Advancements in AI-based Robotics and Automation with Emerging Cybersecurity Threats and Challenges

Doshi Krisha[1*], Shah Diya[2], Deep Solanki[3], Jigar Gajjar[4]

Lok Jagruti Kendra University, Ahmedabad, GJ, India[1*]
Lok Jagruti Kendra University, Ahmedabad, GJ, India[2]
TechD Cybersecurity Limited, Ahmedabad, GJ, India[3]
TechD Cybersecurity Limited, Ahmedabad, GJ, India[4]

krishadoshi444@gmail.com[1*],shahdiya1164@gmail.com[2],deepsolanki5799@gmail.com[3],cyberian.jg@gmail.com[4]

Abstract: Mechanics and automation technology provide the capability for machines to perform actions with minimal involvement of the human factor, which positively affects the efficiency, precision, and safety of the process and products created by a machine. Advanced robotic systems integrate sensors, control systems, and artificial intelligence for the purpose of facilitating intelligent, adaptable, and automated technology in various industries. The incorporation of technology in the field of robotics and automation has enabled traditional systems to advance from fixed and pre-programmed operation systems to flexible and data-based systems that are able to make real-time operational decisions. In the paper, there will be a discussion about the contributions and implications of the incorporation of technology in modern systems per-training to issues of productivity, reliability, and human-robot interaction. The increasing incorporation of intelligent robotic systems into automation systems reveals its necessity in developing a smart industry.

Keywords: Robotics, Automation, Intelligent Systems, Control Algorithms, Artificial Intelligence, Sensors and Actuators, Robotic Automation, Human–Robot Collaboration, Adaptive Systems, Industry 4.0.

I. INTRODUCTION

Robotics is the study and application of robots, which are machines that can perform automatically or with very little human intervention [1]. A robot can perceive its environment, process information according to a program or AI, and act by moving its arms, wheels, or tools. Robots are very useful for performing tasks that are repetitive, hazardous, or require a high degree of accuracy[13].Automation is the use of machines, software, or control systems to perform tasks automatically without continuous human intervention. Automation is more concerned with process control than robotics.

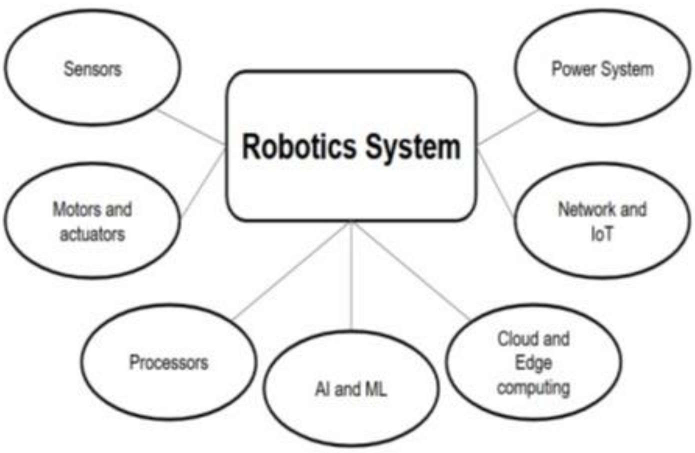

Fig.1.Components of Robotics System

http://doi.org/10.63766/spujstmr.26.000103

ISSN: 3049-1479(Online)

Robotics and automation are some of the latest technologies that have proved to be highly influential in the current development of industry and technology[4]. Robotics is an area that deals with the design and implementation of programmable machines that can carry out tasks with a high degree of precision, while automation is the use of control systems, software, and intelligent technologies to minimize human interaction in a process[7].

Robotics is a field that involves designing, building, controlling, and using robots that can work on their own or with some human help [2][3]. It brings together ideas from different areas like mechanical and electrical engineering, computer science, control systems, and artificial intelligence to create machines that can sense their environment, understand information, and take physical actions [2][7]. Modern robots usually have sensors to see and feel, control systems to make decisions, and motors or actuators to move and do tasks. Robotics is used in many industries such as manufacturing, healthcare, delivery, space missions, farming, and services to help improve efficiency, accuracy, and safety [4][8]. The field keeps growing, focusing on making robots smarter, more flexible, and able to work closely with people in changing environments.

