Blockchain and Federated Learning-based Security Solutions for Telesurgery System: A Comprehensive Review

Article *in* Turkish Journal of Electrical Engineering and Computer Sciences · November 2022

DOI: 10.55730/1300-0632.3950

Sachi Chaudhary
Nirma University
9 PUBLICATIONS **51** CITATIONS
SEE PROFILE

Rajesh Gupta
Nirma University
209 PUBLICATIONS **5,313** CITATIONS
SEE PROFILE

Sudeep Tanwar
Nirma University
673 PUBLICATIONS **19,395** CITATIONS
SEE PROFILE

Smita Agrawal
Nirma University
65 PUBLICATIONS **457** CITATIONS
SEE PROFILE

Turkish Journal of Electrical Engineering and Computer Sciences

Volume 30 | Number 7 Article 1

1-1-2022

Blockchain and federated learning-based security solutions for telesurgery system: a comprehensive review

SACHI CHAUDJARY

RIYA KAKKAR

RAJESH GUPTA

SUDEEP TANWAR

SMITA AGRAWAL

See next page for additional authors

Blockchain and federated learning-based security solutions for telesurgery system: a comprehensive review

Authors

SACHI CHAUDJARY, RIYA KAKKAR, RAJESH GUPTA, SUDEEP TANWAR, SMITA AGRAWAL, and RAVI SHARMA

Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Review Article

Turk J Elec Eng & Comp Sci
(2022) 30: 2446 – 2488
© TÜBİTAK
doi:10.55730/1300-0632.3950

Blockchain and federated learning-based security solutions for telesurgery system: a comprehensive review

Sachi CHAUDHARY[1], **Riya KAKKAR**[1], **Rajesh GUPTA**[1,**], **Sudeep TANWAR**[1,*] , **Smita AGRAWAL**[1,**], **Ravi SHARMA**[2]

[1]Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, India

[2]Centre for Inter-Disciplinary Research and Innovation, University of Petroleum and Energy Studies, Dehradun, India

Received: 06.03.2022 • **Accepted/Published Online:** 19.11.2022 • **Final Version:** 28.11.2022

Abstract: The advent of telemedicine with its remote surgical procedures has effectively transformed the working of healthcare professionals. The evolution of telemedicine facilitates the remote monitoring of patients that lead to the advent of telesurgery systems, i.e. one of the most critical applications in telemedicine systems. Apart from gaining popularity, the telesurgery system may encounter security and trust issues of patients' data while communicating with the surgeon for their remote treatment. Motivated by this, we have presented a comprehensive survey on secure telesurgery systems comprising healthcare, surgical robots, traditional telesurgery systems, and the role of artificial intelligence to deal with the numerous security attacks associated with the patients' health data. Furthermore, we propose a blockchain and federated learning-based secure telesurgery system to secure the communication between patient and surgeon. The results of the proposed system are better than those of the traditional system in terms of improved latency, low data storage cost, and enhanced data offloading. Finally, we explore the research challenges and issues associated with the telesurgery system.

Key words: Telesurgery, telemedicine, artificial intelligence, blockchain, federated learning

1. Introduction

The healthcare system has evolved prominently over the years. Firstly, traditional treatment methods have evolved from simple home remedies to manual appointments with doctors where the patients had to reach the hospitals for treatment. Later, medical equipment has evolved from a simple stethoscope to various modernized surgical and monitoring equipment. However, not every healthcare center can afford to modernize or digitize their centers to provide remote services to their patients. Moreover, the critically ill patients in rural areas or military on border zones cannot reach hospitals as it is a time-consuming and expensive procedure [1]. To resolve this problem, healthcare centers gradually adopted wireless communication technologies which enable surgeons to perform their services remotely, known as telemedicine [2, 3]. Telesurgery is the most prominent telemedicine application, allowing the doctor to perform a medical surgery from a distant place with the help of wireless communication channels and surgical robots, as stated in [4]. Therefore, it reduces transportation costs, time, and resource scarcity, allowing surgeons to perform high-quality operations. Furthermore, doctors, nurses, and patients can interact together remotely to perform any surgery and treat patients accordingly [5].

*Correspondence: rajesh.gupta@nirmauni.ac.in; sudeep.tanwar@nirmauni.ac.in; smita.agrawal@nirmauni.ac.in
**These authors contributed equally.

The medical industry has experienced an evolution from healthcare 1.0 to healthcare 5.0. Healthcare 1.0 mainly focuses on essential patient-doctor interaction, which involves consultation, testing, and diagnosis. With the help of these measures, a physician provides medications (care plan) and follow-ups for the treatment of patients leading to a physician-centered environment in the hospitals [6]. In healthcare 2.0, electronic health or medical records (EHs or MRs) have been enacted, including imaging test equipment, monitoring devices, life support, and surgical equipment. Therefore, it is considered to be technology-centric. Healthcare 3.0 was patient-centric, which provides remote care and telehealthcare but it was incapacitated to handle a huge amount of real-time medical data.[1] The healthcare 4.0 revolution solved the problems of the earlier revolutions by providing connected smart healthcare systems with wearables, Internet of things (IoT), smart sensors, robots, etc., combined with big data analysis, cloud computing, and selection support methods/tools, thereby providing enhanced patient-oriented and digitized medical care as mentioned in [7].

The severe need for intelligent healthcare systems with automated tools leads to the evolution of healthcare 5.0. Artificial intelligence (AI) and computerization are the essence of the latest healthcare technology with enhanced personalized care, mainly focusing on intelligent and smart health equipments. Healthcare 5.0 should contribute to a supersmart and intelligent society, especially for healthcare. It deals with the decentralization and sustainability of the products and services, which are much more customer-oriented, and focus on the quality of life through complete digital transformation.[2] Digital frameworks are proposed to advance the healthcare conditions of patients so that treatment can be done remotely. Moreover, it automates the surgeries, i.e. telesurgery, and makes the medicinal treatment more reliable and secure [8].

Smart healthcare and its advanced technologies with the help of telesurgery systems completely transformed the traditional healthcare industry so that healthcare professionals can keep track of patients' body symptoms to cure the disease accordingly. Many researchers have surveyed and proposed various telesurgery systems using different technologies and communication networks. For example, Elprama et al. [9] presented a survey on challenges associated with robot-assisted surgery. It focuses on clarifying the complex functioning of a working team that conventionally works in close supervision. The results of the survey show that the problems related to communication defects can deteriorate the patients' health [10]. Later, Sobhan et al. [11] surveyed data analysis techniques integrated with various sensors and their technologies to monitor patients remotely related to respiration, health, and sleep-deprived diseases. Amin et al. [12] surveyed state-of-the-art practices for drug intake and treatment monitoring along with its challenges like energy consumption, security, system availability, and complex data management

Sadawi et al. [13] executed a survey on IoT and blockchain-based system to guarantee security and accuracy in the framework using dew and cloudlet computing. The main focus is to provide efficiency and reliability for the healthcare contributors and management sector. The authors in [14] conducted a survey on cloud of things systems and their functions in healthcare to resolve energy efficiency issues. Saranya et al. [15] presented a survey on various machine learning (ML) algorithms used in big data analytics, the importance of big data analytics in health care, and characteristic features of big data [16]. Cai et al. [17] reviewed multimodal data-driven smart healthcare systems, types of decision making processes, multimodal association mining, and multimodal data fusion. These systems have been a driving force for smart healthcare systems containing various applications to detect and diagnose diseases. Nguyen et al. [18] conducted an exhaustive survey on various IoT applications such as information sharing, data discharging, attack disclosure, localization, mobile

[1] https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/risk-sea-healthcare-3.0-healthcare-for-the-new-normal/

[2] https://medium.com/qut-cde/health-5-0-the-emergence-of-digital-wellness-b21fdff635b9

mass sensing, and IoT confidentiality-safety issues using a federated learning model.

Most researchers or authors presented the surveys to overcome the security and latency issues in telesurgery systems so that patients can be monitored remotely. However, these surveys lack privacy, reliability, cost-efficiency, and data offloading and can also encounter different security attacks like modification attacks, spoofing, etc., to perform a patients' remote surgery. Therefore, to attenuate the aforementioned issues, we have conducted a comprehensive survey on telesurgery systems consisting of surgical robots, the role of AI, security and communication issues in telesurgery, and different traditional telesurgery systems. Also, we have proposed a blockchain and federated learning-based framework integrated with a 6G communication network and InterPlanetary File System (IPFS) protocol for secure and reliable patient health monitoring.

A blockchain-based proposed system has been introduced to enable the secure and efficient processing of patients' health data and instruction during surgery equipped with federated learning to ensure privacy without decentralizing the data. The federated learning model trains model of various healthcare data at a global model instead of a centralized model further enhancing the security of the system. For example, individual surgeons in the hospitals can get the patients' feedback from the globally trained model while maintaining the personal and medical data on a particular system rather than uploading and storing it on a centralized server. The integration of IPFS with the proposed system ensures that the data storage is cost-efficient as the blocks of data are stored with the help of IPFS. Furthermore, the usage of an integrated 6G communication network ensures low latency ($< 1ms$) and high reliability ($< 99.99999\%$) between patients and surgeons so that medical staff can get the required information about the patients' health and the surgeons' instructions during the remote surgery to provide them prescription appropriately.

1.1. Scope of the survey

Modernization of the healthcare system has transformed the treatments of the patients. Earlier, patients used to be present physically in the hospital to get themselves treated. However, nowadays, healthcare or hospital centers are gradually adapting the advanced technologies to monitor patients remotely with the help of telesurgery systems, and surgeons can give prescriptions according to the feedback of the patients. The researchers have surveyed many research works to treat patients using modernized computing such as ML, big data, AI, IoT etc. For example, Elmoghazy et al. [19] presented a review on diverse immersive techniques for surgical care telemedicine applications. They have discussed various tools such as robots, headpieces, and cameras, to provide surgeons with a remote experience in telesurgery while treating patients. Gupta et al. [20] conducted a survey on a telesurgery system using the tactile Internet technology for remote monitoring of patients. They further discussed a case study on the proposed telesurgery system with high reliability considering the 5G communication network.

Jin et al. [21] presented an exhaustive survey on telesurgery with the advancements in the technology in the form of telementoring and telemedicine. They discussed the telementoring considering the technologies such as 2D telestration, 3D telestration, and verbal guidance. Furthermore, they have investigated telesurgery and other technologies in various fields such as neurosurgery, obstetrics, and ophthalmology. However, tackling the issues of security, latency, and reliability in telesurgery systems can be challenging to achieve. Therefore, Bailo et al. [22] reviewed various issues related to data transmission, latency, and security in the telesurgery systems of telemedicine. Authors in [23] conducted a survey on robotic telesurgery system considering the 5G communication network to tackle the issues of latency and packet loss of the system.

Tiwari et al. [24] presented an analysis of robotic telesurgery considering the modernization of technologies such as AI, 5G, and tactile Internet to discuss the latency- and efficiency-related issues in the system. Authors in [25] conducted a detailed survey on secure telesurgery systems for healthcare 4.0. They mainly focused on improving the latency, reliability, and security of the system. Xia et al. [26] further reviewed the potential of the future clinical treatment with the help of a telesurgery robotic system. They mainly discussed the applications of telesurgery robotic system, which involves endoscopic, neurosurgical, and orthopedic telesurgery robots.

Furthermore, Aghanouri et al. [27] presented a workspace and kinematic analysis of the master robot in Sinaflex telesurgery system. The derivations show that the system has good manipulability, provides good control over slave surgery robot, and also has a large enough workspace for carrying out efficient postures for the surgeon. Later, Kadu et al. [28] reviewed various e-healthcare systems based on AI and Internet of medical things. It shows that these methods provide better adaptability of healthcare systems, intelligent help in diagnosis, patient monitoring, continuous monitoring, and also resolve difficulties like security and privacy to some extent.

Privacy protection is highly crucial in healthcare systems; therefore, Luong et al. [29] presented a healthcare system using zero-knowledge succinct noninteractive argument of knowledge algorithm and blockchain for IoT devices. These systems protect from various attacks and also reduces the computational costs. Later, Zhang et al. [30] proposed a blockchain-enabled privacy conserving e-healthcare system to increase security and privacy of the patients' health records. This is done using cryptography pairing and it protects from attacks. Moreover, secure payment methods are based on smart contracts and make the system highly efficient with minimum computational overhead. Further in [31], the authors provided a traceable and secure blockchain architecture for supply chain functions using smart contracts. The cryptography techniques enable the customers to view details of single product ID, ensuring the system efficiency and privacy preserving.

Table 1 presents the comparative analysis of various state-of-the-art telesurgery surveys with the proposed survey. Many of these surveys [19, 21] conducted by the authors have not considered various issues such as latency, data storage, and data offloading issues. Most of the surveys [24] utilize the AI and ML model in the telesurgery system, which can be the reason for deteriorating data offloading. To mitigate the aforementioned issues, we have conducted an exhaustive survey on secure telesurgery systems consisting of surgical robots, role of AI, security and communication issues in telesurgery, and traditional telesurgery systems. As a result, a blockchain and federated learning-based system has been proposed to secure the communication between patient and surgeon with low latency, high reliability, cost-effectiveness, and improved data offloading.

Table 1. Comparative analysis of various state-of-the-art telesurgery system surveys with the proposed survey.

Author (references)	Year	Objectives	Pros	Cons
[23]	2018	Conducted a survey on robotic telesurgery system using the 5G communication network	Low latency, reliability, cost-effectiveness	Sensitive to security attacks such as DoS and DDoS, scalability issues, no focus on data offloading
[20]	2019	Presented a comprehensive survey on telesurgery system using tactile Internet for remote monitoring of patients	High reliability, low overhead, low latency, fast response time	No consideration on scalability, security issues, can overburden the system

Table 1. (Continued).

Author (references)	Year	Objectives	Pros	Cons
[24]	2020	Conducted the analysis of robotic telesurgery considering the modernization of technologies such as AI, 5G, and tactile Internet	Reduced cost, improved latency, high scalability	Single point of failure, encounters data offloading and data storage cost issues
[32]	2020	Survey on acceptance of e-healthcare and telemedicine systems in developing countries	Trustworthy, affordable, highly reliable, accessible systems	Less acceptance or usage, security and privacy issues, high latency
[25]	2021	Review the detailed survey on secure telesurgery systems for healthcare 4.0	Low latency, high reliability	No security against malicious attacks such as DoS, single point of failure, overburdened system, no focus on cost-efficiency
[26]	2021	Presented survey on the potential of the future clinical treatment with the help of telesurgery robotic system	Improved clinical treatment	Security and legal issues, no focus on latency, scalability, and reliability, high cost-related issues
[19]	2021	Surveyed various immersive techniques for surgical care telemedicine applications in telesurgery systems	Edge intelligence, high reliability	Need to work on data rate, high cost, latency, and data offloading issues
[21]	2021	Presented an exhaustive survey on telesurgery with the advancements in the technology in the form of telementoring and telemedicine	High reliability, improved latency	Security issues against cyber attack, no focus to improve the legal and ethical issues, data offloading issues
[27]	2021	Analysis of robotic system in Sinaflex Telesurgery System	Kinematic and enough workspace is obtained with good manipulability	Master robot has sometimes less manipulability which can prove to be risky
[28]	2021	Review of telemedicine system based on IoT and AI	Highly accessible, less costly, continuous patient monitoring, intelligent diagnosis using AI	Lower adaptability and use, some reliability issues
[33]	2021	Presented a review on telemedicine and remote systems for COVID-19	Trustworthy, contact-free surgery, healthcare management, video monitoring, better diagnosis	Security and privacy issues, network stability issues

Table 1. (Continued).

