Research and Implement Solutions to Tackle Security Threats in Surgical Robotics

MINT 709 CAPSTONE PROJECT REPORT

Submitted by:

Sruthi Vallabhaneni

MASTER OF SCIENCE IN INTERNETWORKING

Department of Computing Science

Under the guidance of

MS. SANDEEP KAUR

DECLARATION

Sruthi Vallabhaneni declares that this original work was completed on Research and Implement solutions to tackle security threats in surgical robotics in the Department of Computer Science, Master's in Internetworking, University of Alberta. Also, it should be indicated that this study will not be sent to any other educational establishment.

Sruthi Vallabhaneni

1679837

ACKNOWLEDGEMENT

I would like to thank everyone who contributed to the completion of this project in the sincerest possible way. I want to start by expressing my gratitude to my Project Guide **Ms. SANDEEP KAUR** for her direction and assistance throughout the process. Her informative comments and advice were extremely helpful in determining this project's course.

I am grateful to the **UNIVERSITY OF ALBERTA** for providing me with the resources I needed to complete my project.

I also want to express my gratitude to my friends and family who have helped me stay inspired and motivated during the project. Without their unfailing support, I would not have been able to finish my project.

Finally, I want to thank everyone who participated in my study. The success of this project has been greatly influenced by their willingness to share their knowledge and perspectives.

Thank you all for your contributions and support.

Sruthi Vallabhaneni

1679837

ABSTRACT

The security of surgical robotics systems needs to be ensured given the growing usage of technology in healthcare. Cybersecurity risks can potentially compromise the surgical robotics systems' availability, confidentiality, and integrity, with severe repercussions for patients and medical professionals.

An overview of the security concerns relating to surgical robotics and the steps that can be taken to improve their security is provided in this abstract. The concerns connected to surgical robotics are discussed in the report, including hacking, data breaches, and cyberattacks. The document also gives a general review of the security procedures that are currently in place, including access control, authentication, and encryption.

The report also highlights the significance of establishing safety precautions at several levels, including network, hardware, and software. The report emphasizes the necessity of routine vulnerability scanning.

The confidentiality, integrity, and availability of surgical robotics systems must all be guaranteed, which means that security must be provided for surgical robotics. To avoid cybersecurity catastrophes that could jeopardize patient safety and public confidence in the healthcare system, healthcare providers and manufacturers must proactively identify and mitigate potential security risks.

Table of Contents

CHAPTER 1-EVOLUTION OF SURGICAL ROBOTICS........8

1.1 WHAT IS SURGICAL ROBOTICS?........8
1.2 FIELDS IMPLEMENTED USING SURGICAL ROBOTICS........11
  1.2.1 GYNECOLOGICAL SURGERY:........11
  1.2.2 CARDIAC SURGERY:........12
  1.2.3 GASTROINTESTINAL SURGERY:........13
1.3 TECHNOLOGICAL CHALLENGES IN SURGICAL ROBOTICS........16
  1.3.1 NETWORKING CHALLENGES IN SURGICAL ROBOTICS........17

CHAPTER 2- TECHNOLOGIES RELATED TO SURGICAL ROBOTICS........18

2.1 TECHNOLOGIES USED IN SURGICAL ROBOTICS........18
  2.1.1 MECHANIZED ARM:........18
  2.1.2 IMAGE GUIDANCE........19
  2.1.3 COMPUTER VISION:........20
  2.1.4 MACHINE LEARNING:........21
  2.1.5 HAPTIC FEEDBACK:........24
  2.1.6 INSTRUMENT TRACKING:........25
  2.1.7 COMMUNICATION PROTOCOLS IN SURGICAL ROBOTICS........26

CHAPTER 3- NETWORK ARCHITECTURE........28

3.1 NETWORK ARCHITECTURE IN SURGICAL ROBOTICS........29
  3.1.1 TELEOPERATION:........29
  3.1.2 MASTER-SLAVE CONSOLE........30
3.1.3 INDEXING, MOTION COMPENSATION AND SCALING:........36
  3.1.3.1 INDEXING:........36
  3.1.3.2 MOTION COMPENSATION:........36
  3.1.3.3 SCALING........37
  3.2.1 ROBODOC (CUREXO Technology Corporation):........38
  3.2.2 DA VINCI:........39
  3.2.3 SENSEI X (HANSEN MEDICAL):........41
  3.2.4 CYBERKNIFE:........43
  3.2.5 RIO MAKO PLASTY........45
3.3 VULNERABILITIES OF SURGICAL ROBOTICS........47
  3.3.1 CYBERSECURITY........47
  3.3.2 HUMAN ERROR........48
  3.3.3 TECHNICAL MALFUNCTIONS........48
  3.3.4 DEPENDENCE ON POWER AND CONNECTIVITY........49
  3.3.5 COST........49
  3.3.6 REGULATION AND STANDARDIZATION........50
  3.3.7 MAINTENANCE AND UPKEEP........50
  3.3.8 DATA PRIVACY........51

3.4 VULNERABILITIES: 52
3.5 NETWORKING PROTOCOLS 53

CHAPTER 4-ATTACKS INVOLVED IN SURGICAL ROBOTICS 55

4.1 TYPES OF ATTACKS 56
4.2 ROBOTIC SECURITY FRAMEWORK 57
4.3 SAFETY AND SECURITY IN ROBOTICS 58
4.4 PRIVACY IN ROBOTS 59
4.5 CYBER-ATTACKS ON ROBOTICS SYSTEMS 60
4.6 TYPES OF ATTACKS: 61
4.6.1 DENIAL OF SERVICE: 61
4.6.2 SPOOFING 62
4.6.3 MAN-IN-THE-MIDDLE ATTACK 63
4.6.4 TAMPERING 63
4.6.5 REPLAY ATTACK: 63
4.6.6 FAULT INJECTION ATTACK: 64
4.6.7 SYBIL ATTACK: 64
4.6.8 JAMMING ATTACK: 64
4.6.10 REMOTE ACCESS TROJAN 65
4.6.11 STEALTHY ATTACK 65
4.6.12 HOMING ATTACK 65
4.6.13 TEARDROP ATTACK 65
4.6.14 PHISHING 65
4.6.15 HIJACKING 65
4.6.16 MASQUERADE ATTACK 65
4.7 ATTACKS LEVELS 66
4.8 CURRENT ISSUES 68

CHAPTER 5- ESTABLISHING SECURITY FOR ATTACKS 70

5.1 RISK ASSESSMENT IN SURGICAL ROBOTS 70
5.2 CYBERATTACKS ON SURGICAL ROBOTS 71
5.2.1 CONSEQUENCES OF ATTACKS 71
5.3 INITIALIZING LATENCY 74
5.4 CONCLUSION 76

BIBLIOGRAPHY 78

LIST OF FIGURES

Figure 1: The da Vinci surgical Robotic system is a robotic surgical system made by US company Intuitive Surgical. 9
Figure 2:The ROBODOC system for orthopedics. 2(a) The robot is used for total hip replacement surgery. 2(b)close-ups of robotic milling of the femur. 10
Figure 3:THE ZEUS ROBOTIC SYSTEM 13
Figure 4:GASTROINTESTINAL SURGERY 14
Figure 5:ROBOTICS ARMS 20
Figure 6:IMAGE GUIDANCE 21
Figure 7:COMPUTER MOTION SURGERY 22
Figure 8:USE OF MACHINE LEARNING IN SURGICAL ROBOTICS (KHAN, 2019) 24
Figure 9:HAPTIC FEEDBACK (CULMER, 2019) 26
Figure 10:TELEOPERATION IN SURGICAL ROBOTICS (NISAR) 31
Figure 11:A block diagram of a teleoperation system used in surgical robotic systems. 33
Figure 12:An overview of the system architecture including the surgical console (master) and surgical robot (slave) connected through a communication layer with three options. 33
Figure 13:The ROBODOC system by CUREXO 42
Figure 14:The DaVinci Surgical System 44
Figure 15:SURGICAL CONSOLE 45
Figure 16:SURGICAL ROBOTIC ARM 46
Figure 17:ARTISAN CATHETER 46
Figure 18:CYBERKNIFE SYSTEM 48
Figure 19:ROBOTIC ARM INTEROPERATIVE ORTHOPEDIC (RIO) BY MAKO 50
Figure 20:THREATS AND ISSUES 51
Figure 21:GENERAL DESIGN OF A ROBOT. (LACAVA, 2021) 60
Figure 22:CIA TRAID. 61
Figure 23:ROBOT SECURITY FRAMEWORK 62
Figure 24:DENIAL OF SERVICE 66
Figure 25:SPOOFING ATTACK 67
Figure 26:FIREWALL 69
Figure 27:CLASSIFICATION OF ATTACKS 71

CHAPTER 1-EVOLUTION OF SURGICAL ROBOTICS

1.1 WHAT IS SURGICAL ROBOTICS?

The term surgical robotics describes the application of robotics procedures to surgical procedures. These robotic systems assist surgeons in performing minimally invasive procedures and improve precision, control and accuracy compared to traditional automatic methods. The automated systems consist of a surgeon's console, robotic arms and instruments, and an imaging system that provides a high-resolution, magnified view of the surgical areas.

The ability of robotic surgery to conduct precise, minimally invasive surgery that actively confines the surgeon to a safe area is one of the most significant advantages. [1] The applications of robotics surgery are in various fields, such as gynecology, urology, and general surgery. Surgical robotics is a medical robotics subfield that involves robotic systems to perform multiple surgical procedures.

The robots are designed to provide precise and controlled movements and are mainly used in minimally invasive surgeries. Surgical robots can improve the accuracy and outcomes of procedures, reduce patient trauma and recovery time, and allow for enhanced visualization during surgery. Examples of surgical robots include the da Vinci Surgical System and the ROBODOC system.

Figure 1: The da Vinci surgical Robotic system is a robotic surgical system made by US company Intuitive Surgical.

Figure 2:The ROBODOC system for orthopedics. 2(a) The robot is used for total hip replacement surgery. 2(b)close-ups of robotic milling of the femur.

These robots enhance a surgeon's capabilities and provide greater precision, flexibility, and control during surgical operations. The first surgical robot, the da-Vinci surgical system, was approved for use in 2000. Since then, several other surgical robots have been developed for various medical specialties, including gynecology, urology, and cardiothoracic surgery. One of the key benefits of surgical robotics is improved precision. Robots can perform more accurate movements than human surgeons, reducing the risk of surgical errors and complications. [2] Additionally, robots can reach areas of the body that are difficult for a surgeon to access, such as deep within the abdomen or thorax.

Another benefit of using surgical robotics is improved visualization. They often include high-definition cameras that provide a magnified view of the surgical area, which can be helpful in minimally invasive procedures. This enhanced visualization can also help the surgeon make more accurate incisions and reduce the need for additional functions. Surgical robots also offer greater flexibility than traditional surgical techniques.

Most robotic surgery procedures are predefined programs, allowing them to adapt to each patient's specific needs. This can be especially beneficial for procedures that require delicate movements or a high degree of accuracy, such as microsurgeries or procedures involving intricate anatomy. [3] In addition to improved precision and visualization, surgical robotics can enhance the surgeon's control over the procedure. Robotic systems can be programmed to follow sections or movements, which can help the surgeon maintain consistency and control over the procedure.

Despite the benefits, the use of surgical robotics has its challenges. One of the challenges is considered the cost. Surgical robots are much more expensive to purchase and maintain, and their costly costs lead to decreased availability in certain areas. Secondly, it is the learning curve associated with using surgical robots. [4]It also enables remote collaboration and consultation among surgeons, giving them access to the knowledge and assistance of other medical specialists. Surgeons must undergo extensive training and education to become proficient in using these systems, which can be time-consuming and expensive. Additionally, some surgeons may need help to adapt to the new procedures. With the advancement of technology, surgical robots will become even more prevalent in medicine. In conclusion, surgical robotics is a rapidly growing field that offers a range of benefits over traditional surgical techniques. With improved precision, visualization, and control, surgical robots have the potential to revolutionize the way surgeries are performed and improve outcomes for patients. As the field continues to evolve with the new advancements, it is always important to consider the challenges associated with these systems, including cost and the learning curve for surgeons.

Computer networks are crucial in the coordination and communication between all process parts. The surgeon moves the robot via a console, and the movements of the robot are sent to its instruments via computer networking [5]. The robot is also connected to several monitoring systems and medical gadgets that give the surgeon real-time data during the procedure. This is especially helpful for complicated or specialty operations when a surgeon might need support from an expert elsewhere. The Da Vinci surgical system and the Zeus surgical robot are two common examples of surgical robots.

1.2 FIELDS IMPLEMENTED USING SURGICAL ROBOTICS

The author used a robot called Probot in April 1991 to remove his prostate. The ability of a special-purpose robot to independently remove tissue from a human patient had never been developed or used in a therapeutic situation. Since then, there have been numerous robotic surgery research initiatives, only a tiny portion of which have led to businesses developing systems used in clinical cases. But interestingly, such minimal robotic surgery has been performed in the actual clinical situation.

Surgical Robotics is implemented in the following ways:

1.2.1 GYNECOLOGICAL SURGERY:

This robotic approach is in use when vaginal surgery is not feasible. The data on surgery have shown that it is possible, safe, and has superior clinical outcomes than laparoscopy and equal clinical outcomes compared to laparotomy [6]. Developed robotics challenges to overcome the difficulties of laparoscopy and has led to technological advantages such as improved ergonomics, visualization with three-dimensional capabilities, agility, range of motion with instrument articulation, and tremor filtration. To date, robotics applications in benign gynecology include hysterectomy, myomectomy, endometriosis surgery, sacrocolpopexy, adnexal surgery, tubal reanastomosis, and cerclage.

The first gynecological clinical trial evaluated the use of a robot for laparoscopic tubal anastomosis (Falcone et al., 2000). A prospective pilot study was performed to assess the feasibility and safety of a robotic device. Ten patients with previous tubal ligations underwent laparoscopic ligation reversal using an automatic suturing device. Tubal surgery was performed using the ZEUS automated system (Computer Motion Inc., Santa Barbara, CA). Use a two-layered closure for all tubes. Four stitches of 8-0 polyglactin sutures were used for each layer. The ZEUS system has three remotely controlled robotic arms, allowing a single surgeon to simultaneously manipulate the laparoscope camera and two laparoscopic surgical instruments. Voice commands direct the robotic arm that holds the laparoscope. The surgical instruments' components are controlled by two handles housed in a mobile console that can position anywhere in the operating room or a different location.

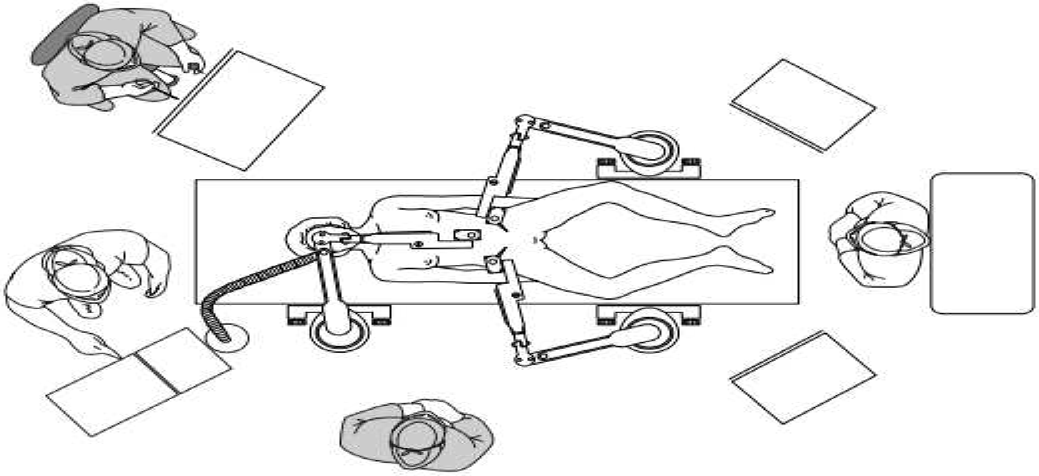

FIGURE 3:THE ZEUS ROBOTIC SYSTEM

A computer controller translates the surgeon's movements from the handles to the robotic arms. No measurable delay exists between the handles' action and the instruments' direction. The operator's movements are scaled according to the surgeon's specifications. For example, a scaling ratio of 15:1 means that for every 1 cm, the surgeon moves the handles at the console, and the robotic surgical instruments move one-fifteenth of a centimetre at the surgical site. Tremors and small unintentional hand motions resulting from holding tools for a prolonged period can be filtered out. Thus, the devices are held steady throughout the procedure.

Robotics may offer extra benefits over other methods in the obese patient group and cases of greater complexity, while more research is required in this area. [7]. With more experience, the use of robots in high-volume centres, and better surgeon and robotic team training, issues that developed in the early adoption stage, such as the steep learning curve, prices, and operating times, are becoming more optimal. Although in its infancy and lacking demonstrable technical advantages over laparoscopic single-site surgery, robotic labour-endoscopic single-site surgery may offer a less expensive alternative to multiport robotics. With comparable postoperative results, the cost may even approach that of laparoscopy.

1.2.2 CARDIAC SURGERY:

The first robotically assisted cardiac procedure was per- 36 formed by a French surgeon, Carpentier, in 1998, demonstrating a successful mitral valve repair. In the same year, a 38 Parisian team performed the first- Endoscopic 39 Coronary Artery Bypass (TECAB). Robotic cardiac surgery is ‘‘any cardiac operation using robot-assisted technology completely or in part”. [8]The specialist machines are operated from a remote-controlled console adjacent to the patient, and the surgeon uses hand and foot controls through tiny incisions with precisely calibrated robotic arms. Amongst many other potential benefits, these small incisions benefit patient recovery.

Devices allow for six degrees of operative freedom, two more than usually afforded by endoscopic instruments. Currently, robotic cardiac surgery is applied in two main areas, namely intra- cardiac operations, and coronary revascularization. Intra-cardiac procedures include surgeries on the mitral and tricuspid valves, septal defect closures and removal of cardiac tumours in selected cases.

In 2000, Chit wood et performed the first robotic mitral valve repair in the USA, paving the way for the US Food and Drug Administration (FDA) trials required to approve the DaVinci automated system used for the procedure. The United Kingdom’s national health service (NHS) bought its first surgical robot in 2007, and there are now robots in hospitals nationwide. [9]

Future issues surrounding the practices include improved training programs, specialized robotic theatre team establishments, and crucially randomized trials to compare automatic and traditional operative approaches. Despite the need for these future improvements, robotic cardiac surgery remains a promising area of medicine set only to increase its utility with technological advancement and time.

1.2.3 GASTROINTESTINAL SURGERY:

The Da Vinci robotic system is the first automated system for intra-abdominal surgery. The system has three major components: the surgeon's console, the surgical cart, and the vision tower. The arms (currently three) are attached by electronic cabling, with all imaging and computer information being transferred electronically.

