SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I12P101

Volume 12 Issue 12, 1-18, December 2025

Original Article

Dual Secure Optimal Trusted Routing for Sensitive Data Transfer to Ensure Accurate Patient Healthcare State Prediction Using IoT-Enabled Wireless Sensor Networks

D. Monica Satyavathi[1], A.Ch.Sudhir[2]

[1,2]*Department of EECE, GIT, GITAM (Deemed to be University), Visakhapatnam, Andhra Pradesh, India.*

[1]*Corresponding Author : monicajiji411@gmail.com*

Received: 01 October 2025 Revised: 03 November 2025 Accepted: 02 December 2025 Published: 27 December 2025

Abstract - *With the rapid advancement of Internet of Things (IoT) and Wireless Sensor Networks (WSNs), healthcare systems have evolved to support continuous patient monitoring, real-time data acquisition, and cloud-based decision support. The secure transmission of sensitive medical data and the reliability of healthcare decision-making remain major challenges. Traditional routing techniques fail to provide robust trust management, making the system vulnerable to malicious nodes and unreliable data paths. The lack of lightweight, end-to-end encryption increases the risk of data breaches during transmission. Compounding the issue is the limited diagnostic accuracy of conventional analytics platforms, which struggle to effectively process complex, high-dimensional healthcare data. To address this, this study introduces a Dual Secure optimal Trusted routing (DST-Route) technique designed to ensure secure, trust-aware data transfer and enhance patient diagnostic decision-making in IoT-WSN. In the data transfer phase, the Enhanced Pomarine Jaeger Optimization (EPJO) algorithm is used to perform trust-based clustering and optimal cluster head selection, ensuring that only reliable nodes participate in data transmission. The sensitive health data collected from patients is protected using SmartNetcryption, a lightweight encryption used to secure information before cloud storage. In the analytics phase, the framework uses pre-trained deep learning models, including ResNet, DenseNet, EfficientNet, and UNet for feature extraction, while a Modular Deep Transfer Learning (MDTL) enables accurate healthcare state prediction and early diagnosis. Experimental results demonstrate that DST-Route significantly improves trust accuracy, energy efficiency, and prediction performance when compared to conventional routing techniques. The proposed UNet, combined with the MDTL model, achieved a healthcare state prediction accuracy of 98% with a loss rate of 0.05, showing 12.54% improvement over state-of-the-art models. This performance underscores the effectiveness of the DST-Route technique in ensuring secure and reliable sensitive data transfer for accurate patient state prediction.*

Keywords - *Secure routing, Trust degree, Sensitive data transfer, Healthcare decision-making, IoT, Wireless Sensor Networks.*

1. Introduction

The Internet of Things (IoT) and Wireless Sensor Networks (WSNs) have revolutionized healthcare by providing better, real-time connectivity and monitoring [1]. IoT-enabled WSNs are changing how healthcare providers gather, analyze, and send patient data, from basic telemetry to real-time health surveillance. In hospitals and isolated areas, continuous health monitoring and emergency response have been enabled. Resource-constrained sensor nodes in WSNs monitor heart rate, blood pressure, oxygen saturation, and body temperature [2]. To minimize misdiagnosis and delayed reactions, the communication infrastructure must offer low latency, high accuracy, and reliable delivery. Despite improvements, hospital communication systems lack routing security, scalability, and energy efficiency [3]. WSNs' dynamic and dispersed nature makes secure data transfer, network durability, and packet loss difficult [4]. The healthcare communication system must be secure and trustworthy, especially when handling sensitive patient data via insecure networks [5, 6]. Historical behavior, energy status, and packet forwarding ratio are used to assess intermediate node trustworthiness [7]. To preserve network health, malicious or dysfunctional nodes must be excluded from routing pathways. To make dynamic, context-aware judgments, the routing algorithm needs an intelligent trust evaluation mechanism. In healthcare environments where patient data is extremely personal and delay-sensitive, data confidentiality and trust assurance are crucial [8]. Misinformed judgments, legal issues, and patient distrust can result from either compromise. A dual secure and trust-based routing technique is needed for constructing real-time, high-risk healthcare IoT systems [9]. Limitations in battery power, processing resources, topological changes, and node failures limit routing in healthcare WSNs [10], which necessitate

lightweight, energy-aware routing algorithms to transport data packets across the best pathways without premature node depletion. Energy efficiency, latency, packet delivery ratio, and route dependability are also traded in WSN routing optimization [11]. In sensitive applications like ICU monitoring or elderly patient surveillance, packet loss or delay might be catastrophic. Routing techniques must balance these characteristics in real time under changing network circumstances. Static routing techniques and shortest-path algorithms fail in such dynamic and demanding environments [12]. Genetic algorithms, ant colony optimization, and swarm intelligence are being employed to determine the most efficient and safe pathways that imitate natural processes to examine numerous routing options and choose the best one under limits. The self-adaptive, autonomous routing architecture is used for diverse and uncertain healthcare contexts [13]. IoT-WSNs capture and transmit data from wearable sensors and implanted devices via several intermediary nodes [14]. At the routing and node levels, effective cryptographic algorithms and intrusion detection must be incorporated. Hashing, digital signatures, and secure multiparty computation ensure data integrity in the end [15]. Lightweight encryption techniques for resource-constrained situations also protect secrecy, which security measures must be balanced with WSN nodes' computational and energy constraints [16, 17]. Data accuracy, timeliness, and reliability are crucial for making accurate and timely healthcare choices [18]. Dual safe optimum trusted routing aims to integrate efficiency, trust, and security into the routing technique [19], which ensures effective performance in resource-constrained healthcare situations using real-time trust measurements, energy-aware route selection, and low-power device encryption standards. Real-time adaptation is achieved by reinforcement learning and heuristic optimizers in this paradigm [20]. Given the high sensitivity, dynamic topology, and energy-constrained nature of healthcare IoT-WSNs, there is an urgent need for an intelligent framework that not only guarantees secure data transmission but also ensures trustworthy routing and accurate disease prediction. Existing routing techniques either focus heavily on data security or energy efficiency, rarely achieving a robust integration of security, trustworthiness, and predictive intelligence. The lack of real-time adaptability in routing strategies undermines performance in high-risk scenarios, where timely and reliable data delivery can be life-saving. This motivates the development of a comprehensive solution that bridges routing intelligence with advanced machine learning and security protocols for sensitive healthcare applications. To address these challenges, a dual secure optimal trusted routing (DST-Route) technique is proposed for secure and efficient healthcare communication in IoT-enabled WSNs. The major contributions of this work are given as follows.

1. Enhanced Pomarine Jaeger Optimization (EPJO) algorithm is used in the data transfer phase to perform trust-based clustering and optimal Cluster Head (CH) selection. It ensures that only trustworthy and energy-efficient nodes participate in routing, thereby enhancing route reliability and network lifespan.
2. Sensitive patient data is secured using SmartNetcryption, a lightweight and energy-efficient encryption scheme that safeguards healthcare data before offloading to cloud storage. It is used for resource-constrained WSN environments without compromising data confidentiality.
3. The analytics phase integrates pre-trained deep learning models such as ResNet, DenseNet, EfficientNet, and UNet used for hierarchical feature extraction. A Modular Deep Transfer Learning (MDTL) is used to improve healthcare state prediction accuracy, supporting timely clinical interventions.
4. The DST-Route technique combines secure routing, trust evaluation, and predictive analytics, making it suitable for dynamic, real-time healthcare applications. Reinforcement learning and heuristic optimization further enable real-time adaptability under varying network and patient conditions.

The rest of the paper is organized as follows. Section 2 provides a literature review of existing routing techniques in IoT-WSNs and healthcare prediction models using machine learning and deep learning models. Section 3 presents the proposed working methodology, which follows the data transfer and handling phase, detailing its mathematical modeling and key features. Section 4 presents the experimental setup, followed by a comparative analysis of simulation results in Section 5. Finally, Section 6 concludes the paper, providing insights into the implications of the proposed DST-Route technique and UNet+MDTL model.

2. Related Work

2.1. Review of Routing Techniques for IoT-WSN

A comprehensive routing protocol for high-traffic IoT-WSN environments was proposed in [21], which integrates SINR, congestion level, and survival factor for efficient cluster head selection using an adaptive fuzzy c-means method. Secure transmission is ensured through Adaptive quantum logic encryption and Adaptive Krill Herd (AKH) optimization. To address these limitations, a sustainable and intelligent IoT framework for smart cities was presented in [22]. While this enhances data reliability and sustainability, it does not cater to domain-specific requirements such as healthcare and education. To fill this adaptability gap, [23] introduced a versatile routing technique, GWFCCV, suitable for diverse sectors. It uses Gray Wolf Optimization (GWO) and Fuzzy C-Means (FCM) for clustering and combines Critic and Fuzzy VIKOR for routing decisions. Focusing on reducing computational complexity, [24] proposed a routing protocol based on the Cheetah Optimization Algorithm (COA), which balances exploration and exploitation in cluster head selection. Despite its performance, the model does not incorporate security mechanisms to handle malicious threats. To overcome this security concern, [25] developed ACTAR,

which integrates Adaptive Hybrid Clustering (AHC), Multi-Objective Cluster Head selection (MOCH), and Trust-Aware Routing (TAR). This strategy improves packet delivery (94.5%), energy efficiency (76.5%), and malicious node detection (93%). Addressing these 3D routing challenges, [26] proposed the Energy-Efficient Anchor Zone-Based Routing (EAZR) method.

However, this method does not provide robust protection against dynamic routing attacks or adversarial behavior. To counter such vulnerabilities, [27] introduced a secure routing using logarithmic helix spiral (LHS) search with the Orca Predation Algorithm (OPA). It significantly reduces energy consumption (as low as 10 J for 1000 cycles), although it struggles with real-time fault handling during node failures. Aiming to improve fault tolerance, [28] presented Intelli BEF, a bio-inspired protocol that uses Particle Swarm Optimization (PSO) for cluster head selection and Convolutional Neural Network (CNN) for detecting failed nodes in real time. This enhances network lifetime and fault resilience, but raises issues of improvement in security against coordinated attacks. Building on these security aspects, [29] proposed the egret-harris optimization (EHO) method, which merges egret search and Harris hawk predation behaviors to optimize routing and enhance robustness under Sybil attacks. To handle mobility-related issues in dynamic IoT-WSN environments, especially those using mobile sinks, [30] introduced an intelligent routing protocol with sink movement tracking.

2.1.1. Problem Definition

Table 1 presents a comparative analysis of IoT-WSN routing techniques, focusing on their core methodologies, employed optimization strategies, outcomes, and key research limitations. Despite numerous advances, current techniques exhibit limitations such as inadequate scalability in dynamic and mobile environments, high computational overhead, and insufficient support for application-specific demands like those in healthcare or smart cities. Moreover, existing solutions often lack real-time fault detection, mobility-aware routing, and robust defenses against coordinated attacks [41, 54]. To address these challenges, the proposed DST-Route technique introduces a dual-secure optimal trusted routing strategy that integrates intelligent clustering and lightweight encryption. It employs trust-based path selection and mobility-aware optimization to ensure reliable, energy-efficient, and secure data transmission. The routing supports domain-specific and sustainable deployment, effectively bridging the critical gaps in scalability, security, adaptability, and resilience observed in existing IoT-WSN routing solutions.