Author (references)	Year	Objectives	Pros	Cons
[31]	2021	Presented a traceable, privacy protecting blockchain architecture for supply chain	Better transparency, higher traceability, higher performance, greater privacy and trust	Higher space complexity of the current architecture, not used lightweight hash functions and high cost of implementation
[34]	2021	Presented a blockchain system based on scalable distributed hash table	Highly accessible, on-demand function, high security, integrity, and efficiency	Lower throughput, not implemented at prototype level
[30]	2022	Proposed a blockchain enabled privacy protecting e-health model for healthcare data in cloud	Efficient storage services, high security along with confidentiality, limited computation overhead, verifiable, better privacy	Cannot resist collusion attacks from malicious doctors and hospitals
[22]	2022	Review the various issues related to the data transmission, latency, and security in the telesurgery systems of telemedicine	High reliability, low overhead, low latency, fast response time	Less accuracy, prone to cyber attacks and single point of failure, low extensibility and high latency issues
The proposed survey	2022	Survey on secure telesurgery systems using blockchain and federated learning-based system	Secure, reliable, cost-efficient, and improved data offloading	-

1.2. Contributions of the research

The major contributions of the present research are listed as follows:

- We present an exhaustive survey on secure telesurgery systems, which include surgical robots, the role of AI, and security and communication issues in the telesurgery systems.
- We propose a blockchain and federated learning-based framework incorporated with a 6G network to enable secure and reliable data exchange between surgeons and patients.
- We highlight the open issues and possible future research challenges in the secure telesurgery systems.
- Finally, the results suggest that the proposed system outperform the conventional systems in terms of low latency, better data offloading, and low data storage cost.

1.3. Methods and materials

This paper provides a deep understanding of a secure and trustable telesurgery system integrated with federated learning and a blockchain-based framework. Firstly, the authors review the traditional telesurgery systems and the associated possible security attacks. Next, the authors investigate several research articles from reputed research databases such as IEEEXplore, Springer Nature, Science Direct, Elsevier, MDPI, ACM digital, IET, and Wiley. The keywords used in traversing this issue include secure telesurgery system, surgical robots, AI/federated learning, security issues, and open issues and challenges in telesurgery systems.

1.4. Organization

The organization of the rest of the paper is as follows: Section 2 explains the evolution of healthcare, telesurgery, and surgical robots. Section 3 discusses the role of AI in the telesurgery system. Section 4 explored several security issues in the telesurgery system. Section 5 presents the communication issues in telesurgery. Section 6 elaborates the traditional telesurgery systems. Section 7 presents the proposed system for secure telesurgery. Section 8 shows the results for the proposed system. Section 9 presents various open issues and research challenges in telesurgery system. Finally, Section 10 concludes the paper.

2. Background concepts

Healthcare systems have evolved to a great extent. For example, the advanced healthcare technologies have greatly affected the working environment of the hospitals by evolving from healthcare 1.0 to 5.0. To better understand the evolution of healthcare, we present the key technologies such as healthcare 1.0 to 5.0, telesurgery, and surgical robots. These technologies are explained in the following subsections.

2.1. Healthcare 1.0 to 5.0

Healthcare 1.0 model has been widespread in healthcare practices for centuries. In the early era, patients have to make appointments with doctors to be present in the hospital accordingly. The healthcare team follows various measures such as consultation, testing, and diagnosis to make the prescription easy for the doctors with the proper instructions and steps to follow for the treatment [35]. For instance, if patients have some emergency, they have to refer to a specialist to acquire the treatment with the help of lab and imaging tests. This equipment consists of ultrasound, MRI, CT scans, etc. Various surgical and life support equipment, such as the da Vinci robotic system and chest tubes, is rapidly used in hospitals to observe the patients' treatment. We can further consider this evolution as healthcare 2.0. [3]

Subramoniam et al. [36] presented the challenges in healthcare 2.0 and proposed a system to solve them. However, at that time, all the patients' health data used to be handled and stored manually by the hospital management. However, advancements in the development of information systems enable the data storage to be easy and accessible with the help of electronic medical records (EMRs) and electronic health records (EHRs). These health-related smart technologies mainly impact the clinical and operational record maintaining processes. Several healthcare activities are time-framed and telerecorded in the EMRs, further computerizing the innumerable manual processes. Moreover, the advent of advanced computer networking techniques has made remote healthcare possible. For example, patients suffering from some disease can directly contact the doctors remotely, which further prevents the delay in the treatment. The current situation of the COVID-19 has tremendously increased the need for telehealth leading to the preferable treatment in online mode for patients. These factors have resulted in complete changes in healthcare delivery and optimization. This innovation is termed as healthcare 3.0.[4]

In healthcare 4.0, the transport procedure becomes a cyber-physical structure that functions with IoT, radio-frequency identification, tracking devices, wearables, surgical robots, and smart sensors, etc. These

[3] https://www.covetus.com/blog/health-20-types-of-web-20-technologies-in-the-healthcare-industry

[4] https://www.rasmussen.edu/degrees/health-sciences/blog/health-30/

technologies are combined with cloud services [37], big data analysis, AI, and choice-based support systems to accomplish intelligent and interrelated well-being delivery systems for full optimization as discussed in [38]. In smart healthcare systems, medical associations and facilities provided in the hospitals and clinics are interconnected with modern tools and devices for the betterment of the patients. For example, Gupta et al. [39] investigated a delivery scheme (outdoor) with the help of blockchain using an unmanned aerial vehicle for critical patients providing security and reliability using ethereum smart contracts and IPFS protocol to solve data storage cost issues. Patient-related healthcare information is shared with the proper protocols and predefined conditions. Patient data such as diagnosis report, medical history, lab reports, medications, pharmacy requirements, and hospital charges are shared through the interconnected network. However, confidentiality, security, and stability concerns remain as major concerns while treating the patients remotely. Bhattacharya et al. [40] presented a blockchain and deep learning-based framework in healthcare 4.0 systems to build security, confidence, and privacy amidst the users in the system. Furthermore, Kumar et al. [41] implemented a healthcare framework using healthcare 4.0 processes with the aid of blockchain and smart contracts. Additionally, AI techniques help to foresee the dedicated treatment, customized medicine, disease forecasting, and strengthened patient care for the betterment of their life. Hence, evolving a huge, intelligent, and interconnected health care community leads to the paradigm of healthcare 4.0.

Development and expansion in advanced healthcare technologies lead people to live a carefree and healthy life. These technologies include smart wearable devices such as sensors and actuators embedded into the patients' body that can collect and extract the symptoms of the disease so that doctors can take action according to the severity of their patients' condition. For that, healthcare management should be attentive enough to manage the healthcare data without delay in the absence of specialists. It can be made possible with the evolution of healthcare.

IoT devices with AI technology do not seem to be a prominent solution to overcome the disadvantages of healthcare 4.0. There are many setbacks in healthcare 4.0, such as not having flawless data broadcasting, high data loss, high cost, trafficked transmission channels, timed data retrieval, and the machine to machine delivery in IoT generation. However, some medical cases like remote surgeries specifically require device-to-device communication methods. Therefore, the sole feasible solution was to acquire a 5G communication elementary network for the proper functioning of the interconnected devices. Motivated by this, Mohanta et al. [42] suggested an AI- and IoT-based system using a 5G communication network to adapt the new generation in the digital healthcare system, i.e. healthcare 5.0.

Figure 1 shows the evolution of healthcare and its technologies which initiates from the implementation of predictive modeling for health monitoring. It further evolves with the advancement in technologies leading to the virtual medical centers with AI and assisted robots in the future.

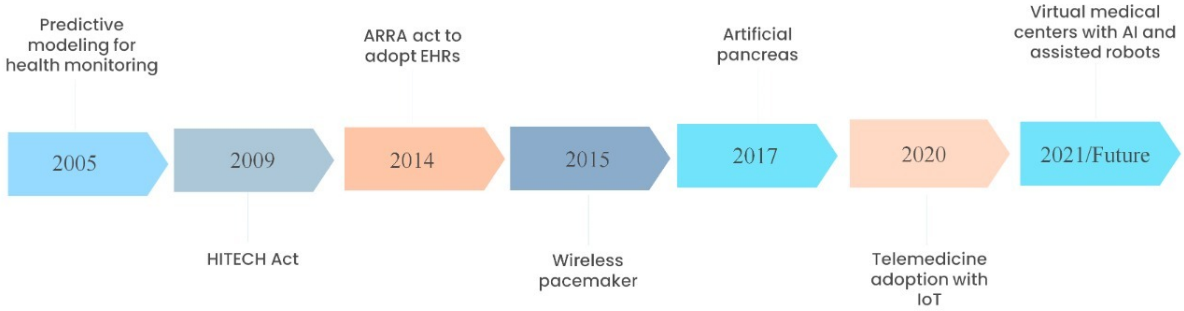

Predictive modeling for health monitoring
2005
HITECH Act
2009
ARRA act to adopt EHRs
2014
Wireless pacemaker
2015
Artificial pancreas
2017
Telemedicine adoption with IoT
2020
Virtual medical centers with AI and assisted robots
2021/Future

Figure 1. Evolution of healthcare and healthcare technologies.

2.2. Telesurgery

Telesurgery is also known as remote surgery, which involves carrying out surgical procedures using advanced technologies such as wireless communication networks, robotic arms, sensory devices, and audio-visual equipment. These technologies allow a surgeon to perform distant surgeries. This system is expanding due to two main causes, i.e. an ill person in a rural or border area will not be able to afford the cost of hospitals. Another reason is patients traveling to the metropolitan cities for their treatment, which requires the guidance of specialist doctors, resulting in an increase in the severity of the patients' health problem. Moreover, it leads to a waste of precious time both for the patient and the doctor, as the patient needs to travel to a specialist, and the specialist needs to travel to a secluded city to perform a specific surgery. These disadvantages are the reason for the emergence of telesurgery for providing real-time healthcare services in faraway places with higher accuracy and efficiency by saving traveling costs and time of both patients and surgeons [43].

Telesurgery systems consist of a master (where the doctor resides)–slave (where the patient resides) model. The two ends of the model are connected with the help of a wireless communication network. The master domain contains haptic devices, doctor's GUI, 3D video display, foot pedal, microphone, and audio devices, which guide and control the robotic arm at the patient's end. The slave domain consists of sensors, surgical robots, haptic feedback devices, 3D-HD video providers, microphones, and audio devices to facilitate the telesurgery for the surgical assistants [20]. The network communication connects two domains, sending control instructions from the master domain to the slave domain. The feedback is then sent from the slave domain to the master domain. The surgeon then translates different feedback messages from haptic devices such as surgical robot movements, speed, and anatomy view, and gets to know if the surgery is getting performed appropriately or not. Disturbance and delay in the communication are highly possible as the network through which the instructions are sent comprises a wireless and open communication channel as mentioned in [4].

Due to the usage of the superior system model, doctors, surgeons, patients, practitioners, and other medical staff utilize the telesurgery system in healthcare services. It is beneficial for patients who cannot travel faraway distances, especially those who live in remote and rural areas, which further helps them save time and money. Patients can get access to doctors who are specialists in other faraway developed countries with the help of telesurgery [44]. It reduces the barrier between patients and doctors with the help of integrated communication technologies using IoT that facilitates the telesurgery system with the interlined devices which help the surgeon in performing operations faster and more accurately.[5]

Modernized technologies such as ML and AI in the telesurgery system safeguard confidential patient data from hackers and malpractices [45]. Space travel emergencies for astronauts and cosmonauts in outer space missions can be responded with ease via telesurgery and integrated communication channels from the ground. Furthermore, in potential battlefield grounds and war scenarios, life-threatening conditions of army and military personnel can be easily treated in real-time situations via telesurgery and communications from distant locations. Therefore, the telesurgery system has a significant potential in the field of medicine as mentioned in [46] due to the following benefits:

- **Efficient and reliable**: Telesurgery treatment procedure is more efficient and reliable than conventional treatment procedures as it eliminates specific unfavorable techniques and measures.

- **Cost-effective**: It is a less expensive and less complicated procedure than the traditional method.

[5] https://www.aimblog.io/2021/01/23/twenty-years-of-telesurgery-improving-healthcare-delivery-to-underserved-locations/

- **Time-saving**: It saves time by accessing secluded cities, especially in deprived areas, to preclude from the local hospitals with fewer administration complexes.
- **Fast and pain-free**: Telesurgery is more precisely handled treatment with less pain, faster recovery, and early discharge with compatible system interface.
- **Real-time surgery**: With the help of wireless communication channels, doctors and clinical practitioners can perform real-time surgical procedures remotely thanks to the advancement of robotics and automation when there are safety concerns.
- **Feasible to use**: It helps in the prevention of certain diseases and is more feasible to control the consequences with the help of robotic maneuver.

Figure 2 shows the evolution of telesurgery systems. The first telesurgery was performed in 2001, which further evolved to digital healthcare with the advancements in the telemedicine using 5G communication network monitored telesurgery.

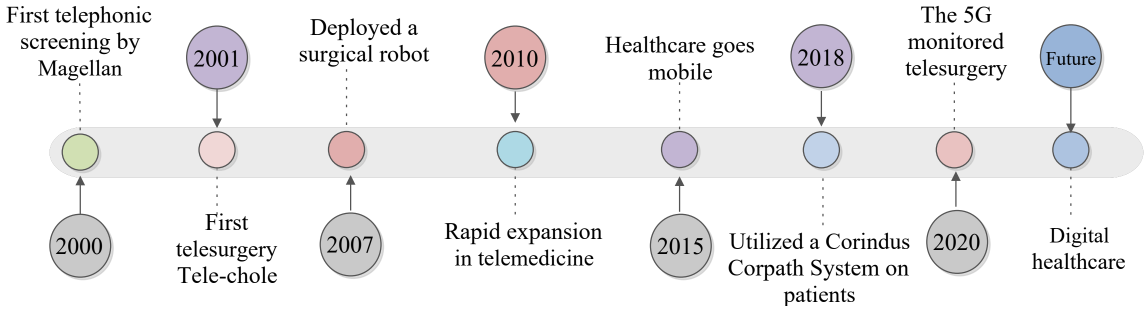

First telephonic screening by Magellan
2000
2001
First telesurgery Tele-chole
Deployed a surgical robot
2007
2010
Rapid expansion in telemedicine
Healthcare goes mobile
2015
2018
Utilized a Corindus Corpath System on patients
The 5G monitored telesurgery
2020
Future
Digital healthcare

Figure 2. Evolution of telesurgery.

2.3. Surgical robots

Surgical robots became one of the fastest growing fields of the healthcare and service robot industries. It provides extensive features such as good repeatability, high accuracy, and strong stability. It enables doctors or surgeons to perform complicated medical procedures or treatment on patients ensuring accurate and flexible treatment. Surgical robotics is adapting new domains with the addition of advanced technologies that require tremendously advanced controlling and directing skills with decision-taking for the patients' betterment.

The most recent surgical robots function as an active extension for surgeon's operation along with the skilled and intelligent coworker facility. The ongoing trends include defined decision making support regarding the surgery's planning, navigation, and flawless illustrations. Surgical operations carried out by robots have been empowered by reliable platforms for both action-oriented and telesurgical control methods [47]. These advanced devices and technologies elevate the performance of surgical steps that are otherwise impossible to achieve. Seamless integration of microimagining processes at a cellular level remarkably helps in expanding the surgeon's capabilities [48].

Some of the research works related to the surgical robots are follows: Qin et al. [49] proposed a method to simultaneously predict the following trajectories of medical instruments along with the upcoming surgical subfunctions in robot-assisted operations using numerous input sources. Furthermore, they presented the da Vinci, i.e. a persistent dual-task prototype for robotic motion and medical state prediction. Nguyen et al. [50]

developed a concentric fusion tube robot for cholesteatoma laser surgery. It combines a robot and a wrist at the distant end, operated by the ligament. It introduces the surgical protocol through two entrance points obtaining the anatomical restrictions and specifying the robot functions. Later, Shi et al. [51] designed a real-time 3D navigation-enabled automated operational robotic system for pelvic fracture that offered a positive and appropriate result, increasing the usability of the system and enhancing the capacity of pelvic fracture surgeries.