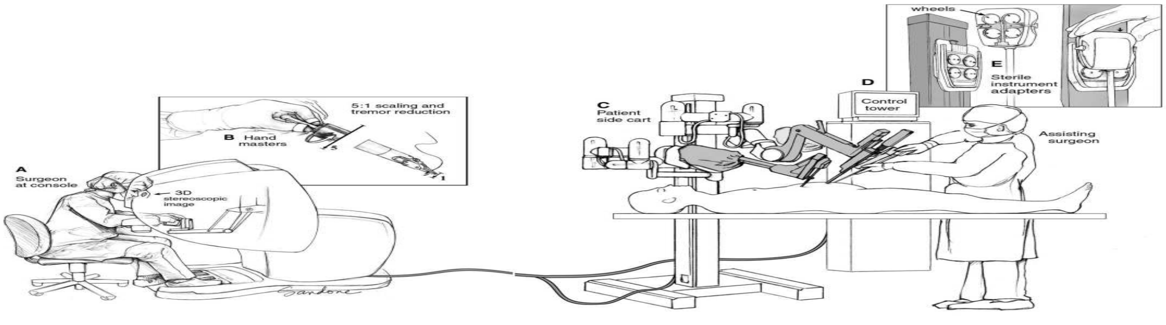

FIGURE 4:GASTROINTESTINAL SURGERY

- A. Console with surgeon sitting comfortably with head leaning into the vision system, hands working via the masters, and feet engaged with Pedals controlling aspects of the procedure.
- B. Details of the masters, with fingers inside Velcro loops.
- C. Patient-side cart hovering over the surgical field.
- D. Control tower with the patient-side monitor and laparoscopic and imaging equipment.

- E. Close-up of the interface between the robotic arm and surgical instrument.

The features of this system are:

1) Physical separation of the surgeon from the patient by operating at a console rather than at the patient's side.

2) Wrist action of the robotic arms providing six degrees of freedom plus grasp (compared with four degrees of freedom plus understanding for standard laparoscopic instruments).

3) Tremor elimination.

4) Optional motion scaling up to 5:1.

5) Three-dimensional stereoscopic image.

The console consists of a workstation from which the surgeon controls a telescope and two robotic arms. The surgeon sits at this workstation and places their head inside a viewing space reminiscent of the devices used for screening children's vision. The surgeon is viewing two separate cathode ray tube monitors via mirrors. Each monitor displays an image inside the patient from one side of the stereo telescope. [10]Two-hand "masters control the operation itself."

These consist of levers for the index finger and thumb of the surgeon, which can be held in place by Velcro straps. Squeezing these levers together approximates the jaws of whatever instrument is inside the patient. Twisting the master rotates the device. The instrument wrists inside the patient's body replicate the wrist-like movements of the masters. The surgeon uses a set of foot pedals to control other aspects of the surgical field. A clutch pedal disengages the master from robotic movement and allows the surgeon to readjust their hands when the movement limits are reached at the console. When the camera pedal is depressed, the direction of the hands in or out adjusts the telescope to make the field closer or farther away. [10]movement to the left or right similarly realms the telescope and rotating the instruments like a flight yoke rotates the telescope. Another pedal controls electrosurgical energy.

It is large and contains three arms, which respond to the surgeon's movements at the console. The center arm controls the stereo telescope. The right and left arms control surgical instruments within the abdominal cavity. The cart is wheeled into place at a vector appropriate for the specific operation and is locked into position. [10]Once closed and engaged with the patient, the table cannot be moved without entirely disengaging the system. Gross movements of the robotic arms are controlled by clutch buttons, which allow the team to move the arms and appropriately engage them with trocar devices.

Additional trocars must be placed out of the way of the robotic arms so that surgeons can assist in the operation without interference from the automatic arm movements. The third main element is the control tower. This is a standard-appearing accessory tower with a high-resolution monitor on top. Dual light sources for the telescope are also on the lookout. The computer equipment synthesizes the video telescope stereo image into a three-dimensional image at the surgeon's console. The system must have an interface between sterile and non-sterile and a means of translating motion to the instrument tips within the patient's abdomen. Unproductive instrument adapters transfer motion via notched wheels. Each separate instrument has four wheels matching the robotic arms' wheels. A computer chip within each device tells the system which unique tool is being attached to the mechanical arm so that coordinated actions of the wheels apply forces and motions distinct to that instrument. The team at the operating table switches these instruments throughout the operation by unlocking them, reattaching them from the robotic arm wheels, and sliding them out of the patient.

Once the procedure is complete, the surgical cart is disengaged from the trocars and backed away from the patient. The trocar defects are then closed as in any laparoscopic operation.

1.2.4 HEAD AND NECK INJURY:

Traditional head and neck surgeries have involved making huge incisions and removing a significant quantity of healthy tissue. However, in the last 20 years, surgical methods and head and neck cancer surgery procedures have evolved significantly. Utilizing minimally invasive techniques and functional preservation are currently the main priorities. Incisions that are less extensive and cause less collateral tissue damage are recommended because they reduce postoperative problems and enhance the quality of life.

The demand from patients and surgeons to develop a minimally invasive approach so that benefits comparable to those of primary surgery can be obtained. [11]Ongoing technological advancements in imaging techniques and robotic surgery are the leading causes of the enthusiasm for applying this exciting technology in the head and neck.

Surgical robots can be categorized as active, semi-active, or inactive depending on how much they participate in the procedure. Functional robots are preprogrammed to complete a course without requiring the surgeon to provide input. The surgeon must provide information for a semi-active robot to perform power-directed activities. [11]Fully Controlled by the surgeon is a passive robot. Almost all surgical procedures done on the head and neck have been done using this method. Robotic arms with articulating surgical tools are inserted into the body through cannulas.

An endoscopic camera and two 8-mm (typical adult size) or two 5-mm (pediatric size) Endo Wrist instruments are held in the three arms of an enslaved person robotic manipulator that is part of the surgical cart. The system's camera supplies a stereoscopic image to the surgeon's console. A crucial part of the system that offers a greater degree of freedom is Endo Wrist

(Intuitive Surgical). Therefore, three-dimensional imaging, [11]tremor filtration, and wristed instrumentation are a few benefits that robotic surgery provides to physicians. [11] With the aid of a robot, a surgeon can now tele operate from a distance in a convenient, skillful, and intuitive way, enabling delicate tissue manipulation. End-laryngeal suturing, regarded as a challenging task, can be completed relatively quickly with this approach.

1.3 TECHNOLOGICAL CHALLENGES IN SURGICAL ROBOTICS

As the field of medicine in robotics is still enhancing, there are very few commercial enterprises and very few medical robots marketed annually. Introducing new technology is challenging in the complicated medical environment, contributing to this issue. Also, establishing a relationship between engineers and physicians to complete a medical robot project takes time and effort. [12]Creating system components and systems are two technological issues and research fields for medical robotics.

Research must be established in the following areas in terms of system components:

1)**SYSTEM ARCHITECTURE**: Creating a system architecture would be a necessary first step for medical robotics to develop into a distinct field and for the price and difficulty of creating prototype systems to go down.

2)**SOFTWARE DESIGN**: These software packages' low cost and widespread availability make their use attractive. Some steps can be taken (such as watchdog timers, backup systems, and error-recovery procedures) to make these systems more reliable.

3)**IMAGING-COMPATIBLE DESIGNS**: With the increasing popularity of image-guided interventions, robotic systems must work within the constraints of various imaging modalities such as CT and MRI. While these systems are, for the most part, still under the direct control of the physician, in the future, they will be increasingly linked to these imaging modalities.

4)**SAFETY**: Safety is a paramount concern in applying these systems. *Safety* is an area that must be addressed to move the field forward. Davies and Elder, and Knight have discussed safety issues. According to Davies, medical robotics is an entirely different application from industrial robotics in that medical robots must operate in cooperation with people to be fully effective.

1.3.1 NETWORKING CHALLENGES IN SURGICAL ROBOTICS

To guarantee surgical robotics are used safely and effectively, networking issues related to them must be solved. The primary networking difficulties in surgical robotics are listed below.

Latency: In surgical robotics, latency—the interval between the command given to the robot and its execution—can be a severe problem. The surgeon's motions and the robot's response can become out of sync with a slight delay, resulting in mistakes or accidents.

Bandwidth: Real-time data transmission through a network is required for the massive amounts of data generated by surgical robotics, including high-resolution video feeds and sensor readings. Maintaining the data stream's quality and dependability depends on sufficient bandwidth and network capacity.

Safety: Surgical robots are linked to networks that can be the subject of cyberattacks, which could result in data theft or hostile intervention. It is crucial to guarantee the network's security and the data's integrity.

Interoperability: Different manufacturers frequently use software and hardware platforms to develop surgical robotics. Ensuring these systems can interoperate seamlessly with each other and hospital networks can be challenging, requiring standardized protocols and interfaces.

Reliability: Surgical robotics are utilized in high-stress, high-risk situations when malfunctioning or disrupting could have detrimental effects. Maintaining the safety and efficiency of surgical robotics depends on the network infrastructure's dependability and resilience.

Finally, surgical robotics present various networking problems that must be solved to enable safe and effective deployment. These difficulties call for creating specific network infrastructure and protocols to meet the requirements of surgical robotics. These difficulties include latency, bandwidth, security, interoperability, and reliability.

CHAPTER 2- TECHNOLOGIES RELATED TO SURGICAL ROBOTICS

2.1 TECHNOLOGIES USED IN SURGICAL ROBOTICS

2.1.1 MECHANIZED ARM:

Mechanized arms are one of the key components of surgical robots. These robot-controlled arms hold and navigate surgical instruments, [13]allowing the surgeon to perform complex procedures with greater precision and accuracy. Mechanized arms can vary in design and functionality, but most are composed of several joints that establish ease of rise in flexibility and mobility. Some surgical robots simultaneously feature multiple arms, allowing repeated use of multiple instruments, increasing the procedure's efficiency.

One of the main advantages of using mechanized arms in surgery is their ability to provide consistent and precise movements. Unlike a human hand, which may tire or shake during a long procedure, a robot arm can repeatedly perform the same precise movements without decreasing accuracy.

Another advantage of mechanized arms is their ability to reach areas of the body that would be difficult or impossible for a human hand to access.

FIGURE 5:ROBOTICS ARMS

For example, some robots have arms that can bend and rotate in various directions, allowing them to reach deep into the body or around obstacles. Overall, the use of mechanized arms in surgical robotics has the potential to revolutionize the field of medicine by enabling the development of new surgical techniques and improving the accuracy and safety of existing procedures with continued technological advances, mechanized arms will likely become an increasingly common feature of surgical robots.

2.1.2 IMAGE GUIDANCE

Image guidance has a vital role in the field of surgical robotics to provide precise navigation and real-time visualization during surgical procedures. This involves the use of pre-operative imaging, such as CT or MRI scans, to guide the robot during the surgery. It involves the overlay of pre-operative imaging, such as CT or MRI scans, onto the real-time view of the surgical site, enabling the surgeon to accurately see the position of their instruments within the body. The use of image guidance has many benefits for both patients and surgeons.

FIGURE 6:IMAGE GUIDANCE

Reducing the risk of surgical errors can lead to improved patient outcomes and reduced recovery times [14]. It also enables the development of new surgical techniques, particularly in minimally invasive procedures, where the surgeon must navigate through narrow or difficult-to-reach areas of the body. Image guidance also provides real-time feedback during the procedure, allowing the surgeon to adjust their movements if necessary. Image guidance minimizes tissue damage, improves the system's accuracy, and reduces the risk of surgical errors.

Integrating image guidance technology into surgical robots requires the integration of multiple technologies, including computer vision, ML, and instrument tracking. Accurate image guidance involves the ability of the system to track the location and orientation of the surgical instruments in real time and overlay this information onto the pre-operative imaging.

However, developing image guidance technology is a complex process, and many challenges must be overcome, including ensuring accuracy and reliability and making the technology user-friendly and easy to use. The continued development and improvement of image guidance technology are critical to the future of surgical robotics and will play a significant role in shaping the future of medicine.

2.1.3 COMPUTER VISION:

Computer vision is a field of artificial intelligence and computer science that focuses on making it possible for computers to understand and analyze visual data from the outside environment. Computer vision involves using cameras and image processing algorithms to provide the surgeon with a high-definition, magnified view of the surgical site. [15]

FIGURE 7:COMPUTER MOTION SURGERY

In surgical robotics, computer vision processes and analyzes visual information from the surgical site, such as images captured during the procedure, to provide real-time guidance and feedback to the surgeon. Image guidance is one of the main applications of computer vision in surgical robotics. Image guidance involves the overlay of pre-operative imaging, such as CT or MRI scans, onto the real-time view of the surgical site, allowing the surgeon to see exactly where they are in the body and to ensure that their movements are precise and accurate. Computer vision uses algorithms to process the images captured during the procedure and to match them with pre-operative imaging, providing real-time feedback to the surgeon.

Another application of computer vision in surgical robotics is instrument tracking. Instrument tracking involves real-time monitoring of the position and orientation of the surgical instruments, allowing the system to provide the surgeon with real-time information on their instruments' function. [15]This information is critical for ensuring the accuracy and safety of the procedure. Computer vision algorithms play a crucial role in enabling the functionality of surgical robots. These algorithms process and analyzes images in real time, allowing the system to provide accurate and reliable information to the surgeon. The usage of the algorithm provides the accuracy and safety of the procedure.

Developing computer vision algorithms for surgical robotics is a complex and ongoing process, requiring a deep understanding of computer vision and surgical procedures. Besides the technological challenges, there are regulatory and ethical considerations, such as ensuring that the algorithms are safe and reliable and comply with relevant regulations and standards.

Despite these challenges, the continued development of computer vision algorithms has the potential to revolutionize the field of surgical robotics. [15] By providing accurate and real-time information to the surgeon, computer vision can improve the accuracy and safety of surgical procedures and enable the development of new surgical techniques.

Computer vision algorithms are also becoming increasingly sophisticated, incorporating new techniques such as deep learning and ML. These advances allow the algorithms to process and analyze visual information increasingly sophisticatedly, enabling the development of new and more advanced surgical robots.

In conclusion, computer vision is the most used technology for developing surgical robots, and its continued development and improvement will play a significant role in shaping the future of medicine. With its ability to provide accurate and real-time information to the surgeon, computer vision can revolutionize the field of surgical robotics and improve the lives of patients worldwide.

2.1.4 MACHINE LEARNING:

Machine learning is a branch involved in artificial intelligence that enhances the design of statistical models and algorithms, allowing computers to learn and draw conclusions without being explicitly programmed. ML consists of algorithms enabling the robot to adapt to different surgical procedures and improve its performance over time. In surgical robotics, ML improves the accuracy and reliability of the robot's movements, enables it to make more informed decisions, and provides real-time guidance and feedback to the surgeon.

ML has the potential to provide an objective, efficient, and scalable surgical assessment. ML can accurately make preoperative diagnoses and surgical risk assessments to optimize surgical candidate selection. ML allows robots to learn surgical procedures autonomously through expert demonstration, trial and error, or both. Future applications of ML require secure and robust surgical data acquisition with close collaboration between surgeons and engineers.

Firstly, image analysis and guidance are the main applications used in surgical robotics. ML algorithms analyze pre-operative imaging, such as CT or MRI scans, to provide the robot with a more detailed understanding of the patient's anatomy. This information guides the robot's movements during the procedure, ensuring it moves precisely and accurately. [16]

The second application of ML in surgical robotics is instrument tracking. ML algorithms analyze the surgical instruments' movement and provide real-time feedback to the surgeon on their position and orientation. This information is critical for ensuring the accuracy and safety of the procedure. ML algorithms improve the performance of surgical robots over time. The algorithms can adapt and improve by continuously learning from the data generated during processes, making the robot more precise and accurate over time.

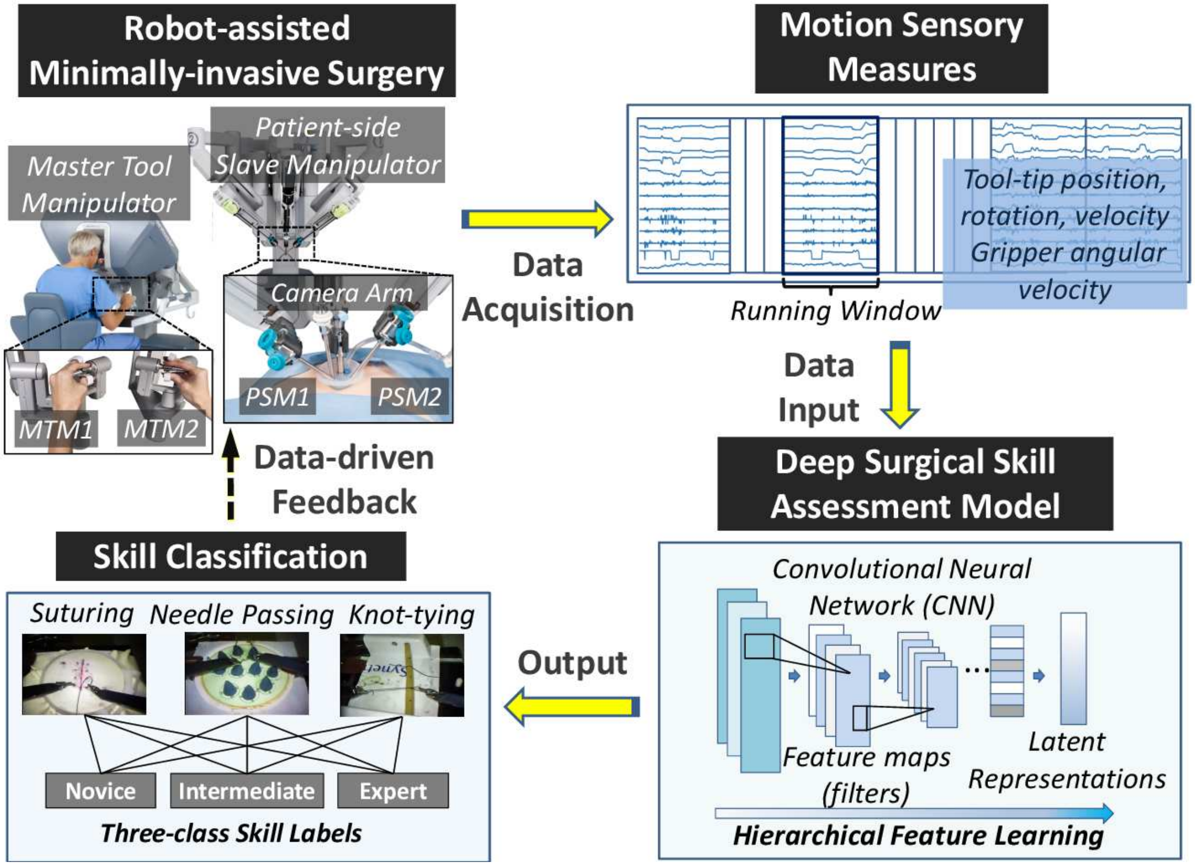

FIGURE 8:USE OF MACHINE LEARNING IN SURGICAL ROBOTICS [17]

Developing ML algorithms for surgical robotics is a complex and ongoing process, requiring a deep understanding of ML and surgical procedures. The algorithms must be designed to work in real-time, processing large amounts of data quickly, and must be accurate and reliable. Despite these challenges, the continued development of ML algorithms has the potential to revolutionize the field of surgical robotics. ML enables the accuracy and reliability of surgical procedures and the development of new surgical techniques. ML algorithms are also becoming increasingly sophisticated, incorporating contemporary styles like deep learning. These advances allow the algorithms to process and analyze data in many ways, enabling the development of new and more advanced surgical robots.

ML is a critical technology for developing surgical robots, and its continued development and improvement will play a significant role in shaping the future of medicine. With its ability to learn and adapt, ML has the potential to revolutionize the field of surgical robotics and improve patients' lives worldwide. [18]However, it is essential to note that while the benefits of ML in surgical robotics are significant, further studies must consider potential risks. The algorithms must be thoroughly tested and validated. ML is a rapidly growing field transforming various industries, from finance and healthcare to retail and transportation. ML algorithms enable computers to learn from data and make predictions or decisions based on that data without being explicitly programmed.