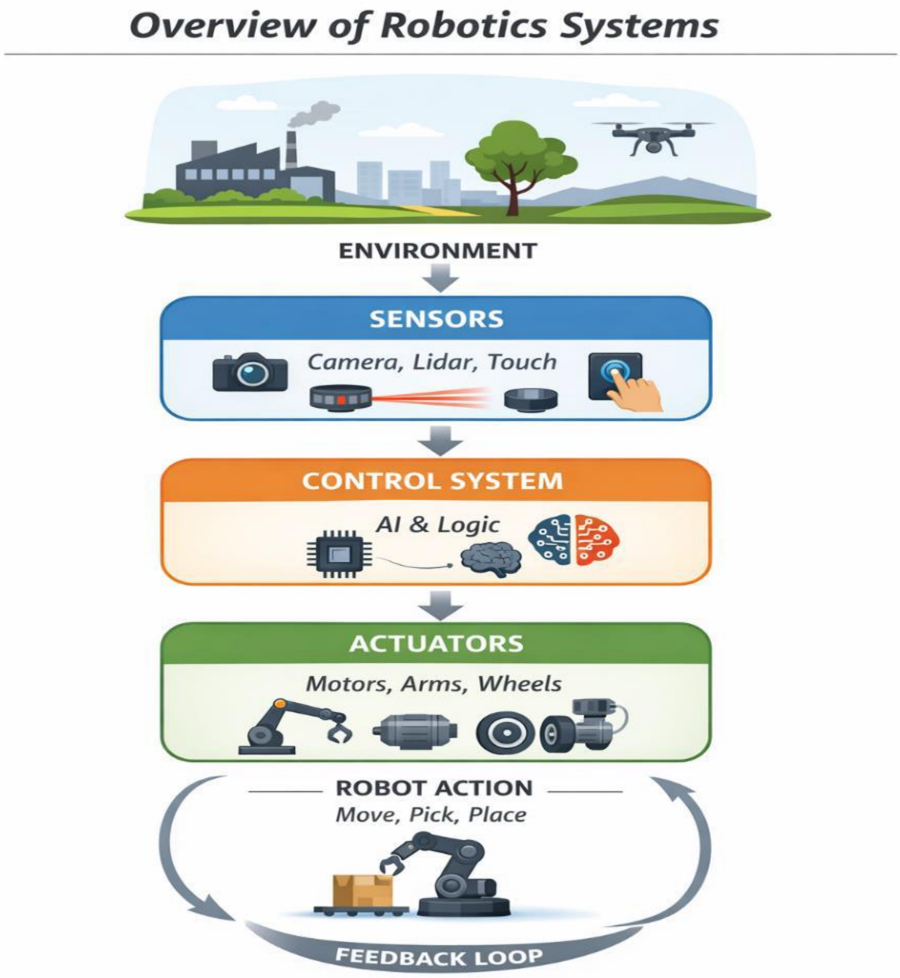

Fig. 2. Overview of the Robotic System

1.1 Evaluation Of Robotics

The evolution of robotics began with simple mechanical machines designed to perform repetitive tasks during the early industrial era. With the introduction of industrial robots in the 1950s and 1960s, automation transformed manufacturing by improving efficiency and precision[15]. Advances in electronics, sensors, and computing led to more intelligent robots capable of perception and basic decision-making. Today, robotics integrates artificial intelligence, machine learning, and IoT, enabling robots to operate autonomously in fields such as healthcare, defense, space exploration, and smart industries[16].

In the last few years, collaborative robots and autonomous systems have appeared that safely cooperate with human beings in common workspaces. The development of cyber–physical systems and cloud robotics should ensure enhanced connectivity, scalability, and real-time data exchange. As robotics continues to evolve, the focus is shifting toward self-learning, adaptive, and context-aware systems that can function reliably in highly dynamic and unstructured environments[17].