The authors in [52] executed SurRoL, a reinforcement learning-centered and the da Vinci Research Kit (dVRK)-compatible simulation platform for surgical robotic learning. Later, Hosseiny et al. [53] validated Robossis (surgical robotic system) to assist long-bone rupture reduction-related surgeries. This technology helps the surgeon to accurately align the fractured bone in the presence of traction forces with the help of an unfamiliar three-armed robot, master controller, and a bone-gripping mechanism. Table 2 presents the comparative analysis of various surgical robots with their year of manufacture and their functions. It shows the advantages and disadvantages of various surgical robots with different applied technologies.

Table 2. Comparative analysis of various state-of-the-art surgical robots.

Name of robot	**Year**	**Manufacturer**	**Function**	**Pros**	**Cons**
Miniature robo	2016	Virtual Incision Corp.	Used for colon cancer treatment, on crohn’s disease patients, ulcerative colitis, and diverticulitis	Accurate and speedy recovery	Surrounding temperature uncertainty
AI epidemiology	2016	AIME system	Used to predict outbreaks of various diseases. Used in predicting dengue outbreaks in Malaysia with 85% accuracy	Helps doctors on ground to prevent pandemic from spreading by saving lives of thousands of people	Sometimes the prediction can be wrong and can lead to severe problems
Stereotaxis	2018	Epoch robotic surgery system	Used to manipulate catheters inside the heart by driving it through magnets	Has ability to treat complicated rhythms and reduces the exposure of X-ray by 90 percent in procedures	Not appropriate for presurgical data
Navio surgical system	2018	Smith Nephews	Developed for partial knee replacement operation	Less pain, faster rehabilitation, smaller incisions, with added natural knee movements	Unicompartmental knee replacement
PRECEYES surgical system	2019	PRECEYES	Dispense gene therapy to the retina	More effective than manual eye surgeries	Hard to perform complex surgeries successfully
Corindus vascular robotics	2019	CorePath system	Performs remote surgeries	Helps in areas where skilled surgeons are not available	Latency and reliability issues

Table 2. (Continued).

Name of robot	**Year**	**Manufacturer**	**Function**	**Pros**	**Cons**
Monarch platform	2019	Auris Health Inc.	Endoscopic platform to perform therapeutic and diagnostic bronchoscopy procedures	Integrates endoscopes, instruments, navigation, and robotics in a single platform	Clinical and safety issues
Mako Rio	2019	Mako Surgical Corp.	Knee surgeries and hip replacement	Provides 3D model based on CT scan and feedbacks	Health and safety concerns
The Versius	2019	Cambridge-based CMR surgical	Performs laparoscopic surgeries also known as keyhole procedures	Can be performed only in 30 min with versuis	Health and safety concerns
AI diagnostics	2019	New York university team	Has a high degree of accuracy for screening over 8000 diseases using facial recognition software	Helps in pinpointing patients at the verge of heart failure, strokes, developing diabetes, etc.	Sometimes disease diagnosed is inaccurate and leads to the reliability issues
Targeted therapy microrobot	2019	Researchers of Caltech's Division of engineering and applied science	It uses near microscopic mechanical molecules to deliver medicines nearby or other treatment to a specific target site within the human body	Deliver radiation directly to a tumour	It might be misguided and has security and health issues
Disinfectant bots	2020	UVD robots	Walk independently to patients' room who are being discharged and cleans the room with energetic UV rays up till no microorganism is left alive	Useful in infectious diseases like corona to prevent the spread to coworkers	It has safety issues
Corepath robotic intervention arm	2020	CorePath system	Used for COVID-19 effected patient	Provide safety to the surgeons from covid	Safety and health issues
Antibacterial nanorobots	2021	China's National Center for Nanoscience and Technology (NCNT) and Arizona State University	Helps in early diagnosis and drug deliver in patient's blood, killing antibiotic-resistant bacteria	Supports patient's body who is no more treatable via medical drugs	Can harm the patient's body if not properly functions

3. Role of AI in telesurgery systems

Earlier, telesurgery was performed without the use of AI. The surgeon used to perform operations with the help of a telesurgery system by operating other equipment manually. However, with the advancement in AI applications, which include analyzing, screening, and diagnosing, it has become easier to perform telesurgery. Since the same operation is frequently performed on different patients, the telesurgery system can be made to learn it with the use of AI to accomplish it without any loss of performance [54]. It can also save a lot of resources and time for doctors in operating the same system repeatedly. AI can also be used for the detection and monitoring of various ailments. For example, if the same symptoms or reports are detected in a particular disease, AI can quickly learn them by itself and treat the patient according to the prescribed knowledge. Usage of technology also reduces the cost as AI in remote checking and makes more progress with less specialty effort [55]. AI came into prominence due to the i) high demand of the health facilities and the need to locate the doctors, patients, and their data together and ii) at operations where the use of advanced applications is required and specialized doctors cannot perform everything with ease.

The usage of AI enables doctors to screen, analyze, and diagnose different diseases at isolated places with ease. The information and communication technology (ICT) tools can be used to mark the issues of demand versus supply of healthcare services. AI can overcome these issues by matching the availability of care providers with clinical skills by developing algorithms. Moreover, there is a need for uninterrupted connection across different chains of healthcare delivery as all health workers cannot always be present. Therefore, there is a requirement for telesupport. AI can tackle these issues by enabling intelligent information and a communication environment through which healthcare workers can communicate and determine the patients' health condition. Komal et al. conducted a state-of-the-art survey and studied that AI is currently being used in diagnosis of different diseases, remote patient monitoring, and distant eldercare [56]. Furthermore, due to its faster capacity to filter big data, the medical issues can be identified rapidly before the disease becomes calamitous. AI has proven to be a boon for the telesurgery system.

AI seems to be a potential solution in various coincident mission-critical implementations one of which is a telesurgery systems. However, several threats such as security, privacy, trust, bandwidth, reliability, and clarity issues are challenging in an AI-qualified TS system as discussed in [45, 57]. Therefore, they proposed a blockchain-based telesurgery system with AI and 6G known as BATS, i.e. a secure and reliable system with low latency communication between users. Outcomes of results show that the proposed system attains better prediction accuracy, high output, low packet loss ratio, low data storage cost, low bandwidth usage, and high mining profit in comparison to the conventional HaBiTs [58] and AaYusH [43] systems.

AI methods are used to detect healthcare issues and diseases that can be hazardous to the patients' health. However, most of these AI systems behave as black-boxes, i.e. directing to a low level of trust for the surgeons and the patients. Moreover, there are a lot of hurdles regarding the use of big data and AI in healthcare that includes accountability, regulation, security, and transparency [59]. To mitigate these issues, Riboni et al. [60] discussed an AI-fueled dashboard that allows medical staff to examine anomalies along with the explanations of predictions computed.

To ensure successful implementation of telesurgery systems, numerous countries planned a durable phase, which includes restarting some surgical course of action. The surgical course of action uses AI and robotics in telesurgery, telemonitoring, and teletraining for surgical methods. Surgeons have to interact with a massive number of staff and patients regularly. Therefore, the risk of infection conduction between them highly increases. Besides this, before- and after-surgery evaluation also raises worry about the increase in the risk of disease transmission. Therefore, it can lead to an increase in cases of mortality due to the ailment. For this, Feizi et al. [61] addressed several challenges and future opportunities associated with the surgery procedure in teleoperation, teleassessment, and teletraining using AI and robotics advanced technology to ensure the treatment of patients' without any delay.

4. Taxonomy of security attacks on telesurgery systems

The telesurgery system is vulnerable to various security and privacy attacks due to the different traditional communication platforms for data interchange. Thus, it can be easily exploited and hacked by any malicious users affecting a patients' life and break the system's ethics. Therefore, it is necessary to get insights into the possible number of threats to overcome these security threats. Several security attacks such as denial-of-service (DoS), data modification, man-in-the-middle (MITM), spoofing, tampering, and malware programs redirect the surgical robot's movement or the feedback properties cause massive harm to the patients' life. In addition, security threats that involve elevation of privilege and repudiation allow the attackers to perform actions without the surgeon's authorization. For example, the information disclosure threat consists of the hacker who snuffles surgical information and commands that may violate one's privacy. A hacker can execute these privacy and security attacks on the network components, human-computer interaction systems, or the slave controller. Figure 3 shows the taxonomy of various security attacks on telesurgery systems, which are described in the following subsections.

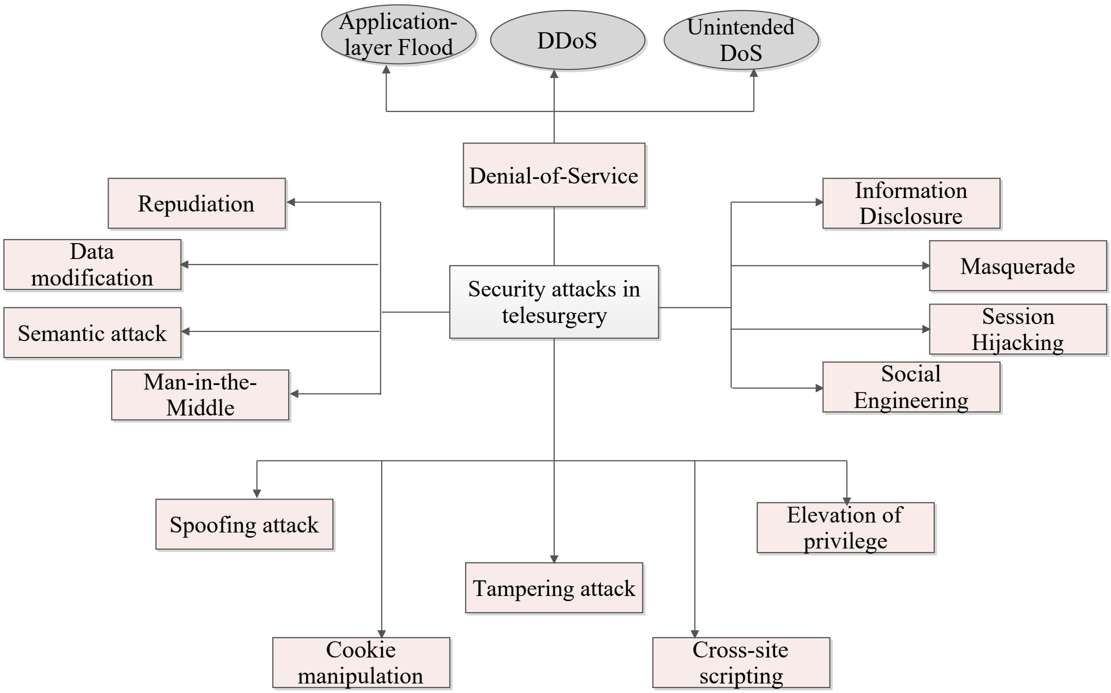


Figure 3. Taxonomy of security attacks on telesurgery systems.

4.1. Denial-of-service

DoS can be defined as a cyber attack where a malicious or anonymous attacker aims to manifest a device and makes it inaccessible to the users, i.e. patient involved in the telesurgery system, by disrupting the device's performance. We can consider an example in which doctors have prescribed some medicines or prescription based on the patient's monitored medical condition. However, due to the DoS attack, that particular information can be manipulated, which can convey incorrect prescription. This type of attack floods the targeted devices with the number of packets, which makes it difficult for other users to access the devices due to the resource constraint resulting in a DoS attack. For that, Kamble et al. [62] presented the digital transformation of healthcare using encryption techniques against DoS attacks to ensure secure communication between the authorized users. These attacks are basically of three types: (i) application layer flood; (ii) distributed denial-of-service attacks (DDoS); and (iii) denial-of-service attacks.

4.1.1. Application layer flood

Application layer flood mainly targets a specific vulnerability or issue in a device to flood the device with the number of packets so that users cannot receive the correct content from the targeted device leading to an attack, i.e. application layer flood. For example, Sinha et al. [63] demonstrated the impact of DoS attacks in IoT systems. They have identified the hacker location for interference attacks that can help to secure the telesurgery systems from the most common threats in all the layers of IoT-enabled system models.

4.1.2. Distributed denial-of-service attacks

In the COVID-19 pandemic, most organizations have announced the guidelines for remote work. However, healthcare organizations have to manage all their patients online, which raises the chance of DDoS attacks with the patients' confidential data. DDoS attacks can be launched to distract the healthcare security team and can modify the patients' appointment and their information. It can be a severe issue that needs to be solved to preserve people's health data. To solve these issues, Khatkar et al. [64] identified the gap and importance of additional research for detection and prevention of DDoS attacks in the application layer of healthcare devices.

4.1.3. Denial-of-service attacks

In this type of attack, the device can unintentionally be overburdened with the data requests. It means if patients and surgeons are interacting with each other through the communication network, but if one side in the communication starts receiving the data from an unknown user randomly. Then, it can slow down the data transmission and can lead to a delay in the patients' treatment. For that, Kurniawan et al. [65] mitigated and detected solution against unintended DDoS attacks on wireless sensor networks using blockchain and intrusion detection systems.

4.2. Spoofing attack

A spoofing attack is an act of impersonating a data transmission or identity so that it seems to be interrelated with an authenticated and authorized source of information. These attacks can be of various forms, from the customary email spoofing attacks to caller ID spoofing attacks that are often used to commit fraud and get confidential information. Attackers may also target elements like slave or master domain and send the feedback information or instructions for telesurgery as a part of a spoofing attack. Moreover, technical elements of an organization's network system, such as domain name system (DNS) server, IP address, or address resolution protocol (ARP) service can also be attacked. For example, Chen et al. [66] proposed a new prototype for spoofing attacks identification, i.e. Spoofprint that consists of an enrollment stage and a verification stage at the end. Furthermore, they have combined spoof embeddings and speaker embeddings which is being extracted with the help of Deep Neural Network model to perform the spoofing detection efficiently.

4.3. Tampering attack

Tampering attack is deployed on the confidential parameters exchanged between the client/receiver and server/sender to modify the system data, user credentials, permissions, patient medical history, location, etc. Generally, this information is stockpiled in cookies hidden from users and is used to improve the application's functionality and command. This attack is performed by malicious attackers who want to exploit the application/system for their interest or a hacker who wishes to attack using an MITM attack. In both cases, mechanisms including Web-scarab and Paros proxy are mostly used. However, the success of the attack depends on the integrity and rationale validation mechanism errors. Moreover, the manipulation can result in other consequences such as cross-site scripting attacks, file inclusion, SQL injection, and path leak attacks [67].

4.4. Elevation of privilege

This type of attack is initiated when a user tries to gain the privilege or right to access confidential information. The user can be an external threat, or it can be someone from the internal network. For example, only surgeons can access the health status of the patient. However, some internal or external attackers may try to gain that authorized right, which leads to the elevation of privilege attack. These types of attacks can be of two kinds. One is vertical privilege escalation, in which a user who already has some of the privileges will try to gain more privileges or rights. Another is horizontal escalation, in which the user will try to gain access to another account with the same level of privilege. To lessen these attacks, Jaafar et al. [68] introduced a systematic approach for privilege escalation prevention. This method detects various abnormal activities which indicate security and privacy issues concerned with privilege escalation using pattern recognition and outline detection.

4.5. Repudiation

A repudiation attack can be defined as any malicious attacker or activity trying to disrupt the system. There is no specific protocol tracking the user's activities involved in the system. For example, a telesurgery system consists of patients, surgeons, and caregivers interacting using advanced technologies to monitor the patients' health symptoms. However, any user can modify the patients' health data in the system, and the system cannot track that particular user leading to a repudiation attack in the system.[6]

4.6. Data modification attacks

Data modification attack is based on the interception of the exchanged data between the two systems. The data is either modified or deleted based on the attacker's motive to alter the comprehension of the message or to avert the information arriving at the receiver's end. For example, changing the master (surgeon) domain's instruction arriving at the slave's (patient) end in the telesurgery can disrupt the surgical procedure. Moreover, falsified instructions about the treatment can make the system less efficient and reliable. For that, Nithiavathy et al. [69] designed the data integrity and data dynamics secure platform using storage services in the cloud.