2.2. Review of Healthcare Decision-Making using IoT Data Gathering

A smart decision-making that leverages Blockchain and Federated Learning (FL) was introduced to ensure secure ECG data processing in micro-service-based IoT medical applications [31]. To address the lack of adaptive context-awareness, a design science-based integration of wearable IoT (w-IoT) with AI was proposed, employing various machine learning algorithms (e.g., KNN and DT) for real-time physiological data analysis [32]. To overcome these resource and interference challenges, a smart resource allocation strategy called iRASH for NB-IoT networks was proposed using DBSCAN clustering and ACO metaheuristic with BDI agents to enhance D2D communication efficiency [33]. Addressing these security and data privacy concerns, a blockchain-integrated federated matrix meta-learning system was introduced using Matrix-prototype Graph Networks (MGN) and intelligent contracts to train models over IoT environments while preserving data integrity [34]. This method handles heterogeneous, sparse data but still faces challenges with complex anomaly detection and model overfitting in real-time applications. To solve the anomaly detection problem in complex datasets, the Real-Time Anomaly Detection (RTAD) paradigm was proposed, integrating SRTrans-ConvRNN for sequential and contextual pattern learning in healthcare IoT [35].

To address this limitation, a noninvasive IoT-based health monitoring system was developed using basic sensors and cloud-based analytics for real-time event recognition in rural healthcare scenarios [36]. To enhance scalability and security, the AdaSec-Health system was proposed—built on a shredded blockchain architecture using the Enhanced Coati Optimization Algorithm (ECOA) to minimize orphan blocks and forks in EHR systems [37]. ECOA ensures high throughput and attack resistance, but lacks disease-specific analytics for proactive medical intervention. This gap was addressed by an IoT-based architecture using wearable and mobile applications combined with the MIBO algorithm and FI-CNN hybrid model for real-time health pattern analysis and early disease detection [38].

Table 1. Comparative analysis of recent IoT-WSN routing techniques

Ref.	Routing Name	Methodology	Techniques Used	Key Findings	Research Gaps
[21]	AKH-FCM Routing	Adaptive fuzzy logic & swarm optimization	SINR, Congestion, AKH, FCM	19.7% latency drop, 26.4% energy savings	Not scalable under high dynamic topologies; static scenarios only
[22]	SORT	Design science for smart cities	CMBS, EDS, ODF, Signcryption	91% trust accuracy, 30% data reliability gain	Not adapted for sector-specific domains like healthcare

[23]	GWFCCV	Versatile cluster-based routing	GWO, FCM, Critic + Fuzzy VIKOR	23.26% network lifetime gain	High computation cost; limited real-time scalability
[24]	COA-Based Routing	Nature-inspired low-complexity routing	COA (Cheetah Optimization)	17.5% energy savings, 14% throughput improvement	No integrated security mechanisms
[25]	ACTAR	Secure hybrid clustering & trust routing	AHC, MOCH, TAR	94.5% packet delivery, 93% attack detection, 76.5% energy efficiency	Not optimized for 3D topologies and mobility
[26]	EAZR	3D Routing with Anchor Zones	Anchor zone mapping	28.2% delay reduction, 33.5% packet delivery gain	No security features for dynamic attacks
[27]	LHS-OPA	Secure spiral routing with predator search	LHS, OPA	Energy use dropped to 10 J (1000 cycles), 89% route success	Ineffective real-time fault recovery
[28]	Intelli-BEF	Bio-inspired resilient routing	PSO, CNN	24% lifetime boost, real-time fault detection (95% accuracy)	Weak resistance to coordinated attacks
[29]	EHO	Hybrid predator-prey optimization	Egret search, Harris hawk algorithm	18% latency cut, 27% energy efficiency under attack	No adaptive features for mobility or node churn
[30]	SinkTrack Routing	Intelligent routing with mobility support	AI controller, INRwLF, Cluster Tables	38% network velocity boost, 42% E2E latency drop	High processing overhead in sink tracking and control channel congestion

Table 2. Summary of prediction models used for healthcare state prediction

Ref.	Methodology	Technique Used	Dataset(s) Used	Key Findings	Research Gaps
[31]	Smart Decision using FL & Blockchain	Microservice in Edge-Fog-Cloud	ECG synthetic data	Edge-based FL reduced energy usage by 0.1%, network usage by 1.1%, and cost by 3–20%	Lack of evaluation under high-volume data traffic and long-term deployment conditions
[32]	Design Science Approach for Wearable IoT and AI	ML (DT, KNN, XGBoost, SVM, LR)	Physiological wristwatch data	KNN achieved 91% accuracy; an adaptive, context-aware, scalable monitoring framework	Limited validation with large and demographically diverse user groups
[33]	Resource allocation optimization in NB-IoT for D2D	DBSCAN, ACO, BDI Agents, MILP	NS-3 Simulation	35% performance improvement and 50% energy savings with the iRASH system	Practical viability in real-time clinical environments has not yet been explored
[34]	Privacy-preserving federated meta-learning framework	MGN, Federated Learning	CheXpert, CIFAR-100	85% enhancement over traditional models in security and privacy	Insufficient testing in real-time hospital or clinical environments
[35]	Real-time anomaly detection in a healthcare information system	SRTrans-ConvRNN, ASM, LSTM, MHSA	ECU-IoHT, WUSTL-EHMS 2020, CICIDS2017	99.6% accuracy and 99.3% F1-score; effective for anomaly detection	Scalability issues in large, heterogeneous HIS deployments are not addressed
[36]	IoT-based remote health monitoring system	Cloud Computing, Decision Support System (DSS)	Real-time patient sensor data	91.68% accuracy in detecting critical health events; proof-of-concept validated	Requires full-scale integration with hospital IT systems and workflows
[37]	Sharded blockchain for HER	ECOA, IPFS	EIP-1559 Network Simulation	Achieved 3280 transactions/sec (tps), 28s latency; 7087 tps	Challenges with dynamic shard management and system overhead

[38]	Smart health monitoring with energy efficiency	MIBO, S3T, FI-CNN	Synthetic dataset	52.43% energy savings; proactive and scalable patient monitoring	High model complexity and deployment costs in large-scale healthcare facilities
[39]	Decision support using fractional fuzzy aggregation	Hamacher Sum/Product, TOPSIS, TODIM	Real-world Healthcare Case Study	Outperformed conventional aggregation models in system selection reliability	Requires broader validation across diverse clinical decision-making scenarios
[40]	Routing optimization in SDN-enabled IoT healthcare system	INRwLF, AI-SDN	Simulated Intelligent-IoT Scenarios	Reduced latency and energy usage; extended network lifetime by 50–90%	Deployment in real-world SDN-integrated healthcare systems remains untested

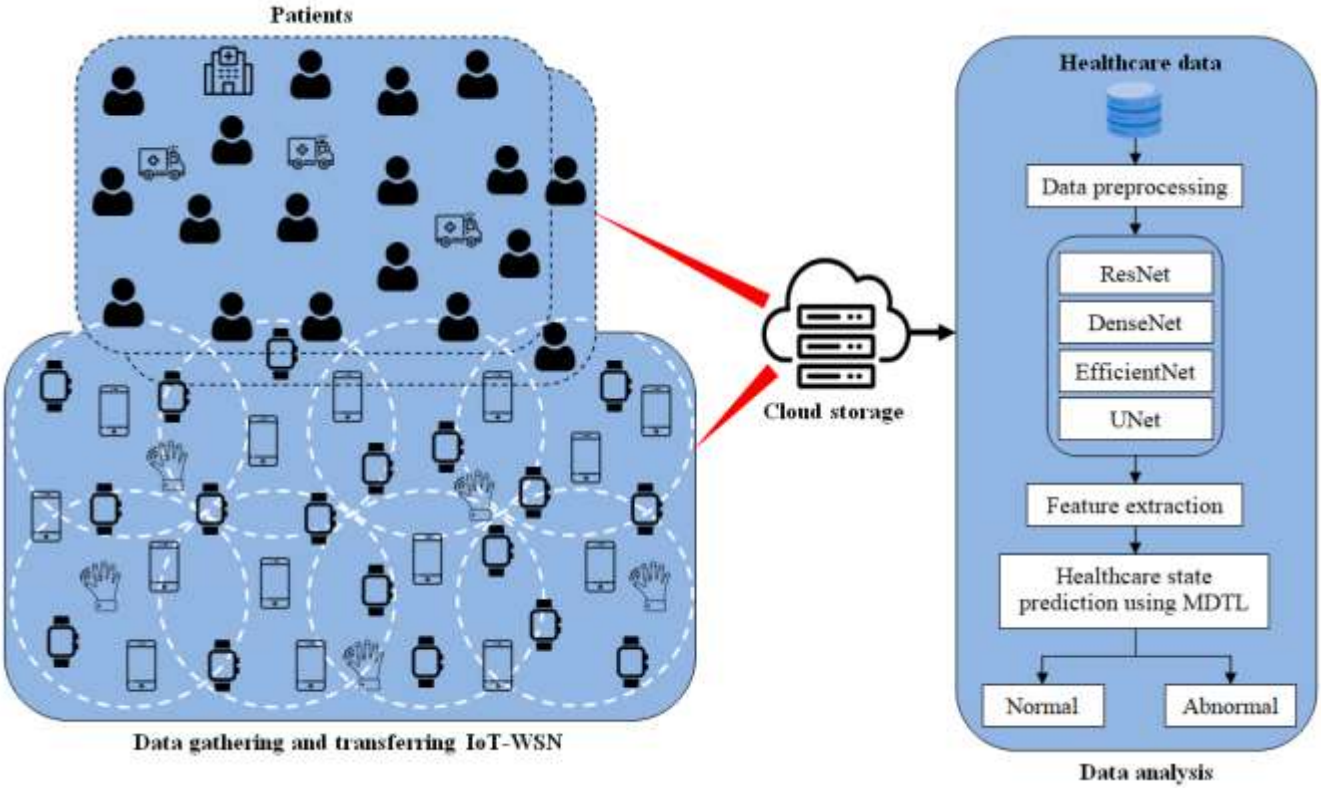


Fig. 1 Conceptual structure of dual secure optimal trusted routing (DST-Route) for data transferring and data handling using a DL model for healthcare state prediction

The system demonstrates strong energy efficiency but still lacks flexibility in handling multi-criteria healthcare decisions. To tackle this, Fractional Fuzzy Set (FFS)-based decision-making was employed, using Hamacher-based aggregation operators to enhance models such as Extended TOPSIS, TODIM, and Extended GRA for complex healthcare system selection [39]. These models offer robust multi-criteria decision support but rely on centralized communication, which may not scale well with expanding healthcare IoT systems. To solve the centralized routing bottleneck, the Interior Neighbors' Route with the Low Fault (INRwLF) routing method was developed using an AI-driven SDN controller to ensure fault-resilient, low-latency communication across healthcare IoT environments [40]. It shows up to 90% reduction in energy usage and latency, making it highly suitable for synchronized, real-time data transmission in dynamic medical settings.