Various types of ML techniques are in use, such as supervised, unsupervised, semi-supervised, and reinforcement learning. In supervised learning, a labelled dataset, where the correct answers are known. It is the most common ML type used for tasks such as classification and regression. Unsupervised learning involves training the algorithm on a dataset without labels. In semi-supervised knowledge, the algorithm combines labelled and unlabeled data, and when labelled, data is scarce. Reinforcement learning involves the algorithm learning from interactions with its environment for game playing and robotics tasks.

Healthcare in ML is multiplying and used for various functions, including diagnosis and treatment planning, patient monitoring, and drug discovery. ML increases the advancements of the robot's movements, provides real-time guidance and feedback to the surgeon, and improves the robot's performance over time. One of the main challenges in using ML in healthcare is ensuring the accuracy and reliability of the algorithms. ML requires a large amount of high-quality data and rigorous testing and validation. In addition, several ethical and regulatory issues must be considered, such as data privacy, algorithmic bias, and the accuracy and reliability of the predictions made by the algorithms.

Despite difficulties, ML's ongoing advancement has the potential to transform the healthcare sector and enhance patients' lives worldwide. The technology has the potential to provide more accurate diagnoses and treatments, enable more effective and efficient patient care, and reduce the cost and burden of healthcare. In conclusion, ML is a rapidly growing and changing field with the potential to impact the healthcare industry profoundly. As the technology is in its early stages, the potential benefits are significant, and the future of healthcare looks bright.

2.1.5 HAPTIC FEEDBACK:

Haptic Feedback from here onwards we call it HF, refers to the sense of touch in a virtual or simulated environment, it involves using sensors that give the surgeon a sense of touch, allowing them to feel the tissues and structures they are manipulating. It is a technology that provides physical feedback to the user through vibrations, force, or pressure. [19]HF is becoming increasingly important in a wide range of applications, from gaming and entertainment to education and training, and is playing an increasingly important role in surgical robotics. HF is created to replicate the sense of touch in a virtual or simulated environment, allowing the user to experience physical sensations corresponding to virtual actions. For example, a video game might use HF to simulate the feeling of holding a weapon or being hit by an opponent. In surgical robotics, HF can provide the surgeon with information about the tissue's location, orientation, and properties and allow the surgeon to feel the tissue's resistance as the robot manipulates it.

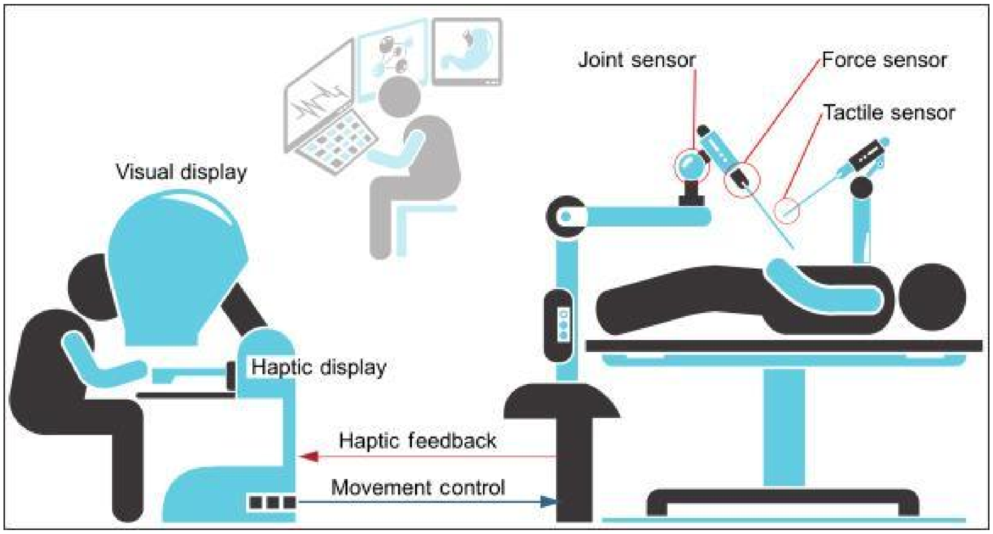

FIGURE 9:HAPTIC FEEDBACK [19]

Several types of HF devices exist, including haptic gloves, vests, and exposits. Haptic gloves are typically worn on the hands and equipped with sensors and actuators to simulate various physical sensations. Haptic vests are similar but worn on the upper body, providing more immersive haptic Feedback. Haptic exposits are wearable devices that can be worn on the entire body and are designed to provide HF to the body. Using HF in surgical robotics is still early, but the potential benefits are significant. By providing the surgeon with information about the location, orientation, and properties of the tissue manipulated, HF can improve the accuracy and precision of the robot's movements.

In addition, HF can provide the surgeon with real-time Feedback about the tissue's resistance, allowing the surgeon to adjust the robot's movements in real time. Several challenges are associated with using HF in surgical robotics. One of the main challenges is the development of HF devices that are accurate, reliable, and safe. The devices must be able to replicate the sensation of touch accurately and must be able to do so in real time. In addition, the devices must be safe for the patient and not introduce any additional risks to the procedure. Historically, skill assessment methodology relied on subjective and laborious evaluations prone to observer biases, making them impractical for the timely delivery of surgical feedback.

Another challenge is the development of algorithms and software that can use to interpret and process data from HF devices. The algorithms must be able to interpret the data from the devices accurately and must be able to provide the surgeon with real-time Feedback about the resistance of the tissue. Finally, several ethical and regulatory issues are in consideration when using HF in surgical robotics. For example, there are concerns about the accuracy and reliability of the HF devices and about the potential for algorithmic bias. There are also concerns about data privacy and security, as the data collected by the HF devices may contain sensitive information about the patient.

In conclusion, HF is an important and rapidly growing technology that can potentially transform various applications, including surgical robotics. The technology is still in its early stages, and several challenges to overcome, but the potential benefits are significant, and the future of HF looks bright. With the continued development of HF devices and algorithms, the technology has the potential to revolutionize how we interact with virtual and simulated environments and improve the lives of people worldwide.

2.1.6 INSTRUMENT TRACKING:

Instrumental tracking is a critical component of surgical robotics, as it allows the surgeon to precisely control the movement of the robotic instruments during a procedure. This involves the use of sensors to track the position and orientation of surgical instruments in real time, allowing the robot to precisely control its movement. Instrumental tracking refers to the use of sensors and tracking systems to monitor the position and orientation of the instruments in real time and to provide this information to the robotic control system.

Several different types of instrumental tracking systems exist, including optical, electromagnetic, and acoustic systems. Optical tracking systems use cameras and markers to track the movement of the instruments, while electromagnetic tracking systems use magnetic fields to track the activity of the tools. Acoustic tracking systems use ultrasound to follow the direction of the devices. The use of instrumental tracking in surgical robotics provides several key benefits. First, it allows the surgeon to have precise control over the movement of the instruments, which is essential for the success of the treatment. Second, it will enable the surgeon to accurately visualize the devices and the surrounding tissue, which helps to lower risks for the patient.

Finally, instrumental tracking enables real-time feedback to the surgeon, allowing for precise and accurate movements of the instruments during the procedure. Several challenges are associated with using instrumental tracking in surgical robotics. One of the main challenges is the accuracy of the tracking systems. The tracking systems must be able to track the movements accurately and precisely of the instruments, even in complex and dynamic environments. In addition, the tracking systems must be able to track the devices in real time, which can be challenging in highly active procedures.

Another challenge is the compatibility of the tracking systems with the robotic control system. The tracking systems must be able to integrate with the robotic control system seamlessly and must be able to provide the necessary data in real time. Tracking requires the development of sophisticated algorithms and software that can process the tracking data and provide it to the robotic control system. several regulatory and ethical issues must be taken care of during instrumental tracking in surgical robotics. There are concerns about the accuracy and reliability of the tracking systems and about the potential for algorithmic bias. There are also concerns about data privacy and security, as the tracking data may contain sensitive information about the patient.

In conclusion, instrumental tracking is a critical component of surgical robotics and is essential for the procedure's success. The use of instrumental tracking provides several key benefits, including precise control of the instruments, accurate visualization of the devices and surrounding tissue, and real-time feedback to the surgeon. Several challenges are associated with using instrumental tracking, including the accuracy of the tracking systems, compatibility with the robotic control system, and regulatory and ethical considerations. With the continued development of tracking systems and algorithms, instrumental tracking in surgical robotics is becoming significant and its plays a vital role in saving patients' lives.

2.1.7 COMMUNICATION PROTOCOLS IN SURGICAL ROBOTICS

The ability of the various parts of the robotic system to interact and cooperate flawlessly makes communication protocols a crucial component of surgical robotics. The following are a few of the common surgical robotics communication protocols:

Transmission Control Protocol/Internet Protocol (TCP/IP): This protocol is used to establish communication between the robot arm, surgical instruments, and control console, among other components of the robotic system. TCP/IP is an excellent option for surgical robots since it is a dependable and extensively used protocol for data transfer over the internet.

USB: is frequently used to link peripheral devices like cameras, sensors, and other tools. USB is a standard protocol for connecting devices to a computer.

CAN: Robotic surgery uses the Controller Area Network (CAN) protocol, which is also utilized in industrial and automotive settings. CAN make it possible for devices to communicate in real-time, which makes it perfect for operating the robot arm and other vital elements of the surgical system.

ETHERNET: While linking the various parts of the surgical robotics system, Ethernet, a widely used standard for local area networks (LANs), is employed. High bandwidth is provided by Ethernet, which is necessary for the real-time transmission of high-quality video and other data streams.

OPEN PROCESS COMMUNICATION (OPC): OPC is a protocol used for industrial automation and data sharing between devices in surgical robotics. OPC offers a standardized method for devices to communicate with one another, making it simpler to integrate various robotic system components.

Overall, communication protocols are essential to the effective use of surgical robots because they allow various devices and components to collaborate effectively.

CHAPTER 3- NETWORK ARCHITECTURE

3.1 NETWORK ARCHITECTURE IN SURGICAL ROBOTICS

3.1.1 TELEOPERATION:

Teleoperation in surgical robotics refers to the remote control of a surgical robot by a surgeon physically located away from the patient. This technology allows a surgeon to perform minimally invasive procedures, such as laparoscopic surgery, with increased precision and control. The surgeon operates the robot using a computer interface, and the robot's instruments are inserted into the patient through small incisions. The robot's movements are guided by the surgeon, who can see high-resolution, 3D images of the surgical site on a monitor. [20]Tele operative surgical robots can improve patient outcomes, reduce recovery time, and increase the accuracy and precision of surgical procedures. Teleoperation in surgical robotics is a technology that enables a surgeon's remote control of a surgical robot.

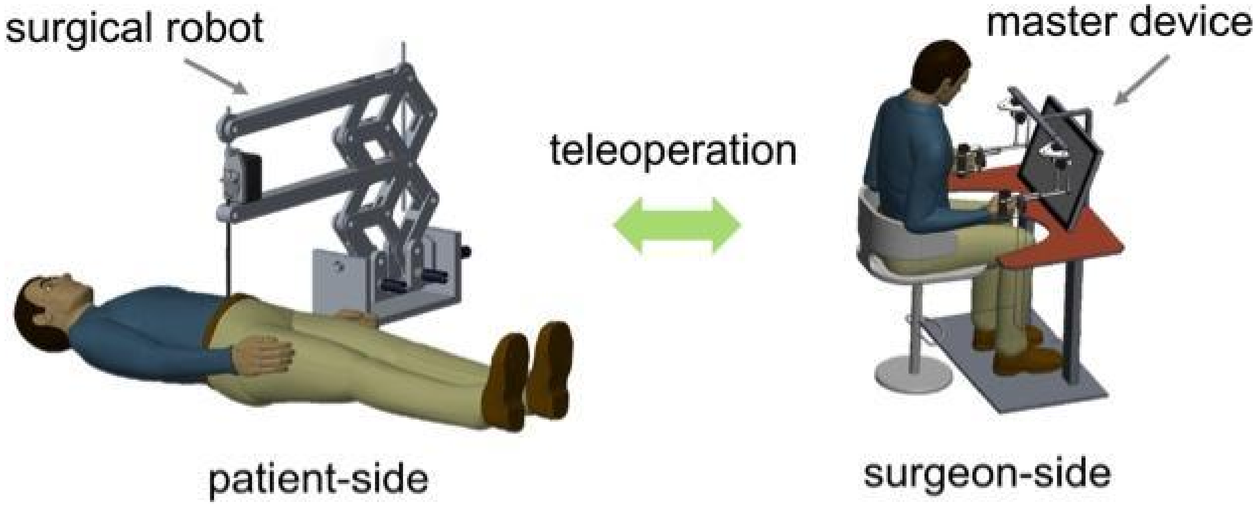

FIGURE 10:TELEOPERATION IN SURGICAL ROBOTICS [20]

The network architecture in surgical robotics includes:

- Control Module*:* The surgeon can manipulate the robot's instruments through a computer interface. The control module typically includes a joystick, buttons, and pedals for controlling the robot's movements.

- Image Module*:* This module provides the surgeon with real-time, high-resolution images of the surgical site. The images are captured by a camera on the robot and transmitted to the surgeon's computer.

- Instrument Module*:* This module consists of the robot's surgical instruments, such as scissors, forceps, and graspers. The devices are attached to the robot's arms and designed to be flexible yet stable for precise movement inside the patient's body.

- Communication Module: This module connects the surgeon's computer to the robot and enables real-time communication between the two. The communication module ensures that the surgeon's commands are transmitted to the robot in a timely and reliable manner.

- Safety Module: This module ensures the safety of the patient and the surgeon during the surgical procedure. It includes safety protocols and mechanisms preventing the robot from making dangerous movements or actions.

In teleoperated surgical robotics, the surgeon sits at a console and remotely controls the robot's movements. The robot's instruments are inserted into the patient through small incisions, and the surgeon uses the image module to guide the robot to the surgical site. The control module allows the surgeon to manipulate the instruments with precise movements, and the communication and safety modules ensure that the procedure is safe and effective.

This network architecture of surgical robotics typically consists of several components, including:

- Master console: This is the control center for the surgeon, which includes a user interface for commanding the robot and visualizing the surgical site.
- Slave robot: The actual robotic device performs the surgical procedure. It is controlled by the master console and equipped with specialized instruments.
- Image guidance system: This component provides visual information to the surgeon about the surgical site, such as X-ray or CT scans.
- Communication network: This allows for real-time communication between the master console and the slave robot, as well as other components in the system.

These components work together to create a seamless and integrated system that allows the surgeon to perform complex surgical procedures with improved accuracy, precision, and control. The communication network is critical to the system's functionality, as it enables real-time exchange of information and control commands between the various components.

3.1.2 MASTER-SLAVE CONSOLE

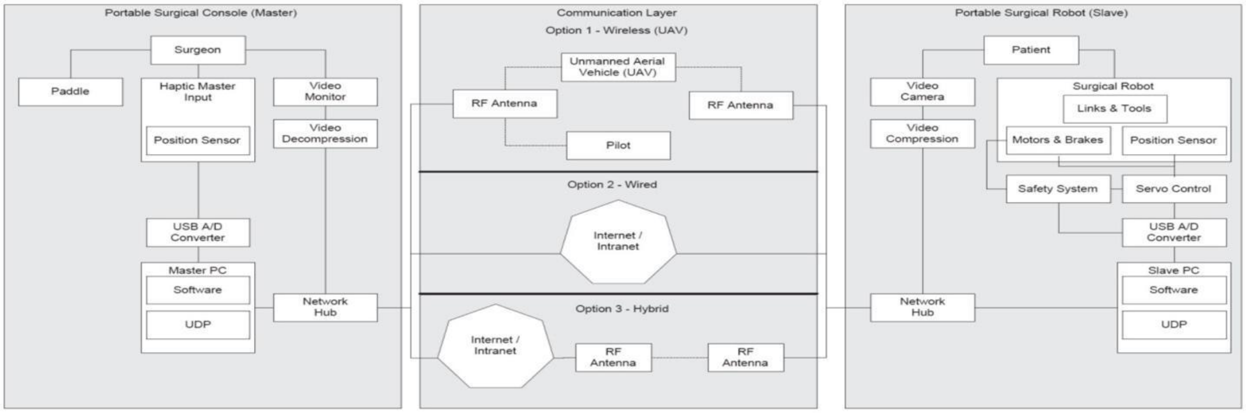

FIGURE 11:A BLOCK DIAGRAM OF A TELEOPERATION SYSTEM USED IN SURGICAL ROBOTIC SYSTEMS.

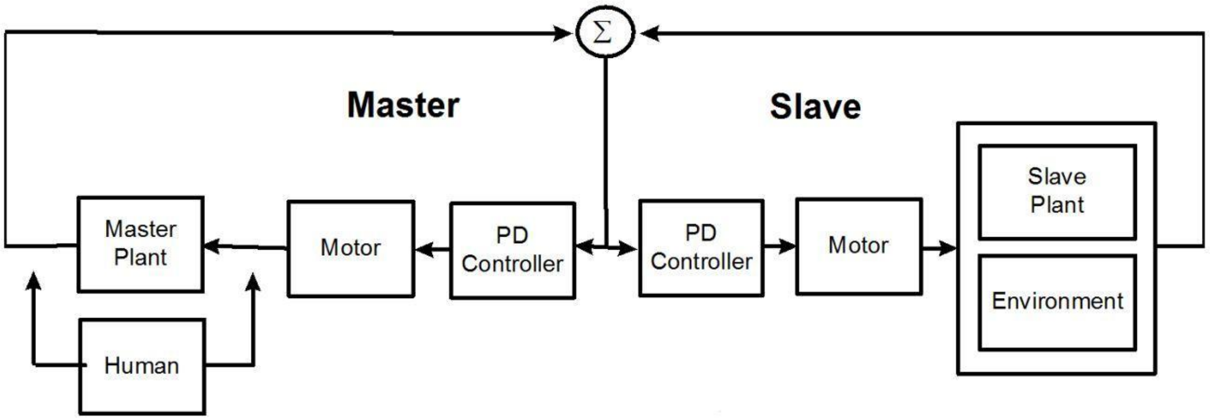

FIGURE 12:AN OVERVIEW OF THE SYSTEM ARCHITECTURE INCLUDING THE SURGICAL CONSOLE (MASTER) AND SURGICAL ROBOT (SLAVE) CONNECTED THROUGH A COMMUNICATION LAYER WITH THREE OPTIONS.

PORTABLE SURGICAL ROBOT (MASTER)

It is a compact, lightweight version of a master console used in surgical robotics. They can be moved from one location to another, allowing the surgeon to perform procedures in different operating rooms or remote areas. A portable surgical console typically has similar features to a traditional master console, including a user interface for commanding the robot, visualization displays, and control devices such as joysticks or foot pedals. The main difference is that a portable surgical console is compact and lightweight, making them easy to move from one location to another.

The use of portable surgical consoles can be beneficial in several ways. For example, it can provide greater flexibility for performing procedures in different locations, reducing the need for additional equipment or setup time. Additionally, portable surgical consoles can be used in remote or underserved areas, helping to increase access to surgical care in these regions. Overall, portable surgical consoles provide a practical solution for performing surgical procedures with the aid of a robot, providing the surgeon with the necessary tools and control they need to perform operations with greater precision and accuracy.

In addition to the features mentioned previously, a portable surgical console may also include the following:

- Wireless connectivity*:* Portable surgical consoles may have wireless connectivity options, allowing them to communicate with the slave robot and other surgical system components without cables or physical connections.

