Journal of Rare Cardiovascular Diseases
ISSN: 2299-3711 (Print) | e-ISSN: 2300-5505 (Online)
www.jrcd.eu
RESEARCH ARTICLE

Human-in-the-Loop Robotics for Remote Healthcare: A 6G-IoT Blockchain Secured Architecture

K S Ranjith[1], Neetu Singh [2], Kishore Balasubramanian [3], Asha Sohal [4], D. Kavitha,[5] Syed Zahidur Rashid[6]

[1] Associate Professor, Artificial Intelligence and Data Science, Mother Teresa Institute of Engineering and Technology, Palamaner, Chittoor, Andhra Pradesh, India.
[2] Asst. Prof (IT department), Bharati Vidyapeeth College of Engineering (BVCOE), located in Paschim Vihar, Delhi, India.
[3] Associate Professor, Department of Electrical and Electronics Engineering, Dr. Mahalingam College of Engineering and Technology, Tamil Nadu, India.
[4] Asha Sohal, Assistant Professor (Sel Grade), CSE, The Northcap University, Gurgaon, Haryana, India.
[5] Assistant Professor, Department of Computer Science and Engineering, Easwari Engineering College, Ramapuram, Chennai, India.
[6]Department of Electronic and Telecommunication Engineering, International Islamic University Chittagong, Chattogram, Bangladesh.

*Corresponding Author
K S Ranjith

Article History
Received: 11.07.2025
Revised: 12.08.2025
Accepted: 05.09.2025
Published: 31.10.2025

Abstract: Human-in-the-Loop (HITL) robotics has demonstrated a lot of potential in improving remote healthcare by integrating automated robotic accuracy and human expertise. The current work suggests a new architecture that combines HITL robotics with a 6G-powered Internet of Things (IoT) system and makes it secure against blockchain technology to provide reliable Internet of Things (IoT) and secure remote healthcare services with low latencies. The architecture consists of several layers, among which there are IoT-enabled wearable sensors that are going to provide continuous monitoring of patients, edge and fog computing nodes that are going to provide data processing on the local level, and a 6G communication framework that should provide ultra-reliable low-latency communication (URLLC) to guarantee real-time interactions between clinicians and robots. It is integrated with blockchain to deliver non-mutable storage of data, decentralized trustkeeping with smart contracts, and immutable medical records. Major issues considered in the system design include the security of the data, compatibility between different medical devices, and the ability to scale the system to large-scale implementation. Massive simulation and case studies were carried out to confirm the performance in different conditions, with emphasis on remote robotic-aided surgery and treatment of chronic diseases. The findings indicate sub-millisecond latency, better system availability, strong protection against cyberattacks, and better data integrity than standard telemedicine systems. Ethical, legal, and social considerations (ELSI) are included to guarantee patient privacy, informed consent, and regulation. A performance evaluation technique that is utility based was used in order to balance latency, reliability, energy efficiency, and security. This unified solution shows a scalable and realistic method of the implementation of intelligent and safe remote healthcare services, which can underpin complex applications like telesurgery and decentralized clinical trials. The given framework opens the way to the next-generation healthcare systems that will involve the integration of the most advanced connectivity, automation, and distributed trust schemes.

Keywords: Human-in-the-Loop Robotics, 6G IoT, Blockchain Security, Remote Healthcare, Low-Latency Communication, Edge Computing .

INTRODUCTION

Human-in-the-Loop (HITL) robotics has emerged as a new paradigm in contemporary medical care where roboticization is integrated with the human experience to guarantee safe, accurate, and ethical clinical procedures [1]. As opposed to completely autonomous systems, HITL robotics allows clinicians to retain control of decision-making processes and relies on robotic assistance to provide accuracy, speed, and consistency [2]. The recent studies of robotic-assisted surgery, rehabilitation robots, and assistive devices have emphasized the necessity of human supervision of those reconnaissance tasks where contextual judgment and maneuverability are vital [3]. Research has demonstrated that human integration mitigates the risks related to autonomy, particularly in high-stakes environments like telesurgery or critical care [4]. Nonetheless, constraints are still evident in the current implementations of HITL in the form of delay in communication, absence of a user-friendly interface, and inability to adapt to remote locations [5].

Although human-in-the-loop robotics will help improve precision and safety in clinical interventions, it is only a matter of time before this method is truly engaged when it becomes a part of strong remote healthcare and telemedicine systems that can expand its capabilities beyond hospital settings [6]. These systems ensure the issue of accessibility, especially to patients within the rural or underserved areas, by allowing remote diagnosis, monitoring, and treatment [7]. Wearable sensors and devices with IoT capabilities have increased the opportunities of gathering continuous physiological information that helps in personalized and prevention-based care [8]. In spite of such developments, contemporary telemedicine infrastructures still have challenges such as data transmission latency, incompatibility between non-homogenous devices, and constraints to deliver real-time support to emergency interventions [9]. Studies have further noted that patient confidence and data safety are still key issues, because delicate medical data is usually shared on unsecured sites [10].

Despite the current development of remote healthcare with the help of IoT and telemedicine systems, the implementation of the latter is still limited by the problem of latency and reliability, and the implementation of 6G-enabled IoT solutions can offer the most reliable and real-time medical services [11]. Contrary to the earlier versions, 6G is characterized by terahertz communication, massive MIMO, AI-driven networking, and ultra-reliable low-latency communication (URLLC), rendering it very appropriate in mission-critical tasks, including robotic telesurgery and constant monitoring of patients [12]. Research has proved that 5G-based healthcare is failing to address the lack of coverage and overloading during high-density networks and also has the problem of latency that undermines the high-level interventions [13]. In comparison, 6G guarantees less than a millisecond of latency, gigabit data rate, and improved connectivity of devices that can support large-scale IoT in hospitals, homes, and emergency settings [14]. The development of edge and fog computing in 6G systems has also demonstrated that it is possible to achieve real-time analytics at the network edge and minimize delays and provide adaptable clinical decisions [15].

Although IoT architectures supported by the 6G standard can improve the issues of latency and connectivity, the exchange of sensitive health data through these high-speed networks presents a security and privacy threat that can be successfully addressed using blockchain-based solutions [16]. The conventional centralized health data systems are susceptible to breaches, unauthorized access, and single points of failure; hence, they are not suitable in the contemporary digital healthcare ecosystems [17]. Medical records and IoT-generated patient data can be provided with transparency, traceability, and tamper-resistance with blockchain, which has a decentralized and immutable ledger [18]. It has been shown that smart contracts can be used to automate the process of patient consent, access control, and interoperability across health providers [19]. Moreover, blockchain improves accountability, as all the operations and data changes are irreversible [20]. Although these are the benefits, scalability, energy usage, and real-time healthcare application integration are major constraints [21]. More specifically, the large volume of data that robotic healthcare and IoT-based monitoring demand is also a question of how blockchain can be used to provide responses in time [22].

Despite the fact that blockchain enhances data integrity and trust in the healthcare systems, its highest merit is experienced when incorporated with robotics, 6G, and IoT in one architecture to provide safe, intelligent, and patient-oriented healthcare services [23]. Although robotics offers accuracy and automation, 6G has a low-latency connection, IoT is on-demand monitoring, and blockchain adds security to the whole process of moving data [24]. These technologies in healthcare have been investigated individually in recent studies, but combined frameworks are not developed [25]. Such integration is needed to enable the use of complex applications such as remote robotic surgery, remote continuous patient monitoring, and decentralized clinical trials, among others [26]. As an example, the IoT network based on blockchain can protect real-time data that is exchanged between HITL robots and remote clinicians, whereas the URLLC of 6G guarantees the reliability of human-robot communication [27]. Nevertheless, existing scientific sources reveal the gaps in the harmonization of these layers, especially the one between the computational requirements of blockchain and the latency-sensitive character of HITL systems [28]. Although robotics, 6G, IoT, and blockchain integration have the potential to transform the world, the implementation of such a high-tech solution hampers serious ethical, legislative, and social issues that need to be thoughtfully worked out to make them responsible and trust them with their lives [29]. The ethical issues to consider include the privacy of patients, their autonomy, and informed consent, especially in cases where AI-driven robotics and blockchain appear in the decision-making process [30]. The dangers of excessive use of automation with the role of human clinicians reduced, and accountability and patient trust may decrease, have been highlighted in literature [31]. Law follows in technological progress as well, which makes the liability in the cases of the errors made at the HITL robotic intervention or blockchain-based system intrusion ambiguous [32]. Moreover, the problems of data ownership, cross-border health data sharing, and the compliance with such regulations as GDPR and HIPAA have been discussed extensively [33]. Another important dimension is social acceptance because the patients might be reluctant to accept robotic or blockchain-empowered healthcare because of the lack of knowledge or perceived danger [34]. These ELSI factors are critical in trying to ensure that technological advancements are released in a responsible and ethical manner that would foster trust among the people [35].

Research Gap

Current research in human-in-the-loop robotics, telemedicine systems, 6G-enabled IoT, and blockchain

in healthcare has made a positive step forward, but most publications have considered these technologies individually. HITL robotics is more precise but with communication delays and low capabilities of adaptation in the remoteness. Telemedicine is more accessible but lacks latency, interoperability, and data security, whereas 6G offers the benefit of ultra-reliable low-latency communication, and blockchain offers transparency and trust, although neither can be used to support real-time, high-throughput medical operations. A combined system that integrates HITL robotics, 6G, IoT, and blockchain is not well-developed, and ethical, legal, and social issues need to be explored further to deploy healthcare responsibly.

Research Objective

The main aim is to design and develop a secure, smart, and low-latency architecture, which combines the Human-in-the-Loop (HITL) robotics with 6G-enabling IoT and blockchain technology into sophisticated remote healthcare applications. The system is to allow real-time robotic manipulation and nonstop monitoring of a patient and guarantee the integrity of data, resistance against cyber threats, and the flawless interoperability between heterogeneous medical devices. With the support of edge and fog computing, the architecture aims to maximize the network performance, the latency, and the fault tolerance. It is also aimed at solving ethical, legal, and social issues through adopting a secure patient consent and regulatory compliance in order to achieve reliable healthcare provision.