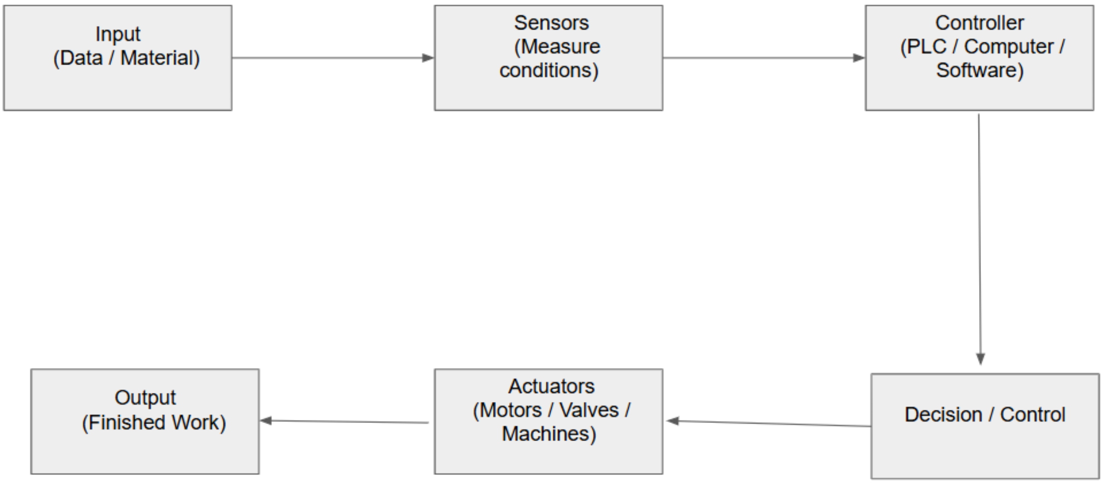

Fig.3 Evaluation of Robotics

1.2 *Major Components and Technologies Used in Robotics*

Robotic systems are made up of different critical components and technologies that work together to perform tasks efficiently and safely. One of the most important components of a robotic system is the sensor. Sensors can detect light, sound, distance, temperature, pressure, and motion, which helps the robot understand its surrounding environment and respond appropriately [2]. Another key component is the actuator, which may be an electric motor, hydraulic system, or pneumatic system. Actuators are mainly responsible for movement and enable the robot to perform physical tasks such as lifting, turning, gripping, or walking [3]. The control system acts as the brain of the robot by processing sensor data and coordinating actuator actions [3].

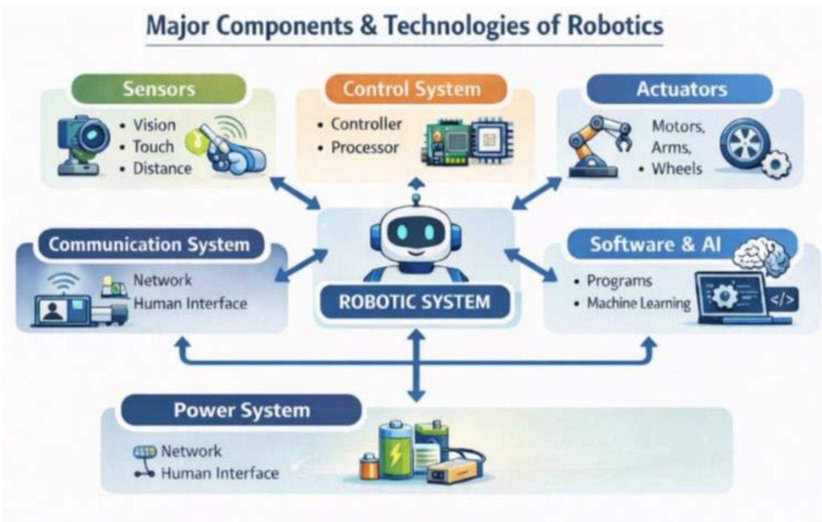

Fig. 4 Major components & Technologies

Software and artificial intelligence (AI) also play an important role in robotics. Software defines how the robot operates and controls its tasks. AI enables robots to think, learn, and make decisions independently. Technologies such as machine learning and computer vision allow robots to recognize objects, navigate safely, and improve-performance by learning from previous experiences [7]. Robots also require power sources, such as batteries or external power supplies, to operate continuously. In addition, communication technologies help robots exchange information with other machines, computer systems, or human operators. Because of these technologies, robots become more intelligent, flexible, and useful in many fields, including manufacturing, healthcare, agriculture, and service industries [2][7].