2.2.1. Problem Definition

Despite significant advancements in IoT-enabled healthcare, current healthcare state prediction models face persistent challenges related to secure data transmission, trust management, and predictive accuracy. Many existing frameworks use FL, blockchain, and anomaly detection, exhibit limitations such as weak adaptability in context-aware decision-making, ineffective interference handling in dynamic environments, and a lack of deployment in real-time clinical settings [42]. The centralized architectures and

computationally heavy models often hinder scalability and efficient resource utilization, especially in resource-constrained or rural healthcare scenarios. While some methods achieve high prediction accuracy or improved energy efficiency, they still lack lightweight encryption, robust trust evaluation, and the ability to process complex, high-dimensional health data effectively. To overcome these limitations, this work presents the DST-Route technique aimed at enabling secure, sensitive data transfer along with accurate patient healthcare state prediction in IoT-WSN. For accurate analytics, pre-trained DL models, ResNet, DenseNet, EfficientNet, and UNet are used for feature extraction, while modular deep transfer learning (MDTL) enhances prediction performance.

3. Materials and Methods

Figure 1 illustrates the conceptual structure of the proposed Dual Secure optimal Trusted Routing (DST-Route) architecture, designed for secure data transfer and intelligent data handling in IoT-WSN-based healthcare systems. In this framework, data transfer begins with multiple patients (P1 to PN) equipped with IoT-enabled wearable sensors (type-1), which continuously collect vital health parameters such as heart rate, blood pressure, oxygen saturation, and more. Additional sensors—type-9 for monitoring specific medical sections (S1 to SN), type-10 for environmental sensing (temperature, humidity, etc.), and type-11 for entry/exit tracking—are deployed throughout the hospital to provide contextual awareness and security. These sensors form an IoT-WSN platform, where raw data is captured and transmitted via interconnected sensor nodes. The captured data undergoes trust-based clustering and CH selection using the EPJO algorithm, which ensures that only highly trusted and energy-efficient nodes are selected for data forwarding. To secure sensitive patient data, SmartNetcryption, a lightweight and efficient encryption technique, is applied at the source node level before data transmission. The encrypted data is then routed through the DST-Route protocol, which ensures dual-layer security and trust-aware transmission to the cloud storage server. In the data handling phase, authorized data handlers access the stored encrypted healthcare data from the cloud. After successful decryption, the data undergoes preprocessing to handle missing values, noise, and standardization. Then, feature extraction is performed using multiple pre-trained deep learning models, including ResNet, DenseNet, EfficientNet, and UNet, which extract both spatial and contextual features from the medical data. These extracted features are input into MDTL for accurate healthcare state prediction. This predictive outcome supports early diagnosis and facilitates automated patient-to-doctor allocation, enhancing treatment speed and accuracy. By integrating secure routing, efficient sensor-level encryption, and intelligent deep learning-based diagnosis, the proposed system ensures real-time monitoring, data integrity, and decision support for modern healthcare environments, significantly improving patient outcomes.

3.1. Data Gathering and Transferring

This section outlines the process of acquiring and securely transmitting healthcare data in an IoT-WSN environment. Patient health data is collected through various IoT-enabled sensors and forwarded through a network of nodes. To ensure both reliability and security, the system employs trust-based clustering with optimal CH selection using the EPJO algorithm, along with SmartNetcryption, a lightweight encryption. The encrypted data is then securely routed via the DST-Route protocol and stored in a cloud server for further analysis.

3.1.1. Trust-Based Clustering and Optimal CH Selection

In this context, trust-based clustering is used to organize the IoT-WSN into efficient groups for optimized data communication and energy management. Clustering refers to the process of grouping sensor nodes into clusters, where every cluster is managed by a designated CH. The assortment of CHs and creation of gatherings are based on key parameters such as node outstanding energy, communication cost (distance to neighbors), node connectivity, and the computed trust level of each node. To evaluate the reliability of nodes, a trust degree is computed using a combination of behavioral and energy-based attributes. These include the Packet Forwarding Ratio (PFR), Packet Drop Rate (PDR), Energy Level (EL), Routing Behavior Consistency (RBC), and Node Interaction History (NIH). Each of these factors is integrated into a weighted trust model, resulting in a composite trust score that reflects the node's reliability in participating in secure data transmission.

To achieve optimal clustering and CH selection, the system uses an Enhanced Pomarine Jaeger Optimization (EPJO) algorithm. A variety of the original procedure, inspired by the hunting behavior of seabirds, with modifications that enhance convergence speed and solution quality. The enhancements include adaptive exploration-exploitation control, a hybrid fitness function that considers both energy and trust metrics, and a noise-resistant selection strategy to prevent compromised nodes from being chosen [43]. EPJO ensures that only the most trusted nodes are selected as CHs, maintaining network longevity and data reliability. Pomeranian jigger breakage is avoided, and an additional parameter is included to calculate the new probe intermediate.

$$\overrightarrow{u_T} = v * \overrightarrow{Z_T}(b) \tag{1}$$

Where, $\overrightarrow{u_T}$ is the location of the survey agent, v is a superfluous parameter, $\overrightarrow{Z_T}$is the current location of the examination agent, and b is the present iteration. The inspection mediator drives activities in the region, which are demarcated as follows.

$$v = F_j - \left(b *\times \left(\frac{F_j}{B}\right)\right) \tag{2}$$

Where, F_j is the frequency governor. B is MaxIter and b=0, 1, 2, 3, …, B, and $F_j = 1$ $F_j$governs the value of v. The direction of the supreme fortitude apt Pomarine Jaeger is defined as follows.

$$\overrightarrow{l_T} = W * \left(\left(\overrightarrow{u_{TF}}\right) \cdot (b) - \left(\overrightarrow{u_T}\right) \cdot (b)\right) \quad (3)$$

$\overrightarrow{l_T}$signifies the specific position of the search intermediary in the course of $\overrightarrow{u_{TF}}$. $\overrightarrow{u_{TF}}is$ Supreme fortitude apt Pomarine Jaeger Wto balance between exploration and exploitation

$$W = 2 \times v^2 \times R \quad (4)$$

Where R is a random number [0,1]. All examination peacekeepers appraise the location interpretation to the fitting examination mediator's spot, therefore all scrutiny mediators endure in neighboring proximity, reporting to the appropriate scrutiny mediator.

$$\overrightarrow{dis\ tan\ c\ e_T} = \left|\overrightarrow{u_T} + \overrightarrow{e_T}\right| \quad (5)$$

Where$\overrightarrow{dis\ tan\ c\ e_T}$ indicates the space between the appropriate inspection mediator and others. As soon as the attack on the prey is maintained by the Pomarine Jaeger in midair, a vortex crusade will happen, and it has been selected in m, n, d planes.

$$m' = h * cos(h) \quad (6)$$

$$n' = h * sin(h) \quad (7)$$

$$d' = h * i \quad (8)$$

$$m' = h * cos(h) \quad (9)$$

$$i = g * E^{ai} \quad (10)$$

Where h specifies the radius of the vortex crusadeu_{TF}. i is a random number (0,2), g and a are constants in the vortex crusade.

$$\overrightarrow{u_T}(b) = \left(\overrightarrow{dis\ tan\ c\ e_T} \times m' \times n' \times d'\right) + \left(\overrightarrow{u_{TF}}\right) \cdot (b) \quad (11)$$

The procedure of nourishment with orientation to the Levy function ($l(t, \gamma, \mu)$) incorporated into the EPJO algorithm is described as follows.

$$l(t, \gamma, \mu) = \begin{cases} \sqrt{\frac{\gamma}{2\pi}} exp\left[-\frac{\gamma}{2(t-\mu)}\right] \frac{1}{(t-\mu)^{3/2}} if 0 < \mu < t < \infty \\ 0 if t \leq 0 \end{cases} \quad (12)$$

Opposition-based learning F(L) is integrated in the EPJO algorithm.

$$F(L) = \begin{cases} \frac{1}{2} Exp(-|L-d|/c), n \leq d \\ 1 - \frac{1}{2} Exp(-|L-d|/c), n > d \end{cases} \quad (13)$$

As shown in Algorithm 1, once collections are formed and CHs are particular, patient data composed by IoT-enabled sensor nodes is encrypted using SmartNetcryption—a lightweight encryption technique—and then transmitted through the network. Data forwarding from the source node to the cloud server is done via highly trusted relay nodes, selected based on their trust scores. Ultimately, encrypted health data reaches the cloud storage, ensuring both security and integrity during the transmission process.

Algorithm 1: Optimal clustering and CH selection using EPJO

Input: node ID, location coordinates, residual energy, trust attributes, population size, step sizes, maximum iterations, control coefficients

Output: Clustering and Trust degree computation

1. Begin;
2. Initialize the step sizes of the population.
3. Compute the new probe intermediate. $\overrightarrow{u_T} = v * \overrightarrow{Z_T}(b)$
4. The inspection mediator drives activities in the region$v = F_j - \left(b * \times \left(\frac{F_j}{B}\right)\right)$
5. All scrutiny mediators endure in neighboring proximity, rendering to the appropriate scrutiny mediator.$\overrightarrow{dis\ tan\ c\ e_T} = \left|\overrightarrow{u_T} + \overrightarrow{e_T}\right|$
6. Levy is incorporated in the algorithm, $l(T) \sim |T| - 1 - \beta where 0 < \beta < 2$
7. Quantum features are integrated for fitness computation$|\Psi|^2 \cdot dx \cdot dy \cdot dz = Y \cdot dx \cdot dy \cdot dz$
8. Define the cost quantity, φ, to evade the zero error. $E_h^s = 1/1 + E^{-d}$
9. The midair a vortex crusade and fix thresholds m, n, d planes
10. $v \leftarrow v + 1$
11. Return
12. End

3.1.2. Lightweight Encryption

In IoT-enabled healthcare systems, where patient data is collected from resource-constrained sensor nodes and transmitted over wireless networks, ensuring data confidentiality without overloading the nodes is critical. Lightweight encryption is essential in this context because traditional encryption algorithms often require high computational resources and power, which are limited in wearable or embedded healthcare sensors. To address this, SmartNetcryption-a specialized lightweight encryption technique-is employed. It ensures end-to-end security by

encrypting sensitive patient data at the source node before transmission. SmartNetcryption uses streamlined cryptographic operations that offer a balance between computational efficiency and strong data protection. SmartNetcryption uses minimal latency and energy consumption while maintaining the integrity and confidentiality of healthcare information during transmission [44]. In SmartNetcryption, the size of the block and key is fixed at 64 bits and 128 bits, respectively. Every one of the sixteen rounds involves a limited OR (XOR) logical process to get original explanations$k_r$for 1 ≤ R ≤ 16. The random variations in the optimal solutions are updated by the key-generation process. An extra key is generated and XOR-ed to get the final ciphertext. The misperception coating is a nonlinear alternative (box) table. In the linear fitness follows the XOR operation by using the 80/128-bit keys of the optimal solution in the random search$k_h \rightarrow k_{63}^h \ldots k_0^1$. Explains sub-keys for 1 ≤ h ≤ 16, and the definite productivity$State_{64} \rightarrow t_{63}t_{62} \cdots t_0$is particular as follows.

