scientific reports

Check for updates

OPEN

Secure and intelligent 5G-enabled remote patient monitoring using ANN and Choquet integral fuzzy VIKOR

Seelammal Chinnaperumal[1], Muthusamy Periyasamy[2], Amel Ali Alhussan[3], Subhash Kannan[4], Doaa Sami Khafaga[3]✉, Sekar Kidambi Raju[5]✉, Marwa M. Eid[6] & El-Sayed M. El-kenawy[7]

Rapid advancements in healthcare technologies necessitate efficient and secure remote patient monitoring systems. This research develops an intelligent system that combines ANN technology and 5G infrastructure with MCDM methods based on Choquet Integral Fuzzy VIKOR to improve medical data acquisition processes. Physical Layer Security (PLS) is a main emphasis point since it protects transmitted healthcare data from eavesdroppers and cyber intruders. The proposed model implements Reinforcement Learning with Hyper-parameter tuning and Lasso regression to obtain a 97.25% accuracy level, which exceeds Physical-Layer Authentication with Superimposed Independent authentication Tags PLA-SIT (97%), Flexible Physical Layer Authentication FPLA (96.8%) and Privacy-Embedded Lightweight and Efficient Automated PLA (95.3%). The proposed model surpasses both CNN-based mechanisms by 94.7%, Shamir's Secret Sharing Algorithm by 90.7%, and the Blowfish Algorithm by 82.3%. The enhanced quality of service alongside reliability produces the model as a dependable solution for MIoT applications that will exist in the next generation.

Keywords Remote healthcare monitoring, Healthcare authentication, Medical IoT, Physical layer security, 5G networks, LiteNet (CNN), Deep reinforcement learning, Choquet integral fuzzy VIKOR

Securing and enabling efficient remote patient monitoring during the 5G era will be an emphasis challenge given the sensitivity of medical information and the constantly changing conditions within health administration. A comprehensive framework combining 5G, LiteNet, AI, and Choquet Integral Fuzzy VIKOR is presented in this paper to offer secured adaptivity and resource conservation in remote healthcare monitoring. A two-fold authentication mechanism based on user credentials and biometrics is imposed to safeguard the patient's data. In contrast, the security of the Physical Layer strengthens the transmission channel from unauthorized access. Improvements in the transfer of bits are made by applying Reinforcement Learning technology that optimizes the moving nature of health information. Multiple evaluations, such as performance benchmarks and security audits, validated the viability of our system for secure, adaptive, and efficient remote patient monitoring. Its suitability for next-generation healthcare solutions is evident in the results. Hoque et al. (2024) critically review the technological trends in 5G networks for IoT-enabled smart healthcare. The paper demonstrates technological developments and their potential advantages by presenting important information to enhance healthcare delivery with novel technology applications. The research delivers vital information that stakeholders need to use 5G technology effectively for patient care improvement and healthcare efficiency enhancement[1].

The research from Rahman et al. (2024) investigates how IoMT and blockchain technology operate within an SDN framework for remote patient monitoring in a 5G network. The presented investigation explores how smart health systems can achieve extraordinary security measures, efficiency, and patient-focused care. New remote healthcare solutions and advanced technological advancements require this essential research to improve

[1]Department of Computer Science and Engineering, Solamalai College of Engineering, Veerapanjan, Madurai 625 020, India. [2]Department of Cyber Security, Paavai Engineering College (Autonomous), Namakkal 637 018, India. [3]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia. [4]K. Ramakrishnan College of Engineering (Autonomous), Samayapuram 621 112, India. [5]School of Computing, SASTRA Deemed University, Thanjavur 613401, India. [6]Jadara Research Center, Jadara University, Irbid 21110, Jordan. [7]Applied Science Research Center, Applied Science Private University, Amman, Jordan. ✉email: dskhafga@pnu.edu.sa; sekar1971kr@gmail.com

patient health outcomes[2]. Srivastava et al. (2024) present an analysis of applying Artificial Intelligence of Medical Things (AIoMT) technology in remote patient care delivery. Research findings demonstrate that AIoMT creates opportunities to expand health service reach while improving system speed and generating superior patient treatment results during remote care delivery. The research is a fundamental requirement for developing AI healthcare technologies through its dual responsibilities for securing and protecting remote medical services[3]. Bala et al. (2024) evaluate the security and privacy solutions to healthcare systems while addressing the role of artificial intelligence systems. The study predicts AI applications while demonstrating how these healthcare trends will enhance hospital security mechanisms.

The research establishes critical knowledge about AI integration in healthcare through comprehensive investigation of complex integration problems, which guides stakeholders with valuable information[4]. Pandey et al. (2024) examined the healthcare management models that implement cloud computing combined with 5G technology. The research demonstrates how advanced technologies enhance healthcare services, productivity measures, and treatment results for patients. The research holds value for creating future healthcare solutions that maximize the advantages of cloud and 5G technology[5]. The research by Mantri et al. (2024) explains how 6G technology will transform telemedicine through improved security systems. Research demonstrates that healthcare delivery will experience fundamental transformation through 6G, which provides safe and efficient high-speed connectivity for distant patient treatment. Research investigations are fundamental for improving telemedicine procedures while developing robust security protocols in upcoming healthcare networks[6]. The research by Singh et al. (2024) provides an extensive interpretation of the legal aspects of implementing IoT and 5G systems in health monitoring solutions. The authors demonstrate that these healthcare innovations create future obstacles and legal issues during their research. The research provides vital information to policymakers and industry stakeholders who must understand the legal aspects of health monitoring system development through advanced technology applications[7]. Patil et al. (2024) investigate how security is affected when 5G enters the operational framework of present-day healthcare management systems. The study outlines security risks with recommended safety measures to provide both efficient and safe healthcare services in the 5G technological framework. To develop robust security frameworks and reliable health management systems, the present work establishes its essential nature[8].

The main research contributions are.

- The system ensures the capability of instant medical data analysis, which allows quick decision-making procedures to improve healthcare performance.
- Through this framework, medical data remains intact and confidential when being transmitted.
- Dynamic optimization and data transmission operation modification are achieved by implementing Deep Reinforcement Learning techniques.

Research by Ravi et al. (2024) investigates how beyond 5G technology allows hospitals to merge connectivity with intelligence in their facilities. The study observes advancements in 6G and describes how these technologies boost medical facility management and treatment delivery. Researching future smart healthcare systems and advanced connectivity roles in delivering better healthcare remains essential[9]. Humayun et al. (2024) present Smart, Secure, and Energy-efficient Health Care Edge Technology (SSEHCET) as an integrated AI and mobile edge computing solution to boost eHealth security and efficiency. The research demonstrates that these technologies provide enormous power to upgrade healthcare management capabilities. Cognitive health development depends on this research to create cutting-edge eHealth solutions with secure operations and reliable functionality[10].

The project combines established and modern technologies to develop a framework that will reshape current remote outpatient monitoring practices by offering precise real-time assessment of relevant patient health metrics. LiteNet functions as the fundamental system architecture that makes use of a highly efficient Convolutional Neural Network design to deliver real-time data analysis. This is complemented by a 5G network offering fast and efficient data transfer. To utilize the data transmission resource efficiently, they implement deep reinforcement learning that deals diligently with the characteristics of non-stationary healthcare data. Furthermore, in this system, the Medical Internet of Things (MIoT) enables obtaining real-time medical data, and a reliable two-factor intelligent identification system based on biometrics markers and user identifiers guarantees high medical information protection and personal confidentiality. Also, Physical Layer Security is incorporated to protect data delivery from interception and interference by unauthorized parties. For the complex multiple criteria decision-making, the system applies Choquet Integral Fuzzy VIKOR, which increases the performance of data analysis. Most importantly, the proposed model achieves an accuracy of 97.25%, outperforming similar models and improving data privacy, reliability and healthcare resources. Through the implementation of these progressive technologies, this study establishes the basis for complex, secure and dependable remote healthcare solutions that are expected to revolutionize patient tracking with demonstrative positive health results.

Regarding claims like ''guarantees quick and low-latency connectivity'' and ''ensures safe, flexible and effective, remote healthcare monitoring,'' the evidence and results captured in Figs. 6, 7, 8, 9 and 10; Tables 8, 9, 10, 11, 12 and 13 give complete responses. These figures and tables present the Key Performance Indicators (KPIs), which show the superiority of incorporating LiteNet, 5G, deep reinforcement learning, and MIoT in Remote Patient Monitoring (RPM). Concerning the proposed system, the results of the obtained data in terms of the speed of the connectivity, latency, reliability, and accuracy of the health monitoring call for the effectiveness and safety of the proposed system.

Novel challenges and opportunities

The proposed system integrates LiteNet, 5G network, deep reinforcement learning, MIoT, and Choquet Integral Fuzzy VIKOR; it is a complete solution for operating medical data in real-time and remote patient monitoring. LiteNet, together with 5G, guarantees low latency and high bandwidth data transmission, which is very important in matters concerning timely medical treatment. Two-factor authentication, along with the high reliability of Physical Layer Security, is reliable in protecting medical data. With Choquet Integral Fuzzy VIKOR, valuable decisions are made in comprehensiveness in the healthcare field while preserving individuality.

Key technologies for ensuring security in remote patient monitoring systems

The technologies play a vital role in exchanging data without security flaws. 5G traffic allows real-time monitoring of patient health indicators, facilitating quick data transmission and enhancing remote medical care. With its low latency, the critical delivery of information is ensured, allowing for more rapid transmission in emergencies and promoting the speed of response. Physical layer authentication at remote patient monitoring takes a step further by verifying the authenticity of device identities on the network right down to its initial layer. This approach makes data accurate and safeguards the integrity and confidentiality of sensitive patient information, thereby increasing protection against unauthorized access to confidential patient information. Twine LiteNet is a good integration with the event of networks, which provides the lightest solution for communicating within a network. Aside from the streamlined architecture, where resource productivity is maximum, and network performance and reliability levels are enhanced, artificial intelligence also backs it. Reinforcement learning in patient monitoring helps modify algorithms for correct decision-making based on the patient's conditions developing over time. It increases the predictive power of models for early diagnostics of Health problems through data analysis of patterns. Another fuzzy system is the optimal relay base station in communication for a better predictive hyperlink. This measure of Shannon entropy in medical health data permits ascertaining the complexity of physiological signals and patients' medical records. It facilitates the evaluation of information content and can help recognize deviations or patterns of great importance during diagnosis or therapy decision-making processes.

Synergistic integration of LiteNet, 5G, deep reinforcement learning, and MIoT

LiteNet, 5G, and MIoT integration in the proposed model guarantees optimal performance of remote patient monitoring. It was chosen for its lightweight design, which makes it possible to implement it on limited resources and power-effective and reliable gadgets. For the latency and bandwidth problems, this 5G network is integrated with solutions for real-time data transfer, which is important in healthcare data. MIoT offers a solid foundation by which different medical devices can be connected, leading to a convenient solution to collect and share vital data across multiple branches. Deep Reinforcement Learning (DRL) is selected because of its learning capacity in a dynamic environment with theoretical guarantees of convergence and adaptability. DRL has proven effective in healthcare systems by enhancing decision-making and tailoring responses to patient needs. Research indicates that DRL improves both patient care and the system's overall performance by optimizing data processing and resource allocation across the healthcare setup. This integration, as a whole, improves the extent of disclosure, sizing, and dependability of the system.

Contributions to the future of secure and efficient remote patient monitoring

The proposed model is a fusion of LiteNet, 5G, deep reinforcement learning, MIoT, and Choquet Integral Fuzzy VIKOR to transform the RPM field. LiteNet guarantees efficient processing for the overall consumption of low-power devices, which is characteristic of IoT applications; on the other hand, 5G guarantees high-speed, real-time communication, which is essential in monitoring IoT devices. Reinforcement learning at a deeper level augments adaptive decision-making by processing patient data in real-time for timely actions. MIoT enables the development of a strong network of interconnected medical products that can support the availability of all essential information. The Choquet Integral Fuzzy VIKOR method enhances the quality of decision-making processes by integrating diverse and intricate patient data. It has been known that some limitations like latency, scalability, and customization have been experienced in remote monitoring; thus, integration has initiated an improved approach. Altogether, these technologies provide better patient care and a more patient-oriented model of health care provision than traditional systems.

Enhancing PLS security in remote patient monitoring with 5G and AI integration

Many IoT applications, such as Vehicle-to-everything (V2X), Unmanned Aerial Vehicles (UAVs), and e-health, require solutions with large ranges, low latency, high dependability, and low energy consumption. Robust security mechanisms are essential to 5G's success. High processing power is frequently needed for traditional approaches, which might be a limitation for devices with minimal resources. Because Physical Layer Security (PLS) uses the physical channel's inherent randomness for security, it does not require computationally demanding encryption, making it perfect for devices with limited resources for remote health monitoring. Physical Unclonable Functions (PUFs) and Secret Key Generation (SKG) can provide devices and communication channels with distinct hardware fingerprints to improve security.sub-6 GHz (3.3–4.2 GHz) and millimeter wave (mmWave) frequencies more than 24 GHz. 5G makes it possible to provide specialized resources for particular uses, such as remote health, guaranteeing dependable and high-priority connectivity. Effective methods, such as orthogonal frequency-division multiple access (OFDMA), enhance network adaptability and resource allocation, which are essential for handling a variety of applications and guaranteeing the quality of service for transmitting distant health data.

Integrating AI with 5G networks, therefore, makes a remotely monitored patient's care a safer endeavor and, as such, offers the ability to execute an instant response to perceived or known threats. These 5G networks may permit ultra-low latency, and even so, AI predictive algorithms determine real-time threats within which AI ensures immediate and automated protection measures on a network. The protection of transferred patient data can be achieved through AI-based encryption and authentication mechanisms. This 5G and AI technology combination creates a framework that enhances RPM system resilience against dynamic cybersecurity threats.

Related work

Secure health data protection is essential for wireless medical sensor networks that provide remote patient care and authentication processes. The system utilizes advanced authentication protocols, distinct IDs, and encryption to protect data validity from medical sensors while verifying data authenticity[11]. The research extensively analyzes IoT-cloud-based e-health security and privacy elements as its core objective. Security requirements are becoming increasingly important because healthcare depends on cloud-based solutions connected with medical equipment. The paper investigates the complexity behind how cloud infrastructure upholds e-health systems through data defense protocols, encryption standards, and Internet of Things (IoT) access management mechanisms[12]. This work implements attack detection within healthcare monitoring systems through a Virtual Private Network VPN-based Optical Transport Layer architecture that enhances protection against cyber attacks. The system increases its detection and blocking capabilities for threat attempts targeting healthcare data by implementing machine learning methods[13]. The Secure Monitoring System safeguards sensitive information from beginning to end during its digital movement. The system implements powerful encryption methods that protect data during transfer and storage. The system allows authorized personnel to see some information while preventing other users from accessing it. Machine learning algorithms perform continuous environmental scans to detect security threats, which they then swiftly prevent from happening[14]. Researchers developed this idea as a special security protocol adapted to Wireless Healthcare Sensor Networks (WHSNs), which maintains a minimal implementation footprint. Three security elements- passwords, fingerprint analysis, and protected tokens- work together inside the system to deliver dependable authentication functionality. The methodology maintains resource efficiency while providing protection features that strengthen security in WHSNs, thus supporting healthcare sensor network operations[15]. The real-time health data acquisition and analysis process occurs through agent-based medical health monitoring systems that employ autonomous software agents. Through wearable devices, these monitoring agents operate 24/7 to deliver specific medical information about individual health parameters and vital signs. Combining user notification procedures with urgency management features helps the system provide an easy platform for proactive healthcare[16]. The data transfer method uses encryption and security protocols to provide safe cloud transmission of IoMT information. Healthcare providers receive essential clinical data through machine learning keystroke protection, enabling patients to guarantee the privacy of their treatment information. Healthcare will proceed toward a safe, data-centric future[17]. Integrating IoT devices and 5G networks enables smart healthcare initiatives, constituting a dominant technological movement. The detailed examination shows that healthcare will transform with 5G technology through fast, secure networking, which unites medical devices and achieves precise remote care monitoring[18]. As a solution for Constrained Application Protocol CoAP-based IoT network security threats, Nathi et al. presented a slim authentication method with key agreement mechanisms. Elliptic curve public key cryptography and shared secrets function within this protocol to create secure communication, which does not reduce anonymity or performance[19].Researchers developed this idea as a special security protocol adapted to Wireless Healthcare Sensor Networks (WHSNs), which maintains a minimal implementation footprint. Three security elements- passwords, fingerprint analysis, and protected tokens- work together inside the system to deliver dependable authentication functionality. The methodology maintains resource efficiency while providing protection features that strengthen security in WHSNs, thus supporting healthcare sensor network operations[15]. The real-time health data acquisition and analysis process occurs through agent-based medical health monitoring systems that employ autonomous software agents. Through wearable devices, these monitoring agents operate 24/7 to deliver specific medical information about individual health parameters and vital signs. Combining user notification procedures with urgency management features helps the system serve as an easy platform for proactive healthcare[16]. The data transfer method uses encryption and security protocols to provide safe cloud transmission of IoMT information. Healthcare providers receive essential clinical data through machine learning keystroke protection, enabling patients to guarantee the privacy of their treatment information. Healthcare will proceed toward a safe, data-centric future[17]. Integrating IoT devices and 5G networks enables smart healthcare initiatives, constituting a dominant technological movement. The detailed examination shows that healthcare will transform with 5G technology through fast, secure networking, which unites medical devices and achieves precise remote care monitoring[18]. As a solution for CoAP-based IoT network security threats, Nathi et al. presented a slim authentication method with key agreement mechanisms. Elliptic curve public key cryptography and shared secrets function within this protocol to create secure communication, which does not reduce anonymity or performance[19].In their approach to managing security issues of IoT-enabled cloud computing environments, Liu et al. developed a lightweight authentication protocol that combines fuzzy extractors with physically unclonable functions (PUFs). The method authorizes users through decentralized biometric measures while avoiding cloud server infrastructure information breaches[20]. The researchers An et al. developed a pragmatic, lightweight authentication protocol that used Bit-Self-Test Physical Unclonable Functions (BST-PUFs). Through the exploitation of BST-PUF security characteristics, the protocol enables users to establish secure sessions while maintaining their identity and privacy. The system demonstrates effective performance and scalability, which allows it to be used in resource-limited IoT devices[21]. Sen et al. presented a established secure authentication method for wireless body area networks (WBANs) that uses PUFs with lightweight security features. Through PUFs, the scheme provides original challenge-response authentication pairs that create secure and resistant

systems against numerous attacks. The security platform demonstrates both efficiency and lightness, which makes it appropriate for resource-limited WBAN devices[22]. Sen et al. established a new server-less mutual authentication protocol that functions within edge networks. Security Utilities (SECUtils) establishes secure autonomous device connections through public-key crypto, challenge-response, and time stamp technologies instead of external servers. The authentication system in edge networks has become more private, secure, and scalable through these improvements[23]. Nyangaresi et al. introduced an adaptable cryptographic key system to secure data transmission as they tackled the security and power consumption problems of smart residences. High security and high energy efficiency result from the protocol's combination of lightweight cryptographic primitives and dynamic key management schemes. This system enables authentication between parties, provides confidentiality and integrity, and prevents denial of action[24]. The authors presented a lightweight authentication process and a privacy protection strategy for the Message Queuing Telemetry Transport (MQTT) messaging protocol widely used in IoT systems. The scheme implements Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and present lightweight symmetric encryption for private, secure message transmission between IoT devices and MQTT servers[25]. The work of Sen et al. brings forward an adaptive Zero-Knowledge Authentication Protocol (ZKAP) that uses adjustable security parameters based on risk assessment levels. Through its challenge-response system and fuzzy extractors, the protocol creates mutual authentication, builds session keys, and protects user identities and secret parameters[26]. A complete explanation of essential Internet of Things (IoT) agreement and authentication methods exists within this survey despite IoT devices' restricted security capabilities and resource availability. The survey investigates different protocols through security analyses and performance evaluations to determine appropriate usage for IoT applications[27]. The examination by Marhoon et al. (2024) presents an innovative network framework in the virtual world for conducting virtual consultations with remote patient monitoring through IoT devices. The system implements Internet of Things (IoT) devices to collect data by using Advanced Encryption Standard AES-256 encryption for secure patient data communication[28]. Safety issues in remote patient monitoring receive attention through Cheikhrouhou et al.'s system, which utilizes fog computing and lightweight blockchain technology. The method supports secure data protection and quick response durations, making it appropriate for IoT devices with limited resources[29]. The paper published in Computers and Electrical Engineering explains remote patient monitoring limitations of battery life and then offers a solution. The system depends on IoT sensors that minimize energy consumption during data retrieval while achieving accurate patient healthcare observation[30]. Chen et al. propose a secure key agreement protocol specifically designed for remote patient monitoring through the Internet of Medical Things (IoMT). This protocol prioritizes established security to ensure patient data remains confidential during communication[31]. Imon Chakraborty, Sisira Edirippulige, and P. Vigneswara Ilavarasan published a systematic review in the International Journal of Medical Informatics examining the evolving role of telehealth startups in healthcare delivery. Their analysis explores these startups' impact, challenges, and business models, emphasizing the potential for sustainable innovation in this growing field[32].Butt et al. (2024) published a comprehensive analysis of Engineering Applications of Artificial Intelligence. They categorize various remote mobile health monitoring frameworks and mobile applications. Their work identifies ongoing challenges, explores the motivations behind this technology, and offers valuable recommendations for future development[33].A recent study by Komal et al. (2024) investigated remote seizure detection devices for epilepsy. Published in Epilepsy Research, their systematic review analyzes the existing literature on these devices. Their findings explore the advantages and limitations of current technology, highlighting the need for improved user comfort and affordability to promote wider adoption[34]. The analysis of related works and their significance is depicted in Table 1.