- Compact design*:* This design of Portable surgical consoles is compact and lightweight, making them easy to transport and set up in different locations.
- Battery-powered operation*:* Some portable surgical consoles may be battery-powered for use in locations where electrical power may not be readily available.
- Touchscreen display*:* A portable surgical console may have a touchscreen display, providing the surgeon with a user-friendly interface for controlling the robot and visualizing the surgical site.
- Integration with other medical equipment*:* Portable surgical consoles may be integrated with other medical equipment, such as image guidance systems or diagnostic tools, to provide a comprehensive solution for surgical procedures.

In conclusion, portable surgical consoles provide a versatile solution for performing surgical procedures with the aid of a robot. Their compact design, wireless connectivity, and integration with other medical equipment make them well-suited for use in various clinical settings, helping to increase the accessibility and efficiency of surgical care.

The **Communication Layer** between the master console and the slave robot in surgical robotics enables the two components to communicate. This layer is critical to the functionality of the surgical system, as it allows the real-time exchange of information and control commands between the master console and the robot. The communication layer typically uses a wired or wireless connection and may use a variety of protocols, such as Ethernet or Wi-Fi, to facilitate communication.

The communication layer may also include additional components, such as data converters or routers, to help manage and direct the flow of information. The data exchange typically happens through the communication layer that has a mechanism for transmitting control orders from the master console to the slave robot as well as data from the robot back to the master control. For example, the master console may send control commands to the robot to move its arms or instruments, and the robot may send data back to the master console to indicate its current position or state.

In addition to facilitating real-time control and communication, the communication layer may also include security features to protect against unauthorized access and ensure the privacy of patient data. [21]These may consist of encryption mechanisms, firewalls, or access controls. Overall, the communication layer between the master console and the slave robot is a critical component of a surgical robotics system, enabling the surgeon to control the robot and perform procedures with greater precision and accuracy.

The communication layer between the master console and the slave robot in surgical robotics ensures that data is transmitted accurately and in real-time. This layer usually comprises multiple components, including hardware, software, and communication protocols.

- Hardware components*:* This layer may include hardware components such as data converters, routers, and network interfaces, which are responsible for transmitting and receiving data between the master console and the robot. The hardware may also include encoders, decoders, and other components that help ensure data transmission accuracy.

- Software components*:* The communication layer may also include software components, such as drivers, libraries, and communication protocols, which are responsible for managing data flow and ensuring that it is transmitted reliably and efficiently. This layer may also include middleware, which acts as an intermediary between the hardware and the application software, to help manage the data flow and ensure its transmission in the correct format.
- Communication protocols*:* The layer also includes protocols facilitating communication between the master console and the robot. These protocols may consist of standard networking protocols, such as TCP/IP or UDP, or proprietary protocols explicitly developed for use in surgical robotics.

In addition to facilitating real-time communication between the master console and the robot, the communication layer may also include additional features to ensure the security and privacy of patient data. For example, the layer may contain encryption mechanisms to protect data from unauthorized access and access controls to ensure only authorized users access the system. Overall, the communication layer is a critical component of a surgical robotics system, enabling the surgeon to control the robot and perform procedures with greater precision and accuracy. By transmitting data accurately and in real-time, the communication layer helps to ensure the safety and effectiveness of surgical procedures performed with the aid of a robot.

PORTABLE SURGICAL ROBOT (SLAVE):

The architecture of a Portable Surgical Robot (Slave) typically includes several key components, which work together to allow the surgeon to control the robot and perform procedures with precision and accuracy. [21]The following are some of the main elements of a surgical robot slave architecture:

- Actuators*:* The actuators of a surgical robot slave are responsible for moving the robot's arms and other components. They are usually high-precision, low-noise actuators that can provide precise and smooth motion, allowing the surgeon to perform procedures with high levels of accuracy.
- Sensors*:* Sensors are a critical component of a surgical robot slave architecture, allowing the robot to gather information about its surroundings and the patient. For example, sensors measure the position and orientation of the robot's arms and the force and torque exerted by the robot on the patient.
- Control system*:* The control system of a surgical robot slave is responsible for receiving commands from the master console and translating those commands into actions performed by the robot. This system typically includes a microprocessor and associated software that control the actuators and sensors.
- Communication layer*:* The communication layer of a surgical robot slave is responsible for transmitting data between the robot and the master console. This layer may include hardware components, such as data converters, routers, and network interfaces, and software components, such as drivers and communication protocols.
- Power supply*:* A surgical robot slave will typically have its power supply, allowing it to operate independently of other equipment in the surgical suite. This power supply may

include batteries or other power storage devices, charging circuits and power management systems.

- Housing and mounting systems*:* A surgical robot slave typically has a housing and mounting system that protects the internal components and allows the robot to be securely attached to other equipment in the surgical suite. This robot slave may include mounting brackets, cable management systems, and other components.

Overall, the architecture of a surgical robot slave supports the surgeon's control of the robot and provides the accuracy, precision, and reliability necessary for successful surgical procedures. By integrating advanced actuators, sensors, control systems, communication layers, and other components, surgical robot slaves provide a powerful tool for enhancing the performance of surgical procedures and improving patient outcomes.

Moreover, the surgical robot slave works with a master console, allowing the surgeon to control the robot and perform procedures with precision and accuracy. The following is a general overview of how the master and slave work together:

Master Console**:** The master console is the main control interface for the surgical robot. The surgeon uses the master console to input commands, such as desired robotic arm movements, and to view images and other data related to the surgical procedure.

Communication Layer: The communication layer transmits data between the master console and the surgical robot slave. This layer may use a wired or wireless connection to share data and employ a range of protocols and algorithms to ensure reliable and secure communication.

Slave Robot: The surgical robot slave is the robotic system that physically interacts with the patient. The slave robot may have one or more articulated arms and may be equipped with various instruments and sensors to help the surgeon perform procedures with precision and accuracy.

Control System: The control system is responsible for processing commands from the master console and translating those commands into the robot's actions. This system may include a microprocessor and associated software, as well as actuators and sensors that control the robot's movements and gather data about its environment.

Image Guidance: Image guidance systems, such as ultrasound or CT scanners, may be integrated into the surgical robot slave to help the surgeon visualize the surgical site.

When the master console sends a command to the surgical robot slave, the communication layer transmits the command to the control system. [21] The control system then processes the command and generates commands to the actuators and sensors, which move the robot's arms and gather data. The control system may also process the data collected by the sensors to provide feedback to the master console, allowing the surgeon to view the robot's status and make any necessary adjustments. In this way, the master console and surgical robot slave work together to provide the surgeon with high control and accuracy when performing surgical procedures. The combination of the master console, communication layer, control system, and robot allows the surgeon to perform procedures with precision and accuracy, improving patient outcomes and enhancing the overall efficiency of surgical care.

A surgical robot slave works with a master console to perform surgical procedures. The master console is the surgeon's main control interface to input commands, while the robot slave physically interacts with the patient and performs the procedures. The communication layer transmits commands from the master console to the robot slave's control system, which processes the commands and generates commands to the robot's actuators and sensors to move the robot's arms and gather data. The robot slave's control system also provides feedback to the master console, allowing the surgeon to view the robot's status and make necessary adjustments. The combination of the master console, communication layer, control system, and robot allows the surgeon to perform procedures with precision and accuracy, improving patient outcomes and enhancing the overall efficiency of surgical care.

HAPTICS

Haptics in the teleoperation of surgical robotics refers to the use of touch feedback to provide the surgeon with a sense of touch during the remote control of a surgical robot. [19]The goal of haptic feedback is to enhance the surgeon's ability to perform delicate and precise procedures by allowing them to feel the interactions between the robot's instruments and the patient's tissue.

Haptic feedback uses the force sensors and actuators in the robot, which can sense and respond to the resistance encountered during surgery. The surgeon's computer receives the haptic information, processes it, and converts it into a tactile feedback signal. Haptic feedback in the teleoperation of surgical robotics has several advantages. It allows the surgeon to perform procedures with greater precision, as they can feel the resistance encountered by the robot's instruments. This feedback can reduce the risk of complications and improve patient outcomes.

Also, haptic feedback can give the surgeon a better sense of the surgical environment, allowing them to make more informed decisions during the procedure. Overall, haptics in teleoperation of surgical robotics represents a significant advance in minimally invasive surgery, as it enhances the surgeon's ability to perform procedures with greater precision and control.

TIME DELAY

Time delay in the teleoperation of surgical robotics refers to the lag between when the surgeon commands the robot and when the robot responds. Time delays can occur due to several factors, such as the speed of the communication system, the computer's processing time, and the physical location of the patient and the surgeon.

Time delay can significantly impact the surgeon's ability to perform procedures with precision and accuracy. If the time delay is too long, the surgeon may have difficulty controlling the robot effectively, leading to decreased accuracy and increased risk of complications. One can employ several techniques to reduce time delays in the teleoperation of surgical robotics. These include:

High-speed communication systems: High-speed communication systems, such as fibre optic cables or wireless networks, can reduce the delay by transmitting data and commands more quickly.

Latency reduction*:* This involves reducing the processing time of the computer, as well as optimizing the algorithms used to control the robot.

Predictive control: Predictive control involves using algorithms to anticipate the robot's movements and compensate for the time delay. This control can help to improve the accuracy and precision of the robot's movements, even with a significant time delay.

Overall, minimizing time delay in the teleoperation of surgical robotics is critical to ensure the safety and effectiveness of the procedure. By using various techniques to reduce time delay, surgeons can perform procedures with greater precision and control, improving patient outcomes and reducing the risk of complications.

3.1.3 INDEXING, MOTION COMPENSATION AND SCALING:

3.1.3.1 INDEXING:

Regarding teleoperation, indexing coordinates the positions and orientations of two or more devices, such as a surgical robot and a camera or tool. The devices are correctly aligned through indexing, and the surgical site is clearly and precisely visible to the surgeon. Indexing is frequently carried out before the procedure begins to ensure that the robot's instruments are correctly positioned and oriented concerning the camera during the teleoperation of surgical robotics. This is crucial for minimally invasive operations because it lets the physician precisely control the robot's instruments and observe the surgical site. There are various indexing techniques used in teleoperation, such as:

- Optical tracking**:** This method involves using a camera or other optical device to track the position and orientation of the robot's instruments and to align them with the camera's view.

- Magnetic tracking*:* This technique uses magnetic fields to track the location and orientation of the robot's equipment.
- Automatic indexing**:** The robot's tools are precisely aligned with the camera using mechanical components like gears or locking mechanisms in this technique.
- Hybrid methods combine different techniques, like optical and magnetic tracking, to produce a more reliable and accurate indexing solution. Overall, indexing is a crucial step in the teleoperation of surgical robotics because it ensures that the surgeon has an exact and clear picture of the surgical site and that the robot's instruments are correctly positioned and oriented. Using various indexing techniques, surgeons can carry out

operations with more control and precision, enhancing patient outcomes and lowering the likelihood of problems.

-

3.1.3.2 MOTION COMPENSATION:

In the teleoperation of surgical robotics, "motion compensation" refers to making up for movements during the surgery, such as movements of the patient or tissue or movements of the robot's instruments. Motion compensation aims to maintain the robot's motions' accuracy and precision despite any external movements or disturbances that may occur while the procedure is being performed. There are several ways to create motion compensation, including:

- Feedback control involves continuously monitoring the robot's movements and adjusting its position and orientation in real-time to compensate for any movements or disturbances.
- Predictive control: Predictive control involves using algorithms to anticipate the robot's movements and compensate for any external disturbances or movements. This can help to improve the accuracy and precision of the robot's movements, even when there are external movements.
- Image-based motion compensation involves using imaging data, such as ultrasound or X-ray images, to compensate for any movements or distortions in the surgical site.
- Hybrid methods involve combining multiple methods, such as feedback control and predictive control, to achieve a more robust and accurate motion compensation solution.

Overall, motion compensation is critical in the teleoperation of surgical robotics, as it helps to ensure that the robot's movements remain accurate and precise, even when there are external disturbances or movements during the procedure. Using various motion compensation methods, surgeons can perform procedures with greater precision and control, improving patient outcomes and reducing the risk of complications.

3.1.3.3 SCALING

Scaling in the teleoperation of surgical robotics refers to adjusting the size and position of the robot's movements to match the scale of the surgical site. Scaling aims to ensure that the surgeon's movements are accurately translated to the robot, allowing for precise control and manipulation of the surgical instruments. There are several types of scaling in the teleoperation of surgical robotics, including:

- Cartesian scaling: This involves adjusting the size and position of the robot's movements in a three-dimensional Cartesian coordinate system.
- Joint scaling: This involves adjusting the size and position of the robot's movements in a joint-based coordinate system.
- Force scaling: This involves adjusting the robot's force on the surgical instruments, allowing the surgeon to control the instruments with greater precision.

- Hybrid methods involve combining multiple methods, such as Cartesian and joint scaling, to achieve a more robust and accurate scaling solution.

Overall, scaling is critical in the teleoperation of surgical robotics, as it helps to ensure that the surgeon's movements are accurately translated to the robot, allowing for precise control and manipulation of the surgical instruments. By using various scaling methods, surgeons can perform procedures with greater precision and control, improving patient outcomes and reducing the risk of complications.

3.2 COMMERCIAL SYSTEMS

3.2.1 ROBODOC (CUREXO Technology Corporation):

Clinical Procedure:

The ROBODOC system's clinical procedure for total hip arthroplasty (THA) involves several key steps. Before the surgery, the surgeon will use computer-aided design (CAD) software to create a surgical plan tailored to the patient's specific anatomy. This plan will include the location and orientation of the implant and the movements of the surgical tools during the procedure. During the surgery, the patient will undergo general anesthesia and be positioned on the operating table with the affected hip exposed. The surgical site will be prepared, and the ROBODOC arm will be attached to the patient's femur using a special fixture. The arm will be positioned over the hip joint, and the robot will be activated. The surgeon will use the ROBODOC system to perform the THA procedure, following the pre-programmed surgical plan to remove the damaged hip joint and install the new implant. The robot will guide the surgical tools to the precise locations needed to complete the procedure, and the surgeon can make adjustments if necessary.

After the surgery, the patient will be taken to a recovery room to be monitored for any adverse reactions. They will then be transferred to a hospital for further observation and rehabilitation. The recovery process can take several weeks or months, and the patient will typically be required to attend physical therapy sessions to help them regain strength and mobility. Using the ROBODOC system in THA can help improve the accuracy and consistency of the procedure.

System Architecture:

ROBODOC is also the name of a surgical robot developed for use in total hip arthroplasty (THA), a procedure used to replace a damaged hip joint with a prosthetic implant. During surgery, the ROBODOC system consists of a robotic arm attached to the patient's femur (thigh bone). The robot is programmed with a precise surgical plan and uses computer-controlled motors to guide the surgical tools, helping to ensure the accurate placement of the implant. The key advantage of using the ROBODOC system in THA is that it helps improve the procedure's accuracy and consistency. The robot's ability to accurately follow the pre-programmed surgical plan helps to ensure that the implant is placed in the correct position, reducing the risk of implant dislocation, hip pain, and other complications. The system architecture of ROBODOC, the surgical robot used in total hip arthroplasty (THA), typically includes several key components:

- Robot arm: The robot arm is the central component of the ROBODOC system and is attached to the patient's femur during the procedure. It consists of a series of robotic joints and motors controlled by a computer to guide the surgical tools.
- Computer control system: It manages the robot arm and guides it through the pre-programmed surgical plan. It includes a graphical user interface that allows the surgeon to adjust the plan if necessary and a motion control system that ensures that the robot arm moves smoothly and precisely.
- Surgical tools: The surgical tools used in THA with the ROBODOC system include cutting tools, reamers, and drills. These tools are attached to the robot arm and are controlled by the computer to perform the various steps of the procedure.
- CAD software*:* The computer-aided design (CAD) software creates the pre-operative surgical plan. This software allows the surgeon to design the implant placement and specify the movements of the surgical tools during the procedure.
- Fixture: The fixture is a device that is attached to the patient's femur to hold the robot arm in place during the procedure. It is designed to provide a stable platform for the robot and to ensure that the arm is positioned accurately over the hip joint.

The components of the ROBODOC system work together to provide a precise, consistent, and controlled surgical experience for the patient. The system architecture is designed to minimize surgical trauma, reduce the risk of complications, and improve patient outcomes.

FIGURE 13:THE ROBODOC SYSTEM BY CUREXO

3.2.2 DA VINCI:

Clinical Procedure:

This surgical system is a minimally invasive robotic surgery platform allowing less invasive procedures than traditional open surgery. It utilizes a robotic arm and a 3D high-definition vision system to enhance the surgeon's precision, flexibility, and control during the procedure. Problems associated with the da Vinci system include the high cost of the device and maintenance, the need for specialized training and experience to operate the system effectively, and limitations in its versatility and capabilities, such as the size and reach of the robotic arms and instruments. [22] The need for the da Vinci system arises from the desire for less invasive surgical options that result in faster recovery times, reduced pain and scarring, and improved patient outcomes. In addition, the precision and control offered by the system can enable more complex procedures to be performed with tremendous success and minimize the danger of problems related to traditional open surgery.

System Architecture:

It is a complex and sophisticated medical technology combining advanced robotics, computer science, and medical engineering. It comprises several main components that work together to enable minimally invasive surgery.

The first component is the patient cart, which houses the robotic arms and instruments. The robotic arms are made to move similarly to a surgeon's hands, with a high degree of dexterity and precision. They are controlled by the surgeon using a console located near the patient cart. The console features an ergonomic interface and a high-definition 3D vision system that gives the surgeon an immersive view of the surgical site.

The second component of the da Vinci system is the instrument cart, which contains the surgical instruments used during the procedure. These instruments are attached to the end of the robotic arms and are designed to be highly flexible, allowing the surgeon to reach and maneuver around challenging anatomy quickly. The instruments are equipped with sensors that enable the surgeon to feel resistance, such as when the instrument encounters tissue or bone, allowing for a more natural and intuitive surgical experience.

The third component of the da Vinci system is the computer system, which acts as the "brain" of the robot. It receives inputs from the surgeon and processes them in real-time, translating them into precise robotic arms and instrument movements. The computer system also manages the video feed and 3D vision system, which provides the surgeon with a clear view of the surgical site and surrounding anatomy.

In addition to these components, the da Vinci system also features software tools designed to enhance the surgeon's experience and improve patient outcomes. For example, there are tools for planning and simulation and navigation and data analysis that help the surgeon make more informed decisions during the procedure. In conclusion, the da Vinci surgical system is a complex and sophisticated technology that combines advanced robotics, computer science, and medical engineering to enable minimally invasive surgery. It gives surgeons enhanced precision, flexibility, and control during procedures, resulting in improved patient outcomes and a more natural surgical experience.

FIGURE 14:THE DAVINCI SURGICAL SYSTEM

3.2.3 SENSEI X (HANSEN MEDICAL):

Clinical Procedure: Sensei X is a robotic catheter system developed by Hansen Medical for use in operative radiology and electrophysiology procedures. The procedure typically involves the insertion of a flexible catheter into the patient's bloodstream, guided by the robotic system. The clinician operates the system from a remote console, using the robotic controls to maneuver the catheter to the targeted treatment area. The procedure may involve the delivery of therapeutic agents or the performance of diagnostic tests. [23] The specific steps and details of the Sensei X procedure can vary based on the specific case and the treatment goals. As with any medical procedure, consulting with a trained medical professional is essential to thoroughly understand the potential risks and benefits.