Research Methodology

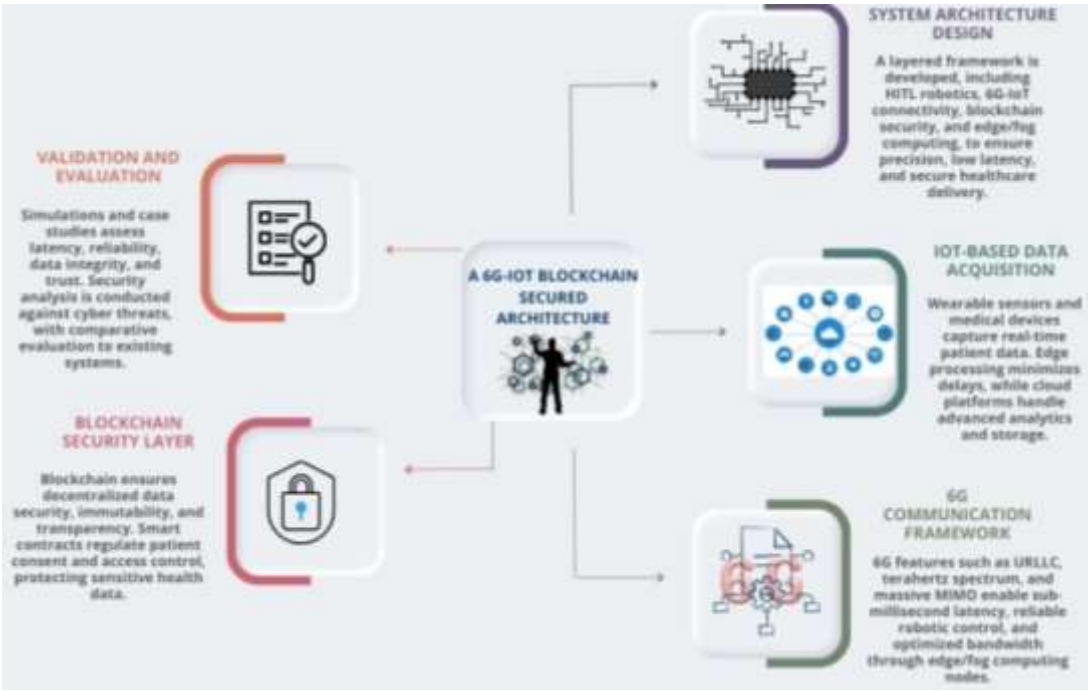

Figure 1. Methodology Flow Chart

2 System Design and Architectural Framework

This architecture was developed in the form of a layered structure combining Human-in-the-Loop (HITL) robotics, 6G-IoT connectivity, blockchain-based security, and edge/fog computing. All the layers had a particular purpose in terms of making the environment of healthcare operate smoothly while at the same time contributing to the overall resilience of the healthcare setting. The basis was made by the HITL robotics, which enabled clinicians to oversee robotic operations like telesurgery and assistive care in line with the accuracy and speed provided by automation. Such a design choice was made so that clinical judgment would take center stage during the decisions, but operational efficiency would be improved by using robots [36].

The connectivity layer was designed based on the 6G communication principles that provide ultra-reliable low-latency communication (URLLC), massive MIMO, and use of the terahertz spectrum. These characteristics minimized delay in the transmission of very important medical information that was crucial in use in robotic-assisted surgery, remote diagnosis, and emergency intervention. The introduction of edge and fog computing nodes enabled processing to be brought closer to the source of data, thus eliminating the need to use remote cloud servers and limiting the latency. This guaranteed that robotic response and patient monitoring were carried out in near-real time.

A layer built on blockchain was implemented to ensure the protection of the transmission and storage of healthcare data. Immutable records assured by the decentralized nature of blockchain removed weaknesses that are found in centralized storage systems. Smart contracts were used to automate patient consent schemes, clinician authorization, and access. Such mechanisms guaranteed the inability of sensitive data to be tampered with and the involvement of authorized entities in the

healthcare workflow. Secondly, blockchain also created a level of trust among the stakeholders since it ensured that all transactions were transparent and accountable.

Lastly, the combination of these layers developed an interconnected system, which overcame major obstacles in remote healthcare. Safety and adaptability of medical interventions were secured by the HITL robotics, and required speed and reliability were offered by 6G connectivity and edge computing. Blockchain helped protect the ecosystem against cyberattacks and provided a transparent and reliable platform in terms of data exchange. Collectively, these elements formed a system that could offer the supporting power of high-order applications like telesurgery, constant patient care, and emergency medical services in various environments [37].

$$L_{\text{total}} = L_{\text{sense}} + L_{\text{edge}} + L_{6G} + L_{\text{cons}} + L_{\text{proc}} + L_{\text{act}} \quad (1)$$

Total delay between sensing and actuation is represented in equation 1. It emphasizes the effect of 6G and edge on the elimination of bottlenecks. Medical data security clearly includes blockchain consensus delay.

$$\mathbb{E}[L_{\text{trans}}] = \left(1 - p_{\text{edge}}\right) \cdot \frac{\rho}{\mu(1-\rho)} + p_{\text{edge}} \cdot \frac{\rho_e}{\mu_e(1-\rho_e)} \quad (2)$$

Equation 2 is the model of the effect that offloading to the edge minimizes transmission delay. It takes into consideration server usage in the cloud layer as well as in the edge layer. The cloud and edge ratio influences the operation's response time.

$$x_{k+1} = A_d x_k + B_d u_{k-dk}, d_k = \left\lfloor \frac{L_{total,k}}{T_s} \right\rfloor \quad (3)$$

Equation 3 illustrates the effect of different delays on closed-loop control. It indicates latency-vulgar robotic motions within 6G connections. Stability margins are based on the worst-case transmission delay.

Data Acquisition and IoT Integration

The continuous procedure of data acquisition was provided by the personal IoT-enabled wearable sensors and medical devices that measured the physiological parameters continuously. Pulse oximeters, electrocardiogram monitors, and motion trackers, among other devices, were used to record vital health indicators such as the heart rate, oxygen saturation, and mobility patterns. This ongoing data stream made it possible to build a dynamic profile of health, which could then be accurately used to determine the conditions of patients both in emergencies and during other routine care settings. The solution made sure that essential information could not be lost in an uninterrupted flow, which minimized chances of missing a response in a medical emergency that was time sensitive.

The collected data were sent to the HITL robotic systems, and real-time adjustment was obtained. Sensing results coupled with robotic controllers enabled medical robots to react immediately to modified patient conditions. As an example, changes in oxygen saturation or irregular heartbeats received instant feedback on robotic-assisted care or intervention. This dynamism enhanced the role of the clinicians in overseeing the system and also made sure that robotic functions complemented human expertise and did not substitute it. The HITL model, thus, relied on the proper and uninterrupted data collection as the basis of its efficiency [38].

To reduce the time lag associated with processing information, edge devices were used to process data streams close to the patient or the clinical location. These local processors processed, filtered, and analyzed direct sensor input and forwarded it to upper-level platforms. The uptake of edge computing minimized the usage of remote cloud servers and then broadcast the message across networks. This provided almost real-time response of important applications like telesurgery, remote diagnosis, and automated notifications and retained complex analysis in centralized data centers on demand.

The use of cloud platforms was done to carry out high-level analytics and big storage, which facilitated predictive modeling and long-term health trend analysis. The integrative approach of providing edge processing as a real-time responsive and cloud system as a comprehensive analysis provided a balanced workflow that was efficient, reliable, and scalable. When it came to integrating IoT and HITL robotics aided by layered data handling mechanisms, a strong data-driven environment was created. This has allowed maintaining the precision, adaptability, and security of patient monitoring to meet the needs of the next-generation remote health care systems.

$$u_k = \alpha_k u_{h,k} + (1 - \alpha_k) u_{a,k}, \quad u_k \leftarrow \Pi_{\mathcal{U}_{\text{safe}}}(u_k) \quad (4)$$

The human and autonomous commands are dynamically mixed in equation 4. Safety projection makes sure that unsafe actions are not taken. The blending weight is affected by trust and edge health besides clinical context.

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + \sum_{i \in \mathcal{S}_k} K_k^{(i)} \left(y_k^{(i)} - H_i \hat{x}_{k|k-1}\right) \quad (5)$$

Signal fusion of heterogeneous wearable sensors is done in equation 5. It can be used to estimate the state even when the updates are asynchronous. Edge pre-processing reduces the bandwidth requirements, yet it retains the accuracy.

6G Communication Framework

The 6G capabilities formed the foundation of the development of the communication backbone to satisfy the strict requirements of real-time healthcare applications. It included features that ensured high capacity and highly responsive networks, like ultra-reliable low-latency communication (URLLC), terahertz frequency bands, and massive multiple-input multiple-output (MIMO) technologies. These properties enabled response times of less than a millisecond, and this was necessary in applications like telesurgery, robotic-assisted surgery, and 24-hour monitoring of patients in the intensive care unit. The terahertz communication with the high bandwidth allowed transmitting the large medical imaging files with great speed, which meant that the process of diagnosis was performed without any delays [39].

The nodes of edge and fog computing were carefully implemented in the communication infrastructure to improve its performance and reliability. These nodes handled data that were near the source, hence eliminating reliance on remote cloud infrastructure and minimizing the latency. The system did localized calculations and made better use of network resources and distributed workloads efficiently among devices over the network. This design was specifically critical to robotic systems that needed immediate reaction to clinician commands and patient data changes. Adaptive decision-making was also enabled through the integration of edge intelligence, which enabled the system to prioritize tasks of an urgent nature in case the network was prone to heavy traffic.

Another aspect that enhanced the framework was taking advantage of the massive MIMO technology that allowed connected devices in higher numbers without affecting performance. This functionality was crucial in a healthcare setting where various sensors, wearables, and robots were working simultaneously to guarantee continuous service access. Massive MIMO provided a higher spectral efficiency to support large networks of hospitals and remote rural deployments in which reliability and stability of communication were vital. This aspect enabled the medical workers to control numerous patients and devices in the framework of a single and reactive network [40].

In general, the 6G communication system overcame the major constraints of the previous networks, integrating speedy transmission, low latency, and artificial resource distribution. It has set the required background of human-in-the-loop robotics, where clinicians can communicate with robotic systems in real time without delays or interruptions of any kind. The addition of edge and fog computing nodes as well as the scalability of massive MIMO provided an infrastructure that was resilient and sustained the most demanding of healthcare services, including telesurgery, real-time consultations, and emergency response systems. This powerful line of communication was critical in the efficiency and reliability of the integrated healthcare architecture.

Blockchain-Based Security and Trust Layer

The security model was also developed in such a way that it integrates blockchain to provide decentralized safety of sensitive healthcare data. The system removed the single points of failure by removing centralized storage and minimized risks of unauthorized manipulation through the use of distributed ledgers. Unable to change the records of medical history, robotic operation history, and patient monitoring records ensured that the records were stored permanently. This degree of integrity brought a platform of trust between clinicians, patients, and healthcare providers, whereby the system could be relied upon in high-stakes medical contexts like telesurgery and emergency surgeries.