Critical flaws in the research work

The presented research offers a generous set of security and authentication protocols for IoT healthcare. Still, one needs help finding a profound analysis of the protocols and comparing the presented protocols to others. Unfortunately, the research does not provide a clear procedure for evaluating the effectiveness and applicability of the protocols in managing various contexts in the health field. Furthermore, the work must consider the barriers and feasibility of utilizing these protocols in a real-world healthcare environment, such as computational complexity, energy cost, and user satisfaction. Similarly, the study does not address ethical aspects such as consent, privacy, and ownership of the collected and analyzed healthcare data.

Significant advancement over the existing research work

MIoT handling in the past year has centered on ultra-low latency and high speed of 5G in MIoT frameworks. This advancement means that new ways of constant monitoring and near-instantaneous processes of the gathered data are possible, thus enhancing the effectiveness and accuracy of remote healthcare systems. For example, new methods of network slicing allow dedicated portions of the communications infrastructure that are optimized for healthcare applications and provide unrestrained network resources in periods when the healthcare applications are usually most congested. One key emerging aspect has been the focused design of low-power neural networks for MIoT-restricted devices. Such neural networks are designed to consume as little power and time as possible, thereby permitting the analysis of health data on the devices. This cuts down on the frequency of data transfer to cloud servers, making the data more secure and with fewer delays.

Another advantage has been yielded from incorporating sophisticated MIoT systems, including AI forecast analytics, to enable early detection of health complications. These systems learn and adapt from the gathered data, making it possible to predict when a patient's health status is likely to worsen and prevent this from getting out of hand. Even better, they enhance the quality of patient care while simultaneously relieving the pressure of working with patients on healthcare providers. Concerning the security aspect, the emergence of efficient encryption and secure key management procedures was initiated and supplemented to fit the 5G-MIoT context.

Ref	Title	Methodology	Outcomes
[35]	Stochastic analysis of fog computing and machine learning for scalable low-latency healthcare monitoring	Stochastic Analysis	Reduced Latency
[36]	Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enabled IoMT system for healthcare workflows.	Deep Reinforcement Learning, Blockchain	Enhanced Security and Privacy
[37]	Modified artificial bee colony-based feature optimized federated learning for heart disease diagnosis in healthcare.	Modified Artificial Bee Colony, Federated Learning	Heart disease diagnosis
[38]	HealthEdge: a machine learning-based smart healthcare framework for the prediction of type 2 diabetes in an integrated IoT, edge, and cloud computing system	Machine Learning	Type 2 diabetes prediction
[39]	Asynchronous federated learning for improved cardiovascular disease prediction using artificial intelligence	Asynchronous Federated Learning, Artificial Intelligence	Cardiovascular disease prediction
[40]	Integrating IoT and Machine Learning for Real-Time Patient Health Monitoring with Sensor Networks	IoT, Machine Learning	Real-time patient health monitoring
[41]	Fog-cloud architecture-driven Internet of Medical Things framework for healthcare monitoring	Fog-cloud architecture	Healthcare monitoring
[42]	Adaptive multi-cost routing protocol to enhance lifetime for wireless body area network	Adaptive multi-cost routing protocol	Enhanced lifetime for wireless body area network
[43]	Anomaly detection in IoT-based healthcare: machine learning for enhanced security	Machine Learning	Enhanced security in IoT-based healthcare
[44]	Healthcare 5.0: From the perspective of consumer internet-of-things-based fog/cloud computing	Integration of CIoT with Fog/Cloud Computing	Enhanced Data Security
[45]	Secure and robust machine learning for healthcare: A survey	Machine Learning	Secure and robust machine learning for healthcare
[46]	From cloud down to things: An overview of machine learning in the internet of things	Machine Learning	Machine learning in the internet of things

Table 1. The Analysis of related work.

Measures such as homomorphic encryption and blockchain secure data sharing have been used in managing patients' health information to keep them secure and the integrity of the data intact.

New low-energy-consuming communication paradigms have been proposed to reduce energy consumption and thus prolong the life of the batteries in MIoT devices. These protocols reduce wireless vitality emissions by incorporating superior vivid power procedures and data forecast frequency of emission, which is very important in long-term patient monitoring. Another great step has been the integration of edge computing with MIoT systems. Using edge computing for data processing reduces the reliance on centralized clouds, lowers latencies, and improves the response time for healthcare monitoring applications.

Our research work differs from the existing research work

Prior studies have explored different architectures regarding neural networks; however, the choice of LiteNet, a lightweight CNN, is especially suitable for establishing a rapid connection. This makes your framework even more useful for real-time data exchange in healthcare organizations when combined with 5G, giving a perfect interface between patients and physicians.

The work is complex data management, using deep reinforcement learning for data transmission optimization and adaptation. This is important in the health care setting since the data loads may vary from time to time; thus, there is a need to optimize the use of the available resources to enable the system to provide data transfer speeds while at the same time maintaining quality data transfer.

The research presents a two-factor authentication where user biometric features and idiosyncratic features are incorporated, and this model is only sometimes used in similar works. This, coupled with the robust PLS protocols, means that the system is less likely to be vulnerable to hacking and other break-ins, especially during data transmission.

Implementing Choquet Integral Fuzzy VIKOR to handle multiple criteria has enriched our work. In decision-making, more options are structurally incorporated. They can accommodate multiple criteria, which are essential prerequisites in the case of healthcare, where often the healthcare decisions involve trade-offs between multiple criteria while staying unique and compelling.

Where many current solutions are implemented concerning security at the Network and Device layers, the work's focus on Physical Layer Security (PLS) is novel and necessary. This way, the research improves the general reliability of the communication against eavesdropping and data fiddling at the physical layer of transmitting information, making it a more holistic approach to the problem of security.

Methods and materials

Some of the requirements that the implementation of reinforcement learning in the healthcare industry requires are: Depending on the chosen problem, the identification of a specific healthcare problem, understanding of the specifics of the problem domain, acquisition and preprocessing of relevant health data, identification of the general structure of reinforcement learning including the states, actions, rewards, and transition dynamics, choosing an appropriate algorithm (for example, Q-Learning or Deep Q-Networks), coding of the algorithm.

This study uses a Choquet Integral Fuzzy VIKOR to determine which base station provides the best coverage for an efficient communication relay. This hesitant fuzzy contributes significantly to the optimal selection.

The proposed algorithm considers fuzzy variables such as high, medium, and low. The member of fuzzy is defined as below,

$$\widetilde{\mathrm{F}} = \{\mathrm{a}_1, \mathrm{a}_2, \mathrm{a}_3, \mathrm{a}_4 \in \mathrm{R}\} \tag{1}$$

Where a_1 represents the probable minimum , a4 represents the probable maximum, and a3 represents the possible values between a_1 and a_4. The fuzzy membership function is expressed as follows,

$$\delta_{\widetilde{\mathrm{F}}}(\mathrm{n}) = \begin{cases} \frac{\mathrm{n}-\mathrm{a}_1}{\mathrm{a}_2-\mathrm{a}_1}, & n \in [\mathrm{a}_1, \mathrm{a}_2] \\ 1, & n \in [\mathrm{a}_2, \mathrm{a}_3] \\ \frac{\mathrm{a}_4-\mathrm{n}}{\mathrm{a}_4-\mathrm{a}_3}, & n \in [\mathrm{a}_3, \mathrm{a}_4] \\ 0 & otherwise \end{cases} \tag{2}$$

The decision-maker offers the fuzzy ratings according to the following criteria,

$$\mathrm{FR}_{\mathrm{ijk}} = \{\mathrm{FR}_{\mathrm{ijk1}}; \mathrm{FR}_{\mathrm{ijk2}}; \mathrm{FR}_{\mathrm{ijk3}}; \mathrm{FR}_{\mathrm{ijk4}}\} \tag{3}$$

The formula for calculating each criteria weight value is as follows,

$$\mathrm{WC}_{\mathrm{jk}} = \{\mathrm{WC}_{\mathrm{jk1}}; \mathrm{WC}_{\mathrm{jk2}}; \mathrm{WC}_{\mathrm{jk3}}; \mathrm{WC}_{\mathrm{jk4}}\} \tag{4}$$

The aggregate fuzzy value of each criterion is determined as follows,

$$\mathrm{WC}_{\mathrm{j}} = \{\mathrm{WC}_{\mathrm{j1}}; \mathrm{WC}_{\mathrm{j2}}; \mathrm{WC}_{\mathrm{j3}}; \mathrm{WC}_{\mathrm{j4}}\} \tag{5}$$

Where

$$\mathrm{WC}_{\mathrm{j1}} = \{\mathrm{WC}_{\mathrm{jk1}}\}\, \mathrm{WC}_{\mathrm{j2}} = \frac{1}{\mathrm{k}} \sum \mathrm{WC}_{\mathrm{jk2}} \tag{6}$$

$$\mathrm{WC}_{\mathrm{j1}} = \{\mathrm{WC}_{\mathrm{jk1}}\} \tag{7}$$

$$\mathrm{WC}_{\mathrm{j2}} = \frac{1}{\mathrm{k}} \sum \mathrm{WC}_{\mathrm{jk2}} \tag{8}$$

$$\mathrm{WC}_{\mathrm{j3}} = \frac{1}{\mathrm{k}} \sum \mathrm{WC}_{\mathrm{jk3}} \tag{9}$$

$$\mathrm{WC}_{\mathrm{j4}} = \max\{\mathrm{WC}_{\mathrm{jk4}}\} \tag{10}$$

The aggregate fuzzy rating of each choice is generated using the criterion described below,

$$\mathrm{FR}_{\mathrm{ij}} = \{\mathrm{FR}_{\mathrm{ij1}}; \mathrm{FR}_{\mathrm{ij2}}; \mathrm{FR}_{\mathrm{ij3}}; \mathrm{FR}_{\mathrm{ij4}}\} \tag{11}$$

Where

$$\mathrm{FR}_{\mathrm{ij1}} = \min\{\mathrm{FR}_{\mathrm{ijk1}}\} \tag{12}$$

$$\mathrm{FR}_{\mathrm{ij2}} = \frac{1}{\mathrm{k}} \sum \mathrm{FR}_{\mathrm{ijk2}} \tag{13}$$

$$\mathrm{FR}_{\mathrm{ij3}} = \frac{1}{\mathrm{k}} \sum \mathrm{FR}_{\mathrm{ijk3}} \tag{14}$$

$$\mathrm{FR}_{\mathrm{ij4}} = \max\{\mathrm{FR}_{\mathrm{ijk4}}\} \tag{15}$$

Direct normalization is used to decrease the criterion dimensions. The advantageous metric Beneficial Criterion (BC) has the highest value divided by the greatest decision matrix value. Temporary, the price metric is expressed as the metric with the lowest values divided by the decision matrices' smallest values, which are defined as follows,

$$\mathrm{FR}\prime_{\mathrm{ij}} = \begin{cases} \left(\frac{\mathrm{FR}_{\mathrm{ij1}}}{\mathrm{FR}^{+}_{\mathrm{ij4}}}, \frac{\mathrm{FR}_{\mathrm{ij2}}}{\mathrm{FR}^{+}_{\mathrm{ij4}}}, \frac{\mathrm{FR}_{\mathrm{ij3}}}{\mathrm{FR}^{+}_{\mathrm{ij4}}}, \frac{\mathrm{FR}_{\mathrm{ij4}}}{\mathrm{FR}^{+}_{\mathrm{ij4}}}\right), \mathrm{C}_{\mathrm{j}} \in \mathrm{BC} \\ \left(\frac{\mathrm{FR}_{\mathrm{ij1}}}{\mathrm{FR}^{-}_{\mathrm{ij1}}}, \frac{\mathrm{FR}_{\mathrm{ij2}}}{\mathrm{FR}^{-}_{\mathrm{ij1}}}, \frac{\mathrm{FR}_{\mathrm{ij3}}}{\mathrm{FR}^{-}_{\mathrm{ij1}}}, \frac{\mathrm{FR}_{\mathrm{ij4}}}{\mathrm{FR}^{-}_{\mathrm{ij1}}}\right), \mathrm{C}_{\mathrm{j}} \in \mathrm{CC} \end{cases} \tag{16}$$

Where

$$\mathrm{FR}^{+}_{\mathrm{ij4}} = \max_{\mathrm{i}\{\text{decision matrix}\}}, \mathrm{C}_{\mathrm{j}} \in \mathrm{BC} \tag{17}$$

$$\mathrm{FR}^{-}_{\mathrm{ij1}} = \min_{\mathrm{i}\{\text{decision matrix}\}}, \mathrm{C}_{\mathrm{j}} \in \mathrm{CC} \tag{18}$$

During the defuzzification method, which is explained below, the normalized mean mass of the measures and alternatives for each measure is computed,

$$\mathrm{FZ_{ij}} = \mathrm{Deffuz}\left(\mathrm{FR'_{ij}}\right) = \left(\frac{\mathrm{FR'_{ij1}} + \mathrm{FR'_{ij2}} + \mathrm{FR'_{ij3}} + \mathrm{FR'_{ij4}}}{4}\right) \tag{19}$$

Figure 5 shows the flowchart for the Fuzzy VIKOR method. The VIKOR alternatives index ($\mathrm{T_i}$), utility ($\mathrm{G_i}$) and regret ($\mathrm{S_i}$) the following functions are stated,

$$\mathrm{G_i} = \sum\nolimits_{\mathrm{j=1}}^{\mathrm{n}} \frac{\mathrm{WC_j^0}\left(\mathrm{FZ^*} - \mathrm{FZ_{ij}}\right)}{\mathrm{FZ^*} - \mathrm{FZ^-}} \tag{20}$$

$$\mathrm{S_i} = \max_{\mathrm{i}}\left(\frac{\mathrm{WC_j^0}\left(\mathrm{FZ^*} - \mathrm{FZ_{ij}}\right)}{\mathrm{FZ^*} - \mathrm{FZ^-}}\right) \tag{21}$$

$$\mathrm{T_i} = \frac{\gamma\left(\mathrm{G_i} - \mathrm{G^*}\right)}{\mathrm{G^-} - \mathrm{G^*}} + \frac{(1-\gamma)(\mathrm{S_i} - \mathrm{S^*})}{\mathrm{S^-} - \mathrm{S^*}} \tag{22}$$

Where $\mathrm{i} = 1, 2, \ldots \mathrm{m}$ the negative and positive aspects $\mathrm{FZ_{ij}}$ is defined as $\mathrm{FZ^-}$ and $\mathrm{FZ^*}$, as well as the metric weight value $(\mathrm{C_j})$is referred to as $\mathrm{WC_j^0}$, γ indicates the decision-making coefficient, and (1- γ) the weight value of regret. Additionally,

$$\mathrm{G^*} = \mathrm{min_i G_i},\ \mathrm{G^-} = \mathrm{max_i G_i};\quad \mathrm{S^*} = \mathrm{min_i S_i}\ , \text{and}\ \mathrm{S^*} = \mathrm{max_i S_i} \tag{23}$$

Here, the Shannon entropy, which is expressed as follows, is used to generate thresholds to provide a better solution,

$$\mathrm{T_h}\left(\mathrm{Y}\right) = -\sum\nolimits_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{P}\left(\mathrm{y_i}\right) \log_{\mathrm{b}} \mathrm{P}\left(\mathrm{y_i}\right) \tag{24}$$

Every objective metric's threshold is determined using the formula below,

$$\mathrm{T_h}\left(\mathrm{LOS}\right) = -\sum\nolimits_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{P}\left(\mathrm{los_i}\right) \log_{\mathrm{b}} \mathrm{P}\left(\mathrm{los_i}\right) \tag{25}$$

$$\mathrm{T_h}\left(\mathrm{LOAD}\right) = -\sum\nolimits_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{P}\left(\mathrm{load_i}\right) \log_{\mathrm{b}} \mathrm{P}\left(\mathrm{load_i}\right) \tag{26}$$

$$\mathrm{T_h}\left(\mathrm{QOS}\right) = -\sum\nolimits_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{P}\left(\mathrm{qos_i}\right) \log_{\mathrm{b}} \mathrm{P}\left(\mathrm{qos_i}\right) \tag{27}$$

The following sets forth the general threshold level for RELAY selection,

$$\mathrm{TH}\left(\mathrm{Relay}\right) = \mathrm{T_h}\left(\mathrm{LOS}\right) + \mathrm{T_h}\left(\mathrm{LOAD}\right) + \mathrm{T_h}\left(\mathrm{QOS}\right) \tag{28}$$

Remote patient monitoring devices provide major benefits in healthcare delivery by enabling constant monitoring of patient health indicators without requiring frequent hospital visits. RPM systems must include authentication procedures to provide secure access and safeguard patient privacy. This research examines two different approaches to authentication implementation in RPM systems: To ensure effective communication during coverage, The Choquet Integral Fuzzy VIKOR method ranks and selects the most suitable base station by evaluating multiple interdependent criteria and through trial and error, an agent learns how to interact with its environment via reinforcement learning (RL).