4.7. Man-in-the-middle

MITM can be considered a type of cyberattack in which a sender transmits a message to the receiver. However, during the transmission, a malicious user can interject to manipulate or steal confidential information before sending it to the receiver. Now, the receiver may receive the modified data, which contains misleading information. If this type of attacker interjects in the telesurgery system, it may negatively affect the patients'

[6] https://owasp.org/wwwcommunity/attacks/Repudiation_Attack

health. For example, authors in [85] presented a secure client-server connection against the MITM attacks. The design concept includes an authentication string that uses the sender's public key and provides the receiver's authenticity through its password without needing the receiver side certificate or a secondary medium.

4.8. Information disclosure attack

Information disclosure attack mainly aims to target the specific information of the system. The targeted information may be stored locally or permanently in the system. If an attacker knows some of the information, then it will be an easy task to disrupt the system. For example, if somehow an attacker gets information about some of the patients' health symptoms, one misleading information may adversely affect the patients' health. For that, Li et al. [75] proposed a framework called Mimosa, which specifically functions to protect private keys against information disclosure attacks using hardware transactional memory.

4.9. Masquerade

It uses an anonymous identity disguising as the authorized person to gain privileged access to the system. It also depends on the security of the system, i.e. if the system is protected using cryptographic algorithms, then masquerade attack may be prevented. For example, in a telesurgery system, if the communication between patient and surgeon is not secured, some unauthorized person may intercept the communication to modify the data referring to a masquerade attack. For example, Xu et al. [86] proposed a deep learning-based system for cloud masquerade attack identification, which can spontaneously collect the patients' data and detect masquerade attacks.

4.10. Social engineering

In a social engineering attack, the attacker tries to manipulate the information by involving with the people for their financial benefit. The main objective is to acquire knowledge about confidential information by tricking people within the organization. In a telesurgery system, a malicious person can interact with their colleagues with the ulterior motive for releasing the patients' health information. For example, Li et al. [87] investigated the nature of social engineering attacks and identified their essential factors.

4.11. Semantic attacks

Wireless medical devices and systems used in telehealth applications involve a huge number of sensors and are susceptible to various security and privacy attacks. The use of false information while patients communicate with the doctor can be the reason for the incorrect prescription. It is also known as semantic hacking. Yan et al. [88] developed a theoretical and statistical approach in which results include incorrect medical detection and treatment further to find the solutions for the attack in the future.

4.12. Session hijacking attacks

In session hijacking, the attacker hijacks the permissible session of the patient/doctor to access the information during the communication. The attacker can participate in the ongoing communication to steal or modify the patients' data. Hu et al. [89] analyzed session hijacking attacks against device-controlled physical layer key agreement. This attack exploits the key agreement by using MITM technique. The attacker runs the device, hijacking the user by running the physical-layer key agreement through randomness protocol. The method further allows users to discover if the changes are due to separate keys from a third party or not.

4.13. Cookie manipulation attacks

A cookie manipulation attack involves the exploitation of the cookies to acquire the patients' identity and confidential information. Usually, the patient information helpful in surgery is stored in the cookies. Once accessed from a web application, the data can also be deposited in the cookies. Hence, the attacker gets to access all the information related to the surgeon and patient, which can endanger the patients' life. A patient/surgeon's medical, financial, location, or any sensitive data can be accessed by this attack. [7]

4.14. Crosssite scripting attacks

The attacker injects malicious code into the web application or trusted websites to execute malicious scripts to obtain the patients' cookies. This type of attack can occur based on the security of the user's information. The attacker can gain access to the patients' system that is the slave domain or the master domain in the telesurgery system through the webcam, microphone, and location by impersonating them.[8] For example, Singh et al. [90] studied that 50% of web applications and systems are vulnerable to these types of attacks.

Table 3 shows the comparative analysis of possible security attacks on the telesurgery systems. It helps to identify the issues that need to be resolved for efficient surgical procedures.

5. Communication issues in telesurgery

The traditional telesurgery systems used 3G, 4G, and LTE conventional communication networks, which turned down the success ratio of remote surgeries due to the high latency ($\leq 100ms$), low reliability, and low accuracy. The delay in the sent control instructions and the feedback messages can endanger the patients' life. This problem was solved with the blooming of 5G technology. The tactile internet-based 5G model provides low latency ($< 5ms$), high reliability (99.999%), and high availability, which makes the telesurgery more accurate and dependable [91]. However, these measures are not ample to carry out complex surgeries as it requires the surgeon to give many control instructions at a time, and the end-to-end delay can affect the patients' life [20].

To mitigate the issues of low reliability, lower accuracy, and low latency, the BITS [44] framework utilizes the 6G network of low end-to-end latency ($< 1ms$), ultrahigh reliability (99.99999%), and high connection density. This system also incorporates AI, which predicts the disease pattern and any security attacks or malpractices on the system. It makes the telesurgery system highly reliable and efficient for healthcare professionals to work from remote locations using 6G communication channels. The main factors determining the communication in telesurgery system are [20]:

- **Reliability**: Reliability means sending data or messages to the destination without any loss or duplication of data in a secure and orderly manner based on the defined order. Therefore, the telesurgery system should have high reliability to operate the surgical procedures appropriately without defects.
- **Latency**: Latency can be defined as the amount of time a data packet takes to be captured, transmitted through multiple systems, and then received to the slave domain to be decoded. Latency should be extremely low for a telesurgery system to work efficiently.
- **Connection density**: It is the ability to deliver messages successfully of a specific size in a particular time interval. For example, 5G supports 1 million devices per square km. Thus, the telesurgery system should

[7] https://securityboulevard.com/2020/01/how-to-prevent-cookie-stealing-and-hijacking-sessions-easiest-guide/

[8] https://www.malcare.com/blog/session-hijacking-cookie-stealing/

Table 3. Analysis of various security attacks on telesurgery systems.

Attack	Definition	Impact on telesurgery system
Data modification attack [4]	An attacker modifies the control instructions, feedback properties, or network components and cause security threats	The data in the telesurgery system gets modified and can prove life threating to a patient's life
Elevation of privilege [68]	An attacker may gain privilege to execute or impersonate unwanted actions on the HCI system or slave controller	It may cause privacy loss and prove troublesome to a doctor and patient as the attacker may gain privilege to perform and manipulate any action
DoS [70]	The attacker may overload or stop the network components or communication channel with snipping devices and send enormous data	It may cause sudden interruption in availability of information and can prove fatal to the patient's life
Spoofing [71]	An attacker may spoof the Human computer interaction (HCI) system on the master side, haptic devices, or slave controller to perform any actions or send any feedback properties	Due to this attack, the system can face severe security and privacy issues as the attacker disguises itself as the master component and performs unfavorable actions on the patient
Tampering [72]	A hacker may alter or update the control instruction sent by a surgeon or the feedback properties through the communication channels	The control instructions are tampered which may cause severe problems as the surgery performed on the patient gets manipulated in a wrong way
Repudiation [73]	The HCI system, slave controller, or the network components affirm that it does not obtain information from outside the trust boundary or an attacker	This kind of attacks are threating as one cannot claim who has performed certain action or communication and even cannot claim that the action never took place
MITM [74]	In this attack, an attacker interrupts communication connecting the master and slave by eavesdropping or stopping the control instruction sent to the system	It disrupts the communication in the telesurgery system
Information disclosure [75]	In this attack, a hacker may get all the information passed through the communication channels leading to the privacy violations	The instructions sent in the telesurgery system can be hacked, which causes privacy threats to the users
Masquerade [76]	A malicious hacker fools the system by misinterpreting the system as another entity	It may affect the integrity and confidentiality of information of the telesurgery system
Social engineering [77]	The attack is carried out by a known or a hostile person who has knowledge about the system. Hence, it becomes easier to deceive the information	The attackers take advantage of the trusted people and easily hack the control instructions and feedback properties for large social engineering attacks
Semantic attack [78]	An attacker replaces the right instruction with the incorrect instructions to defame the credibility of the telesurgery system	The instruction of telesurgery system is modified or disseminated to showcase it in the wrong way and cause direct or indirect harm to the slave controller

possess high connection density to prevent any connection shortage, strengthening the communication between the patient and the surgeon.

- **Throughput**: It is the actual amount of data that is sent or received successfully over the communication channel. Therefore, a telesurgery system should have high throughput to work efficiently.
- **Data rate**: It is the speed at which data is transmitted over a network from one device to another during a specific time interval. Thus, telesurgery systems should have a high data rate to perform surgery efficiently.
- **Availability** : It refers to the amount of uptime in a communication process over a specific time interval. As it defines the operational status and a system's ability to quickly establish the connections, process the traffic, and respond to the requests. A telesurgery system should have high availability to complete both doctor's and patient's requests to perform the surgical procedure efficiently.

6. Traditional telesurgery systems

The traditional telesurgery system is gradually adapting the surgical systems with wireless networking technology and robotic surgery. These wireless technologies connect surgeons and patients to communicate remotely from different locations. Patients with an emergency medical condition can get benefit from a telesurgery system integrated with advanced technologies. There have been numerous technological advancements in telesurgery since the world's first telesurgery in 2001, which was developed by the ZEUS robotic systems. Currently, evolving communication technologies of telesurgery systems equipped with virtual reality interface, haptic feedback technology, and sensors help to improve the patients' treatment [92]. Figure 4 shows the taxonomy of traditional telesurgery systems and how telesurgery systems have been evolved with the introduction of advanced techniques.

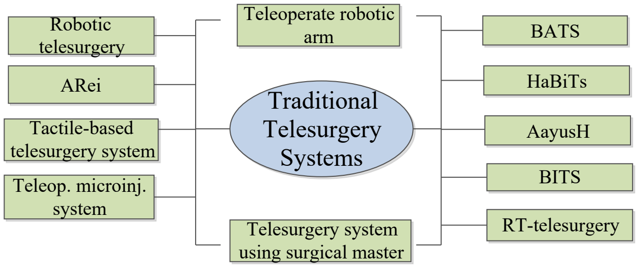


Figure 4. Taxonomy of traditional telesurgery systems.

These traditional telesurgery systems with their aim, benefits, and limitations have been analyzed in Table 4.

6.1. Robotic telesurgery through the Internet

The usage of robotic surgery for surgical implementation has increased drastically in the last few years. In robotic telesurgery through the Internet, Arata et al. [79] studied an operational robotic system that can be used to perform a surgery remotely and further improve the feasibility of telesurgery.

Table 4. Comparative analysis of traditional telesurgery systems.

Year	Name of the system	Aim	Delay	Reliability	AI	Blockchain	Communication channel	Merits	Demerits
2014	Robotic telesurgery through the Internet [79]	To present a system for laparoscopic surgery within long-distance using Internet	62.4 ms	Reliable	No	No	Open test-based Internet environment	Positive feasibility of telesurgery, low latency, performed over long-distances	Large time-delay, poor message transmission quality, safety and communication issues
2017	Telesurgery system using operational master device type of 3PUU [80]	To propose a telesurgery system for spinal operation along with efficiency validation by a surgeon.	2 ms	Reliable	No	No	TCP/IP protocol to communicate in slave robot	Faster communication frequency, easily operatable, weight of master device reduced, secure	Less functions, no doctor's feedback mechanism, less effective
2019	Tactile-Internet-Based Telesurgery system for Healthcare 4.0 [20]	To provide efficiency, low latency, and high reliability to the system	$< 1ms$	99.999%	No	No	5G URLLC service-enabled TI communication channel	Low battery consumption, high density	Security and privacy issues and high communication costs

Table 4. (Continued).

Year	Name of the system	Aim	Delay	Reliability	AI	Blockchain	Communication channel	Merits	Demerits
2020	AaYusH: Ethereum blockchain-based telesurgery system [43]	To provide a secure, high-throughput, low-latency smart contract-based TL system providing feedback-based recommend system	$< 1ms$	99.999%	No	Yes	5G-enabled TI communication channel, Ethereum smart contract, IPFS protocol	Secure, eliminates the need for third party, convenient cost and improved system functioning	Not appropriate for private blockchain, interportability issues
2019	HaBiTs: Blockchain-based Telesurgery Framework for Healthcare 4.0 [58]	To provide a secure and traceable TS system	$< 5ms$	Low	Yes	Yes	Through smart services like GPS navigation	Security and privacy issues solved by integrating blockchain, resolved interportability issues, no third-party service due to digital smart contracts	Reliability issues with high latency
2020	BITS: A Blockchain-based and Intelligence driven Telesurgery system [44]	To predict disease pattern and stop manipulation of systems by AI-based algorithms.	$< 1ms$	99.99999%	Yes	Yes	6G-enabled communication channel	Eradicates the safety, confidentiality, and communication issues of the state of art systems with the help of AI.	high storage cost, no disease classification

Table 4. (Continued).

Year	Name of the system	Aim	Delay	Reliability	AI	Blockchain	Communication channel	Merits	Demerits
2020	BATS: Blockchain and AI-based drone-controlled telesurgery system [45]	To provide secure, ultra-responsive, and trusted system by using AI and 6G communication system.	$< 1ms$	99.99999%	Yes	Yes	6G-enabled communication channel	UAV-assisted, transparent with high throughput, lower storage cost, lower packet loss, high data mining gain, and high prediction accuracy with disease classification	Security at the data sensing and storing not provided
2021	RT-TelSurg: real-time telesurgery using cloud, SDN, and fog as infrastructures [81]	To provide a system that can be used in public Internet and generate a higher deadline hit ratio	Low	Acceptable	No	No	Fiber optics for high-quality communication	Reduced end-to-end jitter, reduced delay, priority-based approach, use of scheduling algorithms, and affordable	Not providing optimization techniques
2021	A teleoperate robotic arm using multisensory and support vector machine [82]	An advanced multisensor directing arm working on adjustable sensors and inertial measurement unit	Low	Highly reliable	No	No	EMG and IMU sensor signals for communication	Quality performance, adjusts quickly with patients' body, increased efficiency of a person	Low accuracy

Table 4. (Continued).

Year	Name of the system	Aim	Delay	Reliability	AI	Blockchain	Communication channel	Merits	Demerits
2021	ARei: augmented reality controlled contactless telesurgery robot [83]	Aims to provide immersive experience with augmented data and used for endoluminal intervention	Low	Highly reliable	No	No	Touchless gesture controlled operation using cable-driven device	Decreases the risk of misoperation, decreases the load on doctors	Errors in calibration and registration, lower efficacy
2020	5G robotic telesurgery system [46]	To provide complex remote transoral laser microsurgery on a human adult	102 ± 9 ms	Highly reliable	No	No	5G-enabled telecommunication channel	High bandwidth, ultralow latency, HD 3D visuals, high efficiency, reduced cost, enhanced treatment	High latency for some time during surgery, privacy and security issues, less knowledge about the usage in different areas
2022	Telesurgery system based on metaverse in Healthcare 5.0 [84]	To propose a blockchain and XAI-enabled metaverse-enabled telesurgery system	101.1 ms	Reliable, 90%	Yes	Yes	6G-enabled TI telecommunication channel	Secured through blockchain, interpretable and trustworthy using explainable AI, high accuracy	Data privacy and security issues, hard to implement in real-time applications, required accuracy hard to achieve

The system is comprised of three modes, i.e. an operation site, communication network, which includes Internet, and the surgery site. The master controller is operated at the operation site to direct the patient to the slave end. The surgery site mainly consists of the slave operator, the patient, and the coworkers (nurses). The two sites, i.e. an operation site and surgical site communicate with the help of the Internet as a communication network to transfer the audio-video data and the control signal of the operators/surgeons further to set the local control frequencies of these manipulators to 1 kHz. The factors that can be considered to impact the system are:

- The conducted laparoscopic cholecystectomy through telesurgery was successful and showed positive test results for the patients providing faster recovery.