System Architecture:

The Sensei X system is a type of robotic surgical system that is used in minimally invasive surgeries. The system architecture includes several key components, including: [24]

- Robotic Arm: The robotic arm is the main component of the Sensei X system and is responsible for positioning the surgical instruments within the patient's body. The arm is designed to be highly flexible and able to move in multiple directions, allowing for greater access to the target area.
- Console: The console is the control centre for the Sensei X system and is used by the surgeon to control the movement of the robotic arm and surgical instruments. The console is typically located outside the patient's body and provides a clear view of the surgical site.

- Endoscopic Camera: The endoscopic camera represents the surgical site visually and is integrated with the robotic arm. The camera provides real-time imaging of the target area, allowing the surgeon to see the surgical site in detail.
- Instrument Control Unit (ICU): The ICU controls the movement and function of surgical instruments. The ICU is typically located within the patient's body and is connected to the robotic arm and console.
- Surgical Instruments: The Sensei X system is compatible with various surgical instruments, including scissors, graspers, and dissectors. The instruments are designed to be highly precise and able to perform various functions, such as cutting, grasping, and dissecting tissue.

These components work together to provide the surgeon with precise control over the movement and function of the surgical instruments, allowing for minimally invasive surgeries with a high degree of accuracy. The Sensei X system architecture provides a flexible and adaptable platform for various surgical procedures.

The following figure will show Sensei X by Hansen Medical.

FIGURE 15:SURGICAL CONSOLE

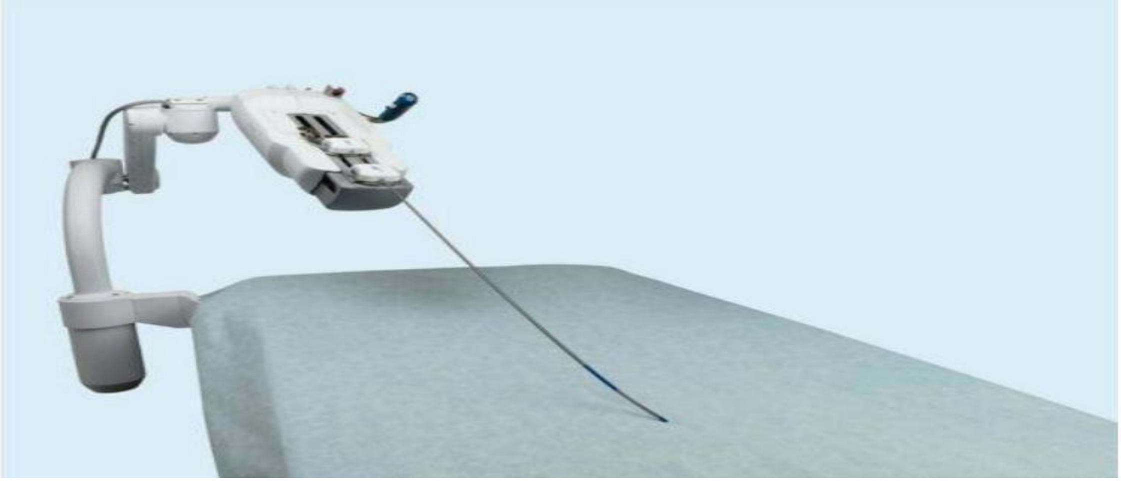

FIGURE 16:SURGICAL ROBOTIC ARM

FIGURE 17:ARTISAN CATHETER

3.2.4 CYBERKNIFE:

Clinical Procedure:

CyberKnife uses image-guidance technology to deliver high doses of radiation to cancerous and non-cancerous tumours in the body with high accuracy. [25]The clinical procedure for CyberKnife typically involves the following steps:

- Preparation: The patient is positioned on a table, and imaging scans are taken to map the tumour's location.

- Localization: Metal markers or a custom body frame may be placed near the target area to aid in precise targeting during treatment.
- Treatment: The patient lies on the treatment table and is positioned so the CyberKnife machine can target the tumour. The machine delivers a series of high-dose radiation beams to the target while the patient is continuously monitored with imaging scans to ensure accuracy.
- Aftercare: After the treatment, the patient may be observed briefly to check for adverse reactions. There is usually no downtime after CyberKnife treatment, and patients can resume normal activities immediately.

It is important to consider that the procedure can vary based on the individual patient and the location and size of the target.

System Architecture:

The CyberKnife system architecture combines hardware and software components to deliver precise, high-dose radiation to target areas within the body. The system consists of several key components:

- Linear Accelerator (Lina): The Linac produces high-energy X-rays directed at the target area.
- Multi-Leaf Collimator (MLC): The MLC is a device that shapes X-rays into a precise beam.
- Robotics System: The CyberKnife system uses a six-axis robotic arm to position the Linac and MLC. The robotics system is designed to track the movement of the target area in real-time and adjust the position of the Linac accordingly.
- Image Guidance System: The image guidance system uses real-time imaging technologies, such as X-rays, CT scans, and MRI scans, to accurately locate the target area and track its movement during treatment.
- Control Console: The control console is used by the operator to control the CyberKnife system and monitor the treatment progress.
- Treatment Planning Software: The treatment planning software creates a detailed plan for delivering radiation to the target area. The software considers the shape, size, and location of the target and the surrounding healthy tissue to ensure that the radiation is delivered with maximum precision.

These components work together to deliver high-dose radiation to the area while minimizing exposure to surrounding healthy tissue. [25] The CyberKnife system can be adjusted in real-time to account for any changes in the position of the target area, ensuring that the radiation is delivered with maximum accuracy. The CyberKnife system architecture is designed to provide high precision and accuracy in delivering radiation therapy. A few features and benefits of the system include the following:

- Real-time Image Guidance: The use of real-time imaging technologies, such as X-rays, CT scans, and MRI scans, allows the system to continuously track the location and movement of the target area during treatment. This ensures that the radiation is delivered to the target's exact location and minimizes exposure to surrounding healthy tissue.
- Non-Invasive: Unlike traditional surgery, CyberKnife is a non-invasive procedure that does not require incisions or general anesthesia. Reduced risk of complications and allows patients to recover more quickly.
- Customizable Radiation Delivery: The CyberKnife system allows customized radiation delivery to the individual patient and target area. The treatment plan can be adjusted to account for the shape, size, and location of the target and the surrounding healthy tissue to ensure that the radiation is delivered with maximum precision.
- High-Dose Radiation: The CyberKnife system can deliver high doses of radiation to the target area, effectively killing cancerous cells while minimizing exposure to surrounding healthy tissue.
- Multiple Treatments: CyberKnife can be used to treat a wide range of cancerous and non-cancerous tumours and can be used for multiple treatments if needed.

The CyberKnife system architecture is designed to provide high precision, accuracy, and customization in delivering radiation therapy. This makes it an effective treatment option for a wide range of tumours, both cancerous and non-cancerous.

FIGURE 18:CYBERKNIFE SYSTEM

3.2.5 RIO MAKO PLASTY

Clinical Procedure:

Rio MAKO plastic is a type of surgery that uses the robotic arm to assist the surgeon in performing the procedure. The surgery is typically performed on the knee or hip joint to treat osteoarthritis. The procedure begins with the surgeon making small incisions in the patient's joint and using specialized instruments to remove the damaged portion of the joint. The robotic arm is then used to precisely position and align the new joint implant, which is made of metal or plastic. The surgeon uses a computer console to control the robotic arm's movements and precisely adjust the implant's positioning during the procedure. This allows for more accurate and customized implant placement than traditional joint replacement surgeries. After the implant is in place, the surgical incisions are closed, and the patient begins a rehabilitation program to help restore mobility and strength to the joint. Rio MAKO plasty is a minimally invasive procedure that offers several benefits over traditional joint replacement surgeries, including a faster recovery time, less pain and scarring, and improved joint function.

System Architecture:

The Rio MAKO plasty system is a robotic-assisted surgical system designed for joint replacement procedures such as knee or hip replacements. The system is comprised of several key components, including:

- Robotic arm: The robotic arm is a computer-controlled device attached to the surgical table. The arm is designed to make precise movements and assist the surgeon in positioning the implant.
- Computer console: The computer console is used by the surgeon to control the robotic arm's movements. The surgeon can use the console to adjust the implant's position and ensure it is appropriately aligned with the patient's joint.
- Surgical instruments: The surgical instruments used in Rio MAKO plasty are specifically designed to be used with the robotic arm. These instruments allow the surgeon to access and prepare the joint for the implant and secure the implant in place.
- Imaging system: The Rio MAKO plasty system also includes an imaging system that allows the surgeon to visualize the joint and surrounding tissue during the procedure. The images are displayed on the computer console and used to guide implant placement.
- Patient-specific guides: The Rio MAKO plasty system uses patient-specific guides based on preoperative images of the patient's joint. These guides help the surgeon achieve the desired implant placement and alignment, leading to a more accurate and personalized joint replacement.

The system architecture of Rio MAKO plastic combines the precision and control of robotic technology with the expertise and judgment of the surgeon to perform joint replacement procedures with improved accuracy and precision. Furthermore, the robotic arm is attached to the surgical table and is controlled by the surgeon through the computer console. The arm is designed to make precise movements, allowing the surgeon to position the implant more accurately than in traditional joint replacement surgeries. The computer console is the central control unit of the Rio MAKO plastic system. The surgeon uses the console to control the robotic arm's movements and visualize the joint and surrounding tissue during the procedure. The console also displays patient-specific guides based on preoperative images of the patient's joint. These guides help the surgeon achieve the desired implant placement and alignment, resulting in a more accurate and personalized joint replacement.

The surgical instruments used in Rio MAKO plasty are designed to be used with the robotic arm. These instruments allow the surgeon to access and prepare the joint for the implant and secure the implant in place. The imaging system provides real-time visual information during the procedure, allowing the surgeon to confirm the accuracy of the implant placement. In conclusion, the Rio MAKO plasty system is a sophisticated surgical platform that combines the precision and control of robotic technology with the expertise and judgment of the surgeon to perform joint replacement procedures with improved accuracy and precision. The system is designed to minimize tissue damage, reduce recovery time, and improve joint function for patients undergoing joint replacement surgery.

FIGURE 19:ROBOTIC ARM INTEROPERATIVE ORTHOPEDIC (RIO) BY MAKO

3.3 VULNERABILITIES OF SURGICAL ROBOTICS

Surgical robotics has revolutionized the field of medicine and has provided numerous benefits to patients and healthcare providers. However, like any other technology, surgical robotics also has its own set of vulnerabilities. Following are some of the critical vulnerabilities of surgical robotics:

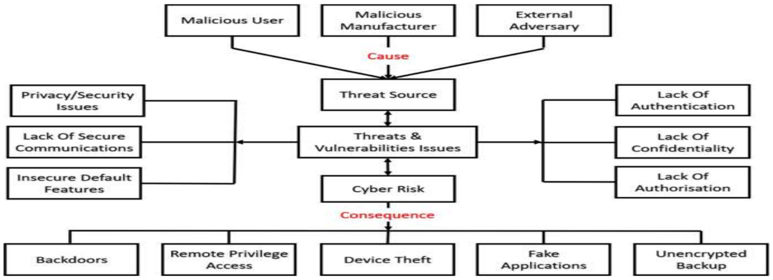

FIGURE 20:THREATS AND ISSUES

3.3.1 CYBERSECURITY

One of the significant vulnerabilities of surgical robotics is cybersecurity. As surgical robots are increasingly connected to hospital networks and the internet, they become vulnerable to hacking and cyber-attacks. The consequences of a successful cyber-attack on a surgical robot can be catastrophic, as it can compromise the safety and well-being of patients. Cybersecurity is a critical vulnerability of surgical robotics, as these systems are increasingly connected to hospital networks and the internet. This connectivity makes surgical robots vulnerable to hacking and cyber-attacks, which can compromise the safety and well-being of patients.

Cyber-attacks can impact surgical robots, including malware infections, unauthorized access, and data breaches. [26] For example, malware infections can cause the robot to malfunction or become inoperable, leading to a delay in treatment or harm to the patient. Unauthorized access can compromise sensitive patient information, while data breaches can result in the theft or exposure of confidential information. To reduce the risk of cyber-attacks, it is essential to implement robust cybersecurity measures. This can include installing antivirus software, implementing firewalls, and using encryption to protect sensitive information.
Additionally, regularly updating software and systems is essential to ensure they are protected against the latest threats. In addition to technical measures, educating healthcare providers and staff on cybersecurity and best practices for protecting against cyber-attacks is essential. This can include training on password protection, secure data handling, and reporting suspected cyber-attacks.

In conclusion, cybersecurity is a critical vulnerability of surgical robotics, and taking steps to protect against cyber-attacks is essential. By implementing robust cybersecurity measures, educating healthcare providers and staff, and regularly updating systems and software, we can ensure that surgical robots remain a safe and effective tool for improving patient outcomes.

3.3.2 HUMAN ERROR

Another vulnerability of surgical robotics is human error. Surgical robots are complex systems that require proper training and skill to operate effectively. However, suppose the operator is not adequately trained, or there is a communication breakdown between the surgeon and the robot. In that case, there is a risk of error that can lead to severe consequences. Human error refers to the mistakes or oversights made by individuals in various situations, including in the use of surgical robotics. In surgical robotics, human error can create vulnerabilities, leading to incorrect actions, miscommunication, or equipment malfunctions. For example, a surgeon might accidentally damage tissue or make a mistake during a procedure because they misused the robotic equipment or misinterpreted information displayed on the console. The risk of human error in surgical robotics underscores the importance of proper training, clear procedures, and comprehensive equipment testing to minimize these vulnerabilities and ensure patient safety.

3.3.3 TECHNICAL MALFUNCTIONS

Technical malfunctions are another vulnerability of surgical robotics. Software bugs, hardware failures, or electrical problems can cause these malfunctions. If a technical malfunction occurs during surgery, it can compromise the patient's safety and result in significant harm. Technical malfunctioning is a vulnerability of surgical robotics that can compromise the safety and well-being of patients. This type of malfunction can occur due to software bugs, hardware failures, or electrical problems and can significantly harm the patient. Software bugs are errors in the code that can cause the surgical robot to behave unexpectedly. These bugs can be introduced during the development process or caused by software updates. If a software bug occurs during surgery, it can compromise the patient's safety and result in significant harm. Hardware failures are another type of technical malfunction that can impact surgical robots. These failures can be caused by manufacturing defects, wear and tear, or exposure to physical stress. If a hardware failure occurs during surgery, it can compromise the patient's safety and result in significant harm.

Electrical problems can also cause technical malfunctions in surgical robots. Electrical surges, power outages, or other electrical disruptions can cause these problems. If an electrical problem occurs during surgery, it can compromise the patient's safety and result in significant harm. Reduce is crucial to implement robust quality control measures during the development and manufacturing process to reduce the risk of technical malfunctioning. This can include regular testing, inspection, and maintenance of surgical robots. Additionally, educating healthcare providers and staff on the proper use and maintenance of surgical robots is vital to minimize the risk of technical malfunctioning.

3.3.4 DEPENDENCE ON POWER AND CONNECTIVITY

Dependence on power and connectivity is a vulnerability of surgical robotics, as these systems require a reliable source of electrical power and a stable network connection to function correctly. If the power supply or network connection is disrupted during surgery, it can seriously harm the patient. Power outages, electrical surges, and other electrical disruptions can cause surgical robots to malfunction or become inoperable. This can result in a delay in treatment or harm to the patient and can also result in a loss of data or other critical information. Similarly, network disruptions can also impact the function of surgical robots. If the network connection is lost during surgery, it can cause the robot to become inoperable or compromise the transmission of critical information.

It is essential to implement robust backup systems and procedures to mitigate the risk of dependence on power and connectivity. This can include using uninterruptible power supplies (UPS) to ensure a stable power supply and implementing backup networks to ensure a stable connection even during a network disruption. In addition to backup systems, it is also important to educate healthcare providers and staff on the importance of power and network stability and to train them to respond in the event of a power or network disruption.

3.3.5 COST

The cost of surgical robots is another vulnerability. The high cost of these systems can be a barrier to entry for many healthcare providers, particularly those in developing countries. This can limit access to cutting-edge surgical technology and may result in a disparity in the quality of care provided to patients in different regions. [1] Cost can be considered a vulnerability in surgical robotics because the high cost of robotic surgical systems may limit their widespread adoption, especially in resource-limited settings. Additionally, the high cost of maintenance, repairs, and replacement parts can increase the overall financial burden on healthcare institutions, potentially reducing the availability of these systems for patients in need. Furthermore, training surgical staff on using these systems effectively can also add to the overall cost of implementing surgical robotics. These financial considerations can be a vulnerability for the technology, potentially affecting its uptake and success in medical settings.

3.3.6 REGULATION AND STANDARDIZATION

The regulation and standardization of surgical robotics are another vulnerability. There is no universal standard for surgical robot design, testing, and certification. This lack of standardization can lead to inconsistent quality and safety among different systems and may harm patients. Regulations and standardization are critical for ensuring the safety and effectiveness of surgical robots. Regulations provide a framework for the design, manufacture, and use of these systems and help to ensure that they meet the minimum standards for safety and efficacy. [1]

Standardization is also essential, as it helps to ensure that surgical robots are consistent in their design, function, and operation. This consistency helps to reduce the risk of technical malfunctions, improves the ease of use, and ensures that healthcare providers can rely on these systems to provide consistent, high-quality care. Several organizations are responsible for setting regulations and standards for surgical robotics, including international and national standardization organizations and regulatory bodies such as the International Organization for Standardization (ISO), the European Committee for Standardization (CEN), and the US Food and Drug Administration (FDA).

3.3.7 MAINTENANCE AND UPKEEP

The maintenance and upkeep of surgical robots are another vulnerability. These systems are complex and require regular maintenance and calibration to function correctly. If maintenance is not performed regularly, the robot may not perform optimally, leading to error and harm to the patient. Maintenance and upkeep are considered a vulnerability in surgical robotics because it involves ongoing costs and responsibilities that affect the effective and efficient use of the technology. The proper functioning of surgical robots is crucial for ensuring patient safety and positive outcomes during surgeries. Neglecting the maintenance and upkeep of these systems can lead to various problems that can compromise the quality of care provided to patients.

One of the main challenges of maintaining surgical robots is the high cost involved. ***Surgical robots*** are complex and sophisticated systems that require regular maintenance to ensure optimal performance. This can include routine software updates, hardware replacements, and equipment calibrations. The high cost of these maintenance procedures can burden healthcare institutions, especially if they have multiple surgical robots. Furthermore, the cost of maintenance and upkeep can increase over time as technology advances and newer systems are developed, requiring healthcare institutions to invest continuously in updating their equipment.

Another challenge is the technical expertise required to maintain surgical robots. Maintenance of these systems requires specialized technical knowledge and expertise, which can be in short supply. This can lead to delays in performing maintenance procedures and repairs and can also increase the maintenance cost if specialized technicians need to be hired. In some cases, surgical robots may need to be sent to the manufacturer for repairs, which can further increase the cost and lead to delays in patient care.

In addition to these financial considerations, there is also the risk of equipment failure during surgery. If the surgical robot malfunctions during a procedure, it can lead to significant patient harm and may result in legal liabilities for the healthcare institution. The maintenance and upkeep of surgical robots are critical aspects of the technology's use in medical settings. However, it also poses a significant vulnerability regarding ongoing costs, the technical expertise required, and the risk of equipment failure during surgeries. These factors must be carefully considered and managed to ensure the safe and effective use of surgical robots in the delivery of medical care.