Experimental setup

The experiment used a dataset that had real health info from people and made-up data. This dataset included important health signs like heart rate, oxygen levels, and blood pressure to mimic real-world remote patient monitoring situations. This is because, to evaluate system resilience and viability of the distinct architecture and models employed, different network conditions like latency, packet loss rates and device constraints like power consumption and memory were included to stress the system. The evaluation process examined numerous performance metrics, including Mean Squared Error (MSE), Root Mean Squared Error (RMSE), computation time, R-squared, packet delivery ratio (PDR), encryption latency, and energy consumption per transaction to determine system efficiency and reliability. Researchers utilized NS3 for network modeling alongside MATLAB to apply the Choquet Integral Fuzzy VIKOR method across diverse scenarios, including 5G networks and device energy levels starting from zero. 5 to 2. 0 Joules, and packet sizes between 64 and 1500 bytes. The tested novel Physical Layer Authentication (PLA) methods included a key size of 128 bits and 256 bits in testing for both encryption effectiveness and power conservation. The scalability issues were reflected, like the workload on the system and the responses of different devices used in the experiment. Sensor Network (SN) Practicality was maintained through tuning PLA algorithms for low-power devices, thus making networks energy efficient without necessarily compromising the data. The Choquet Integral Fuzzy VIKOR method was found relevant in approaching the problem of identifying the most eligible relay station and addressing the interdependent and

vague nature of the criteria, which is beneficial in addressing scalability issues in a high dynamic RPM context. Consequently, these outcomes demonstrate that the proposed system can provide both privacy-preserving and reliable, high-performance and easily scalable services expected from actual healthcare applications.

System model

The Architecture of the System model

We examine the transmission dynamics between M devices (D_i for i = 1 to m) and an access point (AP) within an edge computing-based remote patient monitoring system. Our analysis includes security threats where an attacker (Eve) uses identity-forging techniques to spoof legitimate devices that authentication protocols can detect. Eve, who could try to pose as a legitimate device. This situation is especially pertinent in public spaces with prevalent fixed device installations and APs.

Our work focuses on single-antenna fading channels for narrowband signals carried by single-antenna transceivers, as shown in Fig. 1 in a 5G scenario. We set up a baseline communications infrastructure to which our suggested method may be compared.

Signal Model: Senders encode and shape messages to reduce mistakes during sending. The person getting the message decodes and works with the signals they receive. They then send feedback to the sender to make talking back and forth more effective. The sender uses various methods, including coding, modulation, and pulse shaping, to encode and modulate the message to reduce mistakes during transmission across random channels. We take message symbols to be independently distributed random variables (.i.d.), represented as a block of text M symbols (indicated $F=\{a_1,a_2,a_3,a_4 \in R\}$.

by = $\{b_1,\ldots,b_M\}$). Through the use of packet processing and the encoding functions f_c (b), the message symbols are converted into a message signal denoted by f_e (b). The sent signal, represented as $x=\{x_1,\ldots, x_L\}$, only contains messages if the sender's only task is transmission.

The definition $F\sim=\{a1,a2,a3,a4 \in R\}$ represents the set of message symbols, where a1,a2,a3, and a4 are real numbers. This specific choice of defining the message symbols allows for certain mathematical and practical benefits in the context of communication systems.

Representing message symbols as real numbers R allows straightforward mathematical operations and analysis. It simplifies the process of encoding and decoding messages. Many signal-processing techniques and algorithms are designed to work with real numbers. This compatibility makes the implementation more efficient and less prone to errors. Using real numbers allows for a wide range of values, providing more flexibility in encoding different data types.

A triangular membership function is often used in fuzzy logic systems and is defined by three parameters: the left endpoint, the peak, and the right endpoint. If the message symbols are defined using a triangular membership function, the following implications can arise: Complexity in Encoding and Decoding, Fuzzy Logic Interpretations, Error Handling, and Signal Representation.

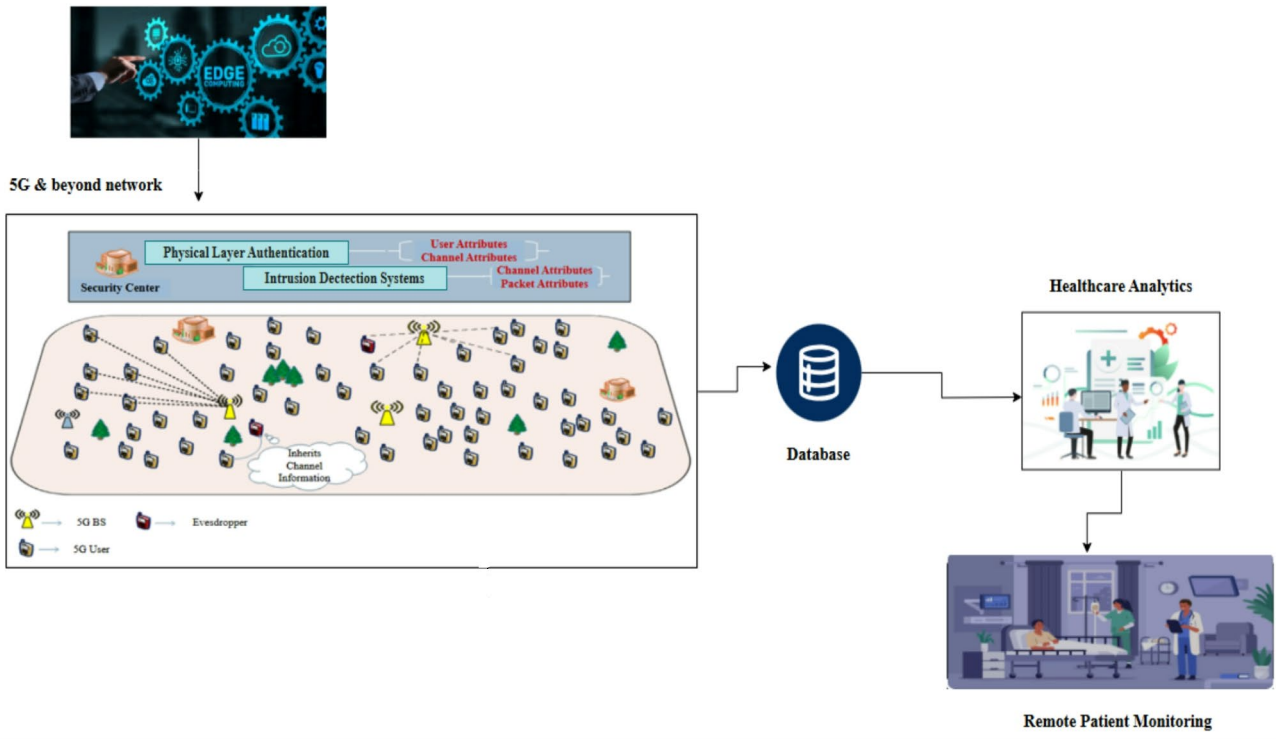

Fig. 1. Overall, remote patient monitoring.

In the following study, we contrast the tagged signal with the reference signal, highlighting its significance in situations like remote patients. With the help of edge computing technologies, this model allows for a deeper understanding of the communication dynamics critical for applications such as remote patient monitoring, where the reliable transmission of healthcare data between devices and access points is necessary for prompt and accurate healthcare interventions. We protect the confidentiality and integrity of private patient data by responding to security threats like Eve, which improves healthcare delivery efficiency in various contexts.

In Fig. 1, the system uses advanced technologies, such as 5G and edge computing, to support remote patient monitoring. 5G offers high-speed, low-latency connectivity for real-time data transmission, while edge computing allows an analysis to be made within a few milliseconds close to the data source, minimizing latency and bandwidth usage. A strong security center protects patient data with encryption and intrusion detection. Collected data is stored in a centralized database, which could help healthcare providers access and analyze patient information from anywhere. This system helps healthcare professionals monitor their patients constantly, identify potential health risks well in advance, provide timely interventions to alleviate them, and thereby enhance patient outcomes as well as access, particularly in geographically disparate locations.

Channel Model: This study assumes that the fading channel is a Rayleigh block fading channel where every block of messages experiences a separate fade. To access the channel, please follow the instructions below $\mathbf{i}$ The block is $\mathbf{h_i}$, and Variables with a zero-mean Gaussian distribution with variances are complex. $\boldsymbol{\sigma}^{2}_{\mathbf{h}}$. The receiver detects the block.

$$\mathbf{y_i} = \mathbf{h_i} \cdot \mathbf{x_i} + \mathbf{w_i}$$

Where w $= \{\mathbf{w}_1, \ldots \mathbf{w_L}\}$ and $\mathbf{u_k} \sim \mathbf{N}\left(0, \boldsymbol{\sigma}^{2}_{\mathbf{w}}\right)$ White Gaussian noise is a white form of noise. Signal-to-noise ratio (SNR) is defined as the ratio between signals and noise $\overleftarrow{\boldsymbol{\gamma}} = \boldsymbol{\sigma}^{2}_{\mathbf{h}}/$; **Each** block experiences SNR with a Rayleigh distribution with a different density for each block.

$$\mathbf{p}(\boldsymbol{\gamma}) = \frac{1}{\boldsymbol{\pi}} \mathbf{e}^{-\gamma/\gamma}$$

When the SNR $\boldsymbol{\gamma}_{\mathbf{i}}$ Falls below a certain threshold, say $\boldsymbol{\gamma}^{0}$, the $\mathbf{ith}$ Message blocks become corrupted to the extent that they cannot be accepted. In other words, the outage probability is the probability that it will happen at some point in the future. There is a probability of an outage occurring. $\mathbf{P}_{\mathrm{Out}}$ is fixed by setting $\overleftarrow{\boldsymbol{\gamma}}$

$$\mathbf{P}_{\mathrm{Git}} = \int_{0}^{\gamma^{0}} \mathbf{p}(\boldsymbol{\gamma})\, \mathbf{d}\boldsymbol{\gamma} = 1 - \mathbf{e}^{-\gamma^{0}/\gamma}$$

$$\boldsymbol{\pi} = \frac{-\gamma^{0}}{\mathbf{ln}(1-\mathbf{P}_{\mathrm{out}})}$$

Physical layer authentication (PLA)

This information from devices to central servers needs legitimate data to ensure the privacy and integrity of patient data. Thus, ensuring the legitimacy of data received within the medical device and forwarded to the central server calls for authentication, which makes explicit the identity of the origin of data. Methods commonly used are spread-spectrum communications and digital signatures, although they consume much bandwidth. A new approach proposed recently integrates authentication directly at the physical layer (PL) and enhances data security without additional bandwidth. Authentication information is embedded in a signal sent via specific waveforms with spread spectrum modulation and frequency hopping to guarantee that a signal cannot be intercepted.LiteNet is a lightweight Convolutional Neural Network in the proposed framework that enables rapid and low-latency data processing with good security connectivity between patients and healthcare providers. The system utilizes 5G networks to operate with speed and reliability for data transfer. Deep reinforcement learning technology achieves optimal resource use for data transmission while performing this function. The combined application of PLA enhances system security by lowering latency, resulting in an improved responsive remote patient monitoring framework (Fig. 2). The proposed model uses PLS in a two-tier architecture with a depth concept in Fig 2.

PLS in a two-tier architecture in-depth concept

Security measures at the physical layer used within a two-tier remote patient monitoring system can be enhanced with cooperative jamming and artificial noise generators. A primary device is the patient data collector, to sends data through a gateway or secondary hub. Reputable devices nearby generate cooperating jamming signals, which mask potential intruders from the communication channel while maintaining normal communication flow. Hub-to-gateway data transmission becomes harder for unauthorized access when fake noise is added to the communication pathway. The RPM system strength can be maintained through dynamic adjustments of security techniques based on environmental changes and threat risk levels.

Results and discussions

The proposed research presents a new method for IoT node authentication based on a physical layer authentication mechanism enabled by Deep Reinforcement Learning (DRL). The authentication method maintains resource efficiency in addition to constructive intruder detection throughout regions and secure access authentication procedures. Channel state information combined with this authentication technique enables nodes transmitting from different global locations to be identified.

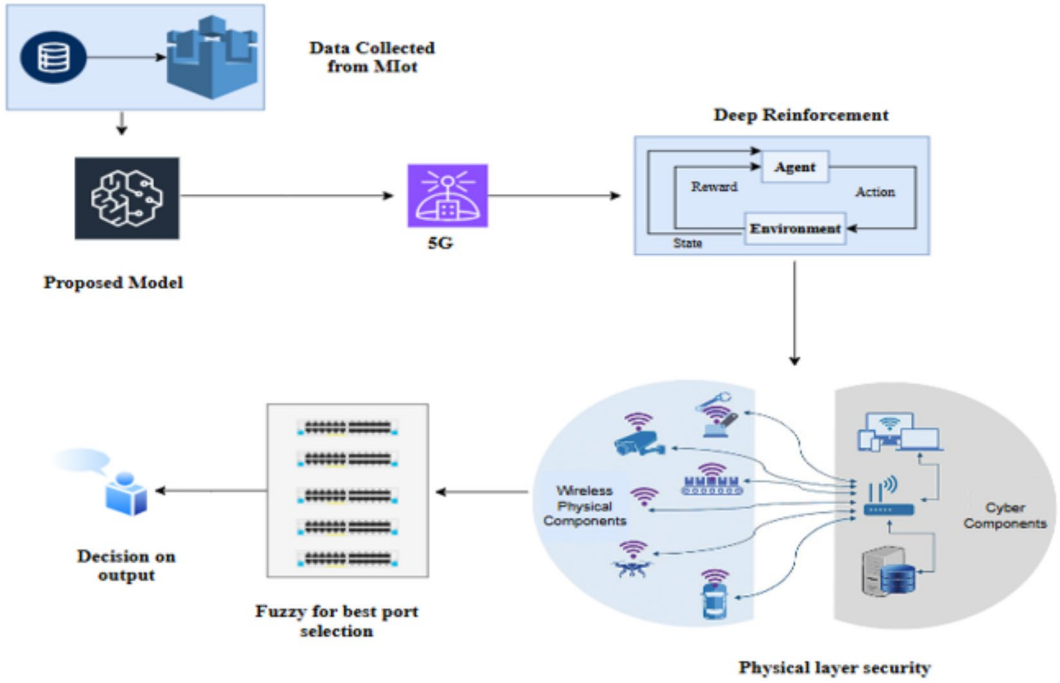

Fig. 2. Construction of the proposed model.

Wireless communication technology uses channel state information (CSI) to evaluate three critical properties, including gain or loss measurements, the degree of distribution, and spatial correlation measurements that explain how signals propagate. The study examines slow-changing fading channels to explore how Alice, the real user, can get reliable feedback about the main channel's condition. The system preserves message confidentiality from Alice even though she observes previous broadcasts, which allows her to determine Eve's communication channels.

The approach distinguishes between real-time channel gain data of the primary channel while analyzing statistical CSI information from both channels, particularly when Alice has CSI knowledge beforehand. For IDS systems to identify packets, they must perform content-scanning operations to recognize normal and abnormal packets. The encryption method LiteNet (CNN type) operates before packet transmission to provide data security through confidentiality and integrity protection. The implemented approach brings significant consequences for edge computing and healthcare and remote patient monitoring frameworks. This authentication technology finds its specific application in 5G authentication processes. The integration of DRL and CSI analysis ensures security advancement through contemporary technologies that provide wireless network confidentiality and protect the integrity of private medical data.

The wireless communication system's essential component of channel estimate appears in Fig. 3 for networks experiencing changing channel characteristics. Secret keys used for encryption tasks depend on key generation processes, while channel estimation remains essential for wireless communication security.

Feature extraction of dataset

Feature extraction is performed based on a nonlinear algorithm known as Soft Actor-Critic (SAC), in which the optimal action is determined by the current state and implemented accordingly. As a beginning, a Markov decision technique involves the consideration of action in the development process $(\mathfrak{F})$, state $(\mathfrak{G})$, and reward $(\mathfrak{R})$. The SAC feature is denoted as $\mathcal{P}_{\varnothing}(\mathfrak{G}|\mathfrak{F})$. The SAC Q function is denoted as $\mathbf{Q}_{\vartheta}(\mathfrak{G},)$ F, and the state value is expressed as $\mathbf{V}_{\boldsymbol{\tau}}(\mathfrak{F})$. The parameters of the SAC network are $\theta, \vartheta, \boldsymbol{\tau}$. In this case, we looked at two states: $\mathbf{U_a}$ and $\mathbf{A_a}$. SAC performs feature development and verification activities according to the present condition. The SAC offers incentives such as approval and restriction. The leftover errors are reduced by employing a soft value function, which is seen below,

$$\mathbf{F_V}(\boldsymbol{\tau}) = \mathbb{E}_{\mathfrak{G}\sim\mathbf{d}}\left[\frac{1}{2}\mathbf{V}_{\boldsymbol{\tau}}(\mathfrak{G}) - \mathbf{E}_{\mathfrak{F}\sim\mathcal{P}_{\varnothing}}\left[\mathbf{Q}_{\vartheta}(\mathfrak{G},\mathfrak{F}) - \log\mathcal{P}_{\varnothing}(\mathfrak{F}|\mathfrak{G})\right]^2\right] \tag{29}$$

Where d denotes the existing state distribution and the gradients function evaluations are specified as follows,

$$\nabla_{\boldsymbol{\tau}}\mathbf{F_V}(\boldsymbol{\tau}) = \nabla_{\boldsymbol{\tau}}\mathbf{V}_{\boldsymbol{\tau}}(\mathfrak{G}) - \left(\mathbf{V}_{\boldsymbol{\tau}}(\mathfrak{G}) - \mathbf{Q}_{\vartheta}(\mathfrak{G},\mathfrak{F}) + \log\mathcal{P}_{\varnothing}(\mathfrak{F}|\mathfrak{G})\right) \tag{30}$$

Based on the current feature, SAC takes action and then adjusts the soft Q value to optimize the stochastic gradient function, which is expressed as follows,