$$State \rightarrow State \oplus k^h \quad (14)$$

T-box follows the fitness functions $f_2^4 \rightarrow f_2^4$to direct the search for the optimal key. The fitness function follows the T-box sub-optimal function in the 32 bits of 128 bits from the overall solution. A binary permutation operation is performed on the permutation matrix.

$$X_{hg} = X_{hg}P_{hg} \quad (15)$$

The key size of SmartNetcryption is optimized through the SLA scheme key scheduling. The random key scheduling follows the optimal key search in the fixed point fitness computation, and the overlap can function as$Key = K_{79}K_{78} \cdots K_0$ the optimum key.

$$k^h = K_{63}K_{62} \ldots K_0 \quad (16)$$

After the 64-bit key was discovered, the catalogue key was updated.

$$key <<< 13; \quad (17)$$

$$[K_{63}K_{62}K_{61}K_{60}K_{59}] = [K_{63}K_{62}K_{61}K_{60}K_{59}] \oplus rd^h \quad (18)$$

The normalized edge counter follows the random operations in the key-registers along with the XOR operation, which belongs to the maximum operating process fromK_{59} to K_{63}. The user-provided 128-bit key, quantified as$Key = K_{127}K_{126} \cdots K_0$, is contained in the key catalogue KEY. The 64-bit sub-keys LSB $K_h = K_{63}K_{62} \cdots K_0$are written as follows from the round h.

$$k^h = K_{63}K_{62} \ldots K_0 \quad (19)$$

The non-linear optimal solution gives the best optimal ideal keys, which are organized as 64-bit.

$$key <<< 13; \quad (20)$$

$$[K_3K_2K_1K_0] = T[K_3K_2K_1K_0]; \quad (21)$$

$$[K_7K_6K_5K_4] = T[K_7K_6K_5K_4]; \quad (22)$$

$$[K_{63}K_{62}K_{61}K_{60}K_{59}] = [K_{63}K_{62}K_{61}K_{60}K_{59}] \oplus rd^h \quad (23)$$

The transformation round keys are used to construct the key table in reverse order. The same amount of encryption is used in the decryption process, which runs through its steps every time. The identical round key on the overall block of SmartNetcryption is XOR-ed to accomplish the inversion in the add_round_key layer. The decoding process follows the median function along with the S-box and permutation layers. The encrypted data is then routed through trusted nodes, selected via the EPJO algorithm, before being securely stored in the cloud server for further prediction.

3.2. Data Analytics

After secure data storage, the analytics phase begins with data retrieval and decryption. The data undergoes preprocessing to ensure quality and consistency. In order to capture pertinent healthcare trends, feature extraction is carried out using pre-trained deep learning models like ResNet, DenseNet, EfficientNet, and UNet. The extracted features are fed into the MDTL model, which enables accurate healthcare state prediction and supports early diagnosis by using knowledge from multiple trained models.

3.2.1. Data Preprocessing

Data preprocessing plays a crucial role in ensuring the accuracy and reliability of healthcare analytics, especially when working with real-time data collected from IoT-enabled wireless sensor networks. Once the encrypted data is securely retrieved from cloud storage, it is first decrypted using the SmartNetcryption algorithm to convert it into a readable format for analysis. The decrypted data often contains noise, inconsistencies, missing values, and redundant entries due to sensor inaccuracies or transmission delays. To address this, a systematic preprocessing workflow is applied to clean and prepare the data [45]. The process begins with data cleaning, where duplicate records and irrelevant values are identified and removed. Structural inconsistencies such as incorrect formats or unit mismatches are corrected to ensure uniformity across the dataset. Following this, missing values are detected and handled appropriately using statistical imputation techniques such as mean, median, or class-based filling, depending on the nature of the data. In many cases, time-series health data may have irregular spikes or dips caused by sensor glitches or environmental interference; hence, noise removal techniques such as smoothing filters are applied to eliminate such fluctuations and preserve the meaningful trends in the

signal. Normalization is also a key part of preprocessing, where all sensor data values are scaled to a common range using min-max normalization or standardization techniques. This step prevents any single feature from dominating the learning process and ensures balanced model training. Finally, categorical data-such as patient conditions, sensor types, or status codes-are converted into numerical format using label encoding to make the dataset compatible with deep learning algorithms.

3.2.2. Feature Extraction using Pre-Trained Models

After preprocessing the sensor-based healthcare data, the next critical step is feature extraction, which transforms raw input into informative representations that can effectively support healthcare state prediction. In this framework, the pre-trained deep learning models-namely ResNet [46], DenseNet [47], EfficientNet [48], and UNet [49]-are not for image analysis, but for their ability to capture temporal and statistical patterns in structured, time-series sensor data. These models, originally trained on large datasets, are adapted through fine-tuning and transfer learning to work with one-dimensional or tabular data typically collected from wireless body sensor nodes. The process begins by formatting the preprocessed data into suitable input sequences. These inputs are fed into modified versions of the pre-trained models, where the initial layers are repurposed to detect abstract features such as trends, signal correlations, sudden fluctuations, and periodic changes in physiological parameters (e.g., heart rate variability, oxygen saturation levels, temperature trends, or motion patterns). For example, ResNet and DenseNet architectures are used to extract deep hierarchical patterns and long-term dependencies in sequential health data. EfficientNet offers a balance between accuracy and computational efficiency, making it ideal for capturing high-level aggregated features. Though UNet is used in segmentation tasks, in this context, it is repurposed to identify transitional states and edge patterns in multi-sensor streams through its encoder-decoder structure. The features extracted from these models include temporal dynamics, frequency-domain signatures, anomalies, and health-related condition indicators derived from sensor signals. These high-level features provide a rich representation of a patient's physiological state, which is then passed on to the modular deep transfer learning (MDTL) model for final classification and prediction. It not only improves model generalization but also enables accurate and early diagnosis by using deep semantic understanding of the sensor data patterns.

3.2.3. Healthcare State Prediction

Healthcare state prediction refers to the process of analyzing patient data to determine their current health condition and to forecast potential future health risks or abnormalities. This prediction helps healthcare professionals make informed decisions for early intervention, treatment adjustments, or emergency response. In this context, a Modular Deep Transfer Learning (MDTL) is used to perform accurate healthcare state prediction by leveraging the combined knowledge of deep learning models pre-trained on large, diverse datasets. MDTL integrates these models into a modular pipeline, where each module is specialized for learning distinct aspects of the input data, such as physiological trends, anomaly detection, and inter-signal dependencies [50].

The process begins by feeding the high-level features extracted from the sensor data (as described in Section 3.2.2) into the MDTL framework. Each module in the MDTL architecture is built upon a different pre-trained model adapted to the healthcare domain using transfer learning techniques. These modules are fine-tuned on the target dataset, allowing them to retain general knowledge from the source domains while learning task-specific patterns from patient sensor data. After independent learning, the outputs from each module are aggregated using a fusion mechanism to produce a final prediction of the patient's health state. This output includes classifications like "normal," "at risk," or "critical," depending on the specific application. The use of MDTL not only improves the prediction accuracy but also expands robustness and generalizability, especially when dealing with heterogeneous or limited healthcare datasets. This results in more reliable and early diagnoses, which are essential for proactive patient care in IoT-enabled healthcare systems. Modelling the h-th subsystem (predicting the state trajectory forp_h) is the aim of the h-th subtask. This may be described by$\dot{\hat{p}}_h = f_h(\hat{p}_h, U_h)$, where $\hat{p}_h$ is the expected value forp_hh=1,…, b. The h-th subsystem in a process network is challenging to represent, though, because its state (p_h) is influenced by the system's overall state (p). The isolated subsystem's dynamics can be roughly described as follows.

$$\dot{\hat{p}}_h = j_h(\hat{p}_h, U_h) \tag{24}$$

Where$\hat{p}_h \in R^{K_h}$, and $U_h \in R^{b_h}$are the state-owned direction for the h-th subsystem and the artificially constructed input are where and, respectively. The prediction result $p_h$depends only on the own state and control actionsU_h. The MDTL model fully captures the dynamics of the n-th solution when connected to the network, because it ignores the interaction between subsystems.

$$\dot{\hat{p}}_h = f_h\left(j_h\left(\hat{p}_h, U_h\right), J_h, i_h(\hat{p}, U)\right) \tag{25}$$

$f_h(\cdot,\cdot,\cdot)$ It is a nonlinear function with three influences. $j_h(\cdot,\cdot)$ It is a separate progression, regardless of the relationship between subsystems. Using only a few examples, the MDTL model rapidly generalized to jobs that were comparable. The reptile technique's search for ideal weight vectors can be shown as follows.

$$\underset{\varphi}{Mine}_K\left[\frac{1}{2}C(\varphi, Z_K^*)^2\right] \tag{26}$$

Where, Z_K^* means the ideal height limitations for the K-th charge and $C(\varphi, Z_K^*)^2$is the Euclidean detachment among the weight directions ϕ and Z_K^*. Assume that there are m blocks in the inventory $A = \{A_1 \dots A_h \dots A_a\}$to complete t tasks$S = \{S_1 \dots S_h \dots S_s\}$. Module selection for every job is carried out via the routing function, which is expressed as follows:

$$m_{h,g} = \begin{cases} 1 if A_h is selected for S_g \\ 0 otherwise \end{cases} \quad (27)$$

The binary matrix is as follows:$M = \left[m_{h,g}\right]_{a \times s}$, which displays the blocks chosen for every task. An understanding of the process network and the functions of its subsystems is necessary to ascertain what $m_{h,g}$ it means. These procedures can be used to choose the blocks and values that $m_{h,g}$ are used. A collection of modules for the h-th subsystem's upstream units, which have an impact on the subsystem's dynamics, is advised. The following optimisation problem represents the ni-tuning procedure for the MDTL model.

$$\underset{j_h \subseteq J, i_h \subseteq I, f_h \subseteq f}{Min} \left| \sum_{h--1}^{b} \left(\dot{p}_h - f_h\left(j_h(\hat{p}_h, U_h), J_h', i_h(\hat{p}, U)\right)\right)\right| \quad (28)$$

Here, J, I, and F denote the set of hypothesis function sets forj_h, i_h, and f_h, respectively. This $J_h'$is a subset of $J_h$the standard routing function selection. When adapting the basic classical model to the objective domain, the net-tuning method is used to train the model parameters. The learning process of MDTL utilizes the search process to find optimal nonlinear functionsj_h^*,i_h^*, and f_h^*. Algorithm 2 describes the working process of health state prediction using MDTL.