- The main limitation is implementing the telesurgery system up to a particular distance only. It has numerous issues such as security, high medical cost, and the requirement of the medical license to perform surgery across different countries.

6.2. Telesurgery system using operational master device type of 3PUU

Ryu et al. [80] described a telesurgery structure for spinal operation and showcased the outcomes of the performed experiment. This demonstration uses a 3PUU type of master gadget to operate the slave domain as it can suitably move along the Z-axis. Most of the surgeries are delicately performed in a limited capacity. Here, they have achieved the verification of the system by reflecting doctor's feedback. The advantages and limitations of this system can be explained in two mentioned steps [25]:

- The experiment was performed in a real-time situation to confirm successful operations without any delay. They have considered various issues such as low delay, faster communication, and slow updates in the hardware.

- In the future, the system can be made more reliable and accessible by defining more functions that need to be performed for improving the patients' feedback.

6.3. Healthcare 4.0 Tactile-Internet-enabled telesurgery system

Telesurgery integrated with the 5G network span can deliver medical services to distant places using speedy data delivery with wireless communication networks. For example, Gupta et al. [20] analyzed and presented a tactile Internet-enabled telesurgery system for healthcare 4.0 using a 5G communication network. They have proposed the architecture considering a 5G-enabled network to solve the reliability and scalability issues of the system. Then, they presented a teleslanting-based world's first case study for heart surgery. This study shows that the proposed framework with tactile Internet exhibits better response time and higher trustability than the preexisting telesurgery systems with the following advantages:

- The system ensures ultralow latency, ultrahigh reliability, lower battery consumption, and high density. It improves the potential of telesurgery in telehealthcare for the future.

- In the future, the researchers can work on the issues such as security, confidentiality, and storage cost, which limits its usage in surgical operations.

6.4. AaYusH

To lessen the abovementioned concern in the tactile Internet-based telesurgery system, AaYusH [43], i.e. a smart contract-built telesurgery system for healthcare 4.0 was introduced. The usage of smart contracts resolved the security and privacy issues of the system while patients communicated with the surgeons. They have considered an IPFS protocol to mitigate the data storage issues of the blockchain. Moreover, they also executed a real-time smart contract using Solidity that is being used in the Truffle Suite. The security glitches of this system are tested in the Mythril security analysis tool, and zero errors have been detected. This system has the following advantages and limitations:

- AaYusH framework outperforms all the traditional telesurgery systems in terms of latency and data storage cost. In addition, it provides a secure, efficient, and high-throughput telesurgery system.
- The main limitation of the AaYusH framework is the scalability issues on the different platforms, which need to be discussed in the future.

6.5. HaBiTs

Telesurgery systems still have various security, confidentiality, and interoperability issues, which restricts their applications in medical care. To resolve these issues, Gupta et al. [58] proposed a blockchain-based telesurgery framework suited for healthcare 4.0, i.e. HaBiTs, where reliability and immutability can be attained with the execution of smart contracts. Smart contract can be written as the line of codes using Solidity programming language to initiate the trust and privacy between all the entities interconnected through the blockchain.

The use of smart contracts in the HaBiTs ensures the safety and reliability of the system by eliminating the intermediary or third parties, providing interoperability and trust in the system.

- The main advantage of HaBiTs is the employed blockchain framework, which ensures the privacy of patients' data that will be useful for the doctors while initiating the treatment for the particular disease.
- However, it still has some limitations: there can be some security attacks against the system that needs to be focused so that patients can be motivated to get their treatment in online mode.

6.6. BITS

BITS [44], a blockchain-based smart telesurgery system with a 6G network was introduced, which has enormous potential to dispatch intelligent ultraaccessible healthcare facilities with high reliability and quality. In addition, the traditional system pertaining to safety, confidentiality, and distrust was solved with the use of a smart contract. Moreover, AI algorithms were also incorporated for training surgical robots. The employed 6G communication channel resolves latency issues in exchanging surgical instructions. The advantages and limitations associated with the BITS framework can be mentioned as follows:

- BITS framework outperforms the traditional systems in terms of low latency, high scalability, and low data storage cost.
- There is one limitation of the BITS framework: it should be implemented considering the real-life scenarios.

6.7. BATS

AI has a huge potential in various real-time implementations of healthcare, and one such implementation is robotic surgery or telesurgery. However, issues such as safety, privacy, performance, bandwidth, and transparency are persisting in AI-based telesurgery systems. Influenced by these issues, Gupta et al. [45] designed a blockchain and AI-based telesurgery system called BATS. BATS framework attains better prediction accuracy, high throughput, low data storage cost, and low bandwidth consumption due to the usage of IPFS storage protocol. Furthermore, several benefits and limitations can be associated with the BATS framework.

- The BATS telesurgery system facilitates various benefits such as low latency, security, efficiency, and a transparent environment for the patients.
- There can be one limitation associated with this telesurgery system: it needs to be implemented in a real-time scenario considering the execution of smart contracts in the future.

6.8. RT-TelSurg

Sedaghat et al. [81] proposed a novel real-time network system, i.e. RT-TelSurg. One approach to achieve real-time telesurgery is to utilize fog and cloud networks with the help of software-defined networking (SDN) as a framework. The presented telesurgery system is operated according to the efficiency specifications. The outcome of the proposed system shows that the mean deadline hit ratio is 98.2% in varied situations of operation, which is acceptable for telesurgery systems. The merits and demerits of the RT-TelSurg can be mentioned as follows:

- The merits of the RT-TelSurg system have been estimated to achieve the real-time demands of the patients and surgeons. The study shows that the communication features that mainly determine the efficiency of a telesurgery system include end-to-end jitter and deadline hit ratio discussed in the RT-TelSurg.
- The demerits of the proposed system involve the need for the enhancement of the security and stability of the telesurgery system. Additionally, the dispersed SDN should be explored for better functioning.

6.9. Teleoperate robotic arm based on multisensory and support vector machine

Chu et al., in [82], proposed the advanced developments in telesurgery system, i.e. a physiological sensor-directed robotic arm deployed on inertial measurement unit (IMU) and electromyography (EMG). It works based on the processing capacity of the data gathered with the help of these detectors embedded on the human body by implementing the support vector machine. It potentially increases the human-robotic interaction in the system. The factors affecting the system can be described as follows:

- The advantages of the distant operated robotic arm involve swiftly adjusting the end user's body with higher accuracy and quality performance.
- It should be more focused on the industrial field to improve the employee's efficiency within the organization.

6.10. Teleoperated robotic microinjection system

Feng et al. [93] proposed a teleoperated robotic framework providing haptic feedback devoted to living microinjection. The system is comprised of a slave controller device and a procedure-based master device. The microcontroller equipped with microfocus detectors performs the microinjection function. A surgeon operates the patient-side device with the help of master-side devices such as haptic devices and touch devices. Here, the haptic devices are based on the functional concept of the syringe. It enables a controller to sense the microinjection procedure when the controller gets the hold on hands.

Furthermore, the location tracking outcomes show that the patient-side microcontroller follows the orders of the surgeon-side device precisely. With the advent of built-in haptic devices, the doctor can sense the touch and decide the injection report to improve the performance status of the microinjection function. The pros and cons of the proposed system are as follows:

- The system proves to be positive in reducing the risk of failed injections by combining haptic feedback and microscopic visual services. However, the efficiency and flexibility of microinjection increase with the help of location mapping to further permit the microcontroller to grasp spatial motion in multiaxis connection modes.
- The limitations of the system include errors in the position tracking, and the reaction rate of haptic feedback needs to be improved for microinjection applications.

6.11. ARei

Lin et al. [83] designed a touchless teleoperated robot, i.e. ARei, which mainly focuses on providing mesmerizing experiences with the help of virtual reality. ARei consists of noncognitive data obtained from an electromagnetic sensor and the head-mounted display (HMD) device. The contactless telesurgery system dominates the system and reinforces the motion-sensing mechanisms. The system with its advantages and limitations can be described as follows:

- The system is advantageous as it enhances the detailed recognition of the sensor's adjustable devices in the survey, enabling the surgeon to use a hand-operated joystick. It also helps to reduce the threat of infection, especially in a global medical situation.
- The system needs to improve the efficacy of the touchless telesurgery system to outperform the traditional telesurgery systems.

7. The proposed system

The integration of remote surgery systems in healthcare has improved the quality of life. It has two main layers, i.e. the slave and the master layer, which consists of a communication channel to pass the instructions for operation and haptic feedback. These instructions are produced from various sensor devices through the patient domain for better functioning of the system. However, traditional telesurgery systems are exposed to security attacks such as DoS, spoofing, tampering, repudiation, etc. An attacker can easily manipulate the remote telesurgery system's data to misguide the surgeons and patients during surgery. Therefore, there is a real need for a secure system with minimum delay and high reliability that can be trusted to protect patients from malicious attackers. Thus, we have federated learning to perform the secure processing of patients' data so that healthcare professionals can prescribe medicines based on their medical conditions for early and correct treatment. However, the federated learning model does not guarantee to preserve and protect the patient's critical health information due to global data storage. To deal with the data privacy and confidentiality issues, Blockchain layer is introduced to confirm the immutable, decentralized, and transparent data transactions between patients and surgeons during telesurgery. Figure 5 shows the working of the proposed framework divided into four layers, which are 1) slave layer, 2) federated learning layer, 3) blockchain layer, and 4) master layer. A comprehensive explanation of each layer is as follows:

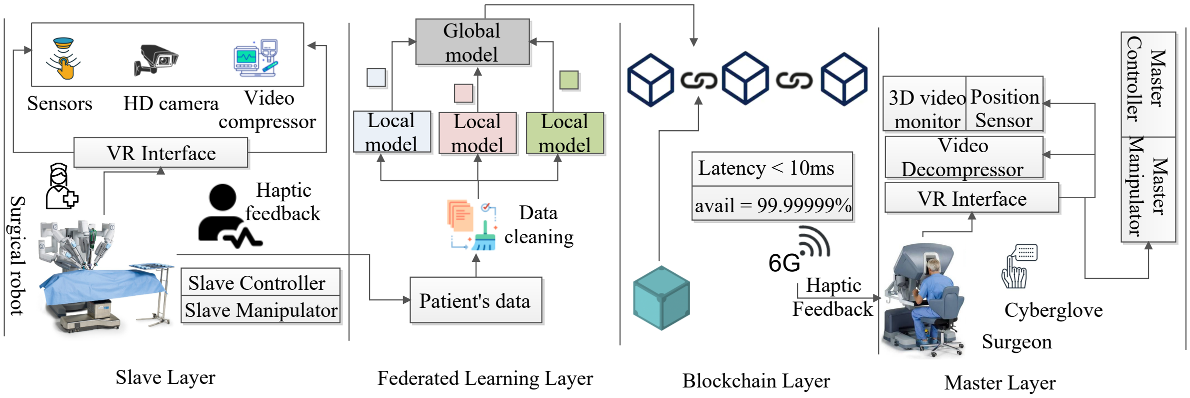


Figure 5. Blockchain and federated learning-based secure telesurgery system.

7.1. Slave layer

The slave layer is often termed the patient layer in which a surgical robot performs the simultaneous operational instructions acquired from the distant master side. The slave layer consists of medical staff, such as nurses to monitor the surgical robot at the telesurgery. The surgical robot is also known as the slave as it accepts the commands stated by the surgeons at different locations. Furthermore, healthcare professionals can treat patients with the help of instructions given to the surgical robot equipped with the camera and instruments to perform the surgical treatment. It uses sensors to interchange instantaneous haptic information such as feeling, sensing the touch, and motion. This layer consists of sensors and actuators (also known as haptic devices), a video compressor, HD display cameras, a microphone, an augmented reality interface (to provide a 3D HD video display), haptic feedback, a slave controller, surgical assistance, and slave manipulator.

After executing the telesurgery operations, the patients and medical staff (nurses) can thoroughly give their feedback in an opinion poll. It further helps to calculate the doctor's performance rating, which facilitates patients in choosing their doctor for remote operations. However, the operation's necessity is based on the severity of the patients' health, which can be determined with the help of a federated learning layer. The performance rating and wallet balance of the surgeon are stored in the blockchain. Any patient can demand the needed doctor to the master operational site for the required surgery. Furthermore, the hospital management can manage the availability of the required surgeon. Patients' health symptoms and haptic feedback can now be stored in the blockchain through the intermediary IPFS. However, before storing the data, it needs to be passed through the federated learning layer for further data preprocessing and to process the patients' data globally. Suppose patients' critical health information has not been made secure in the telesurgery procedure. In that case, any malicious attacker can forge the patient's confidential data, which can lead to the detriment of their health due to the medicines prescribed by the doctors. Thus, we have to forward the data extracted by the sensors to the federated learning layer for further data preprocessing and globalize the data for security purposes.

7.2. Federated learning layer

We have integrated federated learning with the proposed system to secure and preserve the patients' health data, only reflecting the specific information to the users. The data collected from the slave layer through sensors and actuators is passed to the federated learning layer. Foremost, the federated learning model performs the data cleaning on the patients' confidential data to eliminate the missing and imbalanced values. Then, federated learning ensures that the health data of the different patients, such as heart rate, blood pressure, and pulse rate, can be trained at the local model to segregate it into a global model. However, the data at the local model can overburden the system, affecting the performance of the communication between patients and doctors. For example, patients with critical health issues require urgent medical assistance to treat their disease. However, due to the high communication overhead between data transactions of patients and surgeons, patients can face some delay in their treatment which can further deteriorate their health. Therefore, federated learning is utilized to process patients' health data at the global model instead of the local one. Moreover, using federated learning ensures that only specific patients' health information will be visible to outsiders ensuring security and trust in the system. Now, preprocessed global data associated with the patients' health can be passed through the blockchain layer to store their health data in the IPFS, resolving the data storage cost issues of the blockchain.

7.3. Blockchain layer

In this layer, we consider an ethereum-based blockchain, i.e. a distributed ledger that works in a decentralized way to store the data securely. The blockchain-based framework in the telesurgery procedure ensures security and trust in the communication process among patients and surgeons. Blockchain as a decentralized framework provides the secure and trusted storage of patients' health data and their related instructions into the unalterable blocks with the help of the execution of smart contracts. If a patients' health data needs to be added to the blockchain network, then it should be authenticated initially by the smart contract. Therefore, blockchain technology with its data integrity, nontampering, decentralized, and transparent characteristics, proves to be beneficial for telesurgery systems in terms of security and reliability. It facilitates secure communication between patient and surgeon in telesurgery by protecting data against several security attacks such as data spoofing, data manipulation, and cyber attacks. Smart contracts are simply a line of codes stored on a blockchain, which executes based on the fulfillment of certain conditions. Therefore, it eliminates the need for the third party to protect the patients' data from manipulation so that surgeons can cure them according to the severity of the disease.

Before initiating the surgery, surgeons need to register themselves through the hospital authority, which validates their authenticity for the execution of surgery. Then, smart contracts execute to decide whether surgery is required for the patient or not according to their disease. This prediction is performed at the federated learning layer in which a patients' health symptoms get stored into a global model after preprocessing. Therefore, if all the smart contract and blockchain conditions are fulfilled, surgery can be performed securely and appropriately. Now, to satisfy the condition of storing data in IPFS, first condition, i.e. smart contract as self-executing lines of code, should be executed to confirm the validity of patient and surgeon's identity in telesurgery procedure. If smart contract conditions are fulfilled, participants can be considered for data storage in IPFS. Blockchain through an intermediary, i.e. IPFS protocol, can now execute data transactions to perform the surgical procedures for patients' treatment. Moreover, executing surgical procedures with the help of IPFS over a 6G network ensures reliable, secure, and scalable communication between patient and surgeon. Furthermore, IPFS facilitates low-cost data storage for the patient due to its property to store data in the form of a hash.