1.3 Automation of robotics using Al and its use cases:

Refers to the use of control systems and mechanical technology to control machines and industrial processes with minimal human interaction[4]. Human-based automation involves the use of human operators in the system setup, monitoring, control, and maintenance.[9] The system is intended to help human operators by reducing human effort, increasing the speed of operations, and improving accuracy, as opposed to re-placing human judgment[10].

Automation increases productivity because it allows machines to handle repetitive, time-consuming, and physically demanding tasks at a very high speed and accuracy rate, and human intervention is used for monitoring and managing the system's performance [11]. This method helps to minimize manual labor and prevents workers from getting physically strained and mentally stressed, as they can concentrate on planning, monitoring, and decision-making tasks [12]. Human-based automation is also very important for enhancing workplace safety because it allows dangerous tasks to be handled by automated systems, which greatly minimizes the chances of accidents and injuries [13]. Machines are very efficient in performing precision-based tasks, and human intervention is also required for dealing with unexpected events and managing the system's control effectively. The effective combination of machine capabilities and human intelligence greatly improves system flexibility, reliability, and performance [11][12].

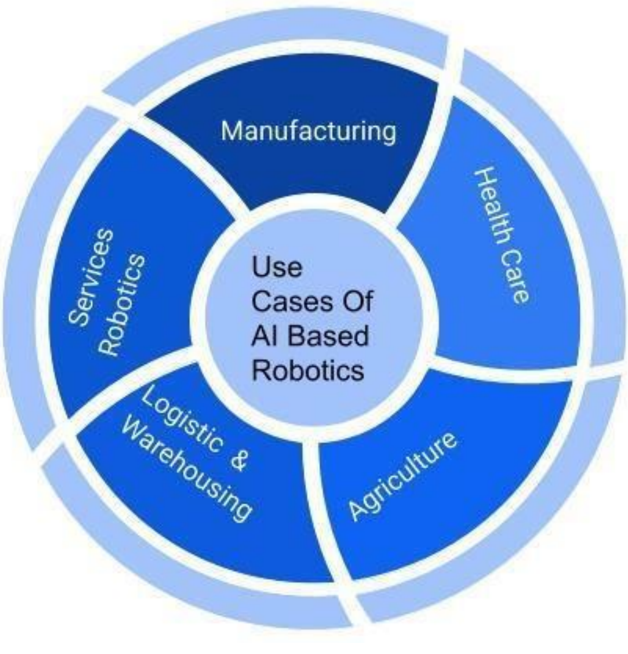

Fig.5 Use Cases of AI based Robotics

1.4 Advantages/benefits of robotics automation

Robotic automation is the use of robots and machines to perform tasks with very little human assistance [3]. The robots are employed in tasks that are repetitive, take a long time, are hazardous, or require precision[4]. The use of robots helps in completing tasks faster, safer, and better[4]. The first advantage of robotic automation is that tasks are completed faster. Robots can work for 24 hours without getting tired or needing a break[3]. This helps companies complete more tasks in a shorter time. Another ad-vantage is that the results are more accurate. Robots always follow instructions, so they make fewer errors and produce the same positive results[2][4].

Usefulness of Robotics Automation: Robotics automation is very useful as it assists humans to work better and safely[2]. Robots can work for a long time without getting tired, which helps in increasing the speed of work and productivity [4]. As robots work according to programmed instructions, they work with accuracy, which reduces errors and improves the quality of work[3]. Another very important advantage is that it is safe. Robots are capable of performing heavy, repetitive, or hazardous tasks, such as lifting heavy weights or operating in hazardous environments, thus minimizing the chances of injuries to employees[2][4]. Robotics automation also helps in minimizing physical and mental efforts of employees by performing mundane and tiresome Tasks. This enables employees to engage in more significant tasks, such as system monitoring, problem-solving, and decision-making. Eventually, robotics automation assists in timesaving and the creation of a safe and organized workplace[2][3].

