, A. (2022). [Retracted] Designing a Healthcare-Enabled Software-Defined Wireless Body Area Network Architecture for Secure Medical Data and Efficient Diagnosis. *Journal of Healthcare Engineering*, *2022*(1), 9210761.
16. Swami Durai, S. K., Duraisamy, B., & Thirukrishna, J. T. (2023). Certain investigations on healthcare monitoring for enhancing data transmission in WSN. *International journal of wireless information networks*, *30*(1), 103-110.
17. Ramana, K., Revathi, A., Gayathri, A., Jhaveri, R. H., Narayana, C. L., & Kumar, B. N. (2022). WOGRU-IDS—An intelligent intrusion detection system for IoT-assisted Wireless Sensor Networks. *Computer Communications*, *196*, 195-206.
18. Jothikumar, C., Ramana, K., Chakravarthy, V. D., Singh, S., & Ra, I. H. (2021). An Efficient Routing Approach to Maximize the Lifetime of IoT-Based Wireless Sensor Networks in 5G and Beyond. *Mobile Information Systems*, *2021*(1), 9160516.
19. Zaman, K., Sun, Z., Hussain, A., Hussain, T., Ali, F., Shah, S. M., & Rahman, H. U. (2023). EEDLABA: energy-efficient distance-and link-aware body area routing protocol based on clustering mechanism for wireless body sensor network. *Applied Sciences*, *13*(4), 2190.
20. Natarajan, R., Lokesh, G. H., Flammini, F., Premkumar, A., Venkatesan, V. K., & Gupta, S. K. (2023). A novel framework on security and energy enhancement based on the Internet of medical things for Healthcare 5.0. *Infrastructures*, *8*(2), 22.