3.3.8 DATA PRIVACY

The use of surgical robots also raises concerns about data privacy. As surgical robots are connected to hospital networks and the internet, there is a risk that sensitive patient information may be compromised. This can lead to privacy violations, data breaches, and potential harm to the patient. Data privacy is a critical vulnerability of surgical robotics, as these systems are often connected to hospital networks and store sensitive patient information. This information includes personal information, medical histories, and treatment plans, all of which must be protected to ensure patient privacy and security. Data breaches are a significant threat to data privacy, as they can result in the theft or exposure of sensitive information. Breaches can occur due to hacking, human error, or other malicious activity and can seriously harm patients and their families.

In addition to data breaches, data privacy can be compromised by unauthorized access to sensitive information. This can occur if healthcare providers or staff access information they are not authorized to see or share sensitive information with unauthorized individuals. Implementing robust data protection measures to mitigate the risk of data privacy violations is essential. This can include using encryption to protect sensitive information, implementing firewalls and other security systems, and regularly auditing access to sensitive information. Educating healthcare providers and staff on the importance of data privacy and best practices for protecting patient information is also essential. This can include training on secure data handling, safe password practices, and the importance of reporting any suspected data privacy violations. Data privacy is a critical vulnerability of surgical robotics, and it is vital to take steps to protect against data privacy violations. Implementing robust data protection measures, educating healthcare providers and staff, and regularly auditing access to sensitive information. It can be ensured that surgical robots remain a safe and effective tool for improving patient outcomes while protecting patient data's privacy and security.

In conclusion, surgical robotics has many benefits but also vulnerabilities that must be addressed. These include cybersecurity, human error, technical malfunctions, dependence on power and connectivity, cost, regulation and standardization, maintenance and upkeep, and data privacy. By addressing these vulnerabilities, we can ensure that surgical robotics remains a safe and effective tool for improving patient outcomes.

3.4 VULNERABILITIES:

Surgical robotics involves the use of computer-controlled devices to perform minimally invasive surgeries. The protocols can be broadly categorized into preoperative planning, intraoperative execution, and postoperative evaluation.

- Preoperative planning: The first stage of surgical robotics involves preoperative planning, which includes determining the patient's medical history, performing physical exams, and creating a surgical plan. Medical imaging techniques such as CT scans, MRIs, and X-rays are used to create a 3D model of the target anatomy, which helps the surgeon plan the procedure and identify potential difficulties.

- Intraoperative execution: During the surgical procedure, the patient is positioned, and the robot is prepared for use. The surgeon uses a computer console to control the robotic arms, which hold the surgical instruments and provide high precision and dexterity. The robot's movements are guided by the surgeon, who uses the 3D model created during the preoperative planning stage to ensure the accurate placement of the instruments. The robot gives the surgeon a magnified view of the surgical site and allows precise movements and control of the instruments.
- Postoperative evaluation: The patient is monitored for postoperative complications after the surgery. The surgeon reviews the data collected during the procedure, including images and recordings of the robot's movements, to evaluate the surgery's success and identify improvement areas. In some cases, additional scans may be performed to assess the outcome of the surgery.

In addition to the three stages mentioned earlier, there are a few other vital protocols involved in surgical robotics:

- Robotic instrument sterilization: Before the surgical procedure, the robotic instruments must be properly sterilized to prevent the spread of infections. This typically involves a series of steps, such as cleaning, disinfecting, and packaging the instruments for sterilization.
- Operating room setup: The operating room must be appropriately set up for surgical robotics, including the placement of the robot and the necessary monitors and controls. The room must be sterile and free from any potential sources of contamination.
- Surgical team training: The surgical team must be trained in using the robotic system and the specific surgical procedure. This typically involves classroom training, hands-on training, and supervised experience.
- Data management and storage: Large amounts of data are generated during the surgical procedure, including images and recordings of the robot's movements. This data must be adequately managed and stored to evaluate the procedure's success and for future reference.
- Maintenance and repair: The robotic system must be adequately maintained and repaired, as needed, to ensure its continued operation. This typically involves routine inspections, servicing, and prompt repair of malfunctions.

The protocols involved ensure the patient's safety, the procedure's accuracy, and the outcome's success. In summary, surgical robotics involves a complex and highly regulated process that requires proper preparation, training, and management to ensure the safety and success of the procedure. The protocols ensure that the robotic system is used effectively and efficiently and that the patient receives the best possible outcome.

3.5 NETWORKING PROTOCOLS

Networking protocol in surgical robotics refers to the set of rules and standards governing communication between the different components of a robotic surgical system. It enables seamless data exchange between the surgeon console, patient-side cart, and any auxiliary devices involved in the procedure. This includes patient anatomy data, robotic arm movements, and instrument status. The protocol ensures that all devices can communicate with each other consistently and reliably, allowing for smooth and efficient surgical procedures. Examples of networking protocols used in surgical robotics include TCP/IP, UDP, and DICOM.

The networking protocol in surgical robotics is a crucial aspect that allows the different components of the surgical system to work together seamlessly. The protocol defines the format and rules for communication between the devices, ensuring that all devices understand and can process the information sent. For example, the surgeon console and the patient-side cart communicate with each other through a wired or wireless network, sending information such as patient anatomy data, robot arm movements, and instrument status. The patient-side cart, in turn, communicates with the robotic arms and instruments, exchanging information about their position, movements, and functionality. The protocol must be robust, reliable, and secure to ensure the surgical procedure is not interrupted by communication issues or data loss. The most common networking protocols used in surgical robotics are TCP/IP (Transmission Control Protocol/Internet Protocol), UDP (User Datagram Protocol), and DICOM (Digital Imaging and Communications in Medicine).

TCP/IP is a widely used protocol for transmitting data over networks. It provides a reliable communication channel by acknowledging the receipt of data packets and retransmitting lost or corrupted packets.

UDP is a connectionless protocol that allows fast data transfer without the overhead of error correction and retransmission of lost packets. It is often used in real-time applications such as surgical robotics, where low latency and fast data transfer are crucial.

DICOM is a protocol that defines the format and structure of medical imaging data. It enables the exchange of medical images and related information between medical devices, including surgical robots.

The networking protocol in surgical robotics plays a critical role in ensuring that the different components of the surgical system can communicate effectively, providing the surgeon with real-time information and control over the robotic instruments during the procedure. The networking protocol in surgical robotics can also include additional features such as encryption, authentication, and access control to ensure the security and privacy of patient information. Encryption ensures that sensitive data is protected from unauthorized access, while authentication ensures that only authorized devices and users can access the network. Access control restricts the permissions of devices and users to only the information and functions required for their specific role in the procedure.

Another critical aspect of the networking protocol in surgical robotics is network management. This includes monitoring and controlling the network to ensure it functions correctly and provides the necessary bandwidth and reliability for the surgical procedure. Network management also includes diagnosing and fixing issues that may arise, such as network congestion, device failures, or data loss. Finally, the networking protocol in surgical robotics must be flexible and scalable to accommodate future developments in the field. As new devices and technologies are introduced, the protocol must adapt and accommodate the changing needs of the surgical system. The networking protocol in surgical robotics is a complex and critical aspect of the surgical system that ensures the seamless and secure exchange of information between the different components. The protocol must provide reliable, fast, and secure communication and be flexible and scalable to accommodate future developments in the field.

CHAPTER 4-ATTACKS INVOLVED IN SURGICAL ROBOTICS

4.1 TYPES OF ATTACKS

Surgical robotics involves the use of robot-assisted devices in the operating room. To date, security has not been a concern for telerobotic surgery. Yet researchers have identified that the open and uncontrollable nature of the communication medium opens these systems to various possible cybersecurity vulnerabilities. [27] As there is a wide range of increases in cyber-attacks when it is combined with automated processes, it leads to a rise in new threats that must be considered and enhance trust in the robotic systems. It is difficult to evaluate the risks in the robotic platforms and their effect in the upcoming days.

Cybersecurity aims to protect robotics systems from cyber-attacks and reduce the impact of vulnerabilities. It is important to introduce requirements to develop effective policies and procedures. These requirements are the “CIA Triad” referred to as the three pillars of security.

Confidentiality refers to an individual or organization's effort to control data access to avoid unauthorized disclosure and ensure that access is enabled only to authorized users for specific assets. This can be violated in many forms, from direct attacks to unintentional or accidental violations caused by human errors or lack of security controls.

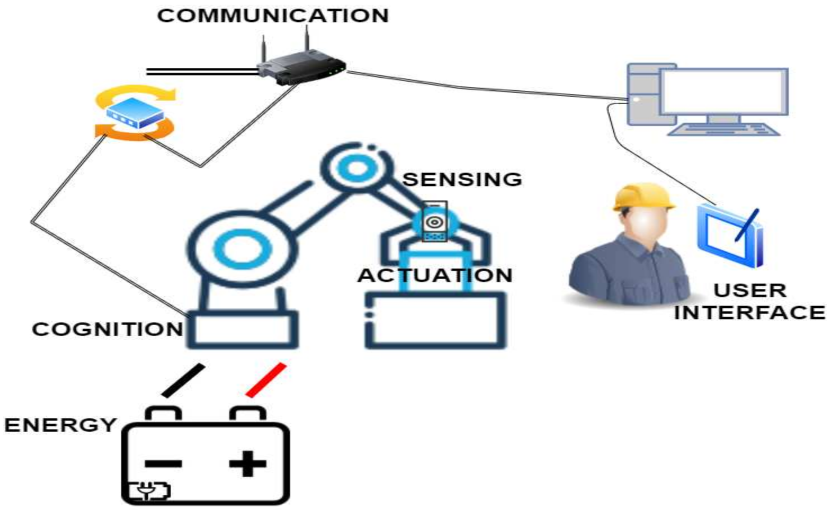

FIGURE 21:GENERAL DESIGN OF A ROBOT. [28]

Integrity: Another important factor in providing security to a robotic system is a violation of integrity, which is modifying and deleting the data. Surgical Robots are mostly exposed to risks that can be managed by Intrusion Detection software to prevent and neutralize cyberattacks.

Availability: The resources can be accessed by authorized users only for limited availability. The inability to access resources can be generally caused by malicious actions such as DoS (Denial of Service). Also, software and hardware failure or data removal can compromise its availability. The better way of optimizing the solution for this network infrastructure is to ensure redundancy between the systems so that the data is accessible continuously without any interruption.

FIGURE 22:CIA TRIAD.

To represent the robotic system, the three principles must be followed:

Accuracy: Robots send the actuators commands to perform precise operations within error margins.

Safety: Robots must make accurate information available to surgeons, as they must make decisions and perform surgeries precisely.

Integrity: The controllers must optimize the incidents that are involved in physical parts.

4.2 ROBOTIC SECURITY FRAMEWORK

For establishing security for Robots contributions have been made which include Reformulation of the categorization terms, overall restructuring of the content, formalized framework layer, Adoption of generic component and module terms, improved internal network security model, improved model for physical tampering attacks, added exemplary scenarios etc.

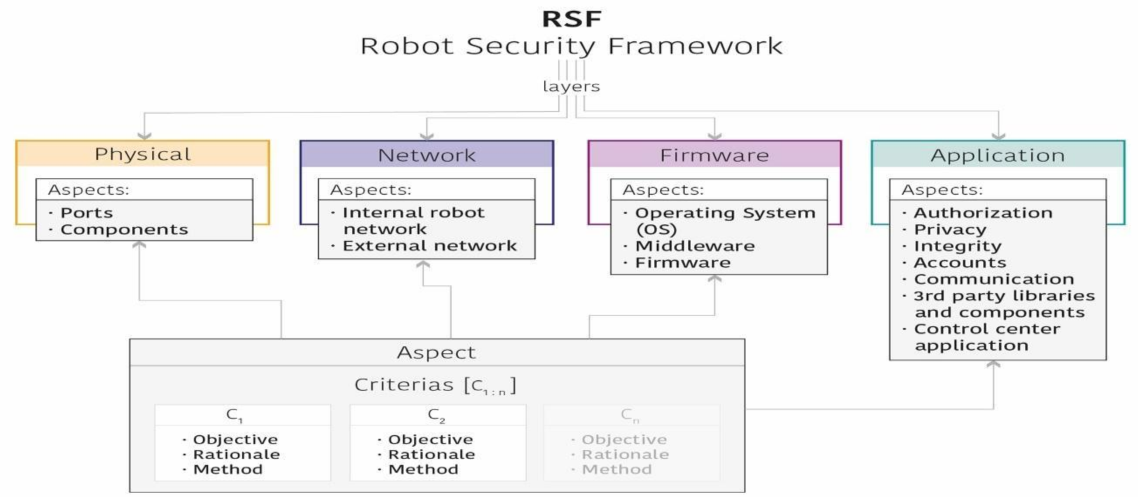

FIGURE 23:ROBOT SECURITY FRAMEWORK

The work of the Robot security framework is mainly focused on risk assessment methodology. For each of these criteria, the authors identified the following factors: what needs to be assessed (Objective), why it is necessary to perform an assessment (Rationale) and how to systematize an evaluation (Method). [28] As shown, the Robot Security Framework provides a methodology that focuses on four layers, which, in turn, cover several security elements. Each *aspect* is analyzed according to three points: 1) *Objective* or description of the evaluation, 2) *Rationale* or relevance of each aspect and 3) *Method* or systematic action plan.

4.3 SAFETY AND SECURITY IN ROBOTICS

The usage of applications in contemporary robotics systems allows humans and robots to work together in typical or industrial settings. In interactions between humans and machines, robot safety is essential. Nevertheless, focusing solely on safety may not be enough to create safe and secure robot applications. With rules and norms that outline the desirable and necessary behaviours, a certain level of safety can be ensured.

The requirement for exhaustive robot safety standards grows dramatically as robots become more advanced and omnipresent. Operating a robot can be challenging, especially if safety precautions are not used. For instance, safety has been addressed in various domains, especially in robotics systems configured for both structured and unstructured situations. The capabilities and safety features of a robot may be considerably impacted by the sort of environment in which it operates.

• Structured environments - A space that is clearly and precisely defined is said to be structured. Working in this kind of setting necessitates that a robot has a comprehensive understanding of potential barriers or impediments within a place, as well as a defined navigation technique.

- Unstructured environments – An unstructured environment is an unpredictable, chaotic space. Unstructured areas may be harder for a robot to navigate since they require more sophisticated tools. Features for recognizing and adjusting to unpredicted changes and variables may be among them (e.g., people, lighting, humidity, temperature, etc.).

Nonetheless, policymakers are updating and modifying existing rules because of the development of new technical systems. Combining and developing international robot standards is a major component of the work done by organizations dedicated to improving robotics safety, such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), and the International Electro-technical Commission (IEC).

4.4 PRIVACY IN ROBOTS

The storage, collection, use, and exchange of private data about persons are what is meant by "privacy" in robotics systems. Robots are essential in developing these boundaries as they can gather and share a lot of information, move through private areas and distances, and interact with humans.

Robots of today's generation are furnished with sensors, wearable technologies, cameras, GPS, rangefinders, accelerometers, etc. One of the topics that are discussed the most in this subject is the development of robotics applications in the context of healthcare. Data protection issues may arise if robots are used to monitor the clinical and medical conditions of senior citizens and then transmit that information in real time to medical facilities or doctors.

For instance, the increased dependency on cloud services and robotics may result in legal and regulatory issues. Applying data protection requirements, modifying safety regulations, and assigning accountability and liability are some difficult factors. A creature that can make decisions autonomously, or without the need for human input, and interact with its environment while processing a significant quantity of data is often referred to as a robot.

GENERAL DATA PROTECTION REGULATION contains criteria for software medical devices that are essential for resolving issues like limiting the liability of each party involved in the robotics chain (e.g., doctors, users, and healthcare centers). Additional publications on collaborative robotics go through where, how, and why data collected by robot sensors are used and kept. For instance, Polytechnic di Milano in collaboration with ABB and the European Institute of Oncology in Milan, Italy, built an application for Yumi, a collaborative robotic system that assisted hospitals with Coronavirus testing.

Yumi was able to evaluate 450 samples per hour and automate up to 77 percent of the testing processes. Although these systems offer a fantastic chance to maximize data collection, they may also give rise to regulatory problems over data transparency and veracity. Nonetheless, despite these initiatives, the processing of personal data in robotics remains a regulatory objective since regulators must harmonize their regulatory strategies and address privacy issues in robotics to advance with privacy laws.

4.5 CYBER-ATTACKS ON ROBOTICS SYSTEMS

By considering the CIA triad as well as highlighting specific issues and attack vectors.

Confidentiality: A malicious user could create a backdoor in general-purpose CPUs, perform buffer overflow attacks to overcome memory range protection or get around control protection techniques to get access to privileged resources during the fabrication phase.

Integrity: Robots may occasionally sustain harm from Hardware Trojan, a malicious addition and modification to Integrated Circuits. The encryption key for the system may be discovered by malicious users, compromising the system (i.e., Malicious off-chip leakage enabled by side channels). Attacks can be carried out using HW Trojans, and stealth attacks can be carried out by changing the sensor output values.

There are two ways to access robotic systems in this context: either through a network or physical components. To carry out the assault (for example, get access through industrial routers and compromise robot operations such as sensor reading, control logic execution, precise movement, and human safety), the attacker needs a network or physical access to a robot controller or robotic setup. [28]

The following is a list of specific sorts of attacks on industrial robots as they are detailed:

1)Alteration of control-loop parameters.

2)Tamper through modification of calibration parameters.

3)Tamper through modification of production logic.

4)Alteration of the user-perceived Robot state.

5)Alteration of the Robot-state.

Attacks like this can change how a robot interacts with its physical surroundings. For instance, in the case of production tampering, an attacker can compromise the manufacturing process, modify a workpiece, or cause the robot to carry out the incorrect task by using a file system or an authentication-bypass vulnerability.

Availability: This kind of approach made use of a fraudulent member to attack the server node with many requests, which caused the servers to drone, degrade, or go offline. Medical robotics is a crucial application area. The diverse robotic platforms utilized in surgical procedures are one example. Teleoperation and human-operator-robot communication are also possible with this technology. For instance, during a hijacking attack, a hacker might convince the robot to entirely disregard the surgeon's goals; as a result, packets might end up routed to the incorrect area of the network, enter an unending loop, and possibly carry out destructive operations.

Problems with robotic systems can affect all aspects of it, they are not just confined to data management. The authors, for instance, listed the most typical ways a robotic system can be vulnerable:

1)Information disclosure, technical materials available on the manufacturer's website, including software images.

2)Outdated Software: Attackers could take advantage of software vulnerabilities thanks to the custom patches that manufacturers apply to update the programme.

3)Default Authentication: Using remote connections, hackers can access devices using the "admin" or empty default password.

4)Poor transport encryption: HTTPS does not support symmetric keys, for instance, or web-based administration.

5)Poor Software Protection: Attackers can change software images that are accessible on manufacturers' websites (for example, debug information).

6)Security by Obscurity: Uncertain security may result from inadequate information regarding robots.

4.6 TYPES OF ATTACKS:

4.6.1 DENIAL OF SERVICE:

Attacks of the "DoS" variety are designed to load a network with traffic until the server goes down. Cybercriminals try to overload the network server with requests during a Denial of Service (DoS) attack until it crashes, which results in severe discomfort for users including the inability to access services. DoS attacks only use one attacking computer, but DDoS (Distributed Denial of Service) assaults use a "botnet," a collection of compromised computers that may do many jobs at once [28]. DDoS assaults are particularly troublesome since they can linger for several days or even weeks, disrupting activities and preventing people from accessing crucial information. The authors present a case study featuring robots being the target of DoS assaults.