7.4. Master layer

The master layer (surgeon layer) incorporates many surgeons interconnected distantly to perform telesurgery operations at the patient side through 6G communication channels. The initiation process starts for the remote surgery, the doctors are to be registered with hospital management, and this registered information must be stored in the blockchain for peer-to-peer information knowledge. As blockchain is decentralized, the data stored on one block is spread across the participating systems in the architecture. This process increases trust and transparency among the patients for the doctor who will operate on them in the telesurgery system. Furthermore, various components are implemented in the master layer, that is: virtual reality interfaces of the surgery site that facilities the doctor in a remote region for viewing the situation accurately through 3D video display of operation site, a master regulator that is the surgeon's GUI system, the manipulator is provided to the surgeon to control the surgical robot on the remote site, smart sensors are also provided that give the surgeon the exact scenario outlook such as foot pedals, the microphone is provided to guide the medical staff around the surgery site, a human-machine interaction system to efficiently interact with the surgical robot, and various audio devices providing audio messages from the surgery site. The instructions that direct the surgical robot are interchanged through the blockchain network in a safe and preserved environment. The master side also receives haptic feedback from the slave layer to sense the real-time procedures. This feedback can be video, audio, rapidness, and exertion. Once the remote surgery is accomplished, the surgeons obtain rankings from the patients and the medical staff at the slave side. The rankings that the patients provide are assigned to the surgeon based on the experience of staff and patients. These rankings can be further used by following patients to decide the surgeon for surgery. Providing this feature increase the reliability and trust regarding the system among its users (patients).

Figure 6 shows the sequence flow of the proposed telesurgery system, which includes the background concepts such as healthcare 1.0 to 5.0, telesurgery, and surgical robots. Furthermore, the role of AI, a taxonomy of several security attacks, and communication issues have been explained in detail to get insights into the telesurgery system. Furthermore, traditional telesurgery systems have been considered to highlight their disadvantages to propose a blockchain and federated learning-based secure telesurgery system which comprises several layers such as slave layer, federated learning layer, blockchain layer, and master layer. Moreover, a dataset is considered to simulate the results for the proposed system in terms of data offloading, latency, and data storage cost. Finally, sequence flow highlights the open issues and research opportunities associated with the telesurgery system.

8. Results and discussion

The concept of telesurgery systems for remote monitoring of patient can prove to be a promising technology for patients' health. However, a security vulnerability is also associated with the patients' health data, leading to the transfer of misinterpreted feedback to the surgeon. Therefore, we have proposed a blockchain and federated learning-based secure telesurgery system for secure and trusted monitoring of patients' health. Furthermore, we have considered a dataset for patients' healthcare that includes blood sugar, blood pressure, heart rate, etc., which is being passed to the federated learning model to train the model globally to enhance the data offloading. Furthermore, we have introduced the blockchain to secure and preserve the global healthcare data of patients for transferring the correct feedback to the surgeon. The simulation results are performed by executing the smart contract of the proposed system which involves data transactions between patient and surgeon to prescribe treatment based on their disease through the usage of a wallet associated with the participants in the system. We have used the Solidity programming language to perform the execution of smart contract of the proposed system considering the performance evaluation metrics, i.e. data offloading, latency, and data storage cost. Moreover, initially, data is being processed using federated learning to improve the data offloading of the system. Federated learning is implemented in the Google Colaboratory, which is an online

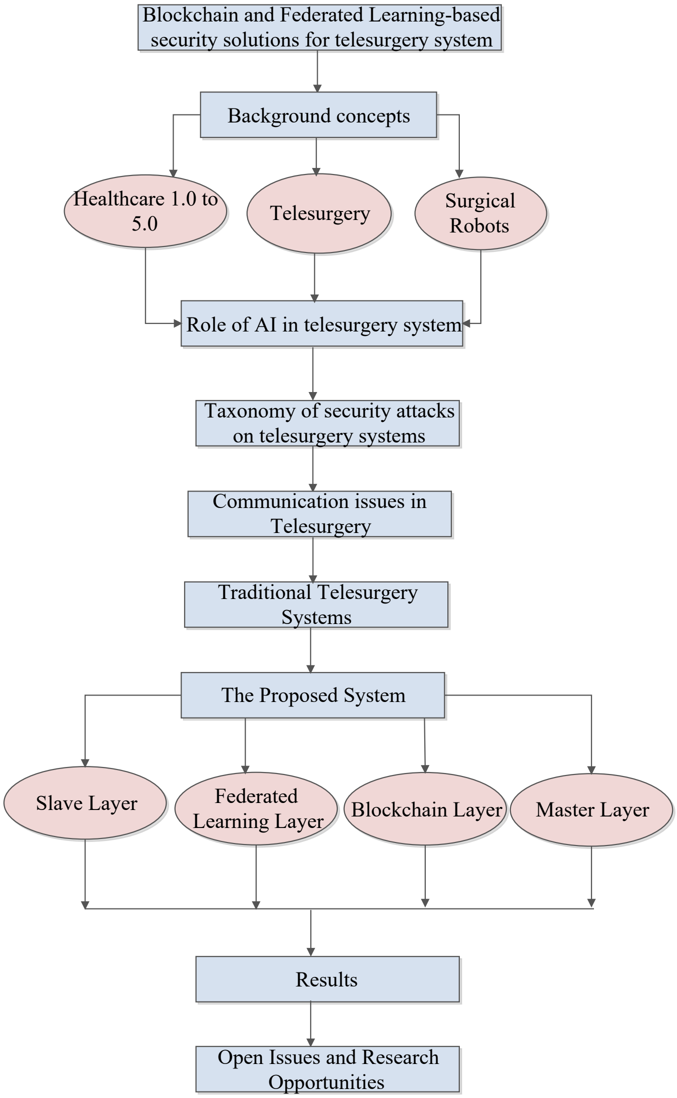

Blockchain and Federated Learning-based security solutions for telesurgery system
Background concepts
Healthcare 1.0 to 5.0
Telesurgery
Surgical Robots
Role of AI in telesurgery system
Taxonomy of security attacks on telesurgery systems
Communication issues in Telesurgery
Traditional Telesurgery Systems
The Proposed System
Slave Layer
Federated Learning Layer
Blockchain Layer
Master Layer
Results
Open Issues and Research Opportunities

Figure 6. Sequence flow of the proposed system.

platform to execute arbitrary python code via browser. In Google Colaboratory, we utilize the TensorFlow federated learning application programming interface (API) that allows simulating dataset values, arranging the dataset into a subset of client devices, and call a pretrained Keras model. With this API, we converted our dataset into a distributed dataset using (client_data()), which is fed into the Keras model. Then, we used *tff.learning.algorithms*, *tf.keras.optimizers* to train the federated dataset. Finally, the result is fetched using *result.state* and *result.metrics*.

8.1. Data description

We have considered a patients' healthcare dataset, which consists of 303×14 number of rows and columns including various features such as blood pressure, heart rate, blood sugar, etc.[9]. Firstly, the healthcare data

[9] https://www.kaggle.com/datasets/redwankarimsony/heart-disease-data

is considered for data preprocessing to eliminate the missing values and normalized values in the features of the considered dataset. Then, this healthcare data is passed to the federated learning model to train the model globally for preserving the confidential patients' data. The data is then transmitted to the blockchain integrated with the IPFS using a 6G network to resolve the security, latency, and data storage issues considering the parameters such as latency, data offloading, and data storage cost.

8.2. Data offloading

Figure 7a depicts the comparison of data offloading of the proposed system with the rise in the number of data transactions with the traditional system which is proposed by Gupta et al. [45]. Therefore, it can be evident from the graph that the proposed system with a federated learning model works in a better way than the traditional system with the surge in the number of transactions among patients and surgeons. Using a federated learning model ensures that patients' data is being trained at the local model, which is segregated into the global model to lessen the system's burden. On the other hand, Gupta et al. utilized a blockchain and AI-based framework for telesurgery system which can overburden the system due to the whole data processed at a local model or centralized server which affects overall data offloading in the system.

8.3. Latency

Figure 7b shows the comparison of latency of the proposed system with the different communication networks such as 5G and 4G. The graph of latency seems to exhibit better performance as the number of transactions increases in the case of the proposed system with 6G networks instead of 4G and 5G networks. It means that using a 6G network with the proposed system ensures efficient communication between patient and surgeon so that disease can be cured without any delay.

8.4. Data storage cost

Figure 7c depicts the survey of data storage cost of the proposed system with the traditional system using blockchain as data storage. It can be observed from the graph that usage of IPFS protocol with the blockchain-based proposed system yields better results than using blockchain, ensuring the cost-efficient system for patients and surgeons to store their data in the IPFS. However, with fewer transactions, both, i.e. IPFS with the proposed system and traditional system with blockchain exhibit the same results in terms of cost. Therefore, the proposed system with IPFS provides patients and surgeons with the privilege of low-cost data storage.

Moreover, we can compute the data storage cost of the transactions performed between patients and surgeons in telesurgery system utilizing the blockchain network considering the metrics that is expressed as gas price associated with a single word (β^{ω}) and to store 1KB of data (β^{ω}_{Kb}) in blockchain. The gas prices $\{\beta^{\omega}$, $\beta^{\omega}_{Kb}\}$ can be mentioned as follows:

$$\beta^{\omega} = 2 * 10^4 Gas \tag{1}$$

$$\beta^{\omega}_{Kb} = (2^{12}/256 * 10^2) * (2 * 10^4) Gas \tag{2}$$

Next, we have to consider M number of words in blockchain to determine the data storage cost (Δ^M) with the help of parameters, i.e. gas price and Ethereum price that is denoted by $\{\beta^{Pr}, \alpha^{Pr_{bc}}\}$ equivalent to {23.186 *gwei*, 232.96 USD}. Therefore, the calculation of Δ^M can be performed with the consideration of $\alpha = 10^9$, which is defined as follows:

$$\Delta^{M} = (m * G^{a})/\alpha \tag{3}$$

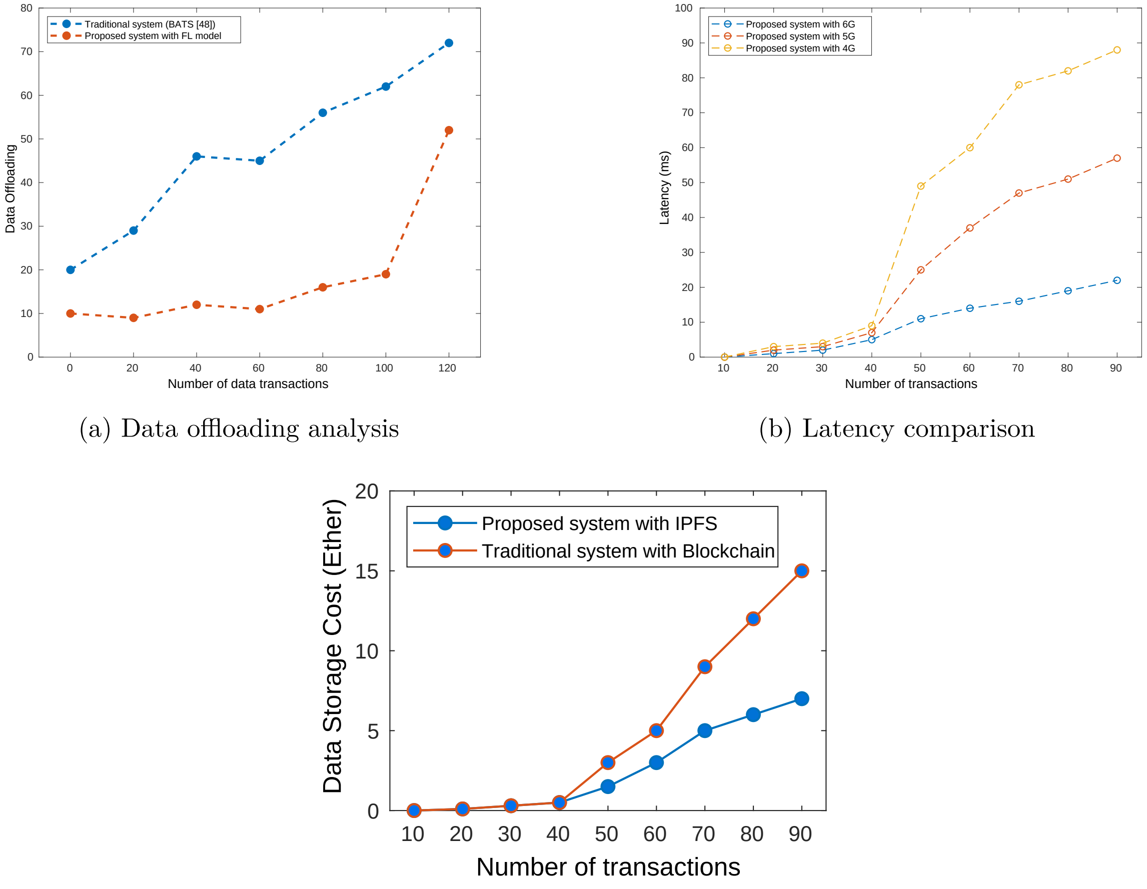
Therefore, the M number of words can be stored in blockchain in USD with data storage cost of $\Delta^{M_{USD}}$, which is expressed as follows:

$$\Delta^{M_{USD}} = (\beta^{Pr} * \Delta^{M}) * \alpha^{Pr_{bc}} \tag{4}$$

Finally, data storage cost of K words in USD can be determined by observing the parameters D_c^K, Gs_{pr}^b, E_{pr}^b, that can be represented as follows:

$$D_c^{K_{USD}} = (Gs_{pr}^b * D_c^K) * E_{pr^b} \tag{5}$$

Thus, the data transactions between patient and surgeon can be stored in blockchain through the usage of IPFS with the strengthened cost-efficiency which further benefits the patients and surgeons for data storage [94].



(a) Data offloading analysis

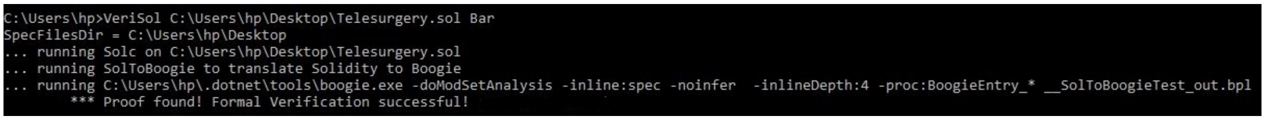
(b) Latency comparison

(c) Data storage cost comparison

Figure 7. Performance comparison of the proposed system with the traditional approaches considering networks, IPFS, and federated learning

8.5. Security verification of the proposed system

Before deploying the smart contract of the proposed system on blockchain, we need to check for existence of any threats or bugs to prevent malicious attackers from manipulating the data transactions between patient and surgeon in the telesurgery system. Therefore, we have considered the Verisol security analysis tool which is developed based on the Boogie tool chain to verify and validate smart contract of the blockchain and federated learning-based telesurgery system to check for any kind of bug or vulnerability for secure treatment. Figure 8 depicts the formal verification of the proposed system over Verisol by considering smart contract as an input which shows that the analysis is performed without any threat [95]



```
C:\Users\hp>VeriSol C:\Users\hp\Desktop\Telesurgery.sol Bar
SpecFilesDir = C:\Users\hp\Desktop
... running Solc on C:\Users\hp\Desktop\Telesurgery.sol
... running SolToBoogie to translate Solidity to Boogie
... running C:\Users\hp\.dotnet\tools\boogie.exe -doModSetAnalysis -inline:spec -noinfer  -inlineDepth:4 -proc:BoogieEntry_* __SolToBoogieTest_out.bpl
        *** Proof found! Formal Verification successful!
```

Figure 8. Security analysis of smart contract over Verisol.