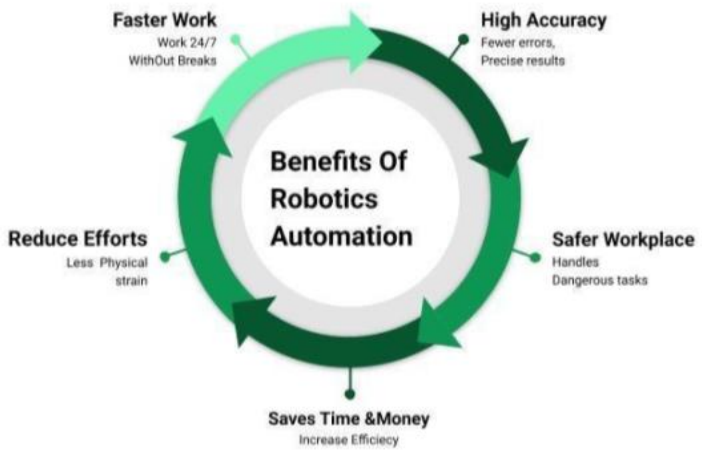

Fig.6 Benefits of Robotics Automation

1.5 Security challenges in robotics automation:

The security risks posed by robotics automation systems are considerable, as they rely on industrial control system architectures, communication systems, and human interaction [17].

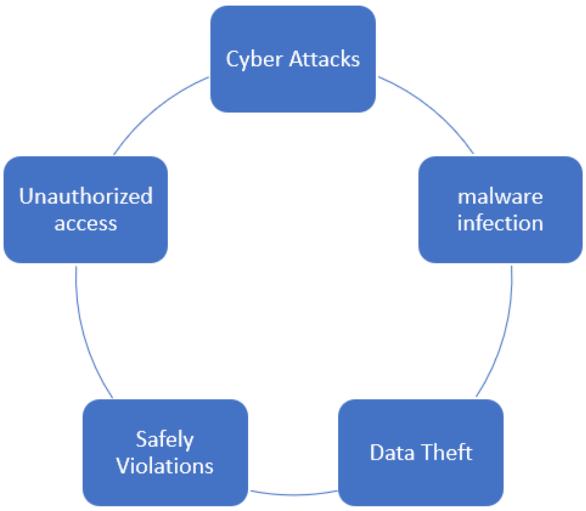

Fig. 7 Challenges of Robotics Automation

Human-based robotic systems function on Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, and field devices that are connected through industrial communication systems[10]. If such systems are not properly secured, they can provide opportunities for unauthorized access, which can enable attackers to manipulate control logic, modify operating parameters, or stop the operation of robots[20].

Moreover, the deployment of more networked and cloud-dependent robotic technologies has created a large threat environment against cyber-attacks like malware, denial of service, and data breaches. Inadequate monitoring facilities, handling of legacy components, and poor authentication methods are also critical issues related to security threats. This must be effectively addressed to provide a secure and reliable robot automation system [21].

1.7 Literature Review and Research Gap

According to recent studies, robotics and automation technologies have been found to enhance productivity, precision, and efficiency within various sectors. Studies have investigated how AI, ML, and IoT technologies can be incorporated into robots to facilitate autonomous decision-making, adaptability, and intelligent process management [2][4][7]. These innovations have expanded the application of robots in sectors such as manufacturing, health care, logistics, agriculture, and smart cities [8][13].

While several research studies emphasize the positive aspects of robotics automation, very few of them address any issues other than the improvements in performance that can be achieved through automation. Very little has been done to study the possible threats that robots pose with respect to their cyber security aspect, particularly because contemporary robots depend heavily on cloud platforms and wireless communication networks [16][17][20].

Furthermore, existing research often discusses security threats individually rather than providing integrated security frameworks for robotic environments. Therefore, there is a need for comprehensive research that examines robotics automation technologies together with emerging cybersecurity challenges and mitigation approaches. This study attempts to address this gap by providing an integrated overview of robotics, automation, AI integration, and cybersecurity concerns [17][18][20].