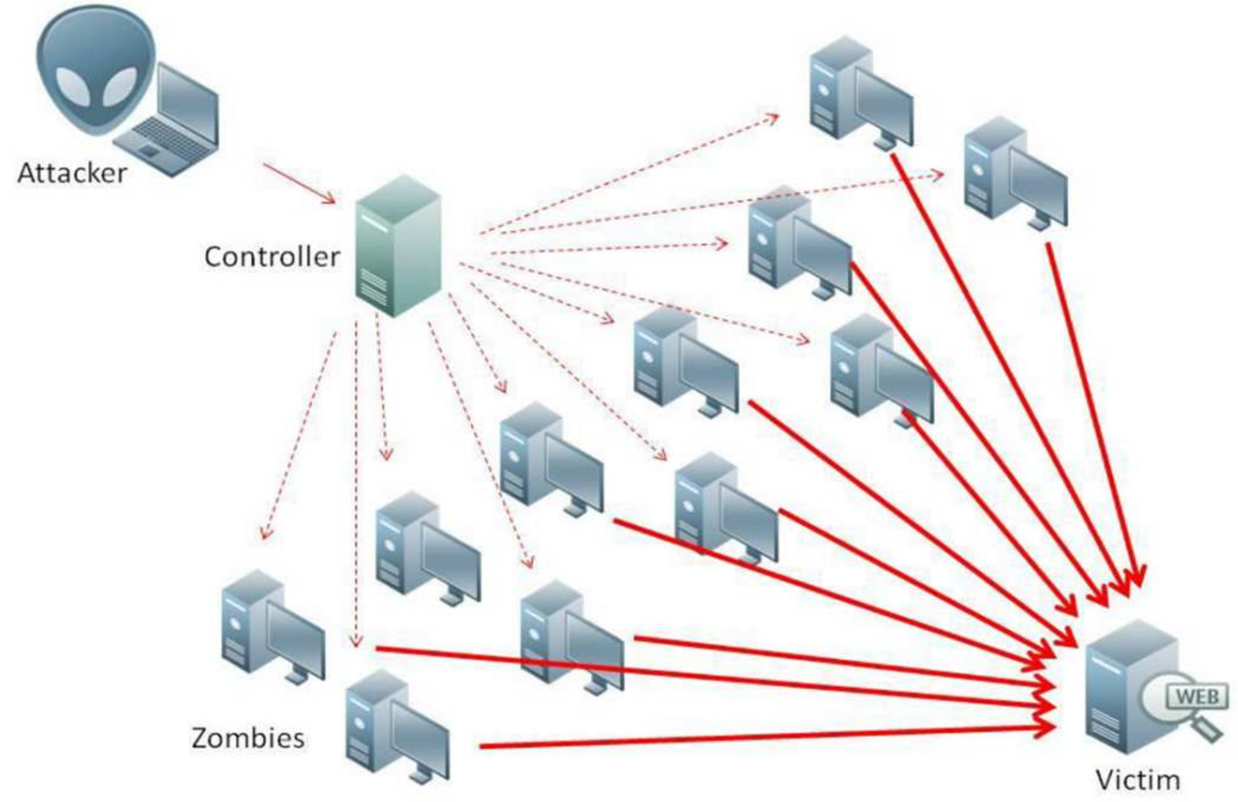

FIGURE 24:DENIAL OF SERVICE

4.6.2 SPOOFING

Spoofing is the process by which an attacker pretends to be another network device or user. Bypassing access controls, spreading malware, or stealing data are all goals of this strategy. One can spoof an IP address, an email address, or a Domain Name System (DNS) server. [29]These are the most typical types. In the world of robotics, a spoofing assault might cause a robot to act inappropriately. For instance, spoofing threats like GPS spoofing could result in users losing control of drones. To accomplish a GPS spoofing on a drone, an attacker sends fictitious GPS coordinates to the drone's control system, which then modifies the trajectory of the drone.

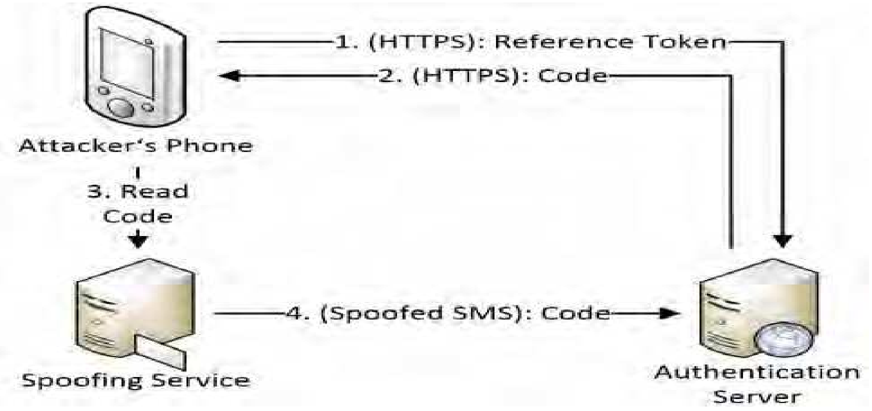

FIGURE 25:SPOOFING ATTACK

4.6.3 MAN-IN-THE-MIDDLE ATTACK

A cyber-attack called MitM allows hackers to snoop on and manipulate internet traffic. Attacks of this kind frequently target robots. Several studies have shown, as was already noted, that most robots use open-source frameworks and libraries, use insecure connections, have weak encryption, expose confidential information, have weak default setups, and have authentication and authorization issues. Some robots can be programmed using software that is installed on PCs or can be controlled by mobile devices. Via cloud-based services, other robots can communicate and share software and upgrades. Attackers can launch man-in-the-middle attacks and implant malicious software commands or updates that will be executed by robots if the communication routes between these various components are unreliable and encrypted. In addition, interface manipulation or man-in-the-middle attacks can target safety features. For instance, by forcibly stopping the robot while it is in regular operation, an attacker could trigger a denial of service (DoS).

4.6.4 TAMPERING

To alter and corrupt application data, tampering attacks often entail changing parameters sent back and forth between the client and server. User credentials, permissions, and other data are examples of the types of things this kind of assault targets. Tampering with Calibration Parameters, in which the attacker tries to alter the calibration to cause the robot to move erratically or inaccurately. Robot damage, as well as difficulties with accuracy, integrity, and safety, may occur in this situation. In this instance, the attacker subtly introduces a fault into the piece of work by manipulating the programme that the robot is running.

4.6.5 REPLAY ATTACK:

Replay attacks are carried out using intentionally repeated or delayed authorized data transmissions. This sort of attack is a real-time variation of the Man in the Middle attack, in which the malicious operator specifically intercepts user data and re-transmits it (sniffs hash and replays hash). The replay attack can be carried out asynchronously once user communication has finished.

4.6.6 FAULT INJECTION ATTACK:

A physical assault on an integrated circuit's data and behaviour is known as fault injection. Fault injection is a physical attack designed to get through safe boot mechanisms, obtain a secret key, interfere with a programme counter, etc. It can be constructed using data injection in the embedded code and implemented using the software as well.

4.6.7 SYBIL ATTACK:

The Sybil attack, specifically, uses numerous fake identities to reject the information-passing mechanism at the Network Layer (ISO/OSI). The location-based/distance-based routing protocol may be harmed.

4.6.8 JAMMING ATTACK:

An example of a DoS attack on a wireless network is jamming. This attack stops the modulation of the signal and blocks communication between other nodes by taking over the channel and often broadcasts on the same frequency. The development of detection algorithms, for instance in the machine learning-based technique to detect and classify different types of jamming attacks on RF channels, focusing on the importance of classifying the type of attack to be able to implement the necessary countermeasures, are some of the solutions being researched to avoid this issue;

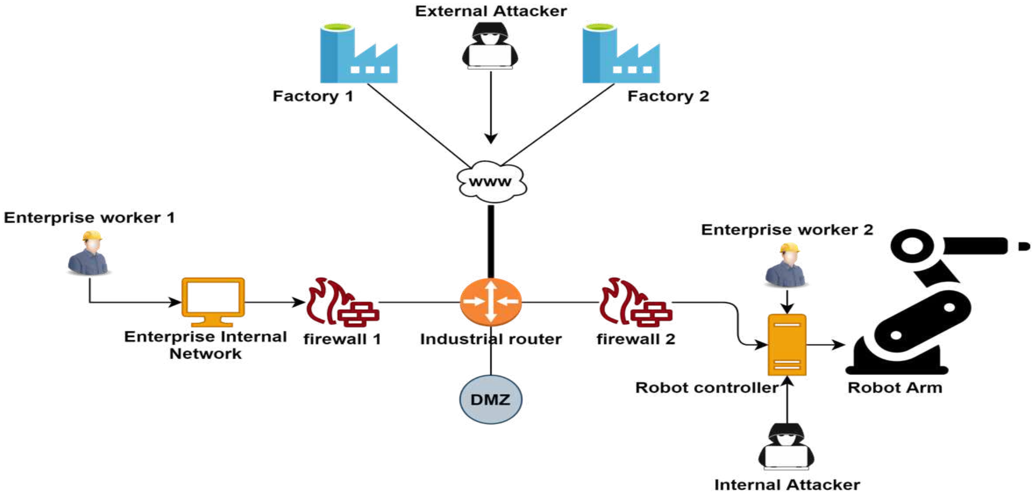

FIGURE 26:FIREWALL

4.6.9 HARDWARE BACKDOOR ATTACK

A backdoor is typically a way to get around an authentication process or encryption in a computer system. It can be produced using integrated circuits (ICs) directly during the manufacturing process, and it can be turned on by software, hardware (turning on a component), or both.

4.6.10 REMOTE ACCESS TROJAN

Malware called the Remote Access Trojan allows a malicious user to take administrative control of the target device. This kind of attack sends an email attachment or downloads a backdoor onto the target system along with user-requested software. Hence, the malicious person can transfer RATs to other vulnerable devices from the hacked target device to establish a botnet.

4.6.11 STEALTHY ATTACK

The cost and visibility of the attacker must be kept to a minimum during a stealth attack. It requires thorough knowledge of the target system or device to execute, and depending on the target type, the stealth assault is built on many stages of actuation (communication, execution, and propagation). In particular, the method of compromising sensor values through code injection is outlined.

4.6.12 HOMING ATTACK

Attackers can carry out attacks against the crucial nodes to compromise or take down the entire network by first analyzing network data to identify specific cluster heads or base stations.

4.6.13 TEARDROP ATTACK

This is a DoS attack, specifically one that bombards the target device with jumbled IP pieces carrying overlapping, large payloads. The communication between a user and a teleoperated device is thus compromised because a vulnerable server is unable to reassemble the packets.

4.6.14 PHISHING

It is an attempt to obtain private information from users, such as passwords and credit card numbers. In this instance, the anatomy of the patients being treated with a surgical instrument is utilized as an access point onto a hospital network to compromise the personal information of patients.

4.6.15 HIJACKING

A particular kind of network security assault called "hijacking" involves the attacker seizing control of communication. For example, the attacker can compromise a session by stealing or anticipating a genuine session to get unauthorized access by first posing as an observer to eavesdrop on communications between the client and server.

4.6.16 MASQUERADE ATTACK

In this attack, a malicious user poses as a legitimate user to obtain access to the target device's information resources without authorization. It is employed to get information from autonomous vehicles. In a Wi-Fi network, security might be threatened on all fronts.

4.7 ATTACKS LEVELS

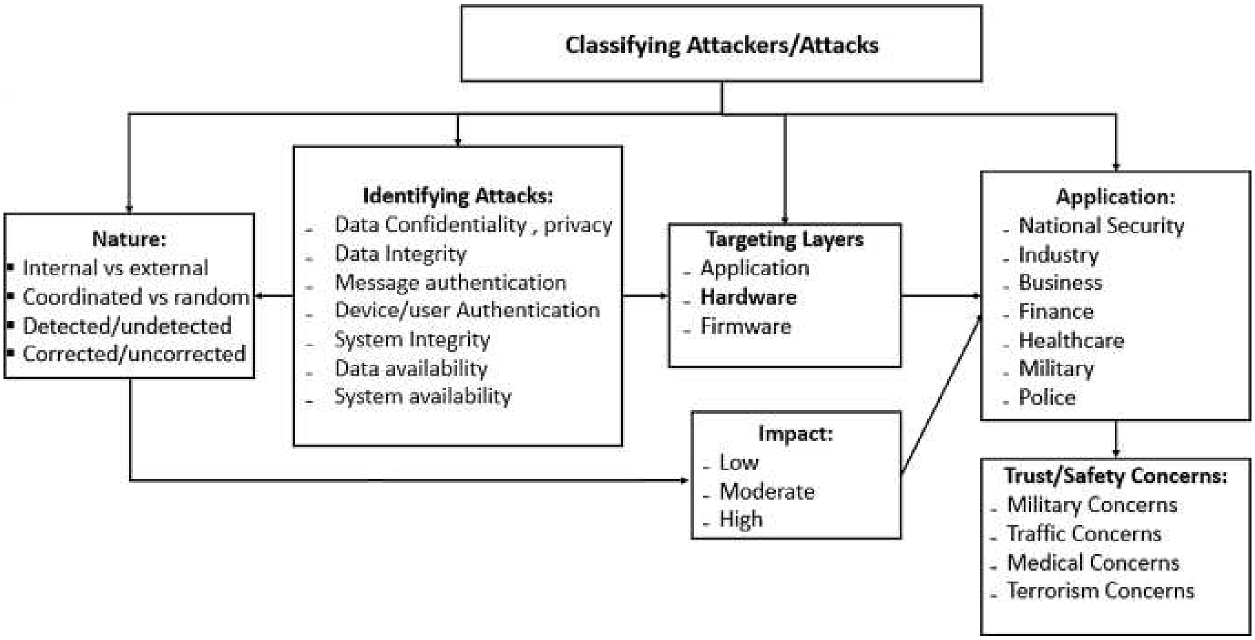

FIGURE 27:CLASSIFICATION OF ATTACKS

Insecure communications: Cybersecurity threats might arise from conflicts between users and robotics systems. This problem was specifically addressed in surgical robotics. They contended that there are numerous possibilities for hackers to access insecure communication channels, particularly if robots are linked to open networks. [30]However, according to some experts, attackers may be able to access a sizable amount of data from robotics systems using raw or inadequately encrypted messages. They contend that the use of Internet-connected libraries or programs may be to blame for the bulk of dangers to communications. Firmware is another area of robotics that is prone to communication problems. Finally, since most robots are networked to the Internet, attackers might take complete control of robots by taking advantage of communication flaws.

Authentication issues: The threat posed by artificial intelligence is one of the most underappreciated in the field of robotics. Certain robot programs are created so that no username or password is required, enabling remote access by anyone. Even though these services employ authentication mechanisms, attackers may nevertheless get around them. Similarly, most networks that robots are connected to lack password protection, making them insecure. On the other hand, when they are protected, authentication procedures might not be current, allowing unauthorized individuals to access the network. Lack of authentication makes it impossible to verify whether the robot's physical components have been accessed. Because of this, attackers might readily engage or tamper with any.

Missing authorization: Robotic devices and their resources should only be accessible to authorized users. If unauthorized access is not effectively managed, it may be possible for attackers to readily use specific robotic characteristics and control the robot from a distance. Most dangers at the application level involve the ability to remotely access robotics through Internet services, software, mobile devices, etc. Furthermore, these programmes communicate across networks, which could be vulnerable points for an attack. Anyone with access to the same network can communicate with the robot and provide commands to it. [30]Robots may potentially be attacked while having their firmware maintained in the event of a failed authentication. For instance, some manufacturers of robots make the device's firmware susceptible by making it accessible online for upgrades. Making firmware accessible to the public, however, only becomes problematic if the firmware is customizable. Unauthorized physical access to a robot can also cause problems with availability. The intrusive party may damage the hardware of the gadget and utilize it to alter its data or behaviour.

Privacy issues: Several experts worry that privacy issues could arise as a result of robotics, providing businesses unrestricted access to people's lives. For instance, without the user's knowledge, mobile robot applications can communicate sensitive information to distant servers. One of the main dangers at the firmware level is that an attacker could gain access to the robot through firmware.

Weak default configuration: When insecure features are included in a robot's initial configuration, they can be readily turned off or accessed. Attacks that take advantage of these features often operate at the network level, but there may also be programmes that are accessible with default passwords or created using open-source code and libraries that are vulnerable. Furthermore, attempts could be made to corrupt firmware that is installed incorrectly or has an outdated configuration.

Overview of attacks

Given their devastating effects on robots and their resources, it is obvious that this kind of attack occurs most frequently in robotics. Another explanation for this is that DoS attacks are simple to carry out and can even be done with the use of freely accessible tools that enable attackers to produce malicious code, such as bots. [30] On the other hand, stealthy and Sybil attacks are the least common due to the need for advanced methods and talented attackers. Due to a variety of availability difficulties, the network layer is the most crucial. A robotics system serves as the foundation for all communications. Since it exposes more vulnerabilities and where defences are frequently most vulnerable, the firmware layer is also one of the most important areas of cyber security.

4.8 CURRENT ISSUES

Robotics equipment and applications are being used by businesses and consumers more and more, which is causing cyber risk to increase exponentially. Robotic systems may have vulnerabilities of any kind, whether they be caused by software, hardware, or user error. Cyberattacks can take advantage of any of them. As a result, many scholars and specialists are putting a lot of emphasis on cyber security when trying to identify ways to limit the growing number of cyber-attacks in this field. [12]

Security by design -Safety by design involves minimizing software and hardware vulnerabilities. This process necessitates that security properties are properly considered right away during the requirements phase of development. For robotics applications, it is very important to consider security requirements in engineering, including privacy and safety concerns. Also, the socioeconomic effects of the requirements evolution across the entire SDLC (systems development life cycle) should be considered. In a similar vein, programming environments need to develop security support. This study topic focuses on innovative programming frameworks that provide runtime and development environments for reliable applications that are used in challenging robotics scenarios. The goal of this field is to protect coding standards as well as language-based security.

Security and safety co-engineering - One of the issues with headrest development is creating a safe and secure system. These two ideas could conflict depending on the situation, and any solutions must address certain risks connected to both domains.

Monitoring - An efficient technique to detect and prevent such assaults is by tracking and monitoring robotic activity, accesses, and the use of privileged accounts. Before an attack's effects are felt by the systems, detection techniques can evaluate their impact in real-time. Systems for detecting and preventing intrusions ought to be used. Investigating specific anomaly detection techniques that can behaviorally fingerprint robot behaviour.

Data usage control - One of the key functions of robotics systems is sensing. Those who frequently collaborate with humans, where sharing and distribution of the data collected should be managed;

Identity management - Robotic systems are often composed of several devices that have input-output capabilities. Considering how to identify the robotic systems is paramount for the consideration of trust issues related, for instance, to collaborative aspects;

Trustworthiness - For humans and robots to connect and have a "safe relationship," trust is a crucial idea. Since the "trustor is dependent on the trustee" and there is never complete certainty while relying on them, trust, which is described as "an attitude involving beliefs and expectations about a trustee's trustworthiness," is frequently linked to vulnerability. Recent studies have demonstrated that when functionality and operation act poorly and fall short of expectations, trust in social or professional robots is lost.