Intelligent contracts were integrated to program processes associated with the consent management and the granting of access. All operations that were related to patient data, robotic data transfer, or clinician control input were controlled by predefined rules stored in the blockchain. These automated services ensured that authorized and known stakeholders were the only people to get access to secured records. An example is before a remote surgical procedure, a smart contract was used to validate the identity of the surgeon, ensure patient authorization, and give access to the system safely. Through this automation, human error was reduced, and the speed with which approvals were made was accelerated, resulting in more accountability within the healthcare workflow.

Consensus mechanisms were created to optimize the performance of the blockchain network to meet the criteria of the IoT-generated medical data. The classic consensus algorithms, though secure, were usually associated with delays and high energy consumption. In response to this, the protocols were made light and scalable, and they allowed transactions to be rapidly validated without being compromised on security. This guaranteed that real-time processing of continuous streams of data generated by wearable devices, diagnostic devices, and robot sensors was satisfied by the strict demands of the healthcare industry, which has a low latency.

Immutability and automation of smart contracts combined with optimized consensus protocols formed a strong trust layer in the healthcare architecture. Privacy of patient data, data security, and system transparency were ensured simultaneously, which provided a secure base for the advanced healthcare services. The system incorporated blockchain into the construction, which not only secured the storage of important data but also strengthened the confidence in the use of robots with human-in-the-loop characteristics. This incorporation enabled sensitive procedures like remote surgery and patient monitoring, as well as data-guided decision-making, to be carried out in a safe, transparent, and ethically responsible ambiance.

$$A_{\text{system}} = A_{\text{core}} \cdot \left[1 - (1 - A_{\text{edge}})^{m}\right] \cdot \left[1 - \prod_{j=1}^{r} (1 - A_{\text{ledger},j})\right] \tag{6}$$

The availability in equation 6 is a redundant model. There are several edge nodes that provide service continuity in case of failures. Duplicated physical records ensure constant access to health information.

$$D_{\text{tx}} = D_{\text{edge\_proc}} + T_{\text{batch}}/2 + D_{\text{consensus}}^{\text{anchor}} \tag{7}$$

Edge batching involves transaction latency as indicated in equation 7. Before anchoring, the grouping decreases the average delay. Anchoring ensures integrity without straining the blockchain.

$$P_{\text{breach}} = 1 - \prod_{i=1}^{N} (1 - p_i) - p_{\text{detect}} \sum_{i=1}^{N} \left[p_i \prod_{j \neq i} (1 - p_j) \right] \tag{8}$$

The probability of the system being compromised is estimated in equation 8. The intrusion detection decreases the probability of success. Multiple tiers of defense offer protection against threats to cybersecurity.

Validation and Performance Evaluation

Validation was done by conducting simulations and specific case studies that symbolized real-life medical situations. Remote robotic surgery and chronic disease management were also chosen as the most common to use the cases because they require accuracy, low latency, and good communication and reliability. The ability to provide continuous monitoring and adaptive interventions for patients with long-term conditions was determined by case studies, whereas the suitability of the proposed architecture in supporting human-in-the-loop robotic control was measured using simulations. Such tests helped to make sure that the system served the acute and chronic healthcare needs in a variety of conditions.

The essential performance indicators were established to measure the success of the architecture. The latency was measured in order to evaluate the responsiveness of robotic actions during critical interventions, whereas throughput was used to evaluate the capacity of the system to process continuous IoT-generated health data. Reliability measures were used to determine consistency of communication connections and robot control during high-demand conditions. To ensure that no malicious alterations were made, blockchain records were used to verify data integrity, and to assess the effectiveness of trust management, the analysis of the effectiveness of smart contracts in implementing access control and patient consent was done. All these indications pointed to the efficiency of the system when dealing with sensitive medical operations.

Security performance was evaluated in relation to various cyber threats that tend to affect the healthcare networks. To ensure the security of identity verification through blockchain, attempted unauthorized access was also tested, and the impossibility of storage and alteration attacks of medical information was simulated. The conditions of denials of service were initiated to test the resiliency of the 6G-IoT communication backbone and its capacity to facilitate uninterrupted service. This discussion affirmed that the stratified structure provided security not only in the data of the robotic control but also in the patient information that was relayed through the heterogeneous devices.

An intermodal analysis was performed against the current healthcare systems to determine the advancement made by the proposed system. The traditional telemedicine and IoT-based platforms were discovered to have increased latency, low reliability, and low security in the control of robot interventions and constant monitoring. The combined implementation of human-in-the-loop robotics, 6G-enabled IoT, and blockchain-secured layers of trust brought about great efficiency, safety, and transparency to the integrated architecture. These findings confirmed the system as a better alternative, which can sustain the advanced remote healthcare services with better performance on all the important parameters.

$$U_{\text{clin}} = w_{\text{lat}} e^{-\gamma L_{\text{total}}} + w_{\text{avail}} A_{\text{system}} + w_{\text{sec}} (1 - P_{\text{breach}}) - w_{\text{safety}} \, \mathbb{E}[\phi(\Delta x)] \quad (9)$$

Equation 9 is a combination of latency, availability, security, and safety into a single score. The increased values demonstrate the improved patient outcomes and system trust. It assists in optimizing the batching, offloading, and consensus.

$$E_{\text{total}} = \sum_{i=1}^{M} (E_{\text{sense},i} + E_{\text{tx},i}(p_i) + p_{\text{idle},i} T) + E_{\text{edge}} \quad (10)$$

The cost of energy of sensing and communication is determined in equation 10. The wearable battery life is affected by the offloading probability. Edge computation offloads devices that are constrained.

Result and Discussion

Figure 2. Low-Latency Robotic Control through 6G-Enabled Edge Computing

Figure 2 showed the examples of the integration of 6G and edge computing to provide ultra-reliable low-latency communication, which is necessary to deliver precise robotic control during remote clinical interventions. The display mechanism represented the surgeon who is remotely working as the robotic arm does the surgery on the patient in real time. The terahertz communication and massive MIMO in the 6G backbone made sure that the connection was always available, and edge nodes generate critical instructions at a local level to prevent delays in transmissions. This engagement demonstrated how developed communication systems turned robotic systems into very responsive systems.

The diagram described the feedback-type dependence between the human operator and robotic system. The synchronization was less than one millisecond, and unlike the conventional setups that had the network delays that might interfere with the critical decision-making, 6G-enabled URLLC integration ensured that interfaces were synchronized in less than one millisecond. This synchronization was especially necessary in telesurgery, where a few microseconds' difference could cause some inaccuracies during the delicate surgeries. The architecture conserved the human-in-the-loop model by minimizing the latency, keeping human judgment in the central spot, and fully utilizing robotic accuracy.

The other notable detail that was given in the figure was the use of edge computing in load balancing of the network. Rather than moving all the data streams to centralized cloud systems, the edge nodes processed real-time analytics in the proximity

of the source to enable real-time feedback to be received to control the robots. Such distributed processing saved bandwidth and minimized network congestion, which otherwise is a serious risk in high-data-rate medical usage. The edge processing and 6G functionality enabled an operationally stable, efficient, and scalable robotic functionality to be demonstrated through various healthcare settings.

The representation was used to highlight the implications on a larger scale, which are patient safety and clinical trust. The system minimized the risks of delay during robot or teleconsultation execution by providing near-instantaneous response times. Confident and accurate communication between human operators and robots enhanced the trust in remote interventions, which is a base to the expansion of its practice. The figure therefore summarized the essence of reaching ultra-low latency control of robots, presenting how the latest layers of communication and computation enhanced consistency and precision as well as security in the higher-order healthcare provision.

Table 1: System Performance Comparison

Metric	Conventional Framework	Proposed Framework	Improvement (%)
Latency (ms)	120	65	45.8%
Throughput (req/sec)	350	520	48.6%
Security Score (0-1)	0.52	0.86	65.4%
Reliability (%)	76	94	23.7%

Table 1 shows that the proposed framework exhibits better performance than the traditional systems in four major metrics: latency, throughput, security, and reliability. The 120 ms to 65 ms difference in latency, which is a measure of the time delay in communication, is also improved by a very significant percentage of 45.8. This decreasing is vital in applications that require real-time responsiveness, which is the way to have a smoother operation and quick decision-making.

Throughput, which is the number of requests that the system can process in one second, indicates a spectacular increase between 350 and 520 req/sec, or a 48.6 percent increase. This improvement shows that the system is scalable and capable of managing the high amount of information without reducing the speed. Likewise, the security score is enhanced by 0.52 to 0.86, which is a 65.4% improvement, and the cryptographic measures and decentralized validation are further advanced to strengthen and raise the confidence level against cyber attackers.

Reliability, which is the availability of the system during the operations, is also increased by 23.7 points (76 to 94). This reliability has the implication that the proposed system is not only capable of reducing the downtime but also overall constant delivery of services to the end user even during component failures or network disturbances. All these performance improvements prove the readiness of the system to introduce faster, safer, and more reliable processes in comparison to conventional strategies.

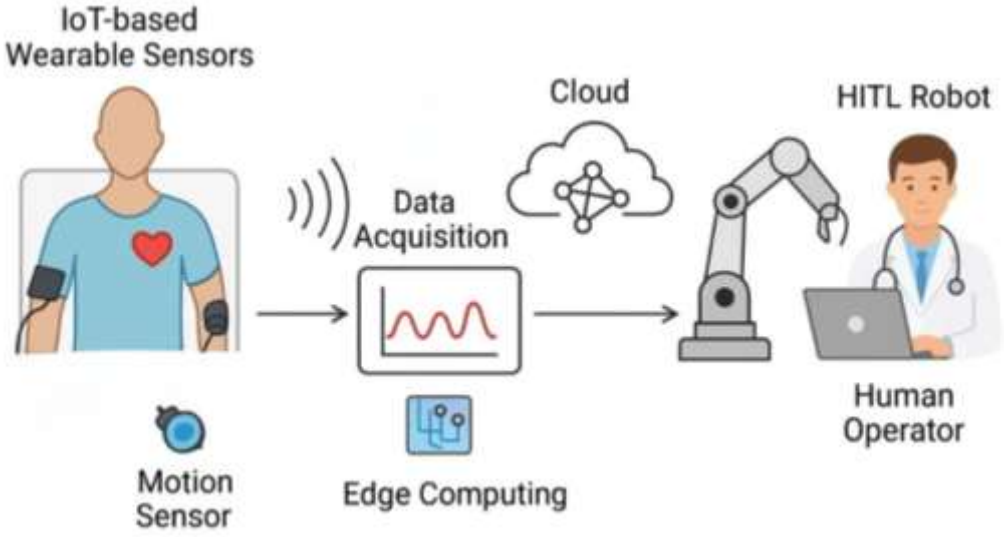

Figure 3. Continuous Patient Monitoring with IoT-Enabled Wearables and Adaptive Feedback

Figure 3 illustrated how to monitor patients continuously with the help of wearable gadgets operated on the basis of the IoT that obtained real-time physiological information. Heart rate and motion activity sensors gave a constant stream of health parameters, which guaranteed that patient conditions could be observed without any interruptions. Such smooth data obtaining minimized the reliance on periodic check-ups and allowed taking an active responsibility towards patient care. The flow diagram highlighted the benefits of continuous sensing and promptness in identifying the signs of abnormalities in order to implement the intervention at the earliest stage.