II. LITERATURE REVIEW

2.1 History and evolution of robotics and robo-automation

History and development of robotics and robotic automation started in the early industrial era with the use of simple mechanical systems to aid human labour [3]. The development of the first industrial robot, named Unimate, in the 1950s was an important milestone in robotics automation because it introduced automation in manufacturing systems [4]. In the latter half of the 20th century, improvements in electronics, sensors, and computer controls made it possible for robots to perform more complex tasks [3][2]. With the advent of the current era, the combination of artificial intelligence, machine learning, and IoT has led to the development of intelligent and autonomous robots in the medical, transportation, space, and smart industry sectors, thus expanding the horizon of robotics automation [4]. The current development in robotic automation has led to increased productivity, accuracy, and safety at the workplace [4]. The current scenario of robotic automation also allows the analysis of data in real-time and has the capability to monitor from a distance, thus making the process more adaptable and efficient [2]

2.2 Table of technologies components used in robo-automation

Below shows the technologies components used in robo-automation and robo-automation use cases in real life in table 1 & 2 respectively

TABLE I

TECHNOLOGIES COMPONENTS USED IN ROBO-AUTOMATION

Technology Component	**Description / Role in Robo-Automation**
Sensors	Help robots sense their environment by detecting light, distance, temperature, pressure, sound, and motion.

Actuators	Enable movement and physical actions such as lifting, rotating, gripping, or walking using motors or hydraulic systems.
Control System	Acts as the brain of the robot; processes sensor data and sends commands to actuators.
Robotic Software	Controls robot operations, task execution, and system coordination.
Artificial Intelligence (AI)	Allows robots to make decisions, learn from data, and adapt to new situations.
Machine Learning	Enables robots to improve performance over time through experience and data analysis.
Computer Vision	Helps robots recognize objects, read images, and navigate safely in their environment.
Power Supply	Provides energy to robots through batteries, power adapters, or external power sources.
Communication Systems	Allow robots to communicate with other machines, networks, cloud systems, or human operators.
IoT & Connectivity	Enables real-time monitoring, data sharing, and remote control of robotic systems.

TABLE II

ROBO-AUTOMATION USE CASES IN REAL LIFE

Use Case / Sector	**Application of Robo-Automation**	**Key Benefits**
Manufacturing	Robots perform assembly, welding,painting,and packaging tasks.	Faster production, high accuracy, consistent quality, reduced human effort.
Healthcare	Surgical robots, patient monitoring, medicine delivery.	Improved precision, safer surgeries, reduced workload on healthcare staff.
Logistics & Ware-housing	Automated picking, sorting, and material handling.	Faster order processing, reduced errors, efficient inventory management.
Agriculture	Automated planting, harvesting, and crop monitoring.	Increased productivity, reduced labor cost, better crop yield.
Transportation	Autonomous vehicles and traffic management systems.	Improved safety, reduced human error, efficient transport operations.
Defense & Security	Surveillance robots and bomb disposal systems.	Enhanced safety for personnel, effective threat detection.
Retail	Automated checkout systems and inventory robots.	Faster service, better stock control, improved customer experience.
Service Industry	Cleaning robots, delivery robots, customer assistance robots.	Reduced manual labor, improved efficiency, continuous operation.
Space Exploration	Planetary rovers and robotic arms for exploration.	Operates in extreme environments, accurate data collection.
Smart Homes	Robotic vacuum cleaners and smart assistants.	Convenience, time-saving, improved daily life quality.

2.3 Case Study: AI-Based Robotic Automation in Smart Manufacturing

There is an example of robotics in automation, which may involve intelligent factories that use collaborative robots working alongside humans. Robots are equipped with the use of sensor technology, computer vision, and AI systems that will help robots perform tasks in assembly, packing, testing, and quality control operations [2][21].

To give an example, robotic arm with AI technology will use imaging technology to find any faults in the products produced and segregate such faulty products from the production line. At the same time, the technique of predictive maintenance is being used to find any potential problems in the machine and inform the operator about such problems [4][7].