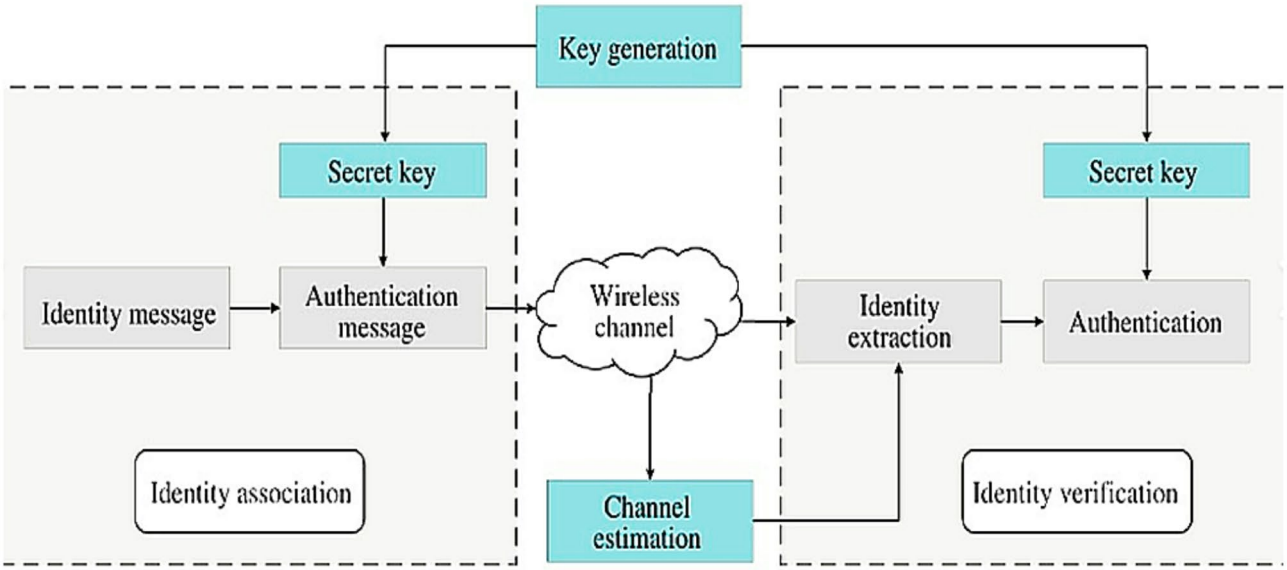

Fig. 3. Channel estimate key generation.

$$\nabla_{\vartheta} \mathbf{F_Q}(\vartheta) = \nabla_{\vartheta} \mathbf{Q}_{\vartheta}(\mathfrak{F}, \mathfrak{G})(\mathbf{Q}_{\vartheta}(\mathfrak{G}, \mathfrak{F}) - \mathfrak{K}(\mathfrak{G}, \mathfrak{F}) - \boldsymbol{\beta}\, \mathbf{V}_{\boldsymbol{\tau}}(+1)) \tag{31}$$

The feature variable learning method is used to produce the best feature, which is defined as follows,

$$\mathbf{F}_{\mathcal{R}}(\varnothing) = \mathbb{E}_{\mathfrak{G}\sim\mathbf{d},\, \mathbf{b_t}\sim\mathbf{m}}\left[\mathbf{log}\mathcal{R}_{\varnothing}(\mathbf{l}_{\varnothing}(\mathbf{b_t}; \mathbb{S}\mathbf{t})\,|\mathbb{S}\mathbf{t}) - \mathbf{Q}_{\theta}(\mathbb{S}\mathbf{t}, \mathcal{R}_{\varnothing}(\mathbf{b_t}; \mathfrak{G}))\right] \tag{32}$$

Where $\mathbf{l}_{\varnothing}(\mathbf{b_t}; \mathfrak{G})$ We can enforce features by representing the current network's actions. The Automated feature enforcement utilizing the SAC algorithm is depicted in Fig. 4, where the ideal reward is created depending on the actions. SAC provides the pseudocode for automated feature enforcement. Received Signal Strength Indicator (RSSI) can be calculated as follows

$$\mathbf{RSSI}(\mathbf{d})[\mathbf{dB}] = 10\mathbf{log}\mathbf{P_r}(\mathbf{d}) \tag{33}$$

where $\mathbf{P_r}(\mathbf{d}) = \|\mathbf{y}\|^{2.}$ Its value measures how powerful the signal received is and $\|\mathbf{y}\|$. As the name implies, it is the norm of Frobenius. As can be seen from the computation, RSSI is impacted by both path loss and Additive White Gaussian Noise (AWGN), except because noise has a lesser effect on RSSI than path loss.

LiteNet is a lightweight technique with six layers: a convolutional, a LiteModule pooling layers, thick layers 1 and 2, and a softmax layer. We cipher the aggregate sensory information parallel to decrease the encryption process time. The suggested LiteNet model's convolution layer incorporates a linear filter, which is utilized to lower the computation complexity of the convolution during encryption. S-shuffle Box's and hexadecimal values are described in Table 1. The values are employed in the encryption and decryption of the input blocks.

The suggested convolutional layers' computation is as follows,

$$\mathrm{X}(\mathrm{n}) = \mathrm{Y}(\mathrm{n}) \times \mathrm{H}(\mathrm{n}) \tag{34}$$

$$\sum_{\mathrm{m}=0}^{\mathrm{s}-1} \mathrm{X}(\mathrm{m})\,\mathrm{H}(\mathrm{n}-\mathrm{m}) \tag{35}$$

Where X(n) is the duration of the incoming data packets, H(n) is the kernel selection, and Y(n) is the output value. The detected packets of data are encrypted in this layer. The suggested TWINE method converts plaintext into ciphertext (encrypted data) using 64 bits by implementing a round function. The ciphertext is generated in 36 cycles. Table 2 defines the S-box permutation values. The indices of permutation blocks are defined as $\rho : \{0,1,\ldots 15\}$, and it is mapped to ρ[j] sub-block, which is illustrated in Table 1. The LiteNet with twine model is given in Fig. 5.

Then, the lite module includes 1×1. The current light module's convolutional layer and filter size are 1×2 and 1×3. The primary goal of this module is to lower the computational complexity among convolutional layers. The light modules are also used to minimize parameter volume efficiency. The 1×1 The convolution is used to enhance the representation of local & cluster feature maps. The sensing data packets

Are treated as input by the LiteNet. It also has one lite module, two thick layers, and one softmax layer, with a total of five units, as stated below,

$$\sum {}_{\mathrm{i}}^{5}\mathrm{S}_{\mathrm{i}} = 1 \tag{36}$$

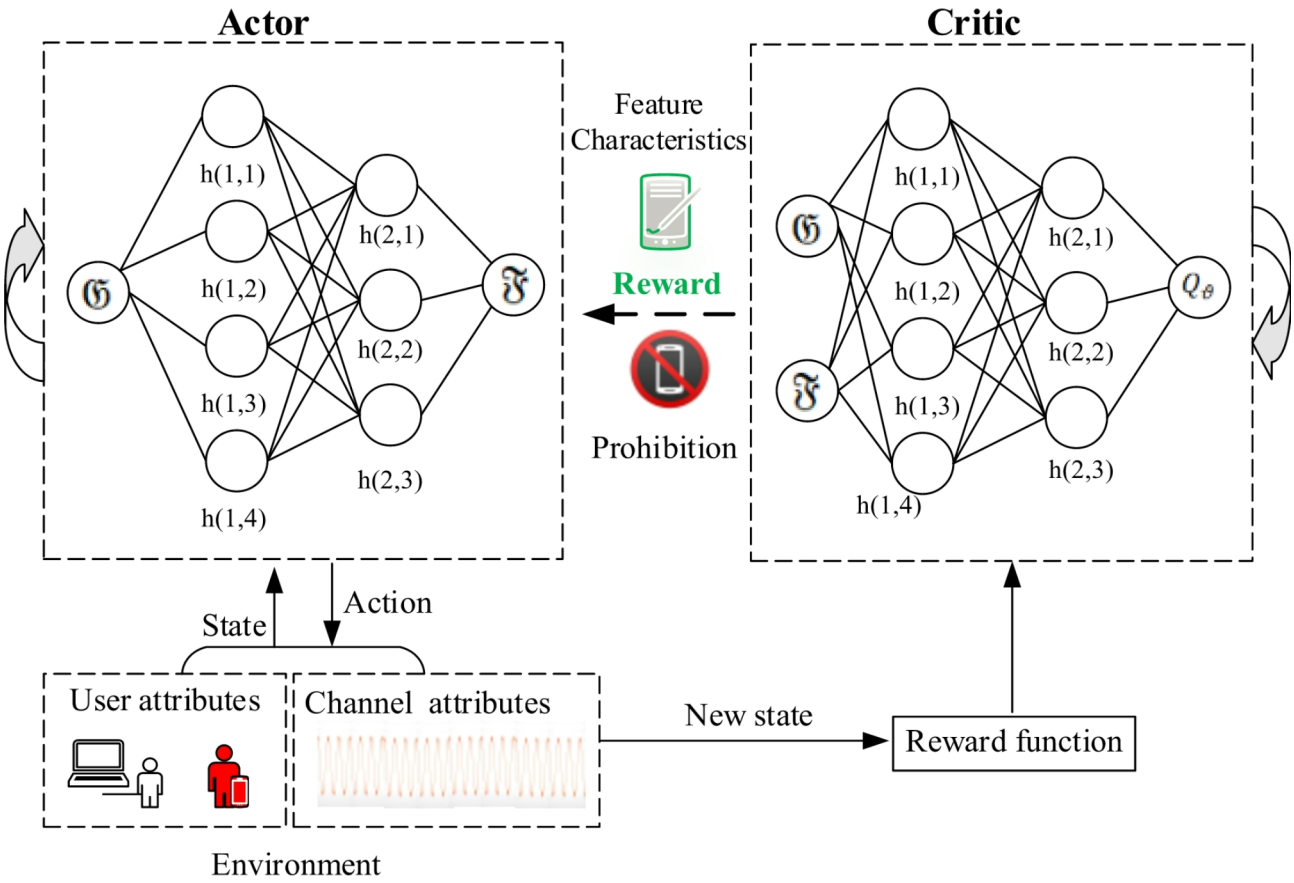

Fig. 4. Automatic feature creation based on SAC.

Shuffle values of block			Hexadecimal values of S-box	
j	ρ [j]	ρ^{-1} [j]	y	S(y)
0	5	1	0	C
1	0	2	1	0
2	1	11	2	F
3	4	6	3	A
4	7	3	4	2
5	12	0	5	B
6	3	9	6	9
7	8	4	7	5
8	13	7	8	8
9	6	10	9	3
10	9	13	A	D
11	2	14	B	7
12	15	5	C	1
13	10	8	D	E
14	11	15	E	6
15	14	12	F	4

Table 2. Shuffle and S-Box hexadecimal values.

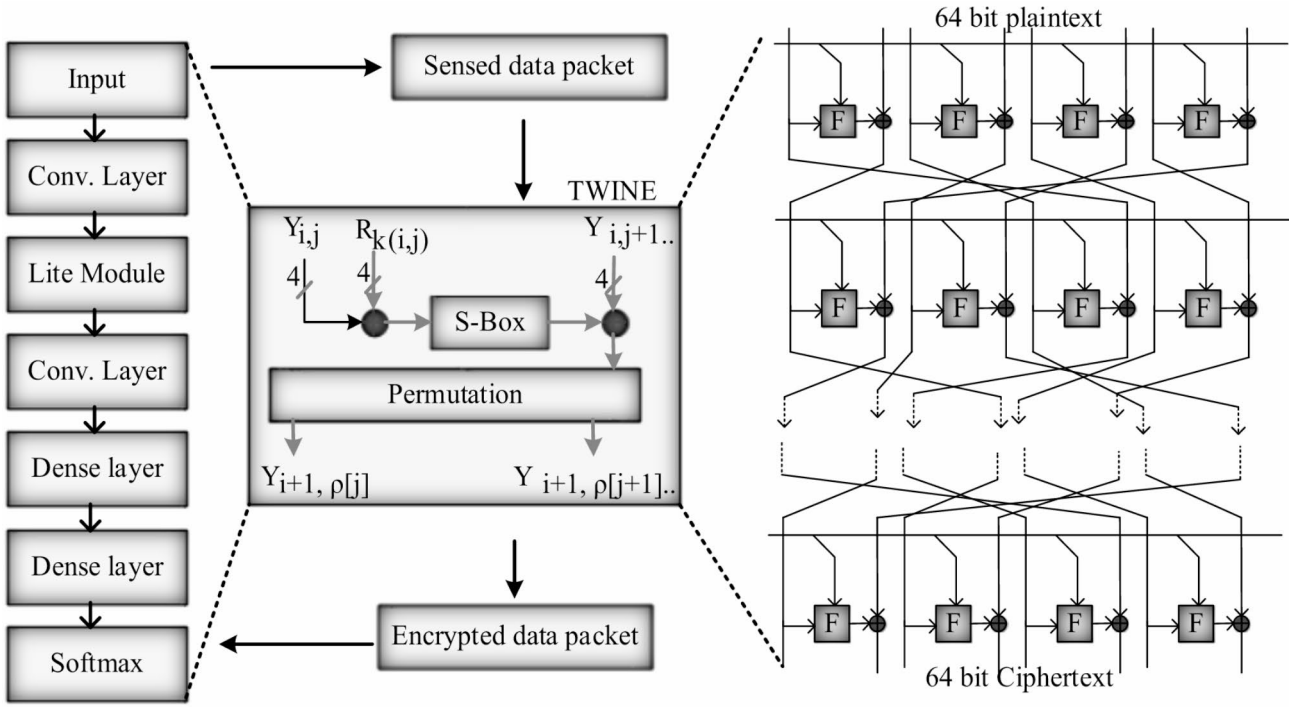

Fig. 5. A LiteNet model using twine.

Where $i = 1,2 \ldots 5$ and S_i denotes the probability distribution.

$$Y_i = \sum {}_n X_n w_{ni} \tag{37}$$

Pseudocode 1: Twine-LiteNet

INPUT: $\mathbf{D_P}$
OUTPUT: $\mathbf{E_D}$
Begin {
Initialize $\mathbf{D_P}$
// convolutional layer
for i from 1 to n, do
for j from 1 to n do{
encrypt the data packets $\mathbf{D_P}$ using TWINE
$\mathbf{Y_{64}^1} \leftarrow \mathbf{D_P}$
for $\mathbf{i} \leftarrow 1$ **to** 35 do
$\mathbf{Y_{2j+1}^{36}} \leftarrow \mathbf{S}(\mathbf{Y_{2j}^{36}} \oplus \mathbf{R_{k_j}^{36}}) \oplus \mathbf{Y_{2j+1}^{36}}$
$\mathbf{E_D} \leftarrow \mathbf{Y^{36}}$ }
// Fully connected layer (Lite module, 2 dense layers and softmax layer)
for i from t to n do
temp = 0
For J from 1 to n, do
$\mathbf{temp} = \mathbf{temp} + \mathbf{w_{ij}} \times \mathbf{X}[\mathbf{j}]$
end for
$\mathbf{Y_i} = \mathbf{temp}$
end for
end for
end for
end

It is used to measure the channel efficiency for data transmission. The channel capacity is affected by bandwidth and data rate. It is calculated based on CSI prediction. The formulation of channel capacity is defined as follows,

$$\mathrm{cap} = B \log\left(1 + \frac{sp}{np}\right) \tag{38}$$

Where B represents the bandwidth , sp shows the strength of the signal, and np reflects the strength of the channel noise.

The model uses a reinforcement learning approach that explores and exploits ($\gamma = 0.95$ to optimize long-term efficiency) the entire process. The LiteNet architecture is lightweight and convex with a kernel of 3×3 and Leaky

Methods	Avg. Accuracy %	Avg. Precision %	Avg. Recall %	Avg. F1-score Measure %
Policy-Based RL	93.5	90	90	90
Value-Based RL	96	91	91.5	93.5
Proposed Model	97.23	96	97.5	97.6

Table 3. Comparison of different models with their metrics.

Activation function	Policy-Based RL %	Value-Based RL %	Proposed %
Leaky Relu	94.5	97	98
Softmax	92.23	94.56	92.43

Table 4. Activation functions and models.

Models	Computational time (s)	MSE	RMSE	R2
Policy-Based RL	27.743	0.371	-0.266	0.678
Value-Based RL	23.269	0.119	-0.199	0.614
Proposed	29.601	-0.125	-0.258	0.577

Table 5. Statistical measures and models.

ReLU activation. It ensures encryption with low latency and real-time processing on resource-poor IoT devices. These choices enhance adaptability, scalability, and energy efficiency, so the performance of the proposed system is sturdy enough to be valid for a real-world healthcare application.

Reinforcement learning

In this research, the Proposed model consisting of Reinforcement learning with Hyper-parameter and Lasso regression provides 97.23% accuracy for our dataset. Where w represents the weight values of the softmax layer and X represents the output of the upper layer. The final calculation of the softmax layer is defined as follows,

$$S^i = \frac{\exp(Y_i)}{\sum_j^5 \exp(Y_j)} \tag{39}$$

The output values are then transformed into probability distributions at the softmax layer, commonly used for classification tasks.

In Table 3, the Proposed Model outperforms Policy-Based RL and Value-Based RL in terms of all metrics (accuracy, precision, recall, and F1-measure). Value-based RL performs better than Policy-Based RL across the board, indicating the superiority of using value estimates in decision-making. The Proposed Method demonstrates strong performance in decision-making accuracy because its precision, recall and F1-measure values are very high. The obtained results may differ based on the selected problem domain and dataset type alongside implementation-specific factors.

Leaky ReLU: A modified ReLU function with a non-zero negative slope can solve the dying ReLU problem; leaky ReLU allows a slight gradient when the unit is not activated. It is defined as $f(x) = x$ if $x > 0$, and $f(x) = \alpha x$ if $x \leq 0$, where α is a small positive constant. The softmax function is used in the output layer of classification models to convert raw scores into probabilities. It exponentiates each score and normalizes them to obtain a probability distribution over classes in Table 4.

In Table 5, statistical measures and models are foundational to machine learning. They enable data understanding, hypothesis testing, prediction, and decision-making. By leveraging statistical principles, machine learning achieves impressive capabilities across diverse applications.

Compared to Policy-Based and Value-Based reinforcement learning models, the statistics in Table 5 show the efficacy of the proposed system. The proposed model takes a slightly longer time of computation (29.601s) but has a higher MSE (-0.125) and lower RMSE (-0.258), indicating that the proposed model is more accurate and precise in terms of error variability. The R^2 value of the model is equal to 0.577, which suggests the moderate accuracy of the model and its compatibility with the works of other authors focusing on similar models' construction, with priority given to stability and adaptability at the same time. The analysis results of paired t-tests also showed that the system has significantly higher MSE and RMSE accuracy ($p < 0.05$). Sensitivity analysis supported this finding, showing that it performed well regardless of the type of data involved and exhibited stability even in high-complexity data, consistent with our hypothesis regarding deep reinforcement learning. These findings resonate with other findings in the model and suggest the potential of real-time decision-making in patient observation. The increase in computational time is minute to require the above advantages of reliability, modularity, and strength to make the system perform in complex and dynamic healthcare facilities.

Models	Policy-Based RL %	Value-Based RL %	Proposed %
Accuracy for training data	0.901	0.954	0.968
Accuracy for testing data	0.913	0.939	0.965

Table 6. Training and testing accuracy.