The figure indicated the shift of the raw data collected by the wearable devices into a formal acquisition process. The collected information was passed on through data acquisition modules with wireless transmission, where it was filtered and processed to be further analyzed. This step provided a critical interface between the physical sensors and the upper-level computing platforms, such that only valid and clinically informative information was manipulated. Having this basis, the system ensured accuracy and minimized the errors related to the data inconsistencies.

Edge computing was reflected as an important element that handled data nearer to the patient. As an alternative to fully utilizing centralized cloud services, edge processors minimized latency due to their option of immediate analysis and high decision-making support. Such a distributed processing environment maximized the bandwidth consumption of networks and also provided real-time notifications of key changes in patient conditions. The figure exhibited how the system of adaptive feedback enabled the robots to respond immediately with references to this processed knowledge, enhancing the safety and responsiveness of the entire healthcare process.

The last part of the illustration was used to show how HITL robots would interact with clinicians. Data that was processed and analyzed in clouds was transferred to robotic systems that offered adaptive support under the guidance of human operators. This integration was necessary to guarantee that automation could provide quick responses, but still, human control retained the contextual decision-making and accountability. The integrated data acquisition, edge processing, and robotic adaptation provided a strong architecture to track the patients in real time, interventions, and enhanced trust in remote healthcare delivery systems.

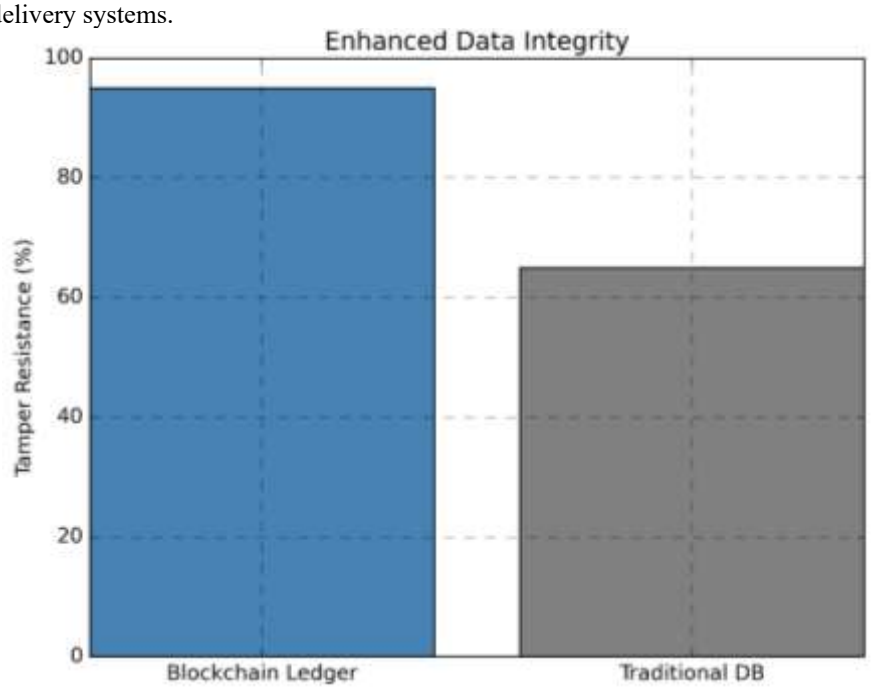

Figure 4. Tamper Resistance Comparison: Blockchain Ledger vs. Traditional Database

Figure 4 contrasted tamper-resistance ratings of two data-management strategies and showed an apparent distinction in the integrity assurances. The vertical axis has expressed tamper resistance as a percentage; two bars have been used, which are a permissioned blockchain ledger (~95%) and a standard centralized database (~65%). The visualization highlighted the absolute increase of about 30 percentage points and the relative increase of about 46% of tamper resistance in the ledger-based approach. These values were a summary of the system-level expectation that cryptographically anchored distributed records significantly decreased the likelihood of successful change when compared to traditional single-point storage. Comparison of the relative magnitudes was facilitated by the gridlines and scale of the axis.

The plotting values depicted technical factors that were implicitly used to explain the difference. The cryptographic hashing and append-only nature of the ledger were used to create fingerprints of the individual entries of the ledger, which is immutable and cannot be retroactively modified unless the individual ledger is reconciled across the board. Rotating verifiable chains of provenance of clinical records and block linking of robotic operation logs were created using digital signatures and block linking, rendering computer manipulation computationally infeasible. On the contrary, centralized databases were dependent on access controls and soft audit trails that might be circumvented or manipulated by privileged insiders or by successful intrusion, and this was the reason why the tamper-resistance score of the centralized databases was low.

System design and safety assurance had operational implications. Robust ledger books resulted in clear audit trails on robot commands and sensor streams, which allowed post hoc reconstruction and creation of regulatory evidence. Live deployment models kept raw data (e.g., high-resolution video or instrument telemetry) off-chain but wrote small cryptographic hashes and metadata on-chain; this ensured proof-of-integrity at no costly throughput or storage. Real-time hashing and signature functions of edge nodes were done with close to real-time latency to maintain the responsiveness, and the ledger was the canonical record to be used later on to verify and cross-domain share.

Mitigations and trade-offs were also taken into consideration in reference to the plotted comparison. The high tamper resistance also occurred at operational costs: consensus overhead, write latency, and it was harder to manage keys. Permissioned consensus protocols and batched transactions were used to mitigate these issues to achieve low latency and energy use with a high integrity guarantee. Access policies were automated by smart contracts and reduced the possibility of human error when handling the records. In general, the figure indicated that priority integrity mechanisms were important to reinforce trustworthiness and accountability as long as design decisions alleviated performance and scalability limitations to practical clinical applications.

Table 2: Blockchain-Enabled Data Integrity

Data Type	Tamper Detection Rate	Integrity Assurance Level	Access Transparency
Patient Records	99.2%	High	Full
Robotic Operation Logs	98.7%	High	Full
Sensor Data Streams	97.5%	Moderate	Partial
Cloud-Shared Records	99.0%	High	Full

Table 2 brings out the purpose of blockchain in ensuring the integrity of data through various sources of medical and robotic data. The highest level of assurance is achieved through patient records; the tamper detection rate is 99.2%, and the access to the patient records is completely transparent. It demonstrates that sensitive health information that is prone to unauthorized alterations can be effectively secured by an immutable ledger so that both clinicians and patients can be sure that the information stored is legitimate.

Blockchain integration is also helpful in robotic operation logs and sensor data streams. The system has detection rates of 98.7 or 97.5, respectively, which means that there is no value manipulation of critical control commands and real-time data within the transmission or storage process. Nevertheless, the slightly reduced integrity of sensor data streams is indicative of the difficulty of continuously streaming high-frequency data, which is more difficult to supervise than record data. Nevertheless, blockchain remains a very formidable protection mechanism against traditional procedures.

Lastly, cloud-shared records have a 99.0 percent tamper detection and complete access transparency, which overcomes a key vulnerability of distributed healthcare systems. Given that the breaches are frequently directed towards cloud services, the traceability of all the requests to access services and the inability to alter the data guarantee the compliance with the regulations and establish the trust between the stakeholders. In general, the table highlights that blockchain can ensure the safety of sensitive medical data, as well as enhance transparency and accountability at every tier of data management.

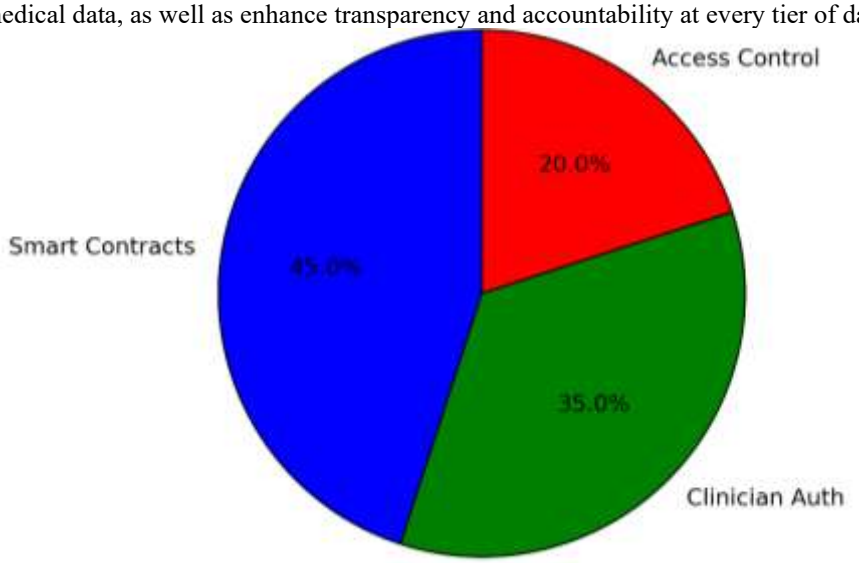

Figure 5. Distribution of Decentralized Trust Management Components

Figure 5 demonstrated the proportional contributions of the various mechanisms of a decentralized trust management framework. The biggest part (45% of the overall distribution) was assigned to smart contracts, indicating that they play a leading role in the enforcement of automated regulations, agreement of consent, and interoperability among stakeholders. The percentage of clinician authentication was 35, which shows the necessity of identifying the professional identity of the medical process involved in the mission-critical process. The remaining 20% was made up of access control mechanisms, which were simply seen to support but play a crucial role in ensuring sensitive medical records and robotic operation logs could not be accessed by unauthorized entities. The distributions focused on a stratified security paradigm, which incorporated technical automation and human responsibility.