There are many benefits of robotic automation by the use of artificial intelligence like increasing efficiency in production, reducing the cost of operations, improving the quality of products, enhancing the safety of employees, and minimizing downtime by the use of predictive maintenance [11][13]. However, there are certain security threats related to these technologies due to their network-based functioning [16][17].

TABLE III.

COMPARATIVE REVIEW OF PREVIOUS STUDIES

Study	Focus Area	Major Contribution	Limitation
Craig (2018) [3][6]	Robotics Fundamentals	Provides comprehensive coverage of robotics principles, kinematics, dynamics, and control systems	Limited discussion on cybersecurity aspects
Groover (2015) [4]	Industrial Automation	Demonstrates improvements in production efficiency through automation technologies	Primarily focused on manufacturing sectors
Siegwart et al. (2011) [7]	Autonomous Robotics	Advances autonomous navigation, perception, and decision-making in robotic systems	Limited analysis of security threats
Goldberg and Kehoe (2013) [16]	Cloud Robotics	Introduces real-time monitoring and cloud-based robotic coordination	Increased exposure to cyberattacks
Proposed Study	Robotics, AI, and Cybersecurity	Integrates applications, benefits, security challenges, and mitigation strategies	Requires future experimental validation

2.4 Security challenges in robo-automation

2.4.1 Cybersecurity Threats and Hacking

One of the major security concerns in robo-automation is the potential for a cyber attack. This is because robots are network and cloud-based, as well as Internet of Things (IoT) devices, which makes it possible for hackers to exploit vulnerabilities in order to gain unauthorized access. A cyber attack may lead to loss of control, data theft, system shutdown, or unsafe robot behavior. Cyber attacks may lead to financial losses, security risks, and operational disruptions[18].

2.4.2 Data Privacy and Information Leakage

The data collected by the robotic automation systems includes information from sensors, cameras, and users. The information may include sensitive data such as operations, employees, and customers. In case the data is not protected by proper security measures, it may be leaked or misused. This may result in privacy breaches and legal problems. It is, therefore, important to ensure that data is stored and accessed in a secure manner that meets data protection requirements[16].

2.4.3 Safety Risks Due to System Failures

The information gathered by the robotic automation systems includes data from sensors, cameras, and users. The data may include sensitive information such as operations, employees, and customers. In the event that the data is not protected by appropriate security measures, it may be leaked or misused. This may lead to breaches of privacy and legal issues. It is, therefore, important to ensure that data is stored and accessed in a manner that is secure and complies with data protection standards[2].

2.4.4 Weak Authentication and Access Control

In most robotic systems, strong passwords and access control are not used. If unauthorized users are able to access the system, they will be able to change the settings of the robots or control the operations of the robots. To avoid this problem, strong passwords, role-based access, and authentication checks should be used to secure the robotic systems from unauthorized access.[17]

2.4.5 Software Vulnerabilities and Updates

Software is a very crucial component in the proper working of a robot. If the software contains bugs or is outdated, it may cause vulnerabilities that can be exploited by attackers. Outdated software can cause system crashes or malfunctions in robots. Software testing and patching are very crucial in ensuring that the robotic automation sys-tem is secure and reliable[19].

2.4.6 Dependence on Network Connectivity

It has also been observed that robotic automation systems require constant connectivity of the network or the cloud [16]. If the network is lost or the robot is subject to an attack, the robot will either stop functioning or will function incorrectly [17]. Secure networks can help to reduce problems related to network dependency . In this case, small network disruptions can cause problems for the robots . It has also been observed that the network dependency of the robotic automation system makes the robot vulnerable to denial of service (DoS) attacks, which can disrupt communication between the robot and the control system [18].

2.5 Cybersecurity Mitigation Strategies for Robo-Automation Systems

The increasing adoption of intelligent robotic systems requires strong cybersecurity measures to ensure operational safety and reliability. Several security mechanisms can be implemented to reduce cyber risks and improve system resilience.

2.5.1 Network Security

Industrial robotic networks should be protected using firewalls, intrusion detection systems (IDS), virtual private networks (VPNs), and secure communication protocols. Network segmentation can help prevent attackers from accessing critical robotic infrastructure [18].