Algorithm 2: Health state prediction using MDTL

Input: Number of features, step sizes, hyperparameters, maximum iteration
Output: Predicted healthcare states S∈{Normal, Risk, Critical}

1. Initialize the step sizes of the population.
2. A set of source processes for some isolated subsystems, first principles models, and data collected for models and process networks.
3. for iteration number $i \leq$ B do
4. Fix the dynamics of the isolated subsystem,$\dot{\hat{p}}_h = j_h(\hat{p}_h, U_h)$
5. Define optimal weight vectors using the reptile method.$\underset{\varphi}{Mine}_K \left[\frac{1}{2} C(\varphi, Z_K^*)^2\right]$
6. Fine-tune fitness using maximum step-size using an optimization problem: $\underset{j_h \subseteq J, i_h \subseteq I, f_h \subseteq f}{Min} \left| \sum_{h--1}^{b} \left(\dot{p}_h - f_h\left(j_h(\hat{p}_h, U_h), J_h', i_h(\hat{p}, U)\right)\right)\right|$
7. End for
8. Combine the features using an adaptive fusion strategy to fix the threshold.
9. Fix foundation blocks
10. Compute black-box neural network components.
11. Optimizes aggregation layers to fix the threshold set for transfer learning
12. End

4. Results and Discussion

The proposed research encompasses two critical phases: data gathering and secure transmission, followed by data analysis for accurate healthcare state prediction. The data gathering and transmission phase was implemented and simulated using NS2 (Network Simulator 2), while the data analysis and healthcare prediction components were developed and executed using Python. Both simulation and implementation were carried out on a laptop equipped with an Intel Core i7 processor and 16GB of RAM, ensuring sufficient computational power for handling real-time data flow and complex model training. In the NS2 simulation environment, a Wireless Sensor Network (WSN) was deployed to mimic an IoT-enabled healthcare monitoring infrastructure.

The IoT devices were represented as WSN nodes configured with UDP and TCP/IP communication protocols. Various network parameters, such as the simulation area, number of nodes, packet size, propagation model, antenna type, and transmission interval, were carefully defined in the NS2 script. The simulation was run for 20 seconds to evaluate the performance and reliability of the proposed DST-Route protocol under typical healthcare data transmission conditions.

For data analysis, the Python environment is used to process and model the extracted data, alongside a publicly available benchmark dataset from Kaggle, the stroke prediction dataset. This dataset includes 5110 records with 12 distinct attributes, such as patient ID, gender, age, marital status, work type, residence type, body mass index (BMI), and others. These features are particularly relevant for identifying the risk of stroke in patients. The dataset was preprocessed to ensure data integrity and then partitioned into three subsets: 80% for training, 10% for validation, and 10% for testing.

4.1. Results Analysis of Routing Techniques

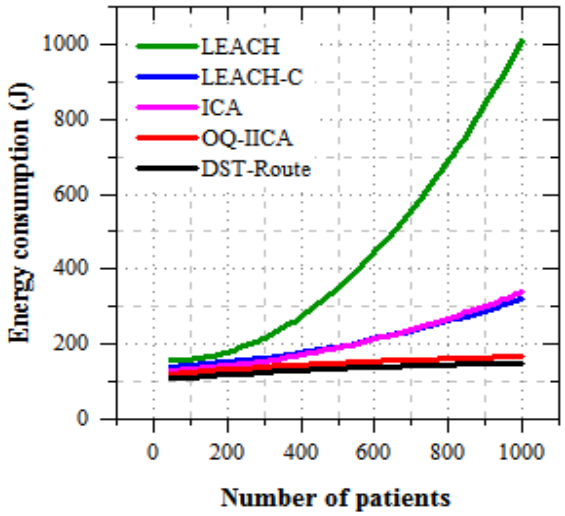
To calculate the presentation of the suggested DST-Route technique, a comprehensive simulation environment was created using NS2. As described in Table 3, the setup includes key aspects such as node configuration, energy constraints, communication models, and network topology. The number of nodes in the network varies from 20 to 100, reflecting scalability in sensor deployments. The simulation area is fixed at 1500×1500 meters, offering sufficient space for nodes to be randomly deployed. Each sensor node starts with an initial energy of 1000 joules. The cluster radius is set at 400 meters, determining the communication range for cluster-based

routing mechanisms such as LEACH and LEACH-C. Transmission power at individual sensor nodes is maintained at 0.819μJ, while the overall network transmission and receiving powers are 0.5819 J and 0.049J, respectively, accounting for energy consumption during communication.

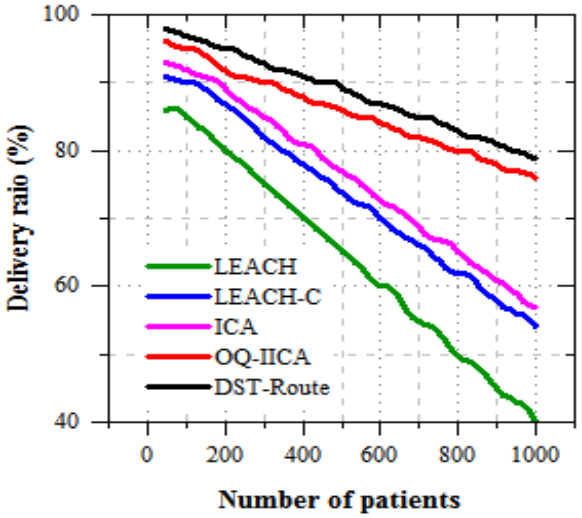
The results of the proposed DST-Route technique are evaluated and compared against several existing routing protocols, including improved clustering algorithm (ICA), low energy adaptive clustering hierarchy (LEACH), its centralized variant LEACH-C, and the QoS-aware intra-inter cluster data aggregation (OQ-IICA).

Table 3. Simulation parameters

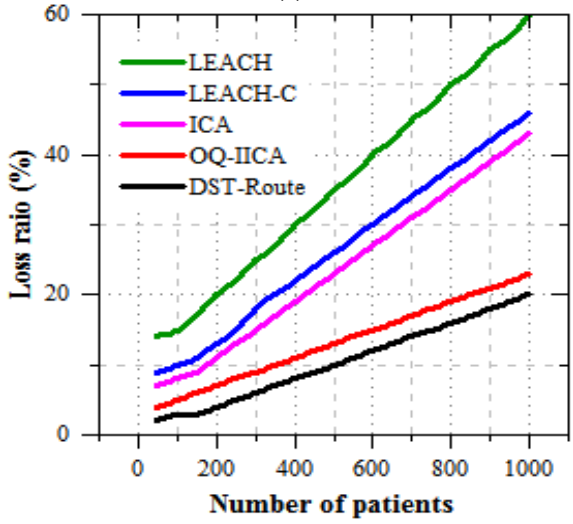
Parameter	Value
Number of nodes	100, 200, 300, 400, 500
Network size	1500 × 1500 m
Initial energy	1000 J
Cluster radius	400 m
Transmission power at the node	0.819 μJ
Channel type	Wireless
Transmission power	0.5819 J
Receiving power	0.049 J
Propagation model	Two-way
Data size	50 – 400 bytes
MAC protocol type	802.11
Simulation time	0 – 800 s
Packet transmission interval	e.g., 1 – 5 seconds
Node deployment	Random
Traffic type	Constant Bit Rate (CBR)
Antenna model	Omni Antenna / Directional Antenna
Mobility model	Random Waypoint



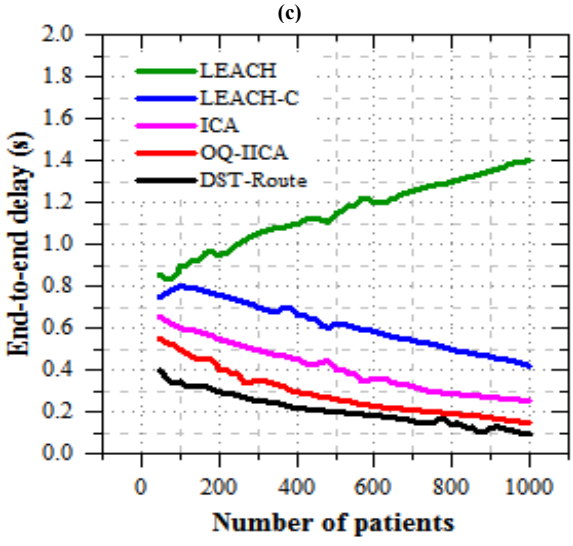
(a)



(b)



(c)



(d)

Fig. 2 Results comparison of routing techniques with respect to varying number of patients (a) Energy consumption, (b) Delivery ratio, (c) Loss ratio, and (d) End-to-end delay.

Figure 2 presents the comparative performance analysis of five routing techniques-LEACH, LEACH-C, ICA, OQ-IICA, and DST-Route-under varying numbers of patients (from 50 to 1000) across four key metrics: energy consumption, delivery ratio, loss ratio, and end-to-end delay. In terms of energy consumption (Figure 2(a)), DST-Route consistently outperforms the other techniques by maintaining the lowest energy usage throughout. At 50 patients, DST-Route records an energy consumption of 108.95J, which gradually increases to only 150.48J at 1000 patients. In comparison, LEACH starts at 157.31J and rises steeply to 1009.6J.

This indicates a significant reduction in energy consumption of approximately 85% compared to LEACH at the highest patient load. Similarly, DST-Route consumes about 53% less energy than LEACH-C and around 55% less than ICA at 1000 patients. Even when compared with the more optimized OQ-IICA, DST-Route still shows a 10% reduction in energy usage, highlighting its superior efficiency in handling data transmission with minimal energy overhead. The delivery ratio results (Figure 2(b)) further confirm DST-Route's reliability, with delivery rates starting at 98% for 50 patients and remaining as high as 79% at 1000 patients. In contrast, LEACH exhibits a rapid decline from 86% to just 40% over the same range, showing a 46-percentage-point drop. LEACH-C, ICA, and OQ-IICA also show decreasing trends but still lag behind DST-Route, which achieves about 3.9% higher delivery at peak load compared to OQ-IICA.

These results clearly demonstrate that DST-Route maintains high data delivery efficiency even under high network stress. For the loss ratio metric (Figure 2(c)), DST-Route again delivers the best performance, maintaining a minimal packet loss rate from 2% at 50 patients to 20% at 1000 patients. In contrast, LEACH records a loss increase from 14% to 60%, which is three times higher than DST-Route at 1000 patients. LEACH-C and ICA show moderate improvement but still incur significantly higher losses. Even compared to OQ-IICA, DST-Route achieves 3% lower loss at higher loads, indicating better control over data packet integrity. End-to-end delay analysis (Figure 2(d)) shows that DST-Route consistently ensures the lowest transmission delay, which is critical in real-time patient monitoring applications. The delay reduces from 0.4 seconds at 50 patients to just 0.1 seconds at 1000 patients, while LEACH shows a steep increase from 0.85 seconds to 1.4 seconds over the same range. DST-Route thus achieves a delay reduction of approximately 92.85% compared to LEACH at maximum load and about 76% lower delay than OQ-IICA, proving its efficiency in fast data delivery. The analysis from Figure 2 across all four performance metrics demonstrates that DST-Route is the most optimal and scalable routing protocol.