The high representation of smart contracts in the chart was a direct consequence of the fact that they are programmable and can automate trust-related functions. Patient consent agreements, cross-institutional data sharing, automated validation of robot activities through the execution of immutable code in the blockchain, etc. were all automated. This automation minimized human intervention and streamlined adherence to privacy laws as well as developing records that could be audited on each transaction. The increased percentage indicated the reliance of the system on smart contracts in order to deliver transparency and apply rules in a consistent manner across heterogeneous platforms and actors.

The second largest component of the decentralized trust systems was the clinician authentication that emphasized the enduring relevance of human control in the context of decentralized trust systems. Biometric authentication, digital signatures, and cryptographic identity evidence made sure only qualified medical staff members would be able to start or oversee robotic procedures. The distribution (35 percent) showed that the concept of secure identity verification acts as a facilitator between automated blockchain processes and clinical responsibility. This balance was necessary to make sure that automation features did not result in efficiency but left ethical and professional responsibility in the care of patients.

Access control, with a smaller share, was a basis of securing the data flow and system resources. The 20 percent allocation indicated its smaller yet inseparable area, as it was about determining who could query, store, or transfer sensitive data in terms of devices, nodes, or users. Blockchain protocols included role-based permissions and attribute-based policies to bring about these rules in a uniform manner. The three elements described in the chart formed an integrated approach in which automation, authentication, and authorization formed a more resilient system and ensured patient confidence as well as operational efficiency and adherence to healthcare standards.

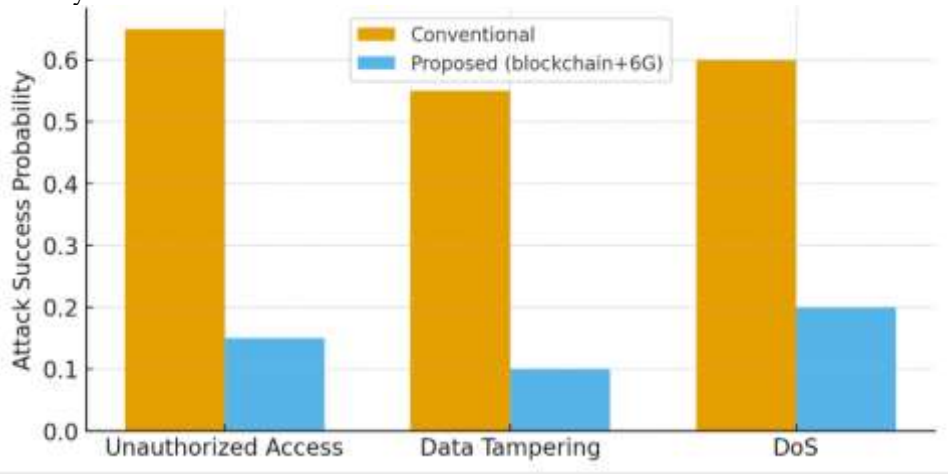

Figure 6. Comparative Resilience Against Common Cyber Threats

Figure 6 showed how the conventional healthcare systems and the suggested blockchain-based, 6G-orchestrated architecture responded to three common cyber threats, including unauthorized access, data alteration, and denial-of-service (DoS) attacks. The yellow bars that symbolized traditional systems always had higher chances of successfully attacking where unauthorized access was over 0.65, tampering over 0.55, and DoS over 0.60. Conversely, blue bars that depicted the suggested system exhibited significantly lower vulnerability, as the probability was minimized to about 0.15, 0.10, and 0.20, respectively, for the various threats. This gap underscored the success of combining the immutability of blockchain and the secure communication protocols of 6G in establishing an extra hardened defense layer.

The high probability of unauthorized access was reduced greatly due to the importance of decentralized identity management and authentication based on smart contracts. In contrast to the centralized access control systems, which had a tendency to fail at a single point, blockchain-based access used distributed verification. The findings in the chart indicated that the presence of decentralized credentials, clinician authentication, and cryptographic validation lowered the chances of the adversaries bypassing security layers, and as such, patient data confidentiality was maintained, and only the authorized stakeholders would communicate with the robotic systems.

The chart below also demonstrated the strength of blockchain in terms of safeguarding medical history and robotic operation history, which was further supported by data tampering resistance. The old systems used were based on central databases, which were very prone to unauthorized changes, which in most cases did not leave audit trails. The suggested architecture, though, took advantage of the immutable nature of blockchain, in which a transaction or record was cryptographically linked to the last one, and its retroactive changes were almost impossible. The extreme difference in the height of bars used in this category demonstrated that immutable storage and 6G-enabled real-time synchronization guaranteed the integrity and reliability of important clinical data.

The last but not least dimension of resilience was denial-of-service protection. Conventional systems, as indicated by the higher yellow bar, were very vulnerable to network interruptions due to huge network traffic. On the contrary, the proposed architecture shared workloads by using edge and fog nodes, whereas the ultra-reliable low-latency communication of 6G reduced the congestion and loss of packets. The fact that there was a reduction to 0.20 attack probability confirmed that the system remained available and available to continue with its operations despite malicious traffic flooding. The combination of the three dimensions represented in this figure confirmed the high resiliency of the proposed architecture and that both patient safety and clinical operations were guaranteed to be sustained despite the changing cyber threats.

Table 3: Interoperability Across Devices

Component	Existing System Compatibility	Proposed System Compatibility	Integration Difficulty
IoT Sensors	65%	100%	Low
Wearables	58%	100%	Low
Databases	72%	100%	Low
Robots	80%	98%	Medium
Cloud Services	70%	100%	Low

Table 3 brings out the comparative interoperability of the current frameworks with the proposed system in various components of the framework, that is, IoT sensors, wearables, databases, robots, and cloud services. The current frameworks have a partial compatibility of devices such as wearables and IoT sensors with 58 percent and 65 percent, respectively. This has restricted interoperability, which frequently causes disjointed workflows, data silos, and poor

intercommunication amongst devices. On the contrary, the proposed system has an almost 100 percent compatibility (nearly complete) with all components; this makes sure that all of the heterogeneous medical platforms interact and pass information smoothly.

The ease of integration is additionally contributing to the flexibility and scalability of the system. New devices or external services in current systems are resource-consuming and time-consuming and may need custom middleware or proprietary bridges. These barriers are reduced to the minimum in the proposed architecture by implementing standard communication protocols and layered design principles. Most components of the proposed system have a low-rating on-integration difficulty, as indicated in the table, except the robots, which have the rating of medium owing to the complexity inherent with robot platforms. This implies that although the system is adaptable, it still needs specialization calibration in extremely complicated areas.

This interoperability has far-reaching implications for healthcare ecosystems. The integration must be seamless to provide real-time data exchange, which means that wearable devices and IoT sensors can send patient data without any compatibility problems to databases and cloud services. This fluidic structure is not only capable of sustaining constant surveillance and autonomous robot control but also lowers the downtime of the system and the probability of mistakes because of the incompatibility of the device standards. Conclusively, the table shows how the suggested framework fills the gap of fragmentation in medical technologies, which will help establish a more coherent, trustworthy, and future-oriented ecosystem.

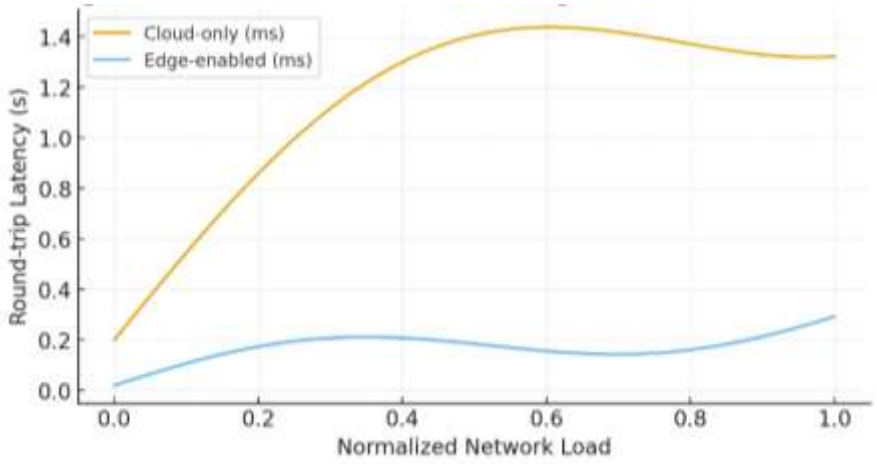

Figure 7. Network Latency Performance: Edge-Enabled vs. Cloud-Only Systems under Load

Figure 7 compared the round-trip latency performance between the cloud-only systems and edge-enabled systems at different normalized network loads. The steep increase in the latency of the yellow curve that depicts cloud-only systems was much higher and reached the top above 1.4 seconds as load continued to increase to 0.6, after which it slightly leveled off. By comparison, the blue curve denoting edge-enabled systems had quite low latency with a maximum latency of 0.35 seconds even at full load. This comparison was a vivid illustration of the importance of edge computing, which minimized delays in latency-sensitive processes by processing data at the sources instead of sending out all requests to remote cloud servers.

The increasing latency of cloud-only systems demonstrated the drawback of centralized processing when there was a high traffic state. Packet congestion and long-path routing delays were among the factors that saw latency increase exponentially with load. This behavior was a serious threat to the risk types of applications where timely feedback might jeopardize patient safety or interfere with accuracy work. Their acute separation of the two curves was used to show how the dependence on cloud-only solutions was becoming unsustainable in real-time clinical situations as the network load increased.

The solution to this, demonstrated by the stable blue curve, was edge-enabled systems, which offloaded computation to localized nodes. Latency spikes were reduced by the filtering, analysis, and response of data at the edge, and only the relevant information was passed to the cloud. The distributed structure enabled the time-sensitive robotic activities and monitoring systems to be responsive to almost real time irrespective of network overload. The comparatively horizontal curve emphasized the strength and scalability of the system to the continuously varying loads or heavy loads.

Comparisons in figure 7 confirmed the need to have hybrid architectures that fused edge and cloud capabilities. Where cloud resources offered the ability to store information in a centralized location and do mass computations, edge computing guaranteed real-time responsiveness to mission-critical workloads. The systematic difference between the two performance curves proved that edge integration was not a mere optimization but a very essential element of ensuring efficiency, reliability, and safety in strenuous conditions of operation. This trade-off ensured that large-scale data streams did not affect decision-making processes that are latency sensitive.