9. Open issues and research challenges/future challenges and research opportunities

In this section, we discuss the challenges of the telesurgery system and areas for future research opportunities.

9.1. Collaborative issues

These issues are generally not focused on but play a huge role in the establishment and usage of telesurgery systems over the world. Doctors used to avoid robotic surgery due to the minimum information about telesurgery's complex procedures and technologies. Surgeons usually have to remotely operate the patients who are separated by international borders, face issues such as billing, insurance coverage, ethics, and medical laws that keep on changing over the regions. There should be a universal law for the efficient functioning of telesurgery systems to prevent security attacks. Manufacturing companies should also be made to promote robotic surgery. The companies should deliver free training and simulation processes to surgeons in varied developing countries, which will reduce the operational cost for training which is generally high as discussed in [96].

9.2. Stability and security issues

The reliability and security of the telesurgery systems play an essential part in accomplishing distant surgery. Remote surgery is more complicated to implement than the physical execution of the surgery in hospitals. Based on the emergency condition, doctors can choose the surgical methodology and solutions which require complex tools and manpower to perform the surgical procedure. Furthermore, it can raise several security issues, which can be fatal to a patients' health. Both the personal and medical records of the patient and surgeon can be hacked, which can lead to numerous privacy issues. Telesurgery systems have a remarkable impact on the growth and globalization of telemedicine. The communication and virtual frameworks of telesurgery systems need multidisciplinary and versatile technological advancement to meet the needs of different patients as surveyed in [26]. Otherwise, it can raise several security issues in the system.

9.3. Investment and operating cost

Many developing countries are still unable to afford the initial infrastructure and complex robotic surgery due to the high cost of implementing these procedures. Furthermore, the cost is overburdened by the rising price

the organization has to pay for an efficient and reliable communication network. In addition, the surgical robots used in telesurgery require special sterilized equipment. The cost of a single replacement of these tools is also soaring, which results in disparity in returns and investment costs;hence, it becomes difficult for general hospitals to implement.
Wireless communication and low latency increase the need for intercommunication tools and transmission media, further increasing the prices. True globalization of telesurgery can only be attained if the cost of robotic framework and networking lessens to an economical rate for every country. These cost issues can be resolved if a global license for robotic platforms is provided to the manufacturers universally. Therefore, as the demand for production increases, the market price will automatically decrease, thereby escalating the need for telesurgery system as mentioned in [97].

9.4. High latency and low reliability

Highly reliable and low-latency high-speed network connection is extremely important for telesurgery systems. Delay time is a concern in traditional telesurgery systems, leading to safety issues by establishing erroneous and increasing the unnecessary surgery duration. The 5G network has decreased latency time from the present 0.27 s to 0.01 s [43]. Applied 5G network in telesurgery procedures in various hospitals in different cities prove reliable for the system. However, a 6G network exhibits potentially reduced latency time, i.e. 1 microsecond, and provides ultrahigh reliability, which can prove to be the finest communication technology in the systems [44].

9.5. Lack of feedback

Feedback availability is crucial during complex and delicate telesurgical operations to adjust the input instructions adequately and avoid excessive forces such as damaging the tissues and fraudulent use of equipment. Force feedback in telesurgery should be available to eliminate challenges related to the instrumentation and stability of robots. These challenges can be achieved by implementing various haptic feedback sensors and advanced instrumentation technologies connected to the master and slave model to provide an intercommunication facility [98]. It is essential to implement feedback at both sides, i.e. patient and surgeon side, as the surgeons can perform accurate surgery with the help of knowledge about the events at the patient side. The patient giving feedback can rate the surgeon based on the skills and operation to help upcoming patients while choosing the surgeon, which can prove advantageous to correct the practice and perform more efficiently.

10. Conclusion

This paper presents an exhaustive survey on secure telesurgery systems, which consists of the evolution of healthcare and telesurgery, and the role of AI in telesurgery systems. A comparative analysis of various state-of-the-art telesurgery systems and surgical robots has been presented. We have analyzed the different traditional telesurgery systems and the associated security issues that can deteriorate the patients' health. We then propose a blockchain and federated learning-based system to secure the communication between patient and surgeon during the surgical procedure. The applied federated learning model with blockchain ensures improved data offloading and preserves the patients' health data by storing the data securely at a global model. Next, we explored several issues and research challenges arising in the telesurgery systems. The results for the proposed system have been evaluated against the parameters such as latency, data offloading, and data storage cost.

Acknowledgments

This work is supported by Visvesvaraya PhD Scheme for Electronics and IT by Department of Electronics and Information Technology (DeiTY), Ministry of Communications and Information Technology, Government of India (MEITY-PHD-2828).

Contribution of authors

S.C. and R.K. wrote the paper, R.G. drew the diagrams and flow, and S.T. and S.A. gave the conceptual idea and flow of the paper.

References

[1] Devedžić G, Koceski S, Savić SP. A Brief Overview of Enabling Technologies for Digital Medicine and Smart Healthcare. In: 2021 10th Mediterranean Conference on Embedded Computing (MECO); Budva, Montenegro; 2021. pp. 1-5, doi: 10.1109/MECO52532.2021.9460172.

[2] Sokolova AV, Buldakova TI. Network Architecture of Telemedicine System for Monitoring the Person's Condition. In: 2021 3rd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA); Lipetsk, Russian Federation; 2021. pp. 361-365, doi: 10.1109/SUMMA53307.2021.9632199.

[3] Mistry C, Thakker U, Gupta R, Obaidat MS, Tanwar S et al. MedBlock: An AI-enabled and Blockchain-driven Medical Healthcare System for COVID-19. In: ICC 2021 - IEEE International Conference on Communications; Montreal, QC, Canada; 2021. pp. 1-6, doi: 10.1109/ICC42927.2021.9500397.

[4] Asif MRA, Khondoker R. Cyber Security Threat Modeling of A Telesurgery System. In: 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI); Dhaka, Bangladesh; 2020. pp. 1-6, doi: 10.1109/STI50764.2020.9350452.

[5] Butner SE, Ghodoussi M. Transforming a surgical robot for human telesurgery. IEEE Transactions on Robotics and Automation 2003; 19 (5): 818-824. doi: 10.1109/TRA.2003.817214.

[6] Kaur J, Verma R, Alharbe NR, Agrawal A, Khan RA. In: Tanwar S (editor). Fog Computing for Healthcare 4.0 Environments: Importance of Fog Computing in Healthcare 4.0. 1st ed. Springer International Publishing, pp. Cham, 2021, pp. 79-101, doi: 10.1007/978-3-030-46197-3_4.

[7] Aggarwal S, Kumar N, Alhussein M, Muhammad G. Blockchain-Based UAV Path Planning for Healthcare 4.0: Current Challenges and the Way Ahead. IEEE Network 2021; 35 (1): 20-29. doi: 10.1109/MNET.011.2000069.

[8] Masuda Y, Zimmermann A, Shepard DS, Schmidt R, Shirasaka S. An Adaptive Enterprise Architecture Design for a Digital Healthcare Platform : Toward Digitized Society – Industry 4.0, Society 5.0. In: 2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW); Gold Coast, Australia; 2021. pp. 138-146, doi: 10.1109/EDOCW52865.2021.00043.

[9] Elprama SA, Kilpi K, Duysburgh P, Jacobs A, Vermeulen L et al. Identifying barriers in telesurgery by studying current team practices in robot-assisted surgery. In: 2013 7th International Conference on Pervasive Computing Technologies for Healthcare and Workshops; Brussels, Belgium; 2013. pp. 224-231, doi: 10.4108/icst.pervasivehealth.2013.252005.

[10] Tanwar S, Kumar N, Niu JW. EEMHR: Energy-efficient multilevel heterogeneous routing protocol for wireless sensor networks. International Journal of Communication Systems 2014; 27 (9): 1289– 1318. doi: 10.1002/dac.2780.

[11] Sobhan S, Islam S, Valero M, Shahriar H, Ahamed SI. Data Analysis Methods for Health Monitoring Sensors: A survey. In: 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC); Madrid, Spain; 2021. pp. 669-676, doi: 10.1109/COMPSAC51774.2021.00097.

[12] Amin S, Salahuddin T, Bouras A. Cyber Physical Systems and Smart Homes in Healthcare: Current State and Challenges. In: 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT); Doha, Qatar; 2020. pp. 302-309, doi: 10.1109/ICIoT48696.2020.9089638.

[13] Sadawi AA, Hassan MS, Ndiaye M. A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges. IEEE Access 2021; 9: 54478-54497. doi: 10.1109/ACCESS.2021.3070555.

[14] Mahmoud MME, Rodrigues JJPC, Saleem K. Cloud of Things for Healthcare: A Survey from Energy Efficiency Perspective. In: 2019 International Conference on Computer and Information Sciences (ICCIS); Sakaka, Saudi Arabia; 2019. pp. 1-7, doi: 10.1109/ICCISci.2019.8716388.

[15] Saranya P, Asha P. Survey on Big Data Analytics in Health Care. In: 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT); Tirunelveli, India; 2019. pp. 46-51, doi: 10.1109/ICSSIT46314.2019.8987882.

[16] Verma C, Stoffová V, Illés Z, Tanwar S, Kumar N. Machine Learning-Based Student's Native Place Identification for Real-Time. IEEE Access 2020; 8: 130840-130854. doi: 10.1109/ACCESS.2020.3008830.

[17] Cai Q, Wang H, Li Z, Liu X. A Survey on Multimodal Data-Driven Smart Healthcare Systems: Approaches and Applications. IEEE Access 2019; 7: 133583-133599. doi: 10.1109/ACCESS.2019.2941419.

[18] Nguyen DC, Ding M, Pathirana PN, Seneviratne A, Li J et al. Federated Learning for Internet of Things: A Comprehensive Survey. IEEE Communications Surveys & Tutorials 2021; 23 (3): 1622-1658. doi: 10.1109/COMST.2021.3075439.

[19] Elmoghazy S, Yaacoub E, Navkar NV, Mohamed A, A. Erbad. Survey of Immersive Techniques for Surgical Care Telemedicine Applications; In: 2021 10th Mediterranean Conference on Embedded Computing (MECO); Budva, Montenegro; 2021. pp. 1-6, doi: 10.1109/MECO52532.2021.9460135.

[20] Gupta R, Tanwar S, Tyagi S, Kumar N. Tactile-Internet-Based Telesurgery System for Healthcare 4.0: An Architecture, Research Challenges, and Future Directions. IEEE Network 2019; 33 (6): 22-29. doi: 10.1109/MNET.001.1900063.

[21] Jin ML, Brown MM, Patwa D, Nirmalan A, Edwards PA. Telemedicine, telementoring, and telesurgery for surgical practices. Current problems in surgery 2021; 58 (12): 100986. doi: 10.1016/j.cpsurg.2021.100986.

[22] Bailo P, Gibelli F, Blandino A, Piccinini A, Ricci G et al. Telemedicine Applications in the Era of COVID-19: Telesurgery Issues. International Journal of Environmental Research and Public Health; 19 (1): 323. doi: 10.3390/ijerph19010323.

[23] Zhang Q, Liu J, Zhao G. Towards 5G enabled tactile robotic telesurgery. CoRR 2018; abs/1803.03586. doi: 10.48550/arXiv:1803.03586.

[24] Tiwari K, Kumar S, Tiwari RK. Fog Assisted Healthcare Architecture for Pre-Operative Support to Reduce Latency. Procedia Computer Science 2020; 167: 1312-1324. doi: 10.1016/j.procs.2020.03.447.

[25] Gupta S, Patel R. Survey on Secure Telesurgery Systems for Healthcare 4.0: A Comparative Analysis. GIT-Journal of Engineering and Technology 2021; 13: 136-140.

[26] Xia SB, Lu QS. Development status of telesurgery robotic system. Chinese Journal of Traumatology 2021; 24 (3): 144-147. doi: 10.1016/j.cjtee.2021.03.001.

[27] Aghanouri M, Kheradmand P, Mousavi M, Moradi H, Mirbagheri A. Kinematic and Workspace Analysis of the Master Robot in the Sinaflex Robotic Telesurgery System. In: 2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC); Mexico; 2021. pp. 4777-4780, doi: 10.1109/EMBC46164.2021.9629933.

[28] Kadu A, Singh M. Comparative Analysis of e-Health Care Telemedicine System Based on Internet of Medical Things and Artificial Intelligence. In: 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC); Trichy, India; 2021. pp. 1768-1775, doi: 10.1109/ICOSEC51865.2021.9591941.

[29] Luong DA, Park JH. Privacy-Preserving Blockchain-Based Healthcare System for IoT Devices Using zk-SNARK. IEEE Access 2022; 10: 55739-55752, 2022. doi: 10.1109/ACCESS.2022.3177211.

[30] Zhang G, Yang Z, Liu W. Blockchain-based privacy preserving e-health system for healthcare data in cloud. Computer Networks: The International Journal of Computer and Telecommunications Networking 2022; 203: 108586. doi: 10.1016/j.comnet.2021.108586.

[31] Sezer BB, Topal S, Nuriyev U. TPPSUPPLY : A traceable and privacy-preserving blockchain system architecture for the supply chain. Journal of Information Security and Applications 2022; 66: 103116. doi: 10.1016/j.jisa.2022.103116.

[32] Mamoun R, Nasor M, Abulikailik SH. Acceptance of Telemedicine and E-Health Applications in Developing Countries. In: 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE); Khartoum, Sudan; 2021. pp. 1-5, doi: 10.1109/ICCCEEE49695.2021.9429558.

[33] EL-Hasnony IM, Elhoseny M, Tarek Z. Telemedicine and smart systems techniques for COVID-19: a systematic review. In: The 2nd International Conference on Distributed Sensing and Intelligent Systems (ICDSIS 2021); Online Conference; 2021. pp. 232-246, doi: 10.1049/icp.2021.2679.

[34] Hassanzadeh-Nazarabadi Y, Küpçü A, Özkasap Ö. LightChain: Scalable DHT-Based Blockchain. IEEE Transactions on Parallel and Distributed Systems 2021; 32 (10): 2582-2593. doi: 10.1109/TPDS.2021.3071176.

[35] Chen C, Loh EW, Kuo KN, Tam KW. The Times they Are a-Changin'–Healthcare 4.0 Is Coming!. Journal of Medical Systems 2020; 44 (2). doi: 10.1007/s10916-019-1513-0.

[36] Subramoniam S, Sadi S. Healthcare 2.0. IT Professional 2010. 12 (6): 46-51. doi: 10.1109/MITP.2010.66.

[37] Bhattacharya P, Tanwar S, Shah R, Ladha A. In: Singh P, Kar A, Singh Y, Kolekar M, Tanwar S (editors). Mobile Edge Computing-Enabled Blockchain Framework—A Survey. In: Proceedings of ICRIC. Lecture Notes in Electrical Engineering, vol 597. Springer International Publishing, Cham, 2019, pp. 797-809. doi: 10.1007/978-3-030-29407-6_57

[38] Wehde MB. Healthcare 4.0. IEEE Engineering Management Review 2019; 47 (3): 24-28. doi: 10.1109/EMR.2019.2930702.

[39] Gupta R, Shukla A, Mehta P, Bhattacharya P, Tanwar S et al. VAHAK: A Blockchain-based Outdoor Delivery Scheme using UAV for Healthcare 4.0 Services. In: IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS); Toronto, ON, Canada; 2020. pp. 255-260, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162738.

[40] Bhattacharya P, Tanwar S, Bodkhe U, Tyagi S, Kumar N. BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications. IEEE Transactions on Network Science and Engineering 2021; 8 (2): 1242-1255. doi: 10.1109/TNSE.2019.2961932.