Hence, trust is a crucial issue to take into account while attempting to trust that robot systems behave securely (e.g., trusting that the information users get from the robotic device is secure and reliable). Building robotics systems with security by design and default is one way to increase confidence in robotics. Understanding that robot inventors and manufacturers take cyber security into account at every level of design and development could help establish a better functional operating system for robots and their users as a guarantee for the entire robotics industry.

Robustness-Robotics companies have increased perimeter security measures and implemented firewalls and other protection systems, especially for those who have experienced the effects of cyberattacks. These security measures are vital, but they still fall short of protecting businesses from serious online dangers.

Due to the ongoing development of robotics systems and the associated dangers and difficulties in the areas of cybersecurity and safety, robotics is a multidisciplinary study field that is becoming more and more important and relevant.

Finally, we saw that, over the past few decades, the area of robotics research and development evolved from being mostly concerned with robots to being primarily concerned with intelligent robotics. This change gave rise to simpler integration techniques for robotics systems that can produce encouraging outcomes in a variety of robotics research fields, including artificial intelligence, cognitive robotics, human-robot interaction, multi-agent systems for collaborative mobile robots, etc.

The employment of AI and ML algorithms created new security and safety problems. Although the rate of robotics development will likely be slowed by the adoption of necessary regulatory constraints, the current generation of highly powerful robotic systems has the potential to significantly alter a wide range of human endeavours. To identify the most frequent risks, threats, and vulnerabilities, this article will compile the most pertinent studies in the field. This work will be used as a body of knowledge and reference tool to assist cybersecurity professionals, users, manufacturers, and academics in better comprehending the dangers posed by this area and raising awareness of the subject.

CHAPTER 5- ESTABLISHING SECURITY FOR ATTACKS

5.1 RISK ASSESSMENT IN SURGICAL ROBOTS

Modern surgical robots are multifunctional mechanical and digital platforms that integrate data and give insights using cutting-edge computational methodologies to improve the procedure. Integrating data sources, hardware, software, and networking required to carry out these tasks creates new vulnerabilities and may make it possible for an attack to expand to multiple robots simultaneously.

Robotic surgery has many uses for artificial intelligence methods like machine learning, including identifying anatomical structures or operative tasks, predicting procedure length, and enhancing visual tissue differentiation. [12] Artificial intelligence (AI) solutions frequently need a lot of data to develop them and a lot of technological infrastructure to run them. As their performance evolves, cybersecurity risks are associated with AI solutions. Beyond sophisticated computational techniques, surgical robotics also relies on numerous network, information, and communication technologies to function.

As an illustration, hardware, firmware, and software components of surgical robots have unique dangers and safety improvement methods. In order to lower the likelihood that specific components, such as field-programmable gate arrays, have not been compromised, hardware concerns, for instance, may require close relationships with manufacturers. From a software standpoint, hardware producers must invest significantly in creating secure software and releasing updates frequently. [18]For instance, the Da Vinci robot receives frequent software updates. Other surgically close-by robot features, such as vendor support features, training tools, and video clips, must also be considered and cybersecurity optimized. To further reduce risk, it should carefully consider how much real-time internet connectivity is required for a robotics platform during a process; alternatively, separate, private networks may do so.

Data encryption, antivirus software, employee training, and a risk-based strategy for cybersecurity are all examples of best practices in cybersecurity hygiene. Preparedness requires the use of mitigation techniques like training OR staff in emergency robotic undocking, threat detection, and incident response planning. Individual workers continue to pose the most significant cybersecurity risk to an organization; all it takes is one successful phishing attempt to obtain credentials that can grant access to internal systems. [30]. Although compliance with best practices will not ever ensure cybersecurity security, it will help to reduce risk and give a defence in case of an assault.

5.2 CYBERATTACKS ON SURGICAL ROBOTS

Cyberattacks on surgical robots can disrupt surgical procedures and compromise patient data, posing a severe risk to patient safety. Here are a few examples of potential surgical robot cyberattacks: [29]

- Malware attacks: Malware, such as viruses and ransomware, can infect surgical robot software, causing it to malfunction or become inoperable. This has the potential to disrupt surgical procedures and jeopardize patient safety.
- Denial-of-service (DoS) attacks involve flooding a network or system with traffic, causing it to become overwhelmed and unresponsive. DoS attacks can disrupt communication between surgical robots and remote operators, making robot control difficult or impossible.
- Man-in-the-middle attacks: Man-in-the-middle (MITM) attacks involve intercepting and manipulating data as it travels across a network between devices. MITM attacks can compromise patient safety by altering data transmitted between surgical robots and remote operators.
- Data breaches: Cybercriminals can gain unauthorized access to patient data stored on surgical robots or other connected devices, resulting in data breaches. This may jeopardize patient privacy and expose sensitive data to cybercriminals.

To tackle cyber-attacks, it is critical to implement strong measures such as firewalls, intrusion detection systems, and encryption.

Regular software updates and patches can also aid in the remediation of known vulnerabilities and protect against emerging threats. Furthermore, staff training and education can raise awareness of cybersecurity risks and promote best practices for securing surgical robots and other connected devices. Finally, contingency plans and backup procedures should be in place to address the possibility of cyberattacks and minimize the impact on patient safety.

5.2.1 CONSEQUENCES OF ATTACKS

- Surgery is delayed or disrupted: A cyberattack can cause surgical robots to malfunction or become inoperable, causing surgery to be delayed or disrupted. For example, if a hacker gains control of a surgical robot during a procedure, the robot may cease functioning, potentially establishing the patient's safety.

- Misinformation: A cyberattack can cause the surgical robot to send incorrect information to the remote operator, such as sensor data. This may cause the remote operator to make incorrect decisions, potentially leading to surgical errors.
- Unauthorized access: A cyberattack can result in illegal access to the surgical robot, allowing a hacker to control the robot or access patient data. This can endanger patient privacy and expose sensitive information to cybercriminals.
- Data manipulation: A cyberattack may involve the manipulation of data transmitted between the surgical robot and the remote operator, potentially altering sensor data or video feeds. This can lead to the remote operator making incorrect decisions, potentially compromising the patient's safety.

Furthermore, staff training and education can help raise awareness of cybersecurity risks and promote best practices for securing surgical robots and other connected devices. Finally, contingency plans and backup procedures should be in place to address the possibility of cyberattacks and minimize the impact on patient safety. Surgical robots have several advantages over traditional surgical techniques, but they also have some disadvantages. [4]

- **Cost:** As surgical robots are expensive to acquire, maintain, and repair, using them could ramp up healthcare prices.
- **Learning curve:** To use surgical robots efficiently, surgeons must undergo significant training, which can be time-consuming and expensive.
- **Technological issues:** Like any other machinery, surgical robots may encounter issues that complicate operations.
- **Low tactile input:** One of the significant limitations of surgical robots is the surgeons' limited tactile feedback, which makes it harder to feel tissue resistance and other crucial clues during surgery.
- **Lack of flexibility:** Certain surgical robots have a limited range of motion, which makes it challenging to carry out specific operations or access certain body parts.
- **Dependence on technology:** Surgical robots rely extensively on technology, which could cause delays if there are technical difficulties such as connectivity problems, power outages, or other issues.
- **Ethical concern:** Some people are worried about the moral ramifications of surgical robots, such as the potential dehumanization of patients or replacing human talents with machines.

Cost: Hospitals and medical facilities might consider developing shared-use agreements or leasing arrangements to replace acquiring their equipment to manage surgical robots' expenses. This might still give healthcare institutions access to the technology while easing their cost load.
Learning curve: More thorough training on surgical robots could be included in surgical training programmes. Moreover, producers may create better simulation and training tools to

assist surgeons in acquiring the knowledge and expertise required to operate these devices successfully.

Technical failures: Surgical robots should undergo routine maintenance and inspections to reduce the possibility of technical failures. To prevent difficulties during surgery, surgical teams should also get training in the early identification and resolution of technical concerns.

Limited tactile feedback: Modern surgical robots with more sophisticated haptic feedback systems are being developed to give surgeons better tactile feedback. Moreover, producers might provide more sophisticated training aids to teach surgeons how to compensate for the absence of tactile input during operation.

Lack of flexibility: To simplify executing a wider range of surgical procedures, manufacturers might create surgical robots with larger degrees of freedom and a better range of motion.

Concerns about ethics: To address these issues, surgical teams should ensure that patients are fully educated about the use of surgical robots and are aware of both the advantages and disadvantages of the technology. Moreover, manufacturers might create more user-friendly, intuitive robot designs to lessen the possibility of dehumanizing patients or replacing human abilities with machines.

- **Artificial intelligence:** Including artificial intelligence (AI) in these systems is one of the most critical trends in surgical robots. By analyzing massive amounts of data and giving surgeons access to real-time insights and decision support, AI can help to enhance surgical results.
- **Miniaturization:** Creating minor, more portable devices that can be employed for minimally invasive surgery is another trend in surgical robotics. These tiny robots can be more precise and less intrusive than powerful ones, leading to better patient outcomes and faster healing.
- **Modular systems:** Another current development gaining favour is modular surgical robots. These systems can be set up to accommodate the particular requirements of each surgical treatment, which can increase effectiveness and lower costs.
- **Collaboration robots:** Often referred to as cobots, collaborative robots are a current development in surgical robots. These machines are made to support and aid human surgeons while they perform surgery. This can lessen the chance of problems and enhance surgical outcomes.
- **Remote surgery:** Remote surgery is a new development in surgical robot technology. In this case, the patient will have surgery while the surgeon is in a different place. Patients in remote or underserved locations may have better access to surgical care thanks to remote surgery, which may also lower the risk of infection transmission during surgery. Before remote surgery is generally accessible, however, considerable technical and legislative difficulties must be resolved.

However, each technology—collaborative robotics and remote surgery—has difficulties. Before remote surgery, there are still technical and regulatory hurdles that need to be overcome with collaborative robots for them to work safely alongside human surgeons. To ensure that real-time data and video can be transmitted between the surgical site and the remote operator with the utmost efficiency and minimal latency or disruption, both collaborative robots and remote surgery require a high level of connectivity and dependability in computer networks.

5.3 INITIALIZING LATENCY

Since even minor data transmission delays can negatively affect patient safety, achieving low latency in computer networks is essential for remote surgery.

Listed below are a few methods for reducing latency: [31]

- **Use high-speed networks**: Remote surgery necessitates networks that can reliably and swiftly send enormous amounts of data. Performance can be increased by reducing latency and utilizing high-speed networks like fibre-optic connections.
- **Enhance network setups**: Network configurations can dramatically impact latency. Reduce latency and boost overall network performance by optimizing network settings including data packet size and traffic routing.
- **Prioritize traffic**: Making sure that vital data, such as video feeds and sensor data from the surgical site, is given priority over less critical data on the network can help. By doing so, latency may decrease and the most crucial data may be reliably and swiftly transferred.
- **Employ edge computing**: Edge computing is the practice of processing data locally, at the network's edge, instead of sending all of it to a central place for processing. Cutting down on the amount of distance that data must travel, can help to reduce latency.
- **Implement redundancy:** Redundancy involves using backup systems and redundant network paths to ensure that data can continue transmitting even if there is a network outage or other issue. This can help to minimize downtime and ensure that critical data is always available.

5G networks have the potential to reduce latency in remote surgery and other applications that require real-time data transmission. Here are a few ways that 5G can help to reduce latency:

- **Faster data transmission speeds**: 5G networks can transmit data up to 100 times shorter than 4G networks. Data can be transmitted faster and with lower latency, enabling real-time communication between remote operators and surgical robots.

- **Lower network congestion**: 5G networks are designed to handle more devices and higher data traffic volumes than 4G networks. This can help reduce network congestion and improve overall performance, leading to lower latency.
- **Edge computing:** 5G networks can support edge computing, which involves processing data locally, at the edge of the network, rather than sending it all to a central location for processing. This can reduce latency by minimizing the distance data needs to travel.
- **Network slicing**: 5G networks support network slicing, which involves dividing the network into virtual segments that can be customized for specific applications or use cases. This can help to optimize network performance for real-time applications like remote surgery, reducing latency and improving overall network reliability.

5.4 CONCLUSION

Unfortunately, robotic systems have several security vulnerabilities that can be used to conduct dangerous attacks. These attacks could have major impacts on these infrastructures, ranging from financial losses to the loss of human lives. These attacks are feasible because robotic systems lack built-in security and depend on open wireless communication channels. As a result, it is strongly advised to take all essential precautions to protect robots from any potential attacks. This involves identifying and defeating attempts by hackers to break into these systems and introduce harmful software or data to disrupt the operation of the robots or leak sensitive information.

It is very important to implement security solutions for data to be secured. There are two types of security measures to consider i.e., threat-centred values and data-centred ones. Robot security should be included in the design, and developers of firmware, hardware, and software must consider security as a critical factor. Very secure cryptographic procedures should be used to accomplish this transfer. The establishment of permission and authentication policies makes the robotic system less vulnerable to insider threats by preventing unauthorized entities from accessing it.

When a security threat is identified, it is necessary to put in place measures that immediately disconnect or/and turn off the robot. This can guarantee that robots won't be under the control of an enemy, preventing any damage from happening along with injuries or/and death. Each robot must have a self-destructive chip—which could be hardware or software—implemented to accomplish this. Robots must go through a routine testing process to determine how much of a hazard they are to human life.

It's important to assess the security of the programs used to control the robots. This makes it easier to identify any exploitable vulnerability or security hole and to close it quickly. Creating automated robotic penetration tests allows for this to be accomplished.

To track down and reconstruct any potential attack events, enhanced forensics are not being given much significance. To compare patterns, locate streams, and study data, network forensics analysis is also used. Safer robotic designs and robotics must go through a safety test both before and after obtaining the necessary design to lower the likelihood of any potential risk that could prove to be damaging or lethal against any human operation. To ensure that robots can withstand a variety of attacks in a smart way that allows them to recover and re-operate normally by identifying the affected node and isolating it to prevent further damage, smart self-healing processing must be adopted by-design phase or added at a later development stage.

Overall,5G networks have the potential to significantly improve the performance of remote surgery and other real-time applications by reducing latency and improving network reliability. However, the widespread adoption of 5G networks is still in the early stages, and technical and regulatory challenges must be addressed before the full benefits of 5G can be realized.

Bibliography

[1] B. Davies, "Robotic Surgery – A Personal View of the Past, Present and Future," International Journal of Advanced Robotic Systems, Genova, 29 September 2014; Accepted 16 January 2015.

[2] I. Avellino, "Why Telemanipulated Surgical Robots Affect Creative Tool Use," Honolulu, HI, USA, CHI 2020, April 25–30, 2020.

[3] E. B. Wilson, "THE EVOLUTION OF ROBOTIC GENERAL SURGERY," Scandinavian Journal of Surgery, Department of Surgery, University of Texas Health Science Center at Houston, Houston, Texas, U.S.A. , 2009.

[4] B. Davies, "Robotic Surgery – A Personal View of the Past, Present and Future," International Journal of Advanced Robotic Systems, Genova, 29 September 2014; Accepted 16 January 2015.

[5] G. N. M. ·. S. R. ·. M. A. M. ·. J. S. Klebanoff1, "Robotic surgery during the COVID pandemic: why now and why for the future," Journal of Robotic Surgery, 27 June 2020 / Accepted: 13 July 2020.

[6] J. H. K. S. S. a. K. P. Mireille Truong, "Advantages of robotics in benign gynecologic surgery," Wolters Kluwer Health, Inc., Virginia, USA , 2016.

[7] T. F. &. C. P. Steiner, "Robotically assisted gynaecological surgery," Cleveland, Ohio, USA, 03 Jul 2009..

[8]

[9] A. HARKY, "Robotic Cardiac Surgery: The Past, Present and the Future," Heart, Lung and Circulation, 25 January 2019.

[10] M. K. C. M. a. C. S. C. MARK TALAMINI, "Robotic Gastrointestinal Surgery: Early Experience and System Description," JOURNAL OF LAPAROENDOSCOPIC & ADVANCED SURGICAL TECHNIQUES, Baltimore, Maryland., 2002.

[11] A. Garg, "Robotic surgery in head and neck cancer: A review," a ENT Dept., Grant Medical College, B.R. Ambedkar Road, Byculla, Mumbai 8, India, 4 March 2010.

[12] K. Cleary, "State of the Art in Surgical Robotics: Clinical Applications and Technology Challenges," Computer Aided Surgery, Washington, DC, 2001.

[13] M. E. Moran, "Evolution of robotic arms," *JOURNAL OF ROBOTIC SURGERY,* 2007.

[14] L. R. K. M.D., "A modular surgical robotic system for image guided percutaneous procedures," in *Springer, Berlin, Heidelberg*, 2006.

[15] J. T. Wilson, "Evaluating remote centers of motion for minimally invasive surgical robots by computer vision," IEEE, Montreal, QC, Canada, 2010.

[16] E. V. Poorten, "Surgical robotics beyond enhanced dexterity instrumentation: a survey of machine learning techniques and their role in intelligent and autonomous surgical actions," *International Journal of Computer Assisted Radiology and Surgery volume,* 2016.

[17] F. KHAN, "ROBOTIC SURGERY AND MACHINE LEARNING," *AITS JOURNAL,* 2019.

[18] K. H, " Robotic assisted suturing in minimally invasive surgery," Rensselaer Polytechnic Institute , Troy, New York, 2002.

[19] P. CULMER, "HAPTICS IN SURGICAL ROBOTS," UNIVERSITY OF LEEDS, LEEDS, UNITED KINGDOM, 2019.

[20] D. S. NISAR, "ROBOTS WITH MEDICAL APPLICATIONS BOTH NEAR AND FAR," KYOTO UNIVERSITY OF ADVANCED SCIENCE.

[21] S. C. L. a. L. PHEE, "A REVIEW OF MASTER–SLAVE ROBOTIC SYSTEMS FOR SURGERY," *International Journal of Humanoid Robotics.*

[22] P. R. A. C. K. S. A. C. &. D. O. Brian S. Peters, "Review of emerging surgical robotic technology," 2018.

[23] J. G. S. G. &. T. T. Nan Xiao, "A robotic catheter system with real-time force feedback and monitor," 2012.

[24] B. S. B. K. R. T. A. F. K.R. Julian Chun, "Catheter Ablation – New Developments," Germany, 2008.

[25] Q. AM, "CyberKnife: a robotic radiosurgery system.," Clinical Journal of Oncology Nursing, 2002.

[26] N. I. H. L. G. P. J. &. A. L. William J. Gordon, "Protecting procedural care—cybersecurity considerations for robotic surgery," 20 September 2022.

[27] T. BONACI, "TO MAKE A ROBOT SECURE:AN EXPERIMENTAL ANALYSIS OF CYBER SECURTY THREATS AGAINST TELEOPERTAED SURGICAL ROBOTICS," UNIVERSITY OF WASHINGTON, SEATTLE, MAY 13 2015.

[28] G. LACAVA, "CYBERSECURITY ISSUES IN ROBOTICS," CNR-IIT ITALY, PISA, 2021.

[29] H. N. N. O. S. Jean-Paul A. Yaacoub, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," International Journal of Information Security, 2022.

[30] K. Chung1, "Smart Malware that Uses Leaked Control Data of Robotic Applications:," 1University of Illinois at Urbana-Champaign.

[31] N. I. H. L. G. P. J. &. A. L. William J. Gordon, Protecting procedural care—cybersecurity considerations for robotic surgery.

[32] F. khan, "Robotic Surgery and Machine Learning," 2015. [Online]. Available: https://medium.com/ai-techsystems/robotic-surgery-and-machine-learning-7f87824228ea.