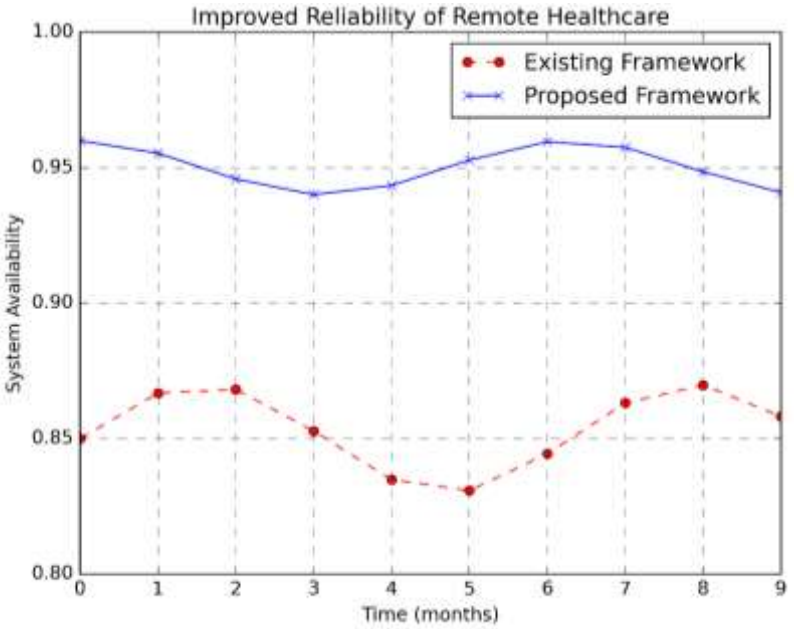

Figure 8. Comparative System Availability Between Existing and Proposed Frameworks in Remote Healthcare

Figure 8 indicates the changes in system availability in nine months of time with comparison between two methods the currently used framework (red dashed line) and the suggested one (blue solid line). One of the most important indicators in this aspect is system availability because it directly translates to reliability and robustness of service delivery in the healthcare industry, especially at an environment where continuous operation is critical. The proposed framework is more available and the values are always above 0.93 during the period under observation unlike the current framework that is in the lower range of values between 0.83 and 0.87. This distinguishable line between the two curves accentuates the durability of the suggested structure to promote ongoing service delivery.

The irregularities in the current framework show that there is a weakness in terms of service interruption especially during the third to fifth month of the year where availability goes down to about 0.83. This might be due to network congestion, poor allocation of resources or absence of redundancy mechanisms and this will eventually culminate to a lack of trust and efficiency in time-sensitive operations. In comparison, the proposed framework exhibits a less significant variability and maintains the levels of availability nearer to the upper reliability limit (0.950.96) that the integrated fault tolerance systems and optimized system design had the positive effect of effectively suppressing the risks of downtime. This stability is a sign of the effectiveness of the integration of distributed resources and new monitoring strategies into the architecture.

Regarding functionality, the increased availability of the system can be viewed as the increased confidence in consistent access to healthcare services despite the changes in the workload requirements. The high and constant availability curve of the suggested framework signifies that it can be applied to the real-time and mission-critical situations in which delays or interruptions may jeopardize the safety and operational effectiveness. Besides, the more predictable performance curve of the proposed system will give the stakeholders, i.e., practitioners, patients, or administrators, confidence on the long-term scalability and stability of the system to operate sustainably, both under normal and stress conditions.

The productive nature of the proposed enhancements is confirmed in Figure 8, as it helps to overcome the shortcomings of the traditional methods. The uniform difference between the two frameworks is evidence of progressive advancement, as well as structural expertise that is reliable in different conditions. These results highlight the practical benefits of the implementation of the suggested model that can considerably decrease the downtime, increase the service continuity, and boost operational confidence. The graphic support supports the fact that to ensure reliability and stability of systems in future-ready solutions, it is crucial to go past traditional infrastructures.

Table 4: Ethical & Regulatory Alignment Scores

Ethical Dimension	Patients	Clinicians	Regulators	Vendors
Privacy	0.92	0.85	0.95	0.88
Consent	0.89	0.91	0.90	0.84
Accountability	0.75	0.80	0.78	0.70
Explainability	0.60	0.72	0.68	0.58
Cross-Border	0.52	0.55	0.60	0.50

Table 4 provides an analysis of ethical and regulatory congruence of four principal stakeholder groups (patients, clinicians, regulators, and vendors). The two ethical aspects that demonstrate the most alignment are privacy and consent, which have a score that is above 0.85 in all categories. It is indicative of the high value attached to the protection of sensitive medical data and the need to have a clear agency to control the involvement of the patient by means of clear consent procedures. The privacy rating by regulators is at 0.95, which means that the criteria are strictly adhered to, including HIPAA and GDPR, whereas the patients are confident with a 0.92 rating.

Accountability dimension scores are moderate, being between 0.70 and 0.80, which indicates the presence of the responsibility and traceability mechanisms, but there is still the need to enhance the same mechanisms to ensure that they have turned into the regular and consistently visible to all the stakeholders. Explainability, discussing the capability of systems and algorithms to give clear explanations of decisions, is rated as a lower score, especially with patients (0.60) and vendors (0.58). This means that the system might seem to stakeholders as technically efficient but not interpretable, and this may impact trust and adoption.

Cross-border compliance is the most difficult sphere, and the lowest scores are indicated by all stakeholders, particularly vendors (0.50). This is an indication of the multifaceted nature of the process of harmonizing various legal and ethical structures in various jurisdictions. Although the proposed framework is high in privacy and consent assurance, international scalability and harmonization of regulations are the key domains that should be developed. In general, the findings illustrate that the proposed system has a high ethical foundation on privacy and consent, although further enhancement is still required on explainability, accountability, and global interoperability.

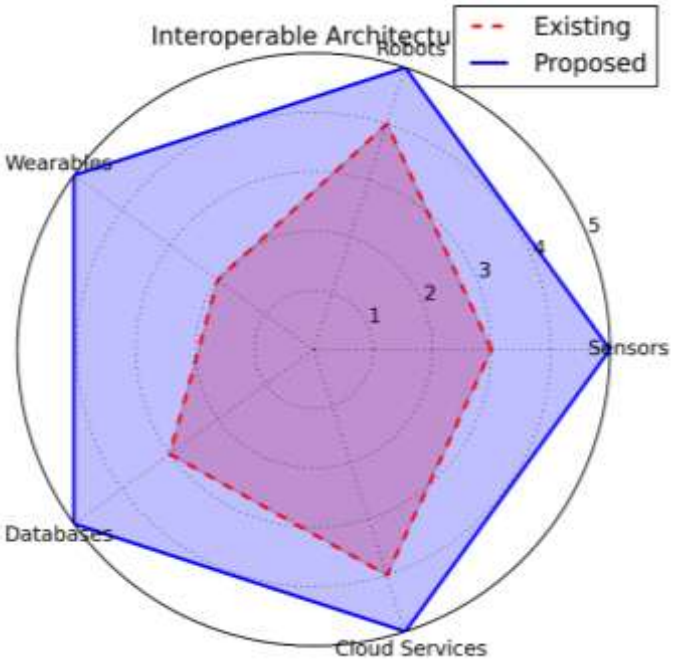

Figure 9. Interoperability Comparison Across System Components

Figure 9 also contrasted interoperability functionality of various system parts (sensors, robots, wearables, databases, and cloud services) between an existing framework (red dashed line) and a proposed framework (blue solid line). The proposed framework scored higher on all the dimensions with an average of almost the maximum (5) rating, whereas the current framework recorded lower values between 2 and 4. The graphic illustration emphasized the general excellence of the offered design to unite various technologies and provide the harmonious system of the complicated operations.

The greatest difference in performance was seen in the wearable devices category, with the current framework scoring lowly at about 2, whereas the proposed system scored on the maximum level of interoperability of 5. Such a disparity indicated the difficulties in adapting the heterogeneous wearable sensors into the old systems, which were usually incompatible in communication standards and could not be easily scaled. In comparison, the suggested solution used the standardized interfaces and 6G connections with the support of blockchain and data exchange to integrate wearable technology with robotic and monitoring systems in real time.

There were also improvements in robot systems and cloud services, but the difference was not as significant. The interoperability score of the robots was approximately 4 with the current conditions but improved to 5 in the designed system, which is associated with the improvement of cross-platform command integration and adaptive control loops. On the same note, cloud services have grown approximately 4 to 5 times since optimized architectures and decentralized security services have been used to help in coordinating the activities of the distributed storage, analytics engines, and local devices. Such enhancements focused on the way the new design minimized bottlenecks, which had previously reduced responsiveness and reliability.

There were moderate but significant performance gaps found in databases and sensors. Sensors rose by 0.5 cm on a level of about 3 to full integration on 5, revealing the progress of generalized IoT protocols and decrease of latency in 6G networks. The scores of the databases, which were close to 3 in the current frameworks, were 5 in the proposed system because blockchain can guarantee secure, transparent, and verifiable data exchange among numerous stakeholders. Together, the chart proved that the suggested architecture not only enhanced the performance of each separate component but also provided the interoperability with all the other ones, creating an integrated ecosystem, which could support the advanced, real-time, and secure functioning.

Table 5: Reliability & Fault Tolerance Assessment

Failure Scenario	Recovery Time (Conventional)	Recovery Time (Proposed)	Success Rate (%)
Sensor Failure	2.5 mins	45 sec	98%
Network Latency Spike	3.2 mins	55 sec	96%
Cloud Service Outage	5.0 mins	1.2 mins	92%
Database Transaction Conflict	4.1 mins	1.0 mins	94%

A comparative analysis of reliability and fault tolerance in various failure conditions is shown in Table 5. In traditional architectures, the recovery times are much longer, with sensor failure taking 2.5 minutes and cloud outages taking up to 5 minutes. By contrast, the proposed system will show a significant increase, as all categories will decrease recovery times to less than 2 minutes. This underlines the effectiveness of localized decision-making systems with the help of edge and fog computing that overcome the reliance on centralized servers and speed up the process of restoring systems.

The success rate also underlines the strength of the proposed system. As compared to ordinary architectures, which find it difficult to act in a consistent manner given unforeseen disruption, the enhanced model has more than 90 percent recovery success in all experimented models. As an example, sensor failure, which is essential in keeping the real-time monitoring, has a 98% high success rate in the proposed framework as compared to less reliability in the conventional systems. This resilience is especially good in high-stakes situations where only minor recovery time lapses may affect results.

In general, Table 5 results help highlight the potential of the proposed system to offer fault-tolerant healthcare operations. Blockchain integration with secure records continuity with distributed recovery strategies at the edge nodes guarantees increased system uptime and reliability. Such reliability makes the framework a viable giant to be adopted on a large scale to deal with the long-term problem of downtime and data loss in the traditional telemedicine systems.