[41] Kumar A, Krishnamurthi R, Nayyar A, Sharma K, Grover V et al. A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes. IEEE Access 2020; 8: 118433-118471. doi: 10.1109/ACCESS.2020.3004790.

[42] Mohanta B, Das P, Patnaik S. Healthcare 5.0: A Paradigm Shift in Digital Healthcare System Using Artificial Intelligence, IOT and 5G Communication. In: 2019 International Conference on Applied Machine Learning (ICAML); Bhubaneswar, India; 2019. pp. 191-196, doi: 10.1109/ICAML48257.2019.00044.

[43] Gupta R, Shukla A, Tanwar S. AaYusH: A Smart Contract-Based Telesurgery System for Healthcare 4.0. In: 2020 IEEE International Conference on Communications Workshops (ICC Workshops); Dublin, Ireland; 2020. pp. 1-6, doi: 10.1109/ICCWorkshops49005.2020.9145044.

[44] Gupta R, Thakker U, Tanwar S, Obaidat MS, Hsiao K-F. BITS: A Blockchain-driven Intelligent Scheme for Telesurgery System. In: 2020 International Conference on Computer, Information and Telecommunication Systems (CITS); Hangzhou, China; 2020. pp. 1-5, doi: 10.1109/CITS49457.2020.9232662.

[45] Gupta R, Shukla A, Tanwar S. BATS: A Blockchain and AI-Empowered Drone-Assisted Telesurgery System Towards 6G. IEEE Transactions on Network Science and Engineering 2020; 8 (4): 2958-2967. doi: 10.1109/TNSE.2020.3043262.

[46] Acemoglu A, Krieglstein J, Caldwell DG, Mora F, Guastini L et al. 5G Robotic Telesurgery: Remote Transoral Laser Microsurgeries on a Cadaver. IEEE Transactions on Medical RobTrotics and Bionics 2020; 2 (4): 511-518. doi: 10.1109/TMRB.2020.3033007.

[47] Haidegger T. Surgical robots of the next decade: New trends and paradigms in the 21th century. In: 2017 IEEE 30th Neumann Colloquium (NC); Budapest, Hungary; 2018. pp. 000081-000082, doi: 10.1109/NC.2017.8263255.

[48] Bergeles C, Yang G-Z. From Passive Tool Holders to Microsurgeons: Safer, Smaller, Smarter Surgical Robots, IEEE Transactions on Biomedical Engineering; 61 (5): 1565-1576. doi: 10.1109/TBME.2013.2293815.

[49] Qin Y, Feyzabadi, Allan, Burdick JW, Azizian M. daVinciNet: Joint Prediction of Motion and Surgical State in Robot-Assisted Surgery. In: 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS); Las Vegas, USA; 2020. pp. 2921-2928, doi: 10.1109/IROS45743.2020.9340723.

[50] Nguyen DVA, Girerd C, Boyer Q, Rougeot P, Lehmann O et al. A Hybrid Concentric Tube Robot for Cholesteatoma Laser Surgery. IEEE Robotics and Automation Letters; 7 (1): 462-469. doi: 10.1109/LRA.2021.3128685.

[51] Shi C, Zhao X, Wu X, Zhao C, Zhu G et al. Real-time 3D Navigation-based Semi-Automatic Surgical Robotic System for Pelvic Fracture Reduction. In: 2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS); Prague Czech Republic; 2021. pp. 9498-9503, doi: 10.1109/IROS51168.2021.9636647.

[52] Xu J, Li B, Lu B, Liu Y-H, Dou Q et al. SurRoL: An Open-source Reinforcement Learning Centered and dVRK Compatible Platform for Surgical Robot Learning. In: 2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS); Prague Czech Republic; 2021. pp. 1821-1828, doi: 10.1109/IROS51168.2021.9635867.

[53] Saeedi-Hosseiny MS, Alruwaili F, McMillan S, Iordachita I, Abedin-Nasab MH. A Surgical Robotic System for Long-Bone Fracture Alignment: Prototyping and Cadaver Study. IEEE Transactions on Medical Robotics and Bionics 2021; 4 (1): 172-182. doi: 10.1109/TMRB.2021.3129277.

[54] Firouzi F, Farahani B, Barzegari M, Daneshmand M. AI-Driven Data Monetization: The Other Face of Data in IoT-Based Smart and Connected Health. IEEE Internet of Things Journal 2022; 9 (8): 5581-5599. doi: 10.1109/JIOT.2020.3027971.

[55] Jahan N, Rashid IB, Numan OA, Hasan ASMT, Begum N. Collaborative AI in Smart Healthcare System. In: 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI); Rajshahi, Bangladesh; 2021. pp. 1-5, doi: 10.1109/ACMI53878.2021.9528125.

[56] Komal, Sethi GK, Ahmad N, Rehman MB, Ibrahim Dafallaa HME et al. Use of Artificial Intelligence in Healthcare Systems: State-of-the-Art Survey. In: 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM); London, United Kingdom; 2021. pp. 243-248, doi: 10.1109/ICIEM51511.2021.9445391.

[57] Pawar U, O'Shea D, Rea S, O'Reilly R. Explainable AI in Healthcare. In: 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA); Dublin, Ireland; 2020. pp. 1-2, doi: 10.1109/CyberSA49311.2020.9139655.

[58] Gupta R, Tanwar S, Tyagi S, Kumar N, Obaidat MS et al. HaBiTs: Blockchain-based Telesurgery Framework for Healthcare 4.0. In: 2019 International Conference on Computer, Information and Telecommunication Systems (CITS); Beijing, China; 2019. pp. 1-5, doi: 10.1109/CITS.2019.8862127.

[59] Kaur A, Garg R, Gupta P. Challenges facing AI and Big data for Resource-poor Healthcare System. In: 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC); Coimbatore, India; 2021. pp. 1426-1433, doi: 10.1109/ICESC51422.2021.9532955.

[60] Riboni D. Keynote: Explainable AI in Pervasive Healthcare: Open Challenges and Research Directions. In: 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and

other Affiliated Events (PerCom Workshops); Kassel, Germany; 2021. pp. 1-1, doi: 10.1109/PerComWorkshops51409.2021.9431134.

[61] Feizi N, Tavakoli M, Patel RV, Atashzar. Robotics and ai for teleoperation, tele-assessment, and tele-training for surgery in the era of covid-19: Existing challenges, and future vision. Frontiers in Robotics and AI 2021; 8. doi: 10.3389/frobt.2021.610677.

[62] Kamble P, Gawade A. Digitalization of Healthcare with IoT and Cryptographic Encryption against DOS Attacks. In: 2019 International Conference on contemporary Computing and Informatics (IC3I); Singapore; 2019. pp. 69-73, doi: 10.1109/IC3I46837.2019.9055531.

[63] Sinha S, B S. Impact of DoS attack in IoT system and identifying the attacker location for interference attacks. In: 2021 6th International Conference on Communication and Electronics Systems (ICCES); Coimbatore, India; 2021. pp. 657-662, doi: 10.1109/ICCES51350.2021.9489041.

[64] Khatkar M, Kumar K, Kumar B. An overview of distributed denial of service and internet of things in healthcare devices. In: 2020 Research, Innovation, Knowledge Management and Technology Application for Business Sustainability (INBUSH); Greater Noida, India; 2020. pp. 44-48, doi: 10.1109/INBUSH46973.2020.9392171.

[65] Kurniawan MT, Yazid S. Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking Approach and Intrusion Detection System. In: 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE); Istanbul, Turkey; 2020. pp. 1-5, doi: 10.1109/ICECCE49384.2020.9179255.

[66] Chen T, Khoury E. Spoofprint: A New Paradigm for Spoofing Attacks Detection. In: 2021 IEEE Spoken Language Technology Workshop (SLT); Shenzhen, China; 2021. pp. 538-543, doi: 10.1109/SLT48900.2021.9383572.

[67] Elhoseny M, Thilakarathne NN, Alghamdi MI, Mahendran RK, Gardezi AA et al. Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions. Sustainability, 2021; 13(21): 11645. doi: 10.3390/su132111645

[68] Jaafar F, Nicolescu G, Richard C. A Systematic Approach for Privilege Escalation Prevention. In: 2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C); Vienna, Austria; 2016. pp. 101-108, doi: 10.1109/QRS-C.2016.17.

[69] Nithiavathy R. Data integrity and data dynamics with secure storage service in cloud. In: 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering; Salem, India; 2013. pp. 125-130, doi: 10.1109/ICPRIME.2013.6496459.

[70] Wood AD, Stankovic JA. Denial of service in sensor networks. Computer 2002; 35 (10): 54-62. doi: 10.1109/MC.2002.1039518.

[71] Lin JD, Lin HH, Dy J, Chen JC, Tanveer M et al. Lightweight Face Anti-Spoofing Network for Telehealth Applications. IEEE Journal of Biomedical and Health Informatics 2022; 26 (5): 1987-1996. doi: 10.1109/JBHI.2021.3107735.

[72] Khan MFF, Sakamura K. A patient-centric approach to delegation of access rights in healthcare information systems. In: 2016 International Conference on Engineering & MIS (ICEMIS); Agadir, Morocco; 2016. pp. 1-6, doi: 10.1109/ICEMIS.2016.7745308.

[73] Sahi MA, Abbas H, Saleem K, Yang X, Derhab A et al. Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions. IEEE Access 2018, 6: 464-478. doi: 10.1109/ACCESS.2017.2767561.

[74] Belkhouja T, Mohamed A, Al-Ali AK, Du X, Guizani M. Light-Weight Solution to Defend Implantable Medical Devices against Man-In-The-Middle Attack. In: 2018 IEEE Global Communications Conference (GLOBECOM); Abu Dhabi, United Arab Emirates; 2018. pp. 1-5, doi: 10.1109/GLOCOM.2018.8647207.

[75] Li C, Guan L, Lin J, Luo B, Cai Q et al. Mimosa: Protecting Private Keys against Memory Disclosure Attacks Using Hardware Transactional Memory. IEEE Transactions on Dependable and Secure Computing 2019; 18 (3): 3-19. doi: 10.1109/SP.2015.8.

[76] Kholidy HH, Baiardi F, Hariri S. DDSGA: A Data-Driven Semi-Global Alignment Approach for Detecting Masquerade Attacks. IEEE Transactions on Dependable and Secure Computing 2015; 12 (2): 164-178. doi: 10.1109/TDSC.2014.2327966.

[77] Gupta S, Singhal A, Kapoor A. A literature survey on social engineering attacks: Phishing attack. In: 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India; 2016. pp. 537-540, doi: 10.1109/CCAA.2016.7813778.

[78] Kumar S, Kumar S. Semantic Web attacks and countermeasures. In: 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), Unnao, India; 2014. pp. 1-5, doi: 10.1109/ICAETR.2014.7012841.

[79] Arata J, Mitsuishi M, Hashizume M. Robotic tele-surgery through the Internet — System development and its feasibility tests. In: 2014 11th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI); Kuala Lumpur, Malaysia; 2014. pp. 11-12, doi: 10.1109/URAI.2014.7057511.

[80] Ryu S, Yang GH. Telesurgery system using surgical master device type of 3PUU. In: 2017 14th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI); Jeju, Koreas; 2017. pp. 546-549, doi: 10.1109/URAI.2017.7992666.

[81] Sedaghat S, Jahangir AH. RT-TelSurg: Real Time Telesurgery Using SDN, Fog, and Cloud as Infrastructures. IEEE Access, 2021; 9: 52238-52251. doi: 10.1109/ACCESS.2021.3069744.

[82] Chu M, Cui Z, Gao S. A Multisensory and Support Vector Machine Based Teleoperate Robotic Arm. In: 2021 IEEE International Conference on Flexible and Printable Sensors and Systems (FLEPS); Manchester, United Kingdom; 2021. pp. 1-4, doi: 10.1109/FLEPS51544.2021.9469757.

[83] Lin Z, Gao A, Ai X, Gao H, Fu Y et al. ARei: Augmented-Reality-Assisted Touchless Teleoperated Robot for Endoluminal Intervention. IEEE/ASME Transactions on Mechatronics, 2021; 27 (5): 3144-3154. doi: 10.1109/TMECH.2021.3105536.

[84] Bhattacharya P, Obaidat MS, Savaliya D, Sanghavi S, Tanwar S et al. Metaverse assisted Telesurgery in Healthcare 5.0: An interplay of Blockchain and Explainable AI. In: 2022 International Conference on Computer, Information and Telecommunication Systems (CITS); Piraeus, Greece; 2022. pp. 1-5, doi: 10.1109/CITS55221.2022.9832978.

[85] Ordean M, Giurgiu M. Towards securing client-server connections against man-in-the-middle attacks. In: 2012 10th International Symposium on Electronics and Telecommunications; Timisoara, Romania; 2012. pp. 127-130, doi: 10.1109/ISETC.2012.6408076.

[86] Xu S, Lai S, Li Y. A Deep Learning Based Framework for Cloud Masquerade Attack Detection. In: 2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC); Orlando, FL, USA; 2018. pp. 1-2, doi: 10.1109/PCCC.2018.8711277.

[87] Li T, Wang K, Horkoff J. Towards Effective Assessment for Social Engineering Attacks. In: 2019 IEEE 27th International Requirements Engineering Conference (RE); Jeju, Korea; 2019. pp. 392-397, doi: 10.1109/RE.2019.00051.

[88] Yan R, Xu T, Potkonjak M. Semantic attacks on wireless medical devices. In: SENSORS, 2014 IEEE; Valencia, Spain; 2014. pp. 482-485, doi: 10.1109/ICSENS.2014.6985040.

[89] Hu Q, Du B, Markantonakis K, Hancke GP. A Session Hijacking Attack Against a Device-Assisted Physical-Layer Key Agreement. IEEE Transactions on Industrial Informatics 2020; 16 (1): 691-702. doi: 10.1109/TII.2019.2923662.

[90] Singh M, Singh P, Kumar P. An Analytical Study on Cross-Site Scripting," In: 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA); Gunupur, India; 2020. pp. 1-6, doi: 10.1109/ICCSEA49143.2020.9132894.

[91] Tanwar S, Tyagi S, Budhiraja I, Kumar N. Tactile Internet for Autonomous Vehicles: Latency and Reliability Analysis. IEEE Wireless Communications 2019; 26 (4): 66-72. doi: 10.1109/MWC.2019.1800553.

[92] Choi PJ, Oskouian RJ, Tubbs RS. Telesurgery: Past, Present, and Future. Cureus 2018; 10 (5). doi:10.7759/cureus.2716

[93] Feng K, Xu Q, Tam LM. Design and Development of a Teleoperated Robotic Microinjection System With Haptic Feedback. IEEE Robotics and Automation Letters 2021; 6 (3): 6092-6099. doi: 10.1109/LRA.2021.3091017.

[94] Gupta R, Nair A, Tanwar S, Kumar N. Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges. The Institution of Engineering and Technology Communication 2021; 15: 1352– 1367. doi: 10.1049/cmu2.12113.

[95] Almakhour M, Sliman L, Samhat AE, Mellouk A. Verification of smart contracts: A survey. Pervasive and Mobile Computing 2020; 67: 101227. doi: 10.1016/j.pmcj.2020.101227.

[96] Mohan A, Wara UU, Arshad Shaikh MT, Rahman RM, Zaidi AZ. Telesurgery and Robotics: An Improved and Efficient Era. Cureus 2021; 13 (3). doi:10.7759/cureus.14124.

[97] Tamalvanan V. Foreseeable challenges in developing telesurgery for low income and middle income countries. International Surgery Journal 2021; 8 (10): 3228-3230. doi: 10.18203/2349-2902.isj20214033.

[98] Mehrdad S, Liu F, Pham MT, Lelevé A, Atashzar SF. Review of Advanced Medical Telerobots. Applied Sciences 2021; 11 (1): 209. doi: 10.3390/app11010209.