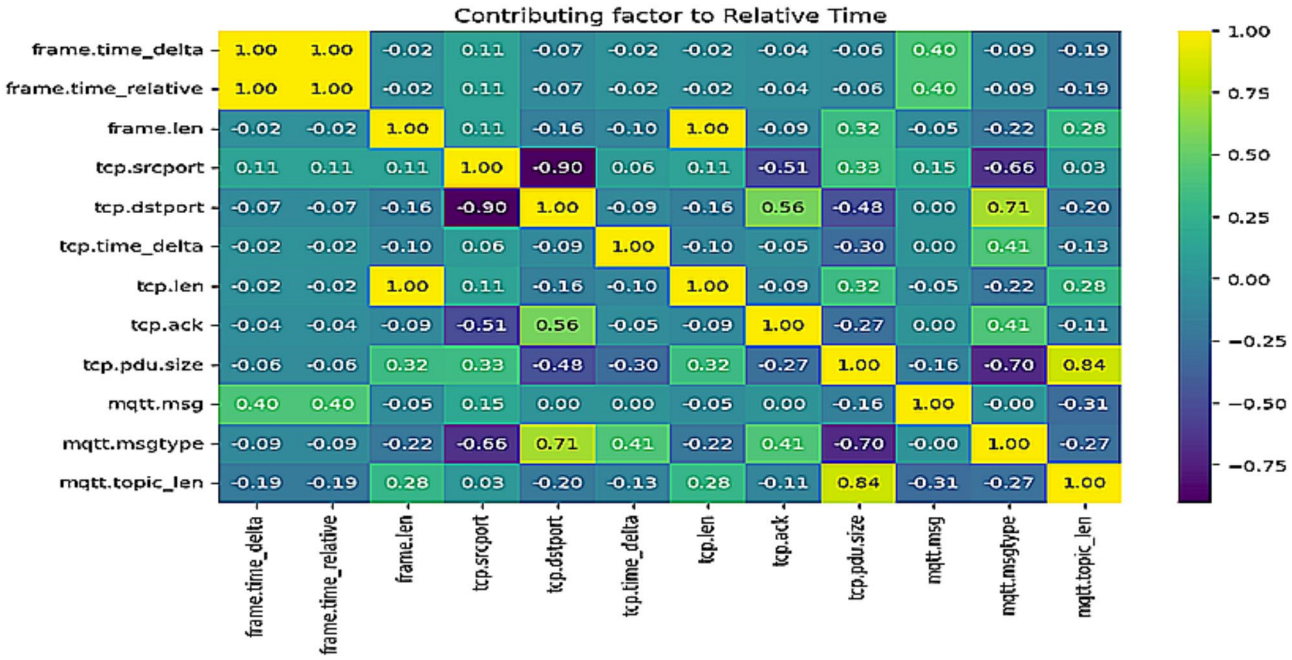

Fig. 6. Optimized way of data transfer from edge computing to remote patient.

In this paper, Yang et al. propose a secure and traceable multikey image retrieval method in cloud-based IoT systems and services, which effectively improves security and traceability while ensuring the effectiveness and accuracy of image retrieval in IoT cloud systems and services. This advancement is essential for the security and enhancement of smart IoT devices[52]. Similarly, in future work, Miao et al. (2024) consider an efficient and secure federated learning scheme to prevent backdoor attacks using adaptive local differential privacy and compressive sensing., their research guarantees strong privacy preservation and model performance, eliminating the main issues affecting conventional federated learning systems. All these improvements are essential for improving the security and reliability of federated learning applications[53]. Furthermore, Miao et al. (2023) describe a time-controllable keyword search scheme with efficient revocation for a mobile e-health cloud to improve the privacy and security of data through access permissions management and proper user revocation technique. This research responds to critical open problems of existing searchable encryption schemes, which is why it is crucial for enhancing the security and functionality of e-health systems[54].

In Table 6, balancing training and testing accuracy is crucial in machine learning. While a high training accuracy is desirable to ensure that the model captures the training data's patterns, it's equally important that the testing accuracy is high as well. A significant gap between training and testing accuracy, with the training accuracy being much higher, could indicate overfitting.

Monitoring.

Figure 6, within the domain of frame-relative time, emphasizes the packet transfer time between patients' wearable IoT devices to the doctors' monitoring equipment. A careful analysis of the relevant variables shows that the message parameter's type is one of the most important. Analysis has shown that, in comparison to large or complex datasets, simplified data yields faster transmission rates. This emphasizes how important it is to prioritize data optimization to increase the efficiency of information sharing within the healthcare monitoring infrastructure.

Figure 7 shows the dynamics of message transport concerning relative time in the hex-bin diagram that was previously mentioned. Specifically, the darker region in the lower left quadrant indicates that packets less than 65 are sent more quickly than packets larger than 65. This intelligent analysis, made possible by our model, suggests using a packet size of 65 to achieve the highest possible level of data transmission efficiency. By implementing this recommended packet size, the system's overall performance and data transmission speed will be improved.

Figure 8 demonstrates rapid transmission effectiveness by the signals coming from vital sources like ECG, EMG, Airflow, and Pulse oximeter using our suggested model. Acknowledging their crucial function in patient surveillance, our approach prioritizes and maximizes the data flow from these essential sources. This emphasis

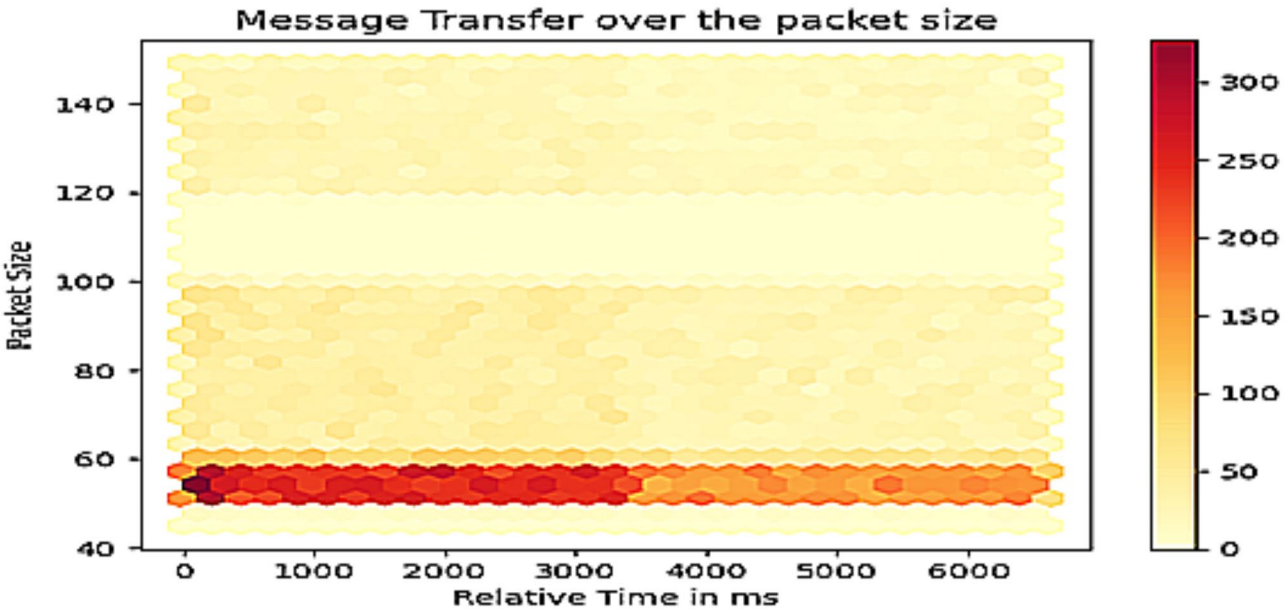

Fig. 7. Patients message transfer over the packet.

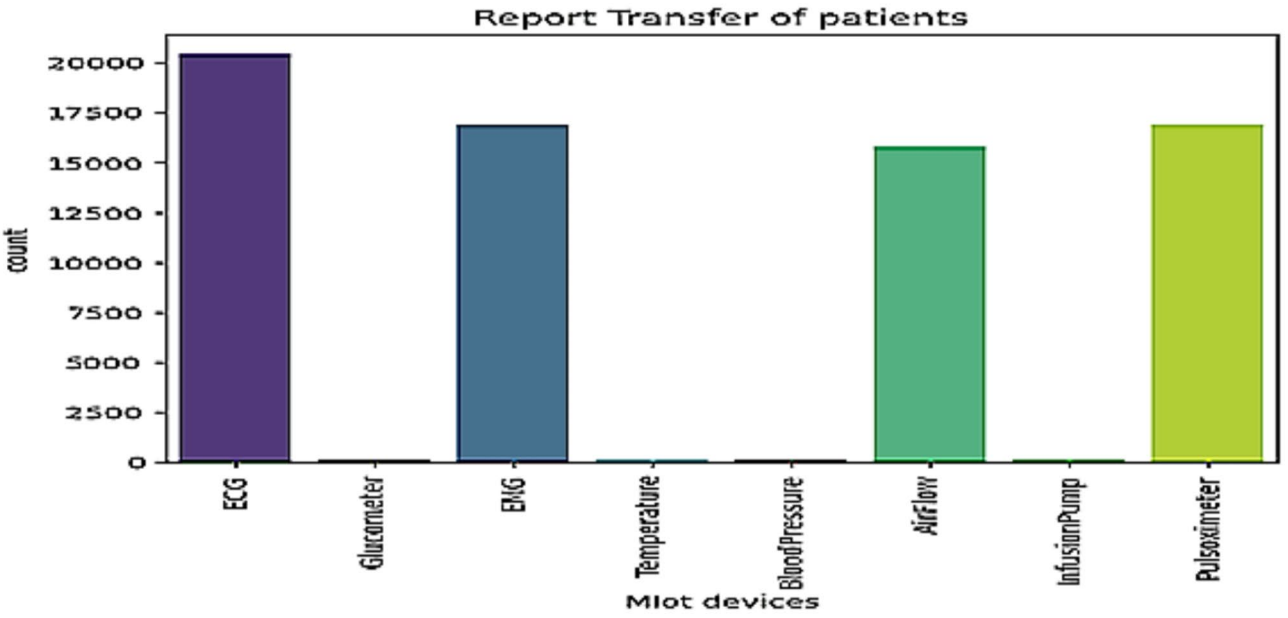

Fig. 8. Remote patient reports are transferred in equal intervals.

Index	Frame.time_delta	Frame.time_relative
frame.time_delta	1.0	0.97
frame.time_relative	0.97	1.0

Table 7. Data optimization of remote patient reports.

helps create a more effective and efficient healthcare monitoring system by guaranteeing that the crucial ECG, EMG, airflow, and pulse oximeter data is sent immediately and reliably.

Table 7, following the recommended packet size limit and data transfer, is the most important thing we do when sending data since it may significantly reduce the time it takes for the data to get to the recipient. Data loss occurs when a packet is resized after the sender's original transmission. To overcome this difficulty, a calculated

Range of Frame Length	No data transfers
68.303–100.286	70,311
100.286–130.571	79
342.571–372.857	2
1493.429–1523.714	2
1130.0–1160.286	2
1735.714–1766.0	2
1251.143–1281.429	1

Table 8. Remote patients range versus data transfers.

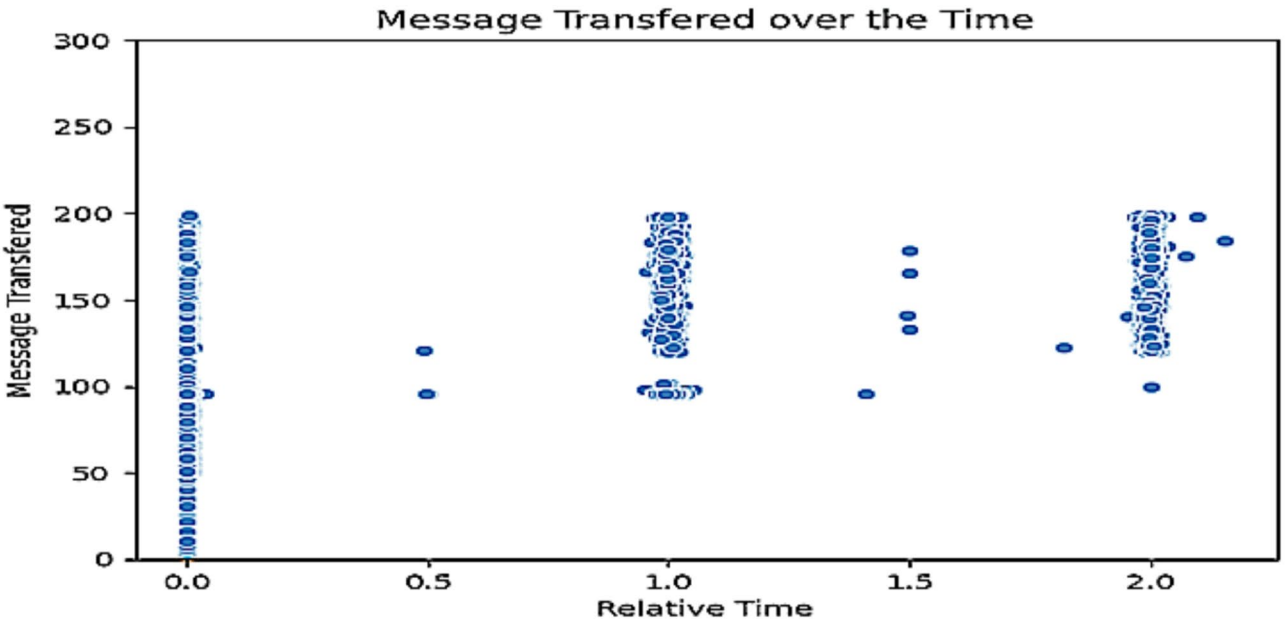

Fig. 9. Remote patient's message transferred concerning relative time.

approach was used, in which data was divided into segments according to the input, each of which made up the first frame. The time difference (frame time delta) will enable transportation to be within the packet time; usually, in frame segmentation, the data will be divided into several packets, increasing transportation efficiency.

Below is a full explanation of how we measured the message passing from MIoT devices to the original frame network, which helps to clarify the fine distinctions of our data transmission optimization strategy. The relative time depends entirely on the delta time or the time difference between the current frame and the prior frame in the packet capture because the relative data and delta time have a strong correlation.

"frame.time_delta": This parameter indicates how much time has passed from the packet capture's previous and current frames. It is frequently used to analyze the timing of network events and shows the time that passes between the two frames. The time difference between the current frame and the beginning of the capture or a user-defined reference point is represented by the variable "frame.time_relative," which functions similarly to "frame.time_delta." Because it offers a relative timestamp, analyzing the time between frames is much simpler.

Table 8, frame lengths between 68 and 100 show a significant trend in data transport. By using our knowledge of the assigned packet size restriction, this data concentration inside specific frame durations is crucial in reducing the total amount of time needed for smooth data transfer between Internet of Things devices. Our method optimizes data transmission efficiency by adhering to the recommended packet size, facilitating a more efficient and rapid flow of information between IoT devices.

"frame. Len": This argument provides the current frame's bytes-long length. It shows the size of the packet that is being sent across the network. It is possible to find trends in the data transmission, probable abnormalities, and variances in packet size by analyzing 'frame. Len'. Contrast the packet that transports more bytes with the packet that transfers less.

Figure 9, our present research aims to determine if message transmission and relative time are correlated. Although it makes sense that fewer message bytes will result in faster data transmission to the recipient, our research reveals an unanticipated but significant component: the TCP port number. With skill, our model determines which TCP port has the most data transfer capacity. The significant significance of the TCP source port is attributed to its essential function in facilitating efficient data routing and communication within the

Frame.time_relative	Frame. Len	Tcp. support	Tcp.time_delta	Tcp. len
0.000018	105	38,197	1.507	37
0.000122	88	38,197	1.054174	20
0.000016	105	38,197	1.566	37
0.000086	78	38,197	1.032102	10
0.00015	78	38,197	1.995659	10

Table 9. TCP packet analysis: source Port 38197.

Frame.time_relative	Frame.len	Tcp. support	Tcp.time_delta	Tcp. len
0.036971	72	1883	0.037479	4
0.000232	72	1883	0.037308	4
2.1e-05	72	1883	0.037483	4
1.8e-05	72	1883	0.037291	4
1.7e-05	72	1883	0.037481	4

Table 10. TCP packet analysis: source Port 1883.

TCP support	TCP support	mqtt msg	MQTT topic	Tcp.time_delta	Tcp. payload
38,197	1883	185	ECG	2.000445	30:08:00:03:45:43:47:31:38:35
38,197	1883	167	ECG	1.999459	30:08:00:03:45:43:47:31:36:37
38,197	1883	178	ECG	1.995659	30:08:00:03:45:43:47:31:37:38
38,197	1883	174	ECG	1.032102	30:08:00:03:45:43:47:31:37:34
38,197	1883	61	Blood Pressure	1.054174	30:12:00:0d:42:6c:6f:6f:64:50:72:65:73:73:75:72:65:2d:36:31

Table 11. Analysis of TCP packet traffic for ECG and blood pressure data.

network. This indirect effect highlights the complex nature of elements influencing message transmission speed and substantially contributes to the overall efficiency of the data transfer process.

Table 9, the use of the TCP source port 38197 is linked to a fascinating finding: data transmission is still very low, even at frame lengths greater than hundreds. This particular TCP port number shows up as a wise decision when sending patient data about their ECG, EMG, and airflow. Our model suggests an optimized data transfer strategy by assigning '38197' for these crucial characteristics to improve the effectiveness and dependability of transmitting crucial patient monitoring data.

Table 10 shows the most powerful data transmission capacity in our network, TCP port number 1883, which is easily reachable and prefers a frequent frame length of 72 while transferring data. When compared to other options, this port number shows itself to be a dependable option, offering an average data transfer speed. Determining which information has to be transmitted quickly is made easier by the perceptive study of the bar graph in Fig. 7 about patient data transfer. Our model suggests explicitly allocating the TCP port number '1883' to the temperature, blood pressure, and Glucometer data to deliver vital patient information rapidly. By utilizing the port's strong data transmission capabilities, this strategic allocation seeks to ensure the timely and effective delivery of critical health measurements.

Table 11, across our large dataset of almost 40,000 communication events, these particular ports are critical conduits that patients and healthcare providers frequently use to communicate effectively. Our next urgent task is to carefully investigate whether there have been any possible security lapses on these vital lines of communication.

Figure 10: The devices have experienced data transfer throughout time, which have caused data transmission delays that are far longer than expected. It is important to acknowledge that the length of time is not the exclusive predictor of a prospective data breach. Our advanced model is built to examine many characteristics, one of which is the payload length. The analysis requires additional investigation of extra protocols because their addition might cause Transmission Control Protocol (TCP) payload lengths to grow longer. One instance of Fig. 11 illustrates the periodic assaults causing an attack.

The data in Table 12 evidences notable variations within payload lengths because this statistic enables investigation of transfer irregularities. The diverse payload lengths reveal an essential reason for our research since such irregularities could indicate security issues or problematic communication paths. Due to its significance, network security requires persistent evaluation and interpretation of these differences between the control and attack traffic.