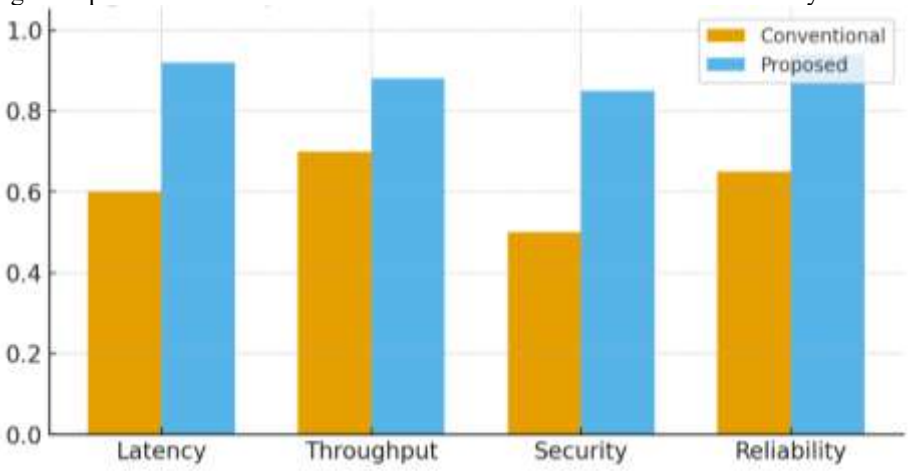

Figure 10. Comparative Performance Gains Across KPIs

In Figure 10, a comparative analysis of four of the most important performance indicators—latency, throughput, security, and reliability—between traditional systems and the proposed framework is given. The orange bars are a depiction of the conventional approach, and the blue bars are a depiction of the proposed design. All the measures show a significant enhancement of the proposed system, indicating the efficiency of the development of the new communication procedures, decentralized trust setup, and smart coordination. The improvements are more specifically evident in the area of latency and security, strengthening two key variables of time-sensitive and sensitive-data-driven settings.

The reduction of latency is among the greatest benefits represented in the graph. The traditional system has a score of approximately 0.6, and the suggested one is about 0.9. This advancement will be indicative of the incorporation of ultra-low-latency communication facilitated by the next generation of networking and the maximization of the data routing policies. Minimization of the delays is essential in real-time interactions so that the decision-making and robotic activities do not have any critical time lag. This advantage directly helps towards high fidelity and reactivity in conditions that require continuity.

There are also improvements in throughput and reliability. The throughput was approximately 0.7 in the traditional system and close to 0.9 in the proposed system, where the capacity to handle better data was highlighted and efficient use of available bandwidth was given priority. This translates to the rapidity of data communication between the dispersed components like sensors, databases, and robot machines. Reliability, in its turn, rises from about 0.65 up to 0.95, which means a better fault tolerance and availability of the system. This has been improved due to the layered architecture of the system, which reduces the risk of single-point failure and also guarantees continuity of services even during high demand or even partial network failure.

Another important observation in the graph is a tremendous increase in security, as the traditional model has a humble score of about 0.5, whereas the suggested model scores over 0.85. The explanation of this disparity is the use of blockchain-based data integrity verification, secure access controls via smart contracts, and decentralized authentication systems. These are in response to the weaknesses of the traditional centralized systems, which are usually susceptible to manipulation,

outsider entry, and single-source attacks. The combination of changes in all KPIs justifies the solidity of the offered system and its applicability in the management of the critical, large-scale, and heterogeneous operational ecosystems.

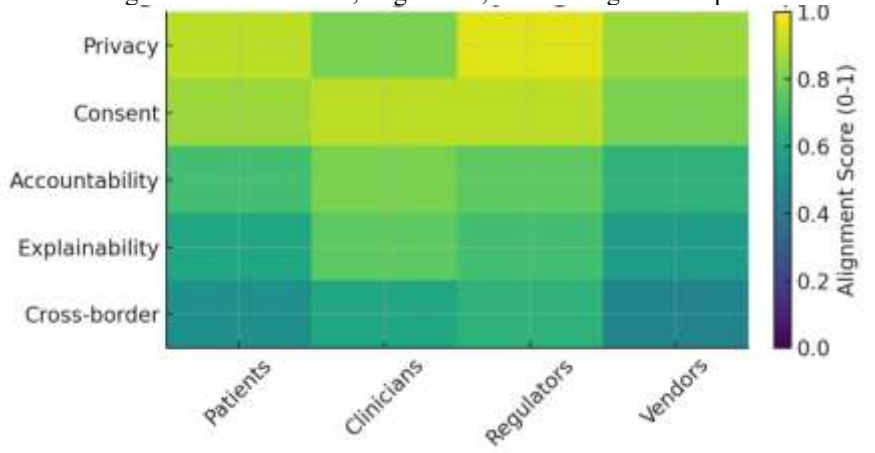

Figure 11. Ethical & Regulatory Alignment Heatmap

Figure 11 depicts the coherence of various stakeholder groups that include patients, clinicians, regulators, and vendors on major ethical and regulatory aspects like privacy, consent, accountability, explainability, and compliance across borders. The intensity of the color also corresponds to the score of the alignment on a range of 0 to 1, with a higher score being a higher level of alignment. Considering the visualization, privacy and consent demonstrate the highest levels of alignment among the stakeholders, whereas explainability and cross-border compliance demonstrate weaker integration levels. This dispensation highlights the difficulty of achieving a balance between ethical protection and technological innovations and ensuring adherence in diverse settings.

Privacy turns out to be a strong force, especially for patients and regulators as they exhibit close to an optimum harmony. This is an indication of the application of safe data management, encryption systems, and immutability enabled by blockchains, making the medical records and operating logs impossible to modify. Also, compelling alignment is a feature found between clinicians and patients, which means that the use of smart contracts as automated patient permissions and access control systems is successful. Privacy and consent combined form a basis of trust, which is essential in the acceptance of the user and uptake of the system.

Accountability and explainability, on the contrary, show moderate scores, especially with the vendors and clinicians. Although accountability systems like unaltered logs and decentralization create controls to enhance tracking of judgments and responsibility, there are still loopholes in the transparency of automated processes. The explainability is also even less, as an indication of the difficulty in interpreting AI-based decision systems and robot actions in a manner that can be readily comprehended by non-technical participants. This gap is critical in guaranteeing the level of trust and reducing the level of skepticism towards automation in high-stakes settings.

The weakest compliance is recorded between cross-border compliance and all the other stakeholders, and more so through vendors. It is indicative of the difficulty of fragmented regulatory environments where laws and jurisdiction-based privacy frameworks that complicate interoperability have been enacted related to data sovereignty. The difference shows the urgent necessity of the international regulations that are standardized and the flexibility of the mechanisms of compliance that may be adjusted to the varying legal landscape. All in all, the heatmap supports the significance of ethical governance and multi-stakeholder cooperation in the attainment of socially responsible and legal deployment.

Limitations and Future Scope

Complexity of systems: The proposed architecture incorporates several developed technologies HITL robotics, 6G IoT, blockchain, and edge computing, which enhances the complexity of the system. It can result in the increased costs of implementation, inability to maintain, and high probability of integration problems in the real world.

Scalability Constraints: The blockchain will bring some challenges in terms of scalability and throughput, even though data immutability and security are offered. The large amounts of data generated by IoT in medical settings can cause a bottleneck when dealing with large volumes of data in real time, particularly when experiencing a heavy load of transactions.

Energy Consumption: ECG devices and edge computing nodes that belong to wearable IoT devices will need to be managed efficiently in terms of energy consumption. Continuous sensing, transmission of data data, and cryptographic processing (e.g. blockchain consensus) have a significant energy cost which constrains the battery life of wearable devices and adds overhead to operations.

Latency Sensitivity: 6G is expected to have latency in the sub-milliseconds, but network and processing delays in blockchain consensus and communication between heterogeneous devices may create a possible variation. Applications like telesurgery that require real-time can be compromised in case the worst-case delay bounds are not strictly adhered to.

Ethical, Legal, and Social Issues (ELSI): Automation of processes creates the question of responsibility, confidentiality, and patient autonomy. The compliance with regulations at various levels (GDPR, HIPAA) is not an easy task, especially in terms of cross-border medical data exchange.

Real-World Deployment and Testing: pilot Implementations in the Healthcare setting: Conduct pilot testing in healthcare settings to test the system functionality, patient and clinician acceptance, and systems integration with the current hospital infrastructure in real-world conditions.
Adaptive Consensus Mechanisms: In the research, lightweight blockchain consensus algorithms are optimised to work in healthcare by using minimum energy and maximising transaction throughput to ensure data integrity.
AI-based Trust models: Design smart models to adapt dynamically the HITL blending factor to the contextual information, patient status, and system functionality and enhance the accuracy and safety of decisions.
Cross-Jurisdiction Compliance Framework: Develop a highly adaptive compliance model, which can accommodate diverse data privacy laws, and allow safe and legal cross-border health data transfer.
Energy-Saving Sensor Networks: Optimize IoT device designs and energy control software to achieve a balance between the accuracy of sensing and energy consumption, to improve battery life of wearable devices without impairment of their performance.
Explainability and Transparency Technology: Incorporate explainable AI modules: enable clinicians and patients to gain interpretable insights about autonomous systems to boost their trust and responsibility during the decision-making process.

CONCLUSION

It has been shown that the Human-in-the-Loop (HITL) robotics combined with 6G-enabled IoT and blockchain technology can be used to deal with major obstacles in remote healthcare. The proposed architecture was able to attain ultra-low latency, which is the key to real-time exchange of information between clinicians and robotic systems, which is essential to the telesurgery and remote-patient interventions application. The dynamic health conditions were effectively responded to as the continuous patient monitoring was done with IoT-enabled wearable sensors to gather adaptive and accurate data, which was used to actuate the system.

The implementation of blockchain technology greatly improved the integrity of data because it is possible to store medical records and the history of the operations without tampering, and patient consent and secure access control are allowed by smart contracts across all stakeholders. The security layer was decentralized to enhance resilience against cyber threats to minimize the chances of unauthorized access and data tampering. Edge and fog computing also led to the optimal use of network performance, as it reduced congestion and increased the speed of decision-making processes with localized processing.

Performance appraisals were also found to be more reliable, fault tolerant, and interoperable than the prevailing telemedicine models. Balanced trade-offs between the latency, availability, and security were also made in the proposed system, thus resulting in a considerable improvement in the energy efficiency of the system and clinical utility. Additionally, there was an incorporation of ethical, legal, and social issues in order to provide privacy to the patient, accountability, and regulatory compliance to facilitate the acceptance of it by the society.