4.2. Results Analysis of Encryption Techniques

Table 4 presents a comparative analysis of various encryption techniques-AES-128, PRESENT, TEA, ECC, Blockchain, and SmartNetcryption—based on their performance, security strength, and resource efficiency for healthcare WSN-IoT. In terms of encryption and decryption time, SmartNetcryption demonstrates the fastest execution, with only 45 µs for encryption and 43 µs for decryption, significantly outperforming all other methods. TEA and PRESENT also show low latency, while Blockchain exhibits the slowest performance, requiring 1200µs for encryption and 1180 µs for decryption, making it unsuitable for a time-critical healthcare solution. ECC also shows high latency, indicating greater computational overhead. When considering memory usage, SmartNetcryption is the most efficient, consuming just 1.8 KB, followed by TEA and PRESENT. AES-128 uses a moderate 12 KB, while ECC requires 24 KB. Blockchain demands more than 30 KB, highlighting unsuitability for resource-constrained healthcare sensors and devices. This comparison emphasizes the lightweight nature of SmartNetcryption, which is critical for embedded systems in WSN-IoT environments. In terms of computational complexity, SmartNetcryption, TEA, and PRESENT maintain a linear complexity O(n), contributing to their efficiency. AES-128 has quadratic complexity of $O(n^2)$, positioning it between the extremes in terms of computational load. With regard to brute-force resistance, ECC and Blockchain offer high protection, while AES-128 and SmartNetcryption provide high resistance. PRESENT and TEA offer only moderate resistance, indicating that they may not be suitable for applications requiring strong protection against exhaustive attacks. In resistance to differential attacks, AES-128, ECC, Blockchain, and SmartNetcryption all show strong resilience, whereas TEA is weak, and PRESENT offers only moderate defense. In confidentiality validation, SmartNetcryption and AES-128 are validated by NIST standards, with SmartNetcryption also meeting the Avalanche effect criteria, indicating robust key diffusion. ECC and Blockchain are classified as strong, while PRESENT is moderate, raising concerns about information leakage.

Table 4. Comparative analysis of encryption techniques based on security, performance, and resource efficiency metrics for healthcare WSN-IoT

Metric	AES-128	PRESENT	TEA	ECC	Blockchain	SmartNetcryption
Encryption time (µs)	220	90	80	350	1200	45
Decryption time (µs)	210	85	78	340	1180	43
Memory usage (KB)	12	2.5	2	24	>30	1.8
Computational complexity	$O(n^2)$	O(n)	O(n)	$O(n^3)$	$O(n^3)$	O(n)
Brute-force resistance	High	Moderate	Moderate	Very High	Very High	High
Resistance to differential	Strong	Moderate	Weak	Strong	Strong	Strong

attacks						
Replay/Impersonation attack	Moderate	Weak	Weak	High	Very High	High
Confidentiality validation	Pass (NIST)	Moderate	Poor	Strong	Strong	Pass (NIST)
Integrity validation	MAC/Checksum	CRC	None	Digital Sig.	Blockchain Hash	MAC + Lightweight Hash

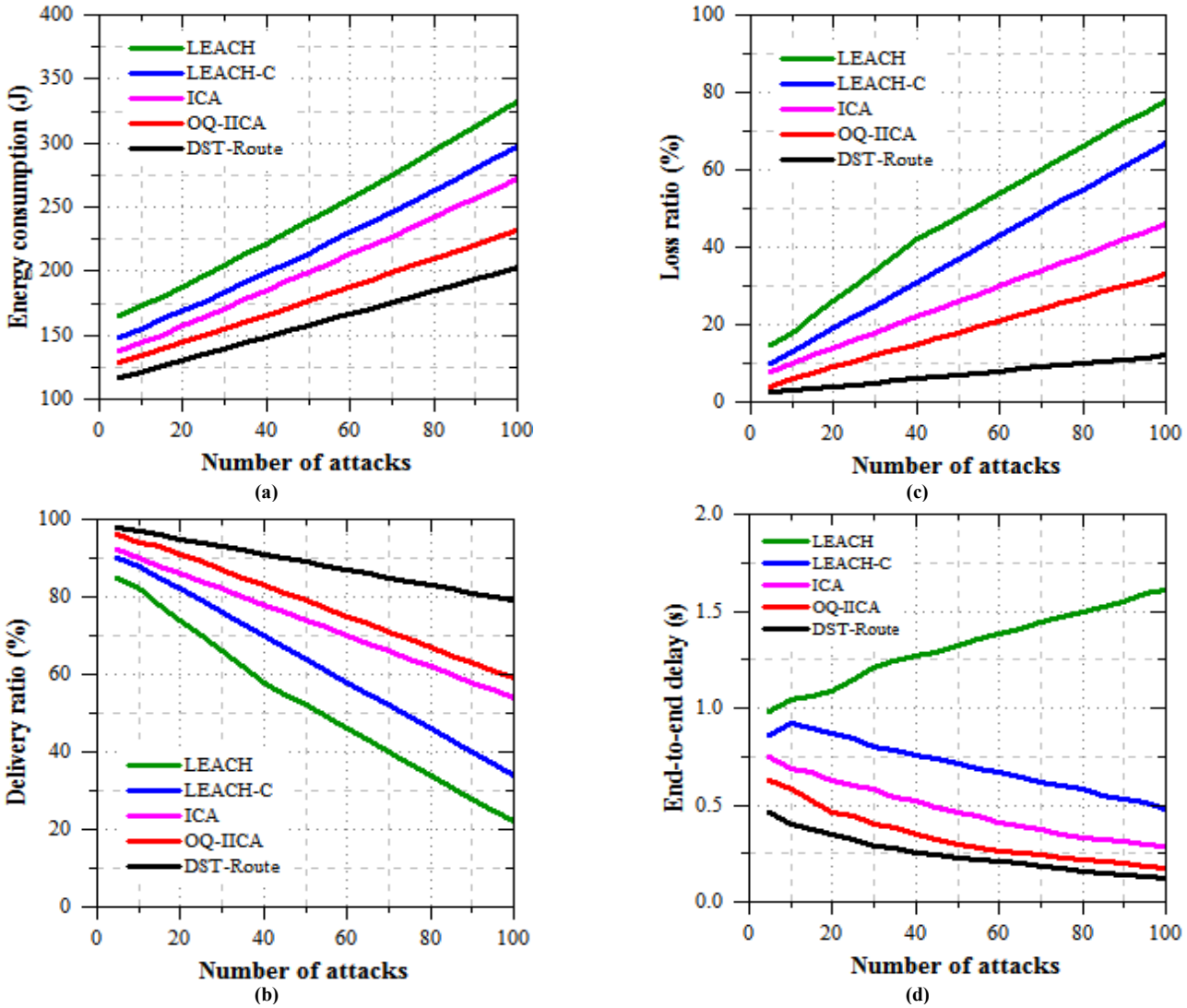


Fig. 3 Results comparison of routing techniques with respect to varying number of attacks (a) Energy consumption, (b) Delivery ratio, (c) Loss ratio, and (d) End-to-end delay.

Regarding integrity validation, Blockchain offers the most advanced mechanism via Hash, ensuring immutability and traceability. ECC utilizes digital signatures, and SmartNetcryption combines MAC and a lightweight hashing mechanism for efficient integrity assurance. AES-128 uses MAC/Checksum, while PRESENT relies on CRC, and TEA provides no integrity support, which limits its applicability in secure environments. SmartNetcryption emerges as the most balanced and efficient encryption method, offering strong security, ultra-low latency, minimal memory usage, and linear computational complexity. PRESENT and TEA are lightweight but lack critical security properties. AES-128 is moderately secure and efficient, but is outperformed by SmartNetcryption in all major aspects, making it a highly promising encryption scheme for next-generation secure healthcare applications.

Figure 3 presents a comprehensive comparison of five routing techniques-LEACH, LEACH-C, ICA, OQ-IICA, and DST-Route-under varying attack intensities, ranging from 5 to 100 attacks. As shown in Figure 3(a), energy consumption increases with the number of attacks across all protocols. LEACH exhibits the highest energy usage, rising from 165 units at 5 attacks to 332 units at 100 attacks, indicating 12.561% improvement. LEACH-C and ICA show improvements over LEACH, but still face substantial

overheads. DST-Route demonstrates the most energy-efficient behavior, increasing only from 117 to 22.5 units-a 73% rise. This highlights that DST-Route consumes approximately 39% less energy than LEACH under heavy attack conditions, due to its intelligent and adaptive routing design. In a no-attack scenario, this minimal increment confirms that DST-Route is highly energy-resilient compared to conventional techniques. In Figure 3(b), the delivery ratio declines progressively as the number of attacks increases. OQ-IICA maintains a relatively higher delivery ratio, dropping from 96% to 59%, indicating an18.5% decrease.

In the without-attack scenario, most protocols would remain near the initial values (98% for DST-Route), confirming the protocol's minimal sensitivity to adversarial disruptions. Figure 3(c) illustrates the corresponding increase in loss ratio. LEACH's loss ratio rises alarmingly from 15% to 78% with increasing attacks, while LEACH-C and ICA escalate to 67% and 46%, respectively. OQ-IICA manages to control the loss up to 33%, but DST-Route again stands out by increasing from just 2.5% to only 12%-a mere 9.5% rise. Compared to the no-attack scenario (where loss would ideally be near-zero), the minimal rise for DST-Route clearly reflects its superior error handling and route recovery mechanisms. Figure 3(d) shows how end-to-end delay is affected by attack intensity. LEACH experiences a substantial rise from 0.98s to 1.61s, while LEACH-C and ICA suffer from significant delays. OQ-IICA offers improved latency control, but DST-Route records the lowest and most stable delay, improving from 0.46s to only 0.12s-a 74% improvement over LEACH under the adverse conditions. The low and stable delay observed in the absence of attacks further reinforces the protocol's adaptability. Compared to the without-attack scenario, DST-Route shows minimal degradation, whereas traditional techniques deteriorate severely under attack conditions.