Table 13 demonstrates that our research model delivers predictions that extend from payload-based assault detection capabilities to identifying hacked port numbers and source and destination IP addresses associated with security events. Based on skill level, the model predicts hacked port numbers and reveals the respective

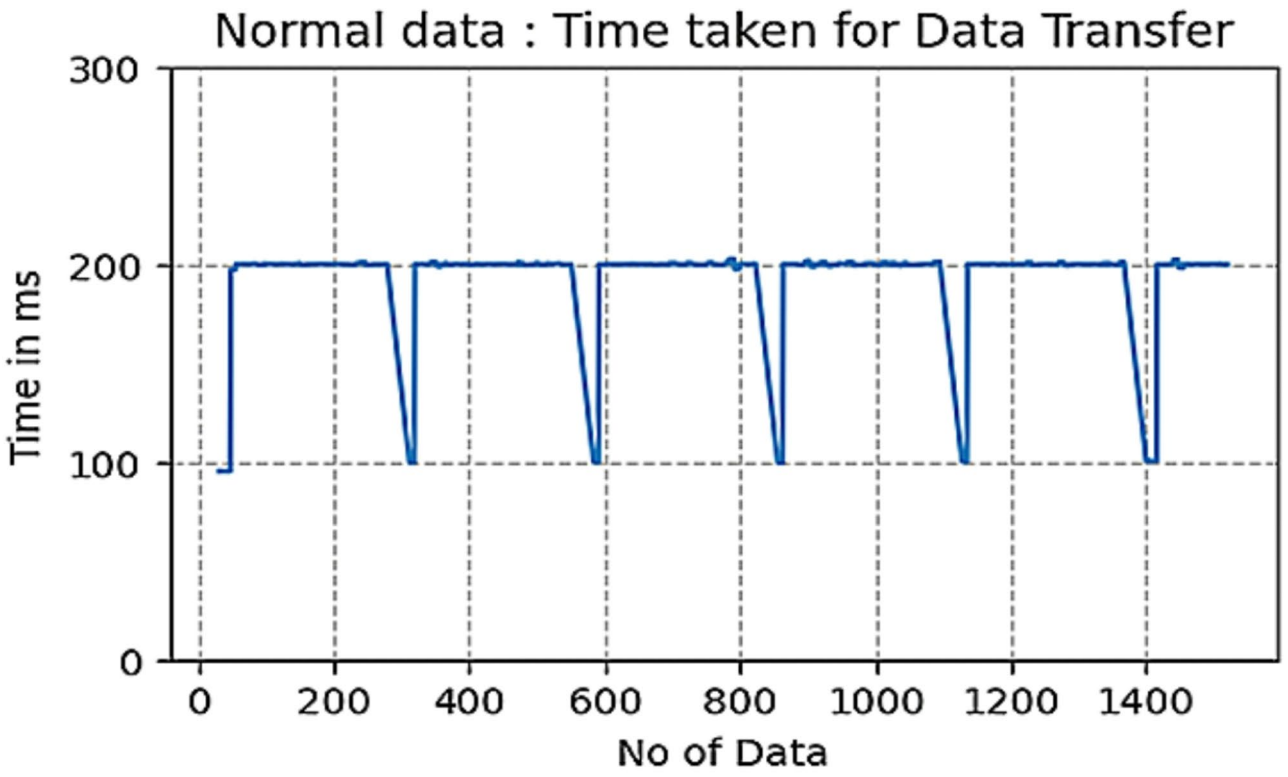

Fig. 10. Time taken for data transfer.

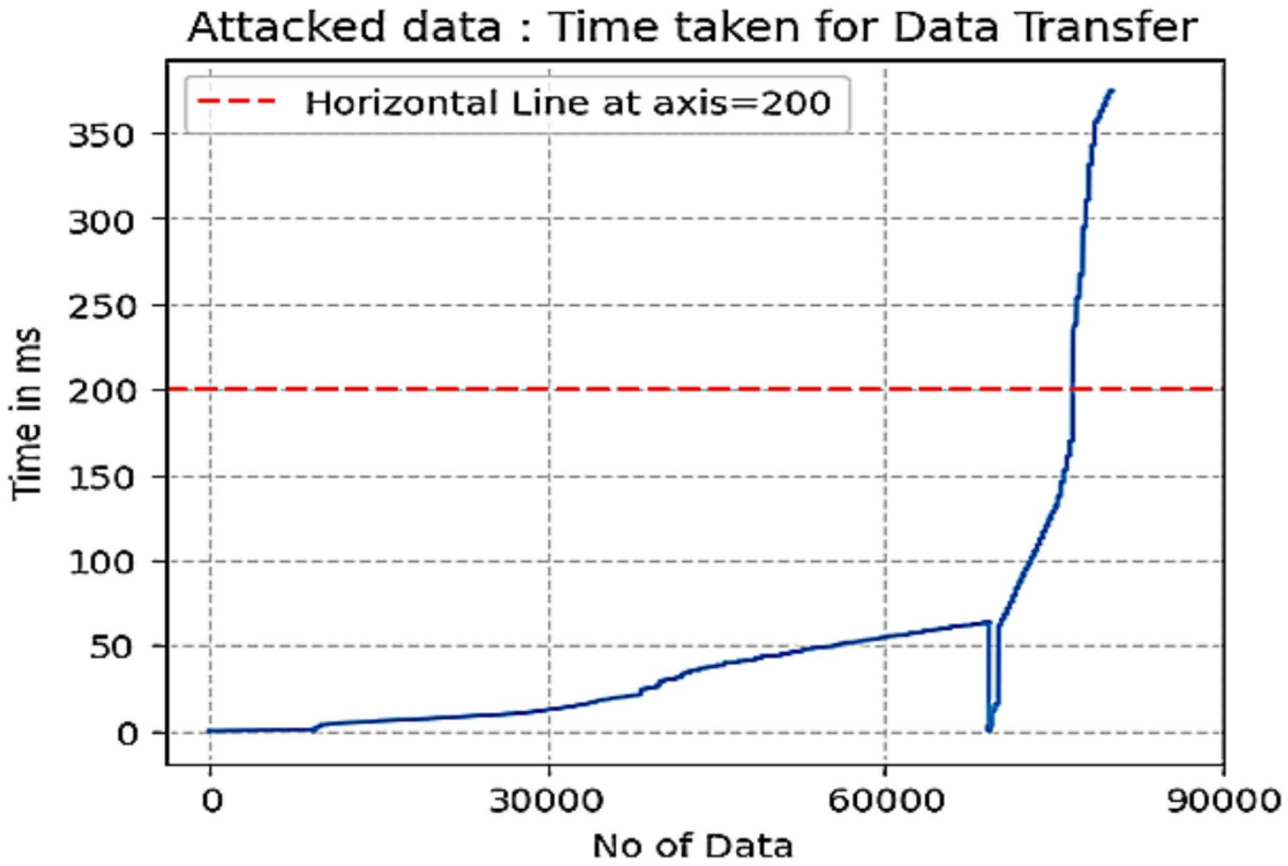

Fig. 11. Attack caused while transferring data.

TCP payload lengths	Normal data	Attacked data
Average TCP payload length	12.37	224
MaximumTCP payload length	290	1460
MinimumTCP payload length	3	0

Table 12. Payload versus attacked data.

ip.src	ip.dst	TCP.srcport	TCP.dstport	TCP.time_delta	TCP.len	payload_length
192.168.1.90	192.168.1.91	54,546	1883	3.36	1460	4379
192.168.1.90	192.168.1.91	54,546	1883	3.64	1460	4379
192.168.1.90	192.168.1.91	54,546	1883	4.02	866	2597
192.168.1.90	192.168.1.91	54,546	1883	4.26	517	1550
192.168.1.90	192.168.1.91	54,546	1883	4.28	1460	4379

Table 13. Potential attacks solely on payload metrics.

source and destination IP addresses behind such security incidents. This extensive research provides patients and healthcare professionals with better network security defense capabilities through proactive threat detection and response capabilities. The healthcare network monitoring solution helps defend communications security across all system components by revealing which parts of the network experience impact.

Choquet integral fuzzy VIKOR for identifying the best base station

Figure 12 The proposed Choquet Integral Fuzzy VIKOR method is a very efficient approach within MCDM, and its superior capacity to solve problems with criteria interdependence and reasoning vagueness, as well as to execute in loosely defined decision environments such as the identification of the best relay station for communication packets. However, unlike the reliance on the method that does not recognize interactions between the criteria, the Choquet Integral considers interactions between the criteria and how they jointly work. Moreover, the fuzzy aspect of the method successfully tackles uncertainty and imprecision of the decision data; these characteristics closely mimic reality. This offers a more sophisticated and reliable rank of the relay stations to enhance package communication and reduce such challenges as interferences and loss of data, making it quite distinct from the conventional and more structured MCDM methods.

In Table 14, relay 5 has the lowest load and the highest QoS, earning it the highest ranking. On the other hand, Relay 3 has the highest load and lower QoS, resulting in the lowest ranking. The rankings are determined by considering both load and QoS attributes, with higher-ranked relays exhibiting better performance in terms of load and QoS. This is for effective communication in the 5G relay.

The proposed model demonstrates the highest accuracy at 97.25%, surpassing other models such as PLA-SIT at 97%, FPLA at 96.8%, and PLA at 95.3% in Table 15. This indicates a marginal yet notable improvement in performance. It also significantly outperforms models like the CNN-based mechanism at 94.7%, Shamir's Secret Sharing Algorithm at 90.7%, and the Blowfish Algorithm at 82.3%. The higher accuracy of the proposed model suggests it could offer better reliability and effectiveness in its application, making it a superior choice for scenarios where accuracy is critical.

Table 15 depicts the proposed model analysis with the existing models discussed. The significance of the model and its accuracy, diversity in methodologies, and relevance to the domain and performance spectrum are also narrated.

The Choquet integral fuzzy VIKOR method is employed to choose the optimal relay stations for RPM so that interdependencies between criteria like network load, QoS, and latency can be resolved, unlike the traditional VIKOR, which fails to manage them. Fuzzy membership functions assign linguistic values for these criteria before ranking is done using VIKOR after applying the Choquet integral in aggregation. This improves decision-making under uncertainty and joint dependencies in 5G-driven healthcare settings.

PLA versus intrusion detection system (IDS) for secured authentication

In two kinds of scenarios, PLA and IDS, it is important to select specific indicators to quantify the errors associated with PLA performance and facilitate the analysis. To quantify the error between the estimated attribute and the actual value, the mean squared error (MSE) is typically used, which is calculated by multiplying the estimated attribute by the actual value.

$$\mathrm{MSE}\,(\widehat{\mathrm{x}}) = \mathrm{E}(\widehat{\mathrm{x}} - \mathrm{x})^2 \tag{40}$$

Where $\widehat{\mathrm{x}}$ represents the estimation value of true value $\mathrm{x}.\mathrm{E}(\cdot)$, in this case, we calculate the expectation. The presence of significant estimation errors harms the verification process for genuine receivers and complicates attackers' efforts to defeat security systems. By measuring the probability of miss detection (MD) and false alarm (FA) of the proposed method, we can determine the performance of our system. Typically, MD refers to the number of times Bob has accepted physical layer attributes as legal from Eve by marking them as legal. There

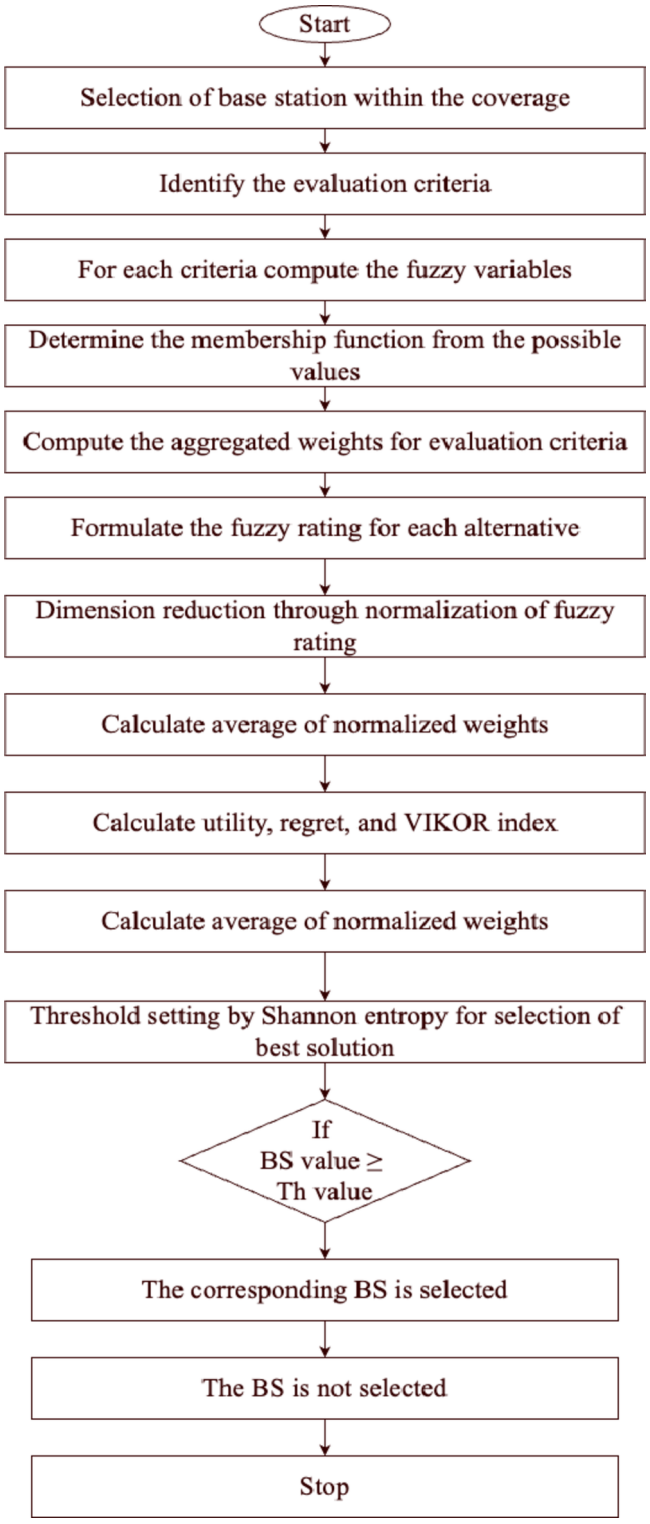

Fig. 12. Choquet Integral Fuzzy VIKOR Method flowchart.

is a way to determine how many times Bob has flagged physical layer information from Alice as being illegal, thus causing a spoof warning to be issued. It appears that signal samples from Alice are correctly classified as true positives (TP) in the test data, while false negatives (FN) are generally classified as false positives (FP). Eve's true negative message sample is classified as a true negative (TN); otherwise, a false positive is labeled as a false positive (FP).

The miss rate of detection (P_m), As a result, we can describe the FP rate in the following way.

RELAYs	Load	QoS	Rank
1	Average	Average	4
2	Average	Average	2
3	High	Lower	5
4	Higher	Higher	3
5	Lower	Higher	1

Table 14. Best RELAY choice.

Ref	Models	Accuracy	Diversity in methodologies	Relevance to the domain	Performance spectrum
[47]	Physical-Layer Authentication with Superimposed Independent authentication Tags (PLA-SIT)	97%	Statistical-based method	High relevance: Addresses physical-layer authentication	High: Top-tier accuracy for its category
[48]	Flexible Physical Layer Authentication (FPLA)	96.80%	Statistical approach with flexibility enhancements	High relevance: Focused on physical-layer authentication	High: Competitive accuracy
[49]	Privacy-Embedded Lightweight and Efficient Automated (PLA)	95.30%	Lightweight cryptographic approach	Medium relevance: Lightweight, less focus on flexibility	Medium: Moderate performance
[50]	CNN-based physical layer authentication mechanism	94.70%	Deep learning-based	High relevance: Integrates modern AI for authentication	Medium: Shows promise but below statistical methods
[51]	Shamir's Secret Sharing Algorithm (SSSA)	90.70%	Cryptographic secret-sharing mechanism	Medium relevance: Cryptography rather than a physical layer	Low: Decent but not competitive
[51]	Blowfish Algorithm (BA)	82.30%	Symmetric key cryptographic algorithm	Low relevance: Focused more on encryption	Low: Outperformed by other models
#	**Proposed Model**	**97.25%**	**Statistical approach with flexibility enhancements**	**High relevance: Focused on physical-layer authentication**	**High: Competitive accuracy**

Table 15. Proposed model analysis with existing models.

$$P_m = \frac{FP}{FP + TN}. \tag{41}$$

The false alarm rate (P_f), that is, the FN rate, can be described as

$$P_f = \frac{FN}{FN + TP}. \tag{42}$$

Figures 13 and 14, and 15 show the performance of authentication of the physical layer given for overall classification accuracy, false alarm rate, and miss detection rate, respectively. As a result of learning user and channel attributes, authentication is implemented successfully. Hence, it obtained a better performance.

Figures 16 and 17, and 18 show the performance of IDS for physical layer security for overall classification accuracy, false alarm rate, and miss detection rate, respectively. As a result of learning channel attributes and packet attributes, IDS is implemented successfully. Hence, it obtained a better performance.

The suggested methods are designed to achieve quick authentication and reduce data packet overhead without sacrificing security requirements. Our systems are resilient. An adversary who penetrates any unit and extracts the user's channel response won't jeopardize the safety of the whole system since the received signals that the entity extracts rely on the state in which the entity is positioned. Based on experimental results, it is clear that attribute estimates obtained from the physical layer are sufficient for the provision of a reliable source of authentication data. The proposed multi-attribute physical layer authentication and IDS schemes are effective in improving authentication accuracy and attack detection accuracy, with false alarm rates reduced to 0.063% and miss detection rates reduced to 0.2466%.

Ethical considerations

The research uses publicly accessible data from Kaggle for its experimental assessment without acquiring any actual patient information. The datasets obtained from Kaggle support ethical requirements because they do not contain any information identifying individuals. Strict data privacy standards apply to this study through encryption combined with anonymization techniques because real-world patient consent must be obtained for implementation. Implementing this system for clinical use needs review and approval from Institutional Review Boards (IRBs) and patient consent requirements to fulfill Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) ethical regulations.

Evaluation results

To thoroughly evaluate the two-tier authentication method and physical layer security protocols, we will provide detailed information on potential vulnerabilities, robustness against attacks, and handling of false positives/negatives. Specific protocols and standards should be clearly stated in the physical layer security. A transparent

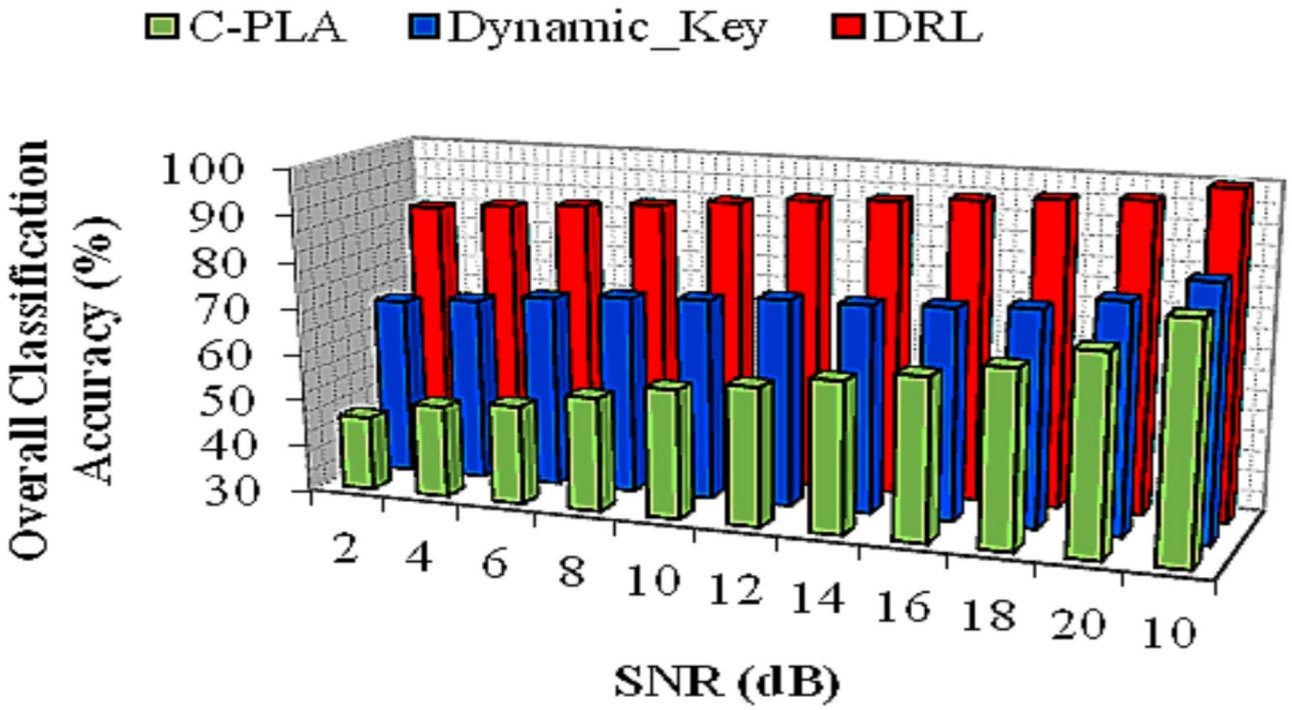

Fig. 13. Overall Classification Accuracy vs. SNR Values.

evaluation methodology and comprehensive results presented in Tables 16, 17 and 18 will strengthen the validity of the security claims and the overall system assessment.