2.5.2 Strong Authentication and Access Control

Multi-factor authentication (MFA), role-based access control (RBAC), and strong password policies should be implemented to restrict unauthorized access to robotic systems. These measures significantly reduce the risk of unauthorized manipulation of robotic operations [17][20].

2.5.3 Software Updates and Patch Management

Regular software updates and security patches are essential to eliminate vulnerabilities and improve system stability. Organizations should establish routine maintenance procedures to ensure all robotic software remains secure and up-to-date [19].

2.5.4 Data Encryption

Sensitive operational and user data should be encrypted during both storage and transmission. Encryption protects information from unauthorized access and reduces the risk of data leakage [20].

2.5.5 Continuous Monitoring and Threat Detection

Real-time monitoring systems and AI-based threat detection mechanisms can identify abnormal activities and potential attacks at an early stage, allowing organizations to respond quickly and minimize damage [17][18].

2.5.6 Security Awareness Training

Human error remains one of the most common causes of cybersecurity incidents. Regular training programs can help employees recognize cyber threats and follow secure operational practices [9][12].

III. ANALYSIS

The analysis of robotics and automation technologies demonstrates that modern intelligent systems have significantly transformed traditional industrial operations into highly efficient, data-driven environments. The integration of Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), computer vision, and advanced control systems has enabled robots to perform tasks with greater accuracy, adaptability, and autonomy than conventional automation systems [2][4][7].

From an industrial perspective, robotic automation has substantially improved productivity by reducing human involvement in repetitive, hazardous, and precision-oriented tasks. Manufacturing industries utilize robotic systems for assembly, welding, packaging, and quality inspection, resulting in faster production rates and improved product consistency [4][13]. Similarly, healthcare organizations employ robotic-assisted surgical systems and automated patient-monitoring solutions to improve treatment precision and reduce human error [8].

The adoption of collaborative robots (cobots) has further enhanced workplace efficiency by enabling safe interaction between humans and machines within shared environments [21]. Unlike traditional automation systems, which often operate in fixed and predictable conditions, modern robotic systems can adapt to dynamic environments through real-time data analysis and intelligent decision-making capabilities [7][16].

However, the increasing connectivity of robotic systems introduces significant cybersecurity concerns. The integration of cloud computing, IoT platforms, and industrial communication networks expands the attack surface and creates opportunities for cyber threats such as unauthorized access, malware attacks, denial-of-service attacks, and data breaches [17][18][20]. These threats can affect not only information security but also operational continuity, equipment reliability, and human safety.

Therefore, the successful implementation of robotics automation requires a balanced approach that combines technological innovation with robust cybersecurity protection. Organizations should integrate security measures such as strong authentication mechanisms, network segmentation, encryption, continuous monitoring, and regular software updates into robotic system architectures. Such measures are essential for ensuring the long-term reliability, safety, and sustainability of intelligent robotic systems in Industry 4.0 environments [17][18][20].

Overall, the findings indicate that robotics and automation will continue to play a vital role in shaping future industries by improving operational efficiency, supporting human workers, and enabling smart decision-making processes. As technologies continue to evolve, intelligent robotic systems are expected to become more autonomous, secure, and capable of operating effectively in increasingly complex environments.

IV. CONCLUSION

Robotics and automation technologies have become fundamental components of modern industrial and service sectors, significantly improving operational efficiency, accuracy, productivity, and workplace safety. The integration of Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), advanced sensors, and intelligent control systems has enabled robots to perform complex tasks with minimal human intervention while maintaining high levels of precision and reliability [2][4][7].

This study examined the evolution of robotics, major technological components, AI-based automation applications, real-world use cases, benefits, and emerging cybersecurity challenges associated with modern robotic systems. The findings indicate that intelligent robotic systems have transformed traditional automation into adaptive, data-driven, and collaborative environments that support Industry 4.0 initiatives and smart manufacturing practices [11][13].

Despite the numerous advantages of robotic automation, increasing connectivity through cloud computing, IoT platforms, and industrial communication networks introduces significant security risks. Cyber threats such as