4.3. Results Analysis of Health State Prediction Models

For the analysis, a benchmark stroke prediction dataset from Kaggle containing 5110 records with 12 relevant features was used. After preprocessing, the dataset was split into training (80%), validation (10%), and testing (10%) sets. Additionally, routing data from NS2 was integrated for enhanced health state prediction. Initially, 10-fold cross-validation was performed to evaluate model stability. The results of proposed models such as ResNet+MDTL, DenseNet+MDTL, EfficientNet+MDTL, and UNet+MDTL are compared with the existing models, probabilistic fuzzy recurrent neural network(P-FRNN) [51], Density-Based Spatial Clustering of Application with Noise (DBSCAN) [52], Naïve Bayes[53], and Deep Convolutional Neural Network and Long Short-Term Memory(DCNN+LSTM) [42]. A detailed comparison of training and testing accuracy and loss was conducted across 500 epochs to observe learning trends. The results summarized in Table 5 present a comparison across four key metrics: accuracy, precision, recall, and F-measure. Across all folds, ResNet consistently outperformed other models in terms of accuracy, with its performance peaking at 94.92% in fold 7 and maintaining an average above 93%. DenseNet also showed competitive performance, especially in fold 4, where it surpassed ResNet slightly, achieving an accuracy of 93.14%. In terms of precision, a similar pattern was observed, with ResNet again leading in most folds. For instance, in fold 6, ResNet achieved a high precision of 92.56%, followed by DenseNet at 90.49%. When analyzing recall, ResNet once more displayed strong performance, with values consistently around or above 93%, peaking at 94.85% in fold 2. DenseNet also maintained competitive recall values, often exceeding 91%. ResNet showed better false positives and false negatives, with values frequently above 92%. The MDTL model's training and validation results for health status prediction are shown in Figure 4.

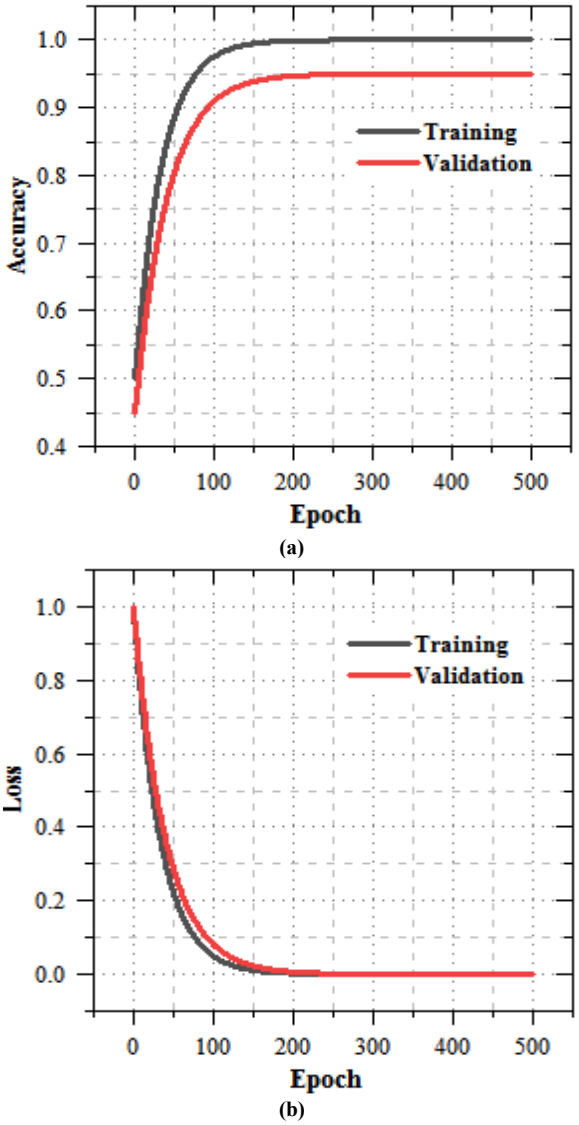


Fig. 4 Training and Validation performance of proposed MDTL model for health state prediction (a) Accuracy, and (b) Loss comparison.

Table 5. Performance of pre-trained models for feature extraction with respect to k-fold cross-validation

k-folds	ResNet	DenseNet	EfficientNet	UNet	ResNet	DenseNet	EfficientNet	UNet
	Accuracy (%)				Precision (%)			
1	92.750	91.590	90.980	88.860	91.610	90.780	89.270	87.910
2	94.750	92.160	91.250	88.140	92.840	90.930	90.180	87.270
3	93.230	91.640	91.660	90.460	91.130	91.360	90.210	88.020
4	92.230	93.140	91.990	88.520	91.290	90.940	90.870	87.420
5	92.860	91.520	91.300	89.770	91.990	91.750	89.450	86.870
6	93.160	91.750	90.680	88.560	92.560	90.490	89.600	86.940
7	94.920	92.980	90.520	89.820	92.810	91.630	90.970	86.900
8	93.310	92.290	90.590	88.530	91.020	90.370	90.610	87.120
9	92.580	91.340	91.860	89.010	91.740	90.950	89.600	88.580
10	94.260	91.970	91.290	89.490	92.060	91.840	89.940	87.890
	Recall (%)				F-measure (%)			
1	93.970	91.570	90.890	89.720	94.080	91.660	91.870	88.710
2	94.850	93.180	91.220	88.910	93.680	92.010	91.690	89.910
3	93.420	91.140	90.060	88.640	92.210	91.450	91.880	90.330
4	92.660	92.310	90.700	88.840	92.880	92.340	91.650	88.610
5	94.090	91.760	91.750	89.380	91.600	91.690	91.700	88.780
6	92.940	91.910	91.490	89.230	92.990	92.570	91.840	89.360
7	92.970	91.320	90.010	88.610	92.590	91.940	90.880	88.570
8	92.300	91.880	91.850	88.450	91.570	90.540	91.600	89.680
9	93.990	90.840	91.650	89.350	93.100	90.810	91.160	89.510
10	93.910	91.730	90.410	88.150	91.530	91.570	91.330	88.580

Table 6. Results comparison for healthcare state prediction models

Model	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)
P-FRNN [51]	92.138	88.457	90.382	89.409
DBSCAN [52]	78.652	75.236	72.814	74.005
Naïve Bayes [53]	95.834	95.382	96.218	95.798
DCNN+LSTM [42]	96.429	90.671	92.417	91.536
ResNet+MDTL	97.316	95.624	96.829	96.223
DenseNet+MDTL	97.542	96.182	96.237	96.209
EfficientNet+MDTL	97.879	96.014	96.998	96.503
UNet+MDTL	97.985	96.764	97.012	96.888

Table 6 presents a comparative analysis of various healthcare state prediction models based on accuracy, precision, recall, and F-measure. The proposed MDTL-based models showed superior accuracy compared to existing methods. DBSCAN shows the lowest accuracy of 78.652%, while Naïve Bayes achieves 95.834%. DCNN+LSTM reaches 96.429%, and P-FRNN stands at 92.138%. With the integration of MDTL, ResNet, DenseNet, EfficientNet, and UNet, we achieve accuracy of 97.316%, 97.542%, 97.879%, and 97.985%, respectively. UNet+MDTL improved accuracy by 2.151% over Naïve Bayes and 1.556% over DCNN+LSTM, confirming the effectiveness of MDTL. In terms of precision, DBSCAN performs the weakest at 75.236%, while Naïve Bayes records 95.382%. The DCNN+LSTM model achieves 90.671%, and P-FRNN follows with 88.457%. MDTL-based models outperform all others, with ResNet+MDTL at 95.624%, DenseNet+MDTL at 96.182%, and EfficientNet+MDTL at 96.014%. The highest precision is observed with UNet+MDTL at 96.764%, which is 1.382% higher than Naïve Bayes and 6.093% higher than DCNN+LSTM. Recall scores reflect a similar trend, with DBSCAN and P-FRNN recording 72.814% and 90.382%, respectively. Naïve Bayes achieves 96.218%, while DCNN+LSTM reaches 92.417%. ResNet+MDTL records 96.829%, DenseNet+MDTL achieves 96.237%, and EfficientNet+MDTL improve further to 96.998%. UNet+MDTL tops the list with a recall of 97.012%, represent4.595% improvement over DCNN+LSTM and 6.63% increase over P-FRNN. The F-measure consolidates precision and recall, where DBSCAN scores the lowest at 74.005% and P-FRNN achieves 89.409%. Naïve Bayes records 95.798%, and DCNN+LSTM improves to 91.536%. MDTL-based models enhance the F-measure: ResNet+MDTL at 96.223%, DenseNet+MDTL at 96.209%, and EfficientNet+MDTL at 96.503%. UNet+MDTL delivers the best performance with an F-measure of 96.888%, marking 1.09% improvement over Naïve Bayes and 5.352% improvement over DCNN+LSTM.

5. Conclusion

The Dual Secure optimal Trusted Routing (DST-Route) technique offers a comprehensive solution for secure, energy-efficient, and accurate data transmission in IoT-based healthcare systems. It achieves dual security by integrating trust-based routing through the Enhanced Pomarine Jaeger Optimization (EPJO) and data-level encryption using SmartNetcryption. The comparison between with and without encryption highlights that, without encryption, sensitive healthcare data remains exposed despite secure routing, whereas the integration of SmartNetcryption significantly enhances data confidentiality and integrity with minimal computational cost. Performance evaluations confirm that DST-Route reduces energy consumption by up to 85%, achieves a high delivery ratio of 98%, and maintains low latency and packet loss even under attack conditions.

Furthermore, the inclusion of Modular Deep Transfer Learning (MDTL) with models like UNet and ResNet boosts diagnostic accuracy, with UNet+MDTL reaching 97.985%. Thus, DST-Route stands out as a scalable, secure, and intelligent framework that effectively addresses the pressing needs of real-time, trust-aware, and privacy-preserving healthcare monitoring in IoT-WSN environments.

References

[1] Maria Trigka, and Elias Dritsas, "Wireless Sensor Networks: From Fundamentals and Applications to Innovations and Future Trends," *IEEE Access*, vol. 13, pp. 96365-96399, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] Nkolika O. Nwazor et al., "Energy Optimization of Wireless Body Area Network (WBAN) Using TDMA Duty Cycling and Thermal Energy Harvesting," *Advances in Science and Technology*, vol. 160, pp. 245-263, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] Farag M. Sallabi et al., "Smart Healthcare Network Management: A Comprehensive Review," *Mathematics*, vol. 13, no. 6, pp. 1-37, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] Shreeram Hudda, and K. Haribabu, "A Review on WSN based Resource Constrained Smart IoT Systems," *Discover Internet of Things*, vol. 5, no. 1, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] Siyuan Li et al., "Trustworthy AI-Generative Content for Intelligent Network Service: Robustness, Security, and Fairness," *IEEE Communications Magazine*, pp. 1-7, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[6] Anum Nawaz et al., "Blockchain Powered Edge Intelligence for U-Healthcare in Privacy Critical and Time Sensitive Environment," *arXiv Preprint*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[7] Vikas et al., "Trusted Energy-Aware Hierarchical Routing (TEAHR) for Wireless Sensor Networks," *Sensors*, vol. 25, no. 8, pp. 1-36, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[8] Basudeb Bera, Ashok Kumar Das, and Biplab Sikdar, "Quantum-Resistant Secure Communication Protocol for Digital Twin-Enabled Context-Aware IoT-Based Healthcare Applications," *IEEE Transactions on Network Science and Engineering*, vol. 12, no. 4, pp. 2722-2738, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[9] T.C. Swetha Priya, and R. Sridevi, "Security Vulnerabilities and Countermeasures for Wireless Sensor Networks in Cyber-Physical Systems," *Challenges and Solutions for Cybersecurity and Adversarial Machine Learning*, pp. 415-448, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[10] Sheeja Rani S., Raafat Aburukba, and Khaled El Fakih, "Wireless Sensor Networks for Urban Development: A Study of Applications, Challenges, and Performance Metrics," *Smart Cities*, vol. 8, no. 3, pp. 1-51, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Avaneesh Singh et al., "Resilient Wireless Sensor Networks in Industrial Contexts via Energy-Efficient Optimization and Trust-Based Secure Routing," *Peer-to-Peer Networking and Applications*, vol. 18, no. 3, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[12] Chakadkit Thaenchaikun, and Komsan Kanjanasit, "A Comparative Study of OSPF Metrics in Routing Algorithms for Dynamic Path Selection in Network Security," *ASEAN Journal of Scientific and Technological Reports*, vol. 28 no. 2, pp. 1-17, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[13] Yiju Zing, and Na Zhao, "Routing Revolution: Strategic Applications of Meta-Heuristic AI in Wireless Sensor Networks-A Comprehensive Survey," *Multimedia Tools and Applications*, vol. 84, no. 35, pp. 44605-44646, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[14] M. Murali, "Advancing Remote Healthcare Monitoring: IoT Integration with XGBoost and Bi-LSTM for Enhanced Prediction and Accessibility," *Smart Healthcare, Clinical Diagnostics, and Bioprinting Solutions for Modern Medicine*, pp. 17-38, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[15] Chris Gilbert, and Mercy Gilbert, "Exploring Secure Hashing Algorithms for Data Integrity Verification," *SSRN*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[16] Rakesh Nayak et al., *Data Privacy and Compliance in Information Security*, Securing the Digital Frontier: Threats and Advanced Techniques in Security and Forensics, pp. 17-33, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] Carlo Mazzocca et al., "A Survey on Decentralized Identifiers and Verifiable Credentials," *IEEE Communications Surveys & Tutorials*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Basem Almadani et al., "A Systematic Survey of Distributed Decision Support Systems in Healthcare," *Systems*, vol. 13, no. 3, pp. 1-43, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] S. Ambareesh et al., "A Secure and Energy-Efficient Routing using Coupled Ensemble Selection Approach and Optimal Type-2 Fuzzy Logic in WSN," *Scientific Reports*, vol. 15, no. 1, pp. 1-24, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] Sofia Petrova, and James Lee, "A Deep Reinforcement Learning Framework for End-to-End Retail Supply Chain Optimization," *Frontiers in Business and Finance*, vol. 2, no. 1, pp. 24-32, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[21] D. Ram Sandeep et al., "Systematic Investigation from Material Characterization to Modeling of Jute-Substrate-Based Conformal Circularly Polarized Wearable Antenna," *Journal of Electronic Materials*, vol. 49, no. 12, pp. 7292-7307, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[22] Charu Gandhi, and Anubhuti Mohindra, "SORT-Secured Optimal Routing Technique for Smart Cities using IoT Enabled Wireless Sensor Networks," *Multimedia Tools and Applications*, vol. 84, no. 34, pp. 42679-42710, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[23] Amir Masoud Rahmani et al., "A Routing Approach based on Combination of Gray Wolf Clustering and Fuzzy Clustering and using Multi-Criteria Decision Making Approaches for WSN-IoT," *Computers and Electrical Engineering*, vol. 122, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[24] M. Archana et al., "Energy-Efficient and Sustainable Cluster-Based Routing in IoT Based WSNs using Metahueristic Optimization," *2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*, Goathgaun, Nepal, pp. 79-83, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[25] Viswanathan Ramasamy et al., "Energy-Efficient and Secure Routing in IoT-WSNs using Adaptive Clustering and Trust-Based Mechanisms," *Information Security Journal: A Global Perspective*, pp. 1-16, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Naveen Kumar Gupta et al., "Energy Efficient Anchor Zone Based Routing Protocol for IoT Networks," *Computers and Electrical Engineering*, vol. 123, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[27] Satyanarayana Nimmala et al., "An Intelli BEF: An Intelligent Bio-Inspired Energy-Efficient and Fault-Tolerant Routing for IoT-Enabled WSNs," *2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*, Goathgaun, Nepal, pp. 942-947, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[28] D. Ram Sandeep et al., "Material Selection to Modeling: A Comprehensive Investigation of a Conformal Circularly Polarized Textile Antenna for Wearable Applications," *IEEE Access*, vol. 13, pp. 110882-110899, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[29] Deepali Bankatsingh Gothawal, and S.V. Nagaraj, "Hybrid Secure Routing and Monitoring Mechanisms in IoT-based Wireless Sensor Networks using Egret-Harris Optimization," *Information Security Journal: A Global Perspective*, vol. 34, no. 1, pp. 88-113, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[30] Parvinder Singh, and Rajinder Vir, "Enhanced Energy-Aware Routing Protocol with Mobile Sink Optimization for Wireless Sensor Networks," *Computer Networks*, vol. 261, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[31] Shinu M. Rajagopal, M. Supriya, and Rajkumar Buyya, "Leveraging Blockchain and Federated Learning in Edge-Fog-Cloud Computing Environments for Intelligent Decision-Making with ECG Data in IoT," *Journal of Network and Computer Applications*, vol. 233, pp. 1-16, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[32] Gurdeep Singh, "Wearable IoT (W-IoT) Artificial Intelligence (AI) Solution for Sustainable Smart-Healthcare," *International Journal of Information Management Data Insights*, vol. 5, no. 1, pp. 1-22, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[33] Nahar Sultana et al., "Context Aware Clustering and Meta-Heuristic Resource Allocation for NB-IoT D2D Devices in Smart Healthcare Applications," *Future Generation Computer Systems*, vol. 162, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[34] Puja Das et al., "Intelligent IoT-Enabled Healthcare Solutions Implementing Federated Meta-Learning with Blockchain," *Journal of Industrial Information Integration*, vol. 45, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[35] Arun Kumar Rai, Deepak Kumar Verma, and Rajendra Kumar Dwivedi, "RTAD-HIS: Regulated Transformer Architecture based Anomaly Detection Framework Towards Security in Healthcare IoT Systems," *Applied Soft Computing*, vol. 177, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[36] Ambarish G. Mohapatra et al., "IoT-Driven Remote Health Monitoring System with Sensor Fusion Enhancing Immediate Medical Assistance in Distributed Settings," *Alexandria Engineering Journal*, vol. 120, pp. 627-636, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[37] J. Mythili, and R. Gopalakrishnan, "Improving Data Transmission through Optimizing Blockchain Sharding in Cloud IoT based Healthcare Applications," *Egyptian Informatics Journal*, vol. 30, pp. 1-19, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[38] Raja Basha Adam Sahib, and R. Bhavani, "IoT-based Smart Healthcare using Efficient Data Gathering and Data Analysis," *Peer-to-Peer Networking and Applications*, vol. 18, no. 1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[39] Yasir Akhtar et al., "A Novel IoT-based Approach using Fractional Fuzzy Hamacher Aggregation Operators Application in Revolutionizing Healthcare Selection," *Scientific Reports*, vol. 15, no. 1, pp. 1-27, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[40] Radwan S. Abujassar, "Intelligent IoT-Driven Optimization of Large-Scale Healthcare Networks: The INRwLF Algorithm for Adaptive Efficiency," *Discover Computing*, vol. 28, no. 1, pp. 1-28, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[41] Hamad Aldawsari, "A Block Chain-based Approach for Secure Energy-Efficient IoT-based Wireless Sensor Networks for Smart Cities," *Alexandria Engineering Journal*, vol. 126, pp. 1-7, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[42] R. Manikandan et al., "A Novel Wireless Sensor Network Deployment for Monitoring and Predicting Abnormal Actions in Medical Environment and Patient Health State," *Alexandria Engineering Journal*, vol. 119, pp. 149-167, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[43] Rob S.A. van Bemmelen et al., "Timing and Duration of Primary Molt in Northern Hemisphere Skuas and Jaegers," *The Auk: Ornithological Advances*, vol. 135, no. 4, pp. 1043-1054, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[44] Joseph Bamidele Awotunde et al., "Enhanced Lightweight Encryption for Energy Efficiency and Security in Wireless Sensor Networks," *The International Conference on Artificial Intelligence and Smart Environment*, Errachidia, Morocco, vol. 2, pp. 572-578, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[45] Tarun Naskar et al., "Spectral Whitening based Seismic Data Preprocessing Technique to Improve the Quality of Surface Wave's Velocity Spectra," *Computers & Geosciences*, vol. 195, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[46] Jing Liao et al., "A Machine Learning-based Feature Extraction Method for Image Classification using ResNet Architecture," *Digital Signal Processing*, vol. 160, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[47] Tahir Hussain et al., "DCSSGA-UNet: Biomedical Image Segmentation with DenseNet Channel Spatial and Semantic Guidance Attention," *Knowledge-Based Systems*, vol. 314, pp. 1-15, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[48] M. Sundara Srivathsan et al., "An Explainable Hybrid Feature Aggregation Network with Residual Inception Positional Encoding Attention and EfficientNet for Cassava Leaf Disease Classification," *Scientific Reports*, vol. 15, no. 1, pp. 1-16, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[49] Anass Garbaz et al., "MLFE-UNet: Multi-Level Feature Extraction Transformer-based UNet for Gastrointestinal Disease Segmentation," *International Journal of Imaging Systems and Technology*, vol. 35, no. 1, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[50] Shuai Ma et al., "A Digital Twin-Assisted Deep Transfer Learning Method Towards Intelligent Thermal Error Modeling of Electric Spindles," *Journal of Intelligent Manufacturing*, vol. 36, no. 3, pp. 1659-1688, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[51] Harsh Doshi, and Achyut Shankar, "Wireless Sensor Network Application for IoT-based Healthcare System," *Data-Driven Approach towards Disruptive Technologies: Proceedings of MIDAS 2020*, pp. 287-307, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[52] Hazilah Mad Kaidi et al., "A Comprehensive Review on Wireless Healthcare Monitoring: System Components," *IEEE Access*, vol. 12, pp. 35008-35032, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[53] E. Aarthi et al., "A Naive Bayes Approach for Improving Heart Disease Detection on Healthcare Monitoring Through IoT and WSN," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 2s, pp. 553-570, 2024. [Google Scholar] [Publisher Link]

[54] R. Manikandan et al., "A Novel Wireless Sensor Network Deployment for Monitoring and Predicting Abnormal Actions in Medical Environment and Patient Health State," *Alexandria Engineering Journal*, vol. 119, pp. 149-167, 2025. [CrossRef] [Google Scholar] [Publisher Link]