Figures and tables indicating packet size and TCP port selection bear immense importance for data transmission optimization in remote patient monitoring. As indicated by Table 7, an optimal range between 68 and 100 bytes provides an advantage in throughput and delay performance, as packet loss and latency rise every time packets are resized midway through transmission. The aggregation approach employed ensures the efficient transmission of data without fragmentation. Also, Table 9 depicts the choice of the TCP port; port 38197 shows failure transmission rates for ECG, EMG, and airflow data, and port 1883 is optimized for temperature, blood pressure, and glucometer readings. The targeted assignment of TCP ports leads to the efficient routing of said communication without congestion and excellent reliability for real-time patient monitoring. Findings suggest that optimizing packet sizes and brilliant TCP port selection are the key factors in improving data transfer efficiency in 5G-based healthcare networks.

The Proposed Model outperforms Policy-Based RL and Value-Based RL regarding MSE and RMSE, indicating lower error variance and greater precision in Table 19. The performance differences proved statistically significant, with the p-value ($p < 0.05$) following a paired t-test. Computational time is more for the proposed model, and this trade-off is justified in exchange for greater accuracy and stability in real-world applications.

Scalability and practicality in healthcare environments

The proposed system demonstrates scalability over different healthcare environments by integrating a modular structure supporting resource-intensive systems and minimal power devices. Many obstacles require resolution to enable this system's broad acceptance, such as infrastructure expenses, device interoperability, and network connectivity problems. 5G-enabled RPM system deployment demands substantial financial commitment because significant spending on network infrastructure and cloud and edge computing assets is needed. Urban hospitals with well-established IT systems need distinctive infrastructure solutions, unlike rural medical facilities, which must establish adaptive deployment methods because of their constrained connectivity abilities. Incorporating diverse IoT sensors and their interoperation with different platforms becomes challenging because device compatibility issues need standardization initiatives. These hurdles need stepwise deployment, economical cloud systems, and structured communication protocols for better system connectivity.

Conclusion

This study analyzed the integration of deep reinforcement learning, cognitive 5G technology, channel state information, the physical layer security, and the Choquet Integral Fuzzy VIKOR on multiple criteria decision-making to advance patient care in the healthcare sector. This study demonstrates how real-time data availability in RPM can be achieved through advancements in 5G technology. Resource control brought by Cognitive 5G goes further to improve this by providing uninterrupted communication. These security techniques protect patient data and ensure confidentiality at the physical layer level. Deep reinforcement learning makes the overall processes of healthcare more efficient by improving the distribution of resources and patients' treatment

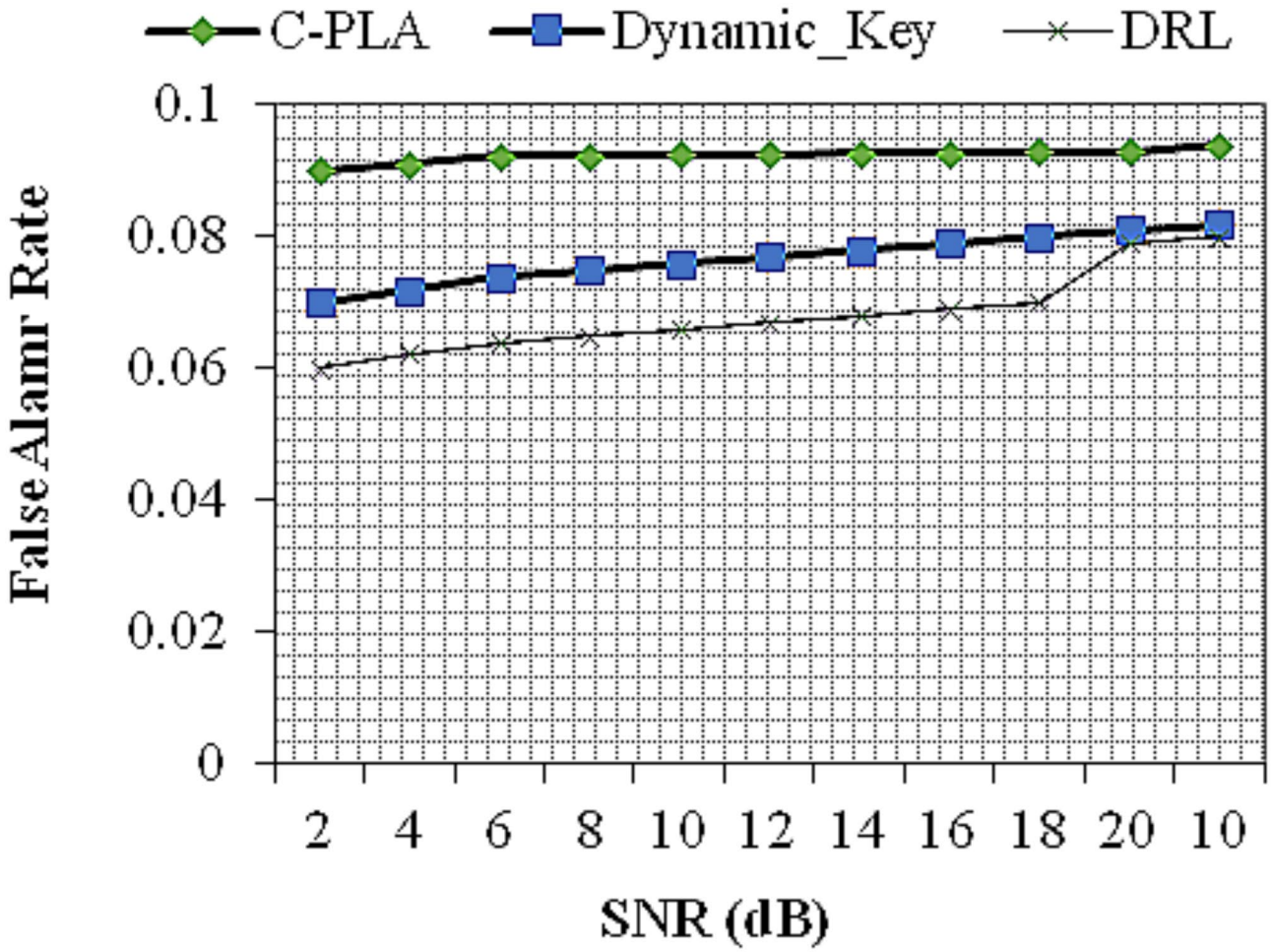

Fig. 14. False Alarm Rate vs. SNR Values.

strategies. Channel State is an essential requirement in the wireless communication system as it facilitates the fight for the appropriate allocation of resources. This integrated approach can break the barriers of health inequality and make health more accessible to people. For Secure Communication to be appropriately deployed and integrated with other systems, four areas of consideration are privacy, interoperability, and ethical issues. The incorporation of Channel estimate key generation, Automatic feature creation, A LiteNet model, the time taken to transfer data, and the analyzed attack show that this method works well. Finally, this research offers a framework for patient-oriented and heterogeneous healthcare facilities that use technological innovations properly. LiteNet is a 5G-enabling framework for RPM that faces challenges in data communication, network availability, bandwidth, and resource management. To improve it, I propose enhancing RPM data handling, prioritizing and transfer by applying Deep Reinforcement Learning algorithms. Real-time scheduling in the transmission of data to regularly update vital signs; intelligent methods for recognizing danger signs of health risks; network slicing to prioritize the most urgent patient data; and additional precautionary features to protect the privacy of patients' personal information. Enhancements include adaptive data transmission scheduling to ensure timely vital sign updates, intelligent anomaly detection for early health risk identification, dynamic network slicing for prioritized transmission of critical patient data, and enhanced security measures safeguarding sensitive patient information. If these drawbacks are eliminated, then the enhanced LiteNet framework will offer timely and efficient communication for RPM applications and allow timely, effective interventions, better patient results, and effective telehealth potential.

Future work

Future research by young scientists should focus on two main areas: disease-specific applications of the proposed framework and AI algorithm improvement for particular decision processes, as well as a practical assessment of the Choquet Integral Fuzzy VIKOR method. The focus of future research needs to shift towards creating secure communication protocols between robots and providers while advancing privacy-preserving methods and examining both economic impacts and ethical considerations related to this technology. 6G networks and quantum computing technology would enhance the suggested framework immensely, facilitating more rapid, reliable smart data transfers for tele-patient care. Quantum computing-based medical real-time decision-making

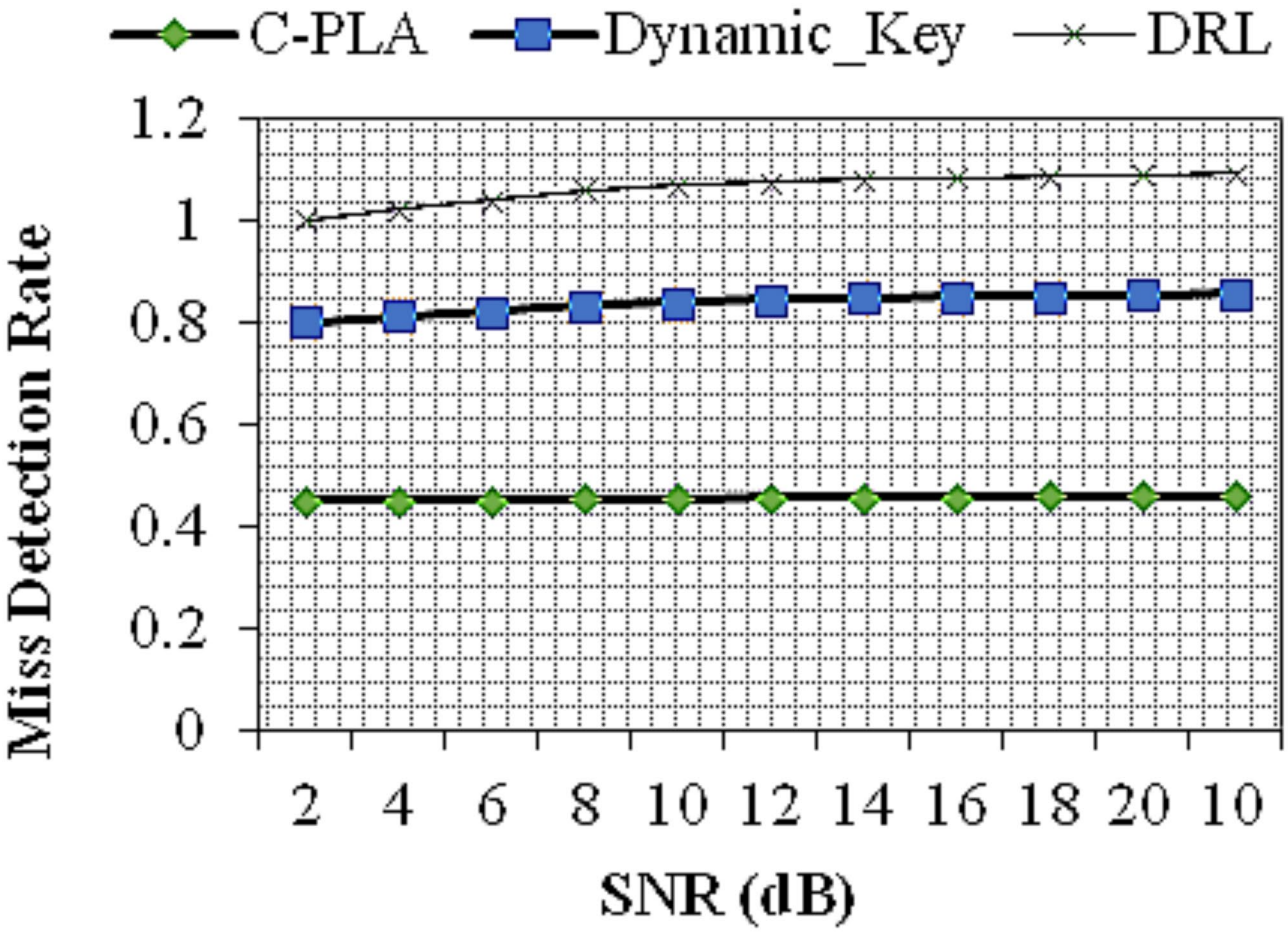

Fig. 15. Overall Classification Accuracy vs. SNR Values.

and AI diagnosis would perform optimally due to these technologies. Quantum computing can secure data encryption and process data at incredible speeds, empowering healthcare organizations to protect their patient data and perform efficient multi-factor decision-making processes. Future research should aim to develop an advanced, secure, and resilient remote healthcare monitoring system by integrating quantum-safe encryption techniques with AI-managed 6G network infrastructure.

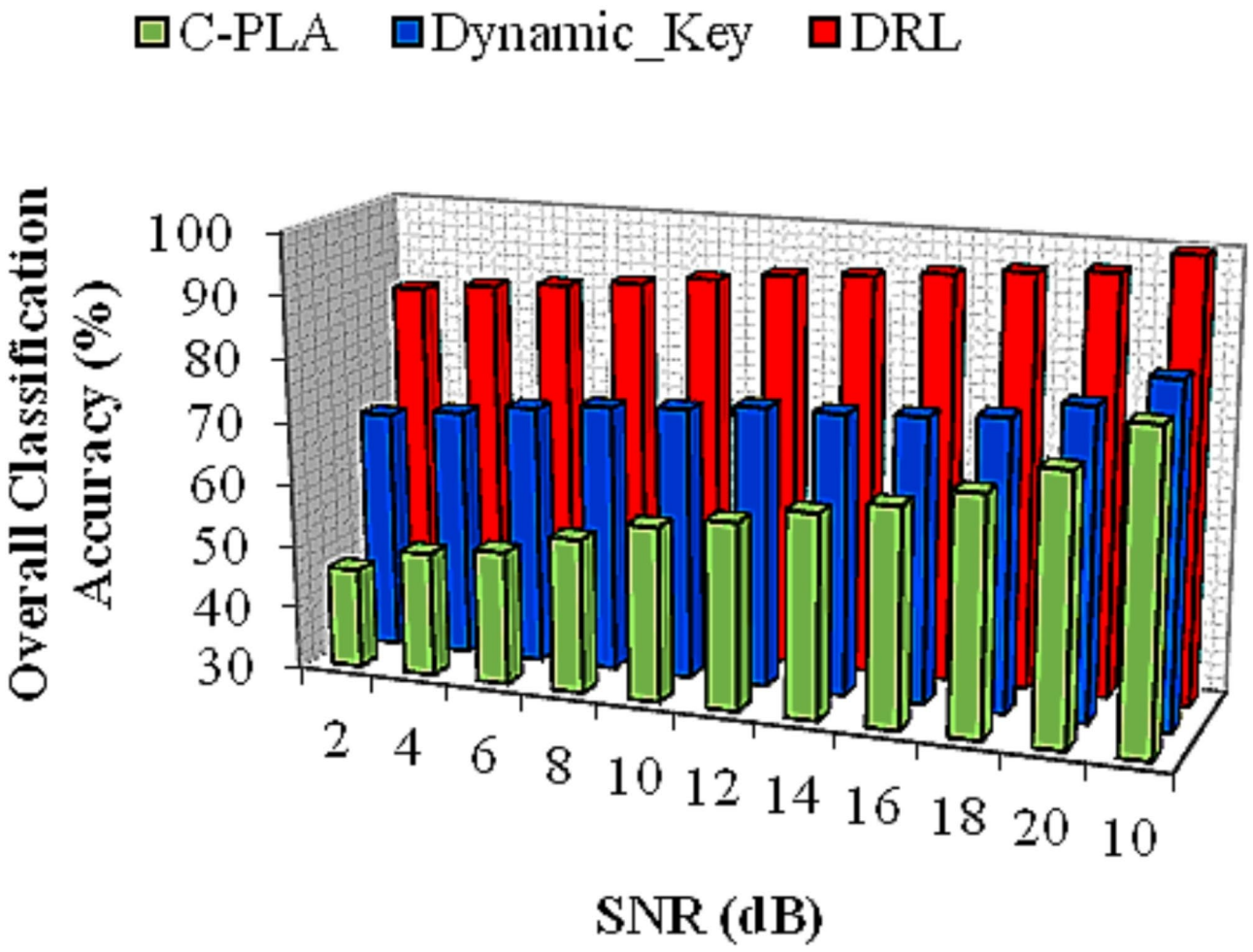

Fig. 16. Overall Classification Accuracy vs. SNR Values.