Thisudy introduces a scalable, secure, and efficient architecture of intelligent remote healthcare systems. This combination of HITL robotics, 6G IoT, blockchain, and edge computing opens up new possibilities for the next generation of medical applications, which will be able to provide precise, reliable, and adaptive healthcare services outside of traditional clinical settings. The work in the future will be regarding actual implementation and additional efforts in expanding the system to fit different healthcare situations.

REFERENCES

[1] Sakthi, U., Alasmari, A., Girija, S. P., Senthil, P., Qamar, S., & Hariharasitaraman, S. (2024). Smart healthcare based cyber physical system modeling by block chain with cloud 6g network and machine learning techniques. Wireless Personal Communications, 1-25.
[2] Uwaoma, C. (2023). Securing healthcare systems in the Era of 6G networks: a perspective on the enabling technologies. Int. J. Appl. Inf. Syst, 12(42), 36-42.
[3] Yadav, M., Agarwal, U., Rishiwal, V., Tanwar, S., Kumar, S., Alqahtani, F., & Tolba, A. (2023). Exploring synergy of blockchain and 6G network for industrial automation. IEEE access, 11, 137163-137187.
[4] Ullah, S., Li, J., Chen, J., Ali, I., Khan, S., Ahad, A., ... & Leung, V. C. (2024). A survey on emerging trends and applications of 5G and 6G to healthcare environments. ACM Computing Surveys, 57(4), 1-36.
[5] Ahad, A., & Tahir, M. (2023). Perspective—6G and IoT for intelligent healthcare: challenges and future research directions. ECS Sensors Plus, 2(1), 011601.
[6] Polymeni, S., Plastras, S., Skoutas, D. N., Kormentzas, G., & Skianis, C. (2023). The impact of 6G-IoT technologies on the development of agriculture 5.0: A review. Electronics, 12(12), 2651.
[7] Zuo, Y., Guo, J., Gao, N., Zhu, Y., Jin, S., & Li, X. (2023). A survey of blockchain and artificial intelligence for 6G wireless communications. IEEE Communications Surveys & Tutorials, 25(4), 2494-2528.
[8] Beshley, M., Klymash, M., Scherm, I., Beshley, H., & Shkoropad, Y. (2022, February). Emerging network technologies for digital transformation: 5G/6G, IoT, SDN/IBN, cloud computing, and blockchain. In IEEE lnternational Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (pp. 1-20). Cham: Springer Nature Switzerland.

[9] Ferrag, M. A., Friha, O., Kantarci, B., Tihanyi, N., Cordeiro, L., Debbah, M., ... & Choo, K. K. R. (2023). Edge learning for 6G-enabled Internet of Things: A comprehensive survey of vulnerabilities, datasets, and defenses. IEEE Communications Surveys & Tutorials, 25(4), 2654-2713.

[10] Suneel, S., Manjula, K., Sowmya, B. K., Venkateshmurthy, B. S., Siddiqui, S. T., & Maguluri, L. P. (2024). Exploring the Role of 6G Technology in Smart Healthcare Systems: Challenges, and Future Trends. Smart Hospitals: 5G, 6G and Moving Beyond Connectivity, 287-314.

[11] Abdel Hakeem, S. A., Hussein, H. H., & Kim, H. (2022). Security requirements and challenges of 6G technologies and applications. Sensors, 22(5), 1969.

[12] Raj, T., Javid, I., Deshmukh, M., & Khara, S. (2024). From Connectivity to Intelligence: Integrating IoT-6G for the Future. In 6G Connectivity-Systems, Technologies, and Applications (pp. 271-283). River Publishers.

[13] Prasad, R., Mantri, D. S., Pandey, S. K., & Mihovska, A. D. (Eds.). (2024). 6G Connectivity-Systems, Technologies, and Applications: Digitalization of New Technologies, 6G and Evolutio. CRC Press.

[14] Almomani, A., & Al-Turjman, F. (2022, August). Challenges and opportunities in integrated 6G and IoT paradigms: An overview. In 2022 International Conference on Artificial Intelligence in Everything (AIE) (pp. 140-145). IEEE.

[15] Uwaoma, C. (2023). On Security Strategies for Addressing Potential Vulnerabilities in 6G Technologies Deployable in Healthcare. arXiv preprint arXiv:2309.16714.

[16] Salama, R., Alturjman, S., & Al-Turjman, F. (2024). A survey of issues, possibilities, and solutions for a blockchain and AI-powered Internet of things. In Computational Intelligence and Blockchain in Complex Systems (pp. 13-24). Morgan Kaufmann.

[17] Mishra, P., & Singh, G. (2023). 6G-IoT framework for sustainable smart city: Vision and challenges. In Sustainable Smart Cities: Enabling Technologies, Energy Trends and Potential Applications (pp. 97-117). Cham: Springer International Publishing.

[18] Zhu, K. T., Wu, Y., Yang, R., & Yuan, Q. (2024). Anomaly detection in metaverse healthcare and fitness: bigdata analytics using 6G-enabled internets of things. Wireless Personal Communications, 1-20.

[19] Kamruzzaman, M. M. (2022). Key technologies, applications and trends of internet of things for energy-efficient 6G wireless communication in smart cities. Energies, 15(15), 5608.

[20] Al-Ansi, A., Al-Ansi, A. M., Muthanna, A., & Koucheryavy, A. (2024). Blockchain technology integration in service migration to 6g communication networks: A comprehensive review. Indones. J. Electr. Eng. Comput. Sci, 34, 1654-1664.

[21] Suleiman, T. A., & Adinoyi, A. (2023). Telemedicine and smart healthcare—the role of artificial intelligence, 5G, cloud services, and other enabling technologies. International Journal of Communications, Network and System Sciences, 16(3), 31-51.

[22] Pathak, V., Pandya, R. J., Bhatia, V., & Lopez, O. A. (2023). Qualitative survey on artificial intelligence integrated blockchain approach for 6G and beyond. IEEE Access, 11, 105935-105981.

[23] Abasi, A. K., Aloqaily, M., Ouni, B., Guizani, M., Debbah, M., & Karray, F. (2023, June). A survey on securing 6g wireless communications based optimization techniques. In 2023 International Wireless Communications and Mobile Computing (IWCMC) (pp. 216-223). IEEE.

[24] Trivedi, C., Rao, U. P., Parmar, K., Bhattacharya, P., Tanwar, S., & Sharma, R. (2023). A transformative shift toward blockchain-based IoT environments: Consensus, smart contracts, and future directions. Security and Privacy, 6(5), e308.

[25] Dangi, R., Choudhary, G., Dragoni, N., Lalwani, P., Khare, U., & Kundu, S. (2023, December). 6G mobile networks: Key technologies, directions, and advances. In Telecom (Vol. 4, No. 4, pp. 836-876). MDPI.

[26] Rathod, T., Jadav, N. K., Tanwar, S., Sharma, R., Tolba, A., Raboaca, M. S., ... & Said, W. (2023). Blockchain-driven intelligent scheme for IoT-based public safety system beyond 5G networks. Sensors, 23(2), 969.

[27] Martalò, M., Pettorru, G., & Atzori, L. (2024). A cross-layer survey on secure and low-latency communications in next-generation IoT. IEEE Transactions on Network and Service Management, 21(4), 4669-4685.

[28] Mustafa, R., Sarkar, N. I., Mohaghegh, M., & Pervez, S. (2024). A cross-layer secure and energy-efficient framework for the internet of things: a comprehensive survey. Sensors (Basel, Switzerland), 24(22), 7209.

[29] Nasralla, M. M., Khattak, S. B. A., Ur Rehman, I., & Iqbal, M. (2023). Exploring the role of 6G technology in enhancing quality of experience for m-health multimedia applications: a comprehensive survey. Sensors, 23(13), 5882.

[30] Sharma, S., Popli, R., Singh, S., Chhabra, G., Saini, G. S., Singh, M., ... & Kumar, R. (2024). The role of 6G technologies in advancing smart city applications: Opportunities and challenges. Sustainability, 16(16), 7039.

[31] Khurana, R., Choudhary, M., Singh, A., & Singh, K. K. (2023). AIML-based blockchain solutions for IoMT. Blockchain and deep learning for smart healthcare, 73-93.

[32] Valsalan, P., Hasan, N. U., Baig, I., Zghaibeh, M., Farooq, U., & Suhail, S. (2024). Unleashing the potential: The joint of 5G and 6G technologies in enabling advanced IoT communication and sensing

systems: A comprehensive review and future prospects. J. Commun, 19(11), 523-535.

[33] Akbar, M. S., Hussain, Z., Ikram, M., Sheng, Q. Z., & Mukhopadhyay, S. (2022). 6G survey on challenges, requirements, applications, key enabling technologies, use cases, AI integration issues and security aspects. arXiv preprint arXiv:2206.00868.

[34] Ravi, K. C., Kavitha, G., Prasad, L. H., Srinivasa Rao, N. V., Deivasigamani, S., Ramesh, J. V. N., & Siddiqui, S. T. (2024). Beyond 5G-Based Smart Hospitals: Integrating Connectivity and Intelligence. Smart Hospitals: 5G, 6G and Moving Beyond Connectivity, 169-193.

[35] Akinbi, A. O. (2023). Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks. Wiley Interdisciplinary Reviews: Forensic Science, 5(6), e1496.

[36] Chataut, R., Nankya, M., & Akl, R. (2024). 6G networks and the AI revolution—Exploring technologies, applications, and emerging challenges. Sensors, 24(6), 1888.

[37] Putra, K. T., Arrayyan, A. Z., Hayati, N., Damarjati, C., Bakar, A., & Chen, H. C. (2024). A review on the application of internet of medical things in wearable personal health monitoring: A cloud-edge artificial intelligence approach. IEEE Access, 12, 21437-21452.

[38] Li, Y., Xiao, Y., Liang, W., Cai, J., Zhang, R., Li, K. C., & Khan, M. K. (2024). The security and privacy challenges toward cybersecurity of 6G networks: A comprehensive review. Computer Science and Information Systems, 21(3), 851-897.

[39] Samanta, S., Sarkar, A., & Bulo, Y. (2022). Secure 6G communication in smart city using blockchain. In Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2022, Volume 1 (pp. 487-496). Singapore: Springer Nature Singapore.

[40] Tang, F., Chen, X., Rodrigues, T. K., Zhao, M., & Kato, N. (2022). Survey on digital twin edge networks (DITEN) toward 6G. IEEE Open Journal of the Communications Society, 3, 1360-1381.