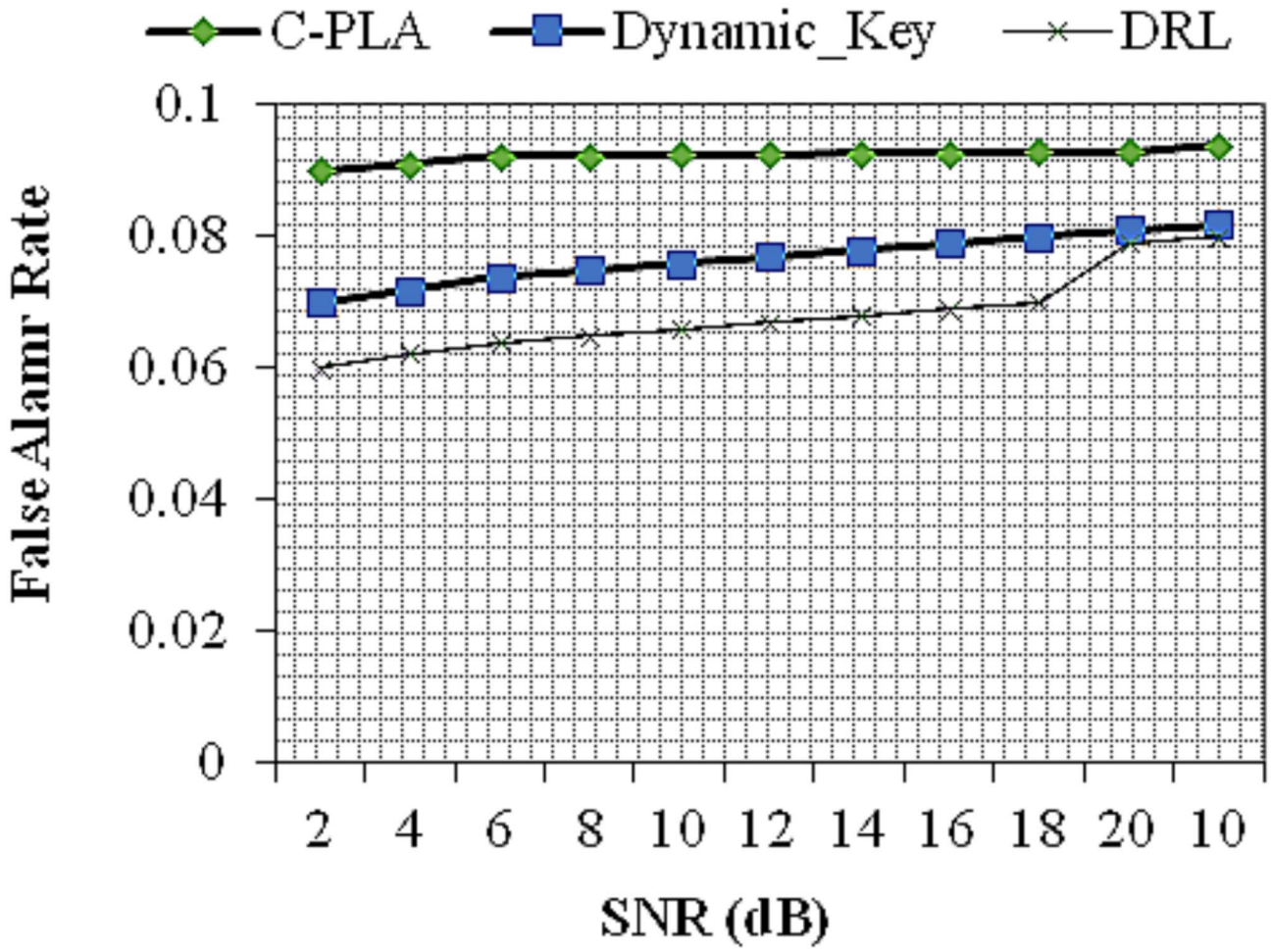

Fig. 17. False Alarm Rate vs. SNR Values.

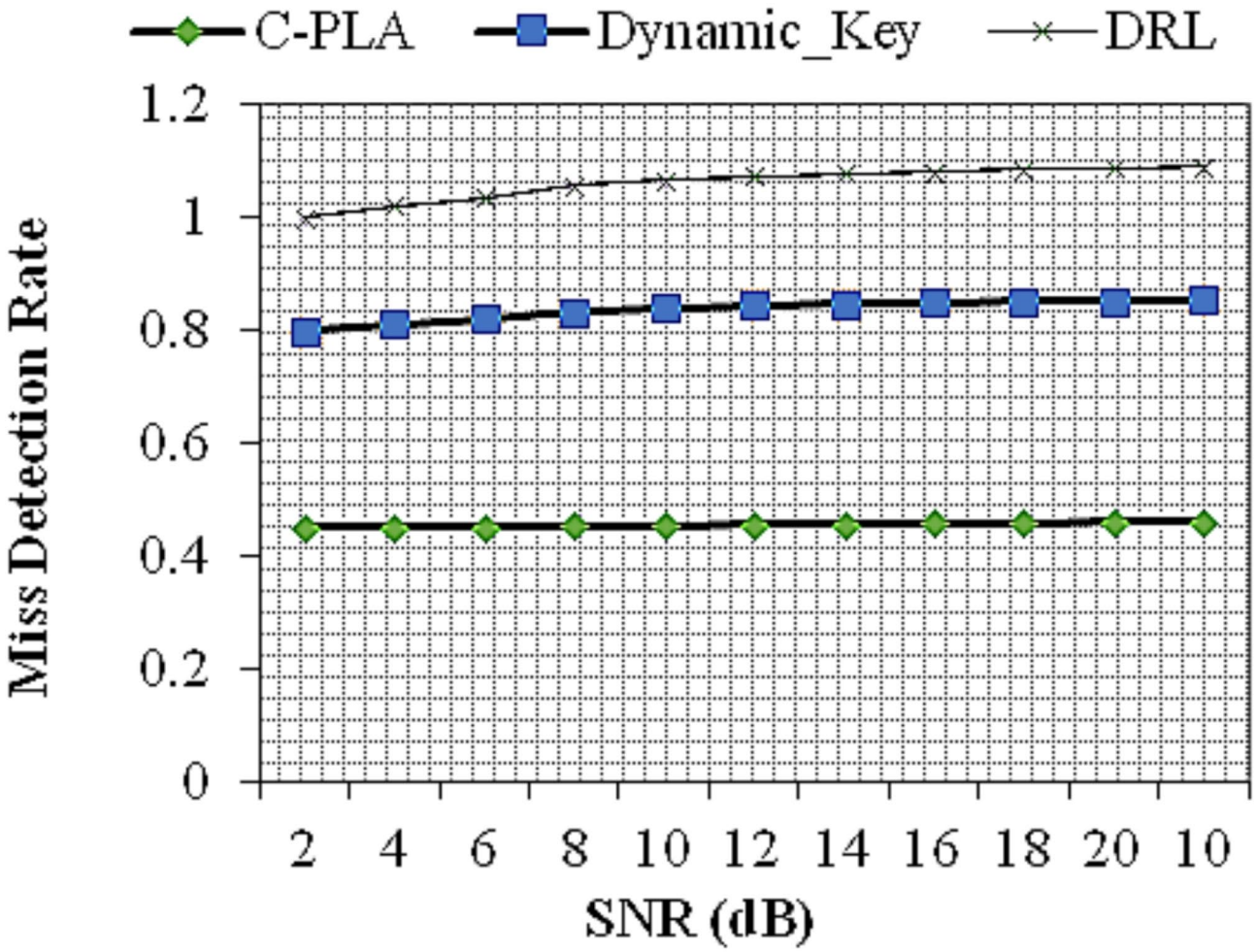

Fig. 18. Overall Classification Accuracy vs. SNR Values.

Metric	Value
False Acceptance Rate (FAR)	0.10%
False Rejection Rate (FRR)	0.20%
Environmental Impact	Minimal
Spoofing Resistance	High (with liveness detection)

Table 16. Biometric system performance.

Metric	Value
Average Login Time	2 s
Phishing Resistance	Moderate (enhanced with multi-factor authentication)
Brute-Force Resistance	High (with strong password policies)

Table 17. Biometric system performance.

Protocol/Standard	Description
AES-256	Encryption standard for data security
WPA3	Wi-Fi security protocol
TLS 1.3	Secure data transmission protocol
Spread Spectrum	Technique to secure the physical layer
Frequency Hopping	Frequency Hopping

Table 18. Physical layer security protocols.

Model	Computational Time (s)	MSE	RMSE	R^2	*p*-value (Paired t-test)
Policy-Based RL	27.743	0.371	-0.266	0.678	$p < 0.05$
Value-Based RL	23.269	0.119	-0.199	0.614	$p < 0.05$
Proposed Model	29.601	-0.125	-0.258	0.577	$p < 0.05$

Table 19. Statistical significance testing of the proposed model.

Data availability

Data is provided within the manuscripthttps://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot? select=Edge-IIoTset+dataset.

Received: 20 November 2024; Accepted: 10 March 2025
Published online: 22 March 2025

References

1. Hoque, K. et al. Technological trends in 5G networks for IoT-enabled smart healthcare: A review. *Int. J. Sci. Res. Archive*. **12** (2), 1399–1410 (2024).
2. Rahman, A. et al. Internet of medical things and blockchain-enabled patient-centric agent through Sdn for remote patient monitoring in 5 g network. *Sci. Rep.* **14** (1), 5297 (2024).
3. Srivastava, M., Siddiqui, A. T. & Srivastava, V. Application of artificial intelligence of medical things in remote healthcare delivery. In *Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things*. 169–190 (CRC, 2024).
4. Bala, I., Pindoo, I., Mijwil, M. M., Abotaleb, M. & Yundong, W. Ensuring security and privacy in healthcare systems: A review exploring challenges, solutions, future trends, and the practical applications of artificial intelligence. *Jordan Med. J.* **58**(3), 1–21 (2024).
5. Pandey, A. K., Devrani, R. & Jamuna, K. V. Cloud computing and 5G-enabled health care management models. In *2024 15th International Conference on Computing Communication and Networking Technologies* (ICCCNT) 24 Jun 2024. 1–6. (IEEE, 2024).
6. Mantri, S. P. et al. Telemedicine in 6G: A secure frontier for healthcare transformation. In *6G Security Education and Multidisciplinary Implementation*. 319–336. (IGI Global, 2024).
7. Singh, B. & Kaunert, C. Integration of cutting-edge technologies such as internet of things (IoT) and 5G in health monitoring systems: a comprehensive legal analysis and futuristic outcomes. *GLS Law J.* **6** (1), 13–20 (2024).
8. Patil, N., Moharana, A. K. & Chauhan, A. Security implications of 5G in modern health care management models. In *15th International Conference on Computing Communication and Networking Technologies* (ICCCNT), 24 Jun 2024. 1–6. (IEEE, 2024).
9. Ravi, K. C. et al. Beyond 5G-based smart hospitals: Integrating connectivity and intelligence. Smart hospitals: 5G, 6G and moving beyond connectivity. *Dec* **5**, 169–193 (2024).
10. Humayun, M., Alsirhani, A., Alserhani, F., Shaheen, M. & Alwakid, G. Transformative synergy: SSEHCET—bridging mobile edge computing and AI for enhanced eHealth security and efficiency. *J. Cloud Comput.* **13** (1), 37 (2024).
11. Hayajneh, T., Mohd, B. J., Imran, M., Almashaqbeh, G. & Vasilakos, A. V. Secure authentication for remote patient monitoring with wireless medical sensor networks. *Sensors* **16** (4), 424 (2016).
12. Butpheng, C., Yeh, K. H. & Xiong, H. Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. *Symmetry* **12** (7), 1191 (2020).
13. Liagkou, V. et al. Attack detection for healthcare monitoring systems using mechanical learning in virtual private networks over optical transport layer architecture. *Computation* **7** (2), 24 (2019).
14. Stergiou, C. L., Plageras, A. P., Memos, V. A., Koidou, M. P. & Psannis, K. E. Secure monitoring system for IoT healthcare data in the cloud. *Appl. Sci.* **14** (1), 120 (2023).
15. Almuhaideb, A. M. & Alqudaihi, K. S. A lightweight three-factor authentication scheme for WHSN architecture. *Sensors* **20** (23), 6860 (2020).
16. Humayun, M., Jhanjhi, N. Z., Almotilag, A. & Almufareh, M. F. Agent-based medical health monitoring system. *Sensors* **22** (8), 2820 (2022).
17. Enshaeifar, S. et al. A digital platform for remote healthcare monitoring. In *Companion Proceedings of the Web Conference 2020*, 20 Apr 2020 . 203–206 (2020).
18. Ahad, A. et al. Technologies trend towards 5G network for smart health-care using IoT: A review. *Sensors* **20** (14), 4047 (2020).
19. Abdrabou, M. & Gulliver, T. A. Adaptive physical layer authentication using machine learning with antenna diversity. *IEEE Trans. Commun.* **70**, 6604–6614 (2022).
20. Wang, L., Wei, Z. & Guo, W. *Securing IoT Communication Using Physical Sensor Data - Graph Layer Security with Federated Multi-Agent Deep Reinforcement Learning* (ArXiv, aRelay/2302.12592, 2023).
21. Mitev, M., Shakiba-Herfeh, M., Chorti, A., Reed, M. J. & Baghaee, S. A physical layer, Zero-Round-Trip-Time, multifactor authentication protocol. *IEEE Access.* **10**, 74555–74571 (2022).
22. Zhao, H., Zhang, Y., Huang, X., Xiang, Y. & Su, C. A Physical-Layer key generation approach based on received signal strength in smart homes. *IEEE Internet Things J.* **9**, 4917–4927 (2022).
23. Ji, Z. et al. Physical-Layer-Based secure communications for static and Low-Latency industrial internet of things. *IEEE Internet Things J.* **9**, 18392–18405 (2022).

24. Sood, K. et al. Intrusion detection scheme with dimensionality reduction in next generation networks. *IEEE Trans. Inf. Forensics Secur.* **18**, 965–979 (2023).
25. Wang, H., Xu, L., Lin, W., Xiao, P. & Wen, R. Physical layer security performance of wireless mobile sensor networks in smart City. *IEEE Access.* **7**, 15436–15443 (2019).
26. Yadav, V., Rahul, M. & Yadav, R. A new efficient method for the detection of intrusion in 5G and beyond networks using ML (2020).
27. Forssell, H., Thobaben, R., Gross, J. & Skoglund, M. Feature-based multi-user authentication for parallel uplink transmissions. In *2016 9th International Symposium on Turbo Codes and Iterative Information Processing* (ISTC). 355–359 (2016).
28. Marhoon, H. A., Nedoma, J. & Martinek, R. A metaverse framework for IoT-based remote patient monitoring and virtual consultations using AES-256 encryption. *Appl. Soft Comput.* **158**, 111588 (2024).
29. Cheikhrouhou, O. et al. A lightweight blockchain and fog-enabled secure remote patient monitoring system. *Internet Things*. **22**, 10069 (2023).
30. Kapoor, B., Nagpal, B. & Alharbi, M. Secured healthcare monitoring for remote patient using energy-efficient IoT sensors. *Comput. Electr. Eng.* **106**, 108585 (2023).
31. Chen, C. M., Liu, S., Li, X., Islam, S. H. & Das, A. K. A provably-secure authenticated key agreement protocol for remote patient monitoring IoMT. *J. Syst. Architect.* **136**, 102831 (2023).
32. Chakraborty, I., Edirippulige, S. & Ilavarasan, P. V. The role of telehealth startups in healthcare service delivery: a systematic review. *Int. J. Med. Informatics*. **174**, 105048 (2023).
33. Butt, S. A. et al. Remote mobile Heath monitoring frameworks and mobile applications: taxonomy, open challenges, motivation, and recommendations. *Eng. Appl. Artif. Intell.* **133**, 108233 (2024).
34. Komal, K., Cleary, F., Wells, J. S. & Bennett, L. A systematic review of the literature reporting on remote monitoring epileptic seizure detection devices. *Epilepsy Res.* **27**, 10733435 (2024).
35. Amzil, A., Abid, M., Hanini, M., Zaaloul, A. & El Kafhali, S. Stochastic analysis of fog computing and machine learning for scalable low-latency healthcare monitoring. *Cluster Comput.* **21**, 1–21 (2024).
36. Lakhan, A., Mohammed, M. A., Kozlov, S. & Rodrigues, J. J. Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows. *Trans. Emerg. Telecommunications Technol.* **35** (4), e4363 (2024).
37. Yaqoob, M. M. et al. Modified artificial bee colony based feature optimized federated learning for heart disease diagnosis in healthcare. *Appl. Sci.* **12** (23), 12080 (2022).
38. Hennebelle, A., Materwala, H. & Ismail, L. HealthEdge: a machine learning-based smarthealthcare framework for prediction of type 2 diabetes in an integrated IoT, edge, and cloud computing system. *Procedia Comput. Sci.* **220**, 331–338 (2023).
39. Khan, M. A. et al. Farooq Khattak U. Asynchronous federated learning for improved cardiovascular disease prediction using artificial intelligence. *Diagnostics* **13** (14), 2340 (2023).
40. Vimal, S. P., Vadivel, M., Baskar, V. V., Sivakumar, V. G. & Srinivasan, C. Integrating IoT and machine learning for real-time patient health monitoring with sensor networks. In *2023 4th International Conference on Smart Electronics and Communication* (ICOSEC), 2023 Sep 20. 574–578. (IEEE, 2023).
41. Yıldırım, E., Cicioğlu, M. & Çalhan, A. Fog-cloud architecture-driven internet of medical things framework for healthcare monitoring. *Med. Biol. Eng. Comput.* **61** (5), 1133–1147 (2023).
42. Mateen Yaqoob, M. et al. Adaptive multi-cost routing protocol to enhance lifetime for wireless body area network. *Computers Mater. Continua*. **72** (1), 1089–1103 (2022).
43. Khan, M. M. & Alkhathami, M. Anomaly detection in IoT-based healthcare: machine learning for enhanced security. *Sci. Rep.* **14** (1), 5872 (2024).
44. Chi, H. R. et al. Healthcare 5.0: In the perspective of consumer internet-of-things-based fog/cloud computing. *IEEE Trans. Consum. Electron.* (2023).
45. Qayyum, A., Qadir, J., Bilal, M. & Al-Fuqaha, A. Secure and robust machine learning for healthcare: A survey. *IEEE Rev. Biomed. Eng.* **14**, 156–180 (2020).
46. Samie, F., Bauer, L. & Henkel, J. From cloud down to things: an overview of machine learning in internet of things. *IEEE Internet Things J.* **6** (3), 4921–4934 (2019).
47. Xie, N., Zhang, S. & Liu, A. X. Physical-layer authentication in non-orthogonal multiple access systems. *IEEE/ACM Trans. Networking*. **28** (3), 1144–1157 (2020).
48. Li, Y., Han, J., Liu, G., Zhou, Y. & Liu, T. FPLA: A flexible physical layer authentication mechanism for distributing quantum keys securely via wireless 5G channels. *Appl. Sci.* **13** (13), 7699 (2023).
49. Yan, C. et al. PLA—A Privacy-Embedded lightweight and efficient automated breast cancer accurate diagnosis framework for the internet of medical things. *Electronics* **12** (24), 4923 (2023).
50. Li, X., Huang, K., Wang, S. & Xu, X. A physical layer authentication mechanism for IoT devices. *China Commun.* **19** (5), 129–140 (2021).
51. Sharmila, G. & Sridhar, S. Comparing and protecting data privacy and security of Novel Shamir's secret sharing algorithm over Blowfish algorithm for cloud computing based on secret sharing mechanism. In *AIP Conference Proceedings 2023 Nov 21*. Vol. 2821(1). (AIP Publishing, 2023).
52. Yang, T. et al. Secure and traceable multikey image retrieval in cloud-assisted internet of things. *IEEE Internet Things J.* **10** (2024).
53. Miao, Y. et al. Efficient and secure federated learning against backdoor attacks. *IEEE Trans. Depend. Secur. Comput.* **16** (2024).
54. Miao, Y. et al. Time-controllable keyword search scheme with efficient revocation in mobile e-health cloud. *IEEE Trans. Mob. Comput.* **23** (5), 3650–3665 (2023).

Acknowledgements

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R754), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Author contributions

Methodology, S.C., Conceptualization, M.P., Resources, A.H.A., Software, S.K., Validation, D.S.K., Original Draft Writing, S.K.R., Data Curation, M.M.E., Formal Analysis, E.M.E. All authors have read and agreed to the published version of the manuscript.

Funding

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R754), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Ethical statement

Competing interests
The authors declare no competing interests.

Informed consent
Informed consent was obtained from all the participants.

Additional information
Correspondence and requests for materials should be addressed to D.S.K. or S.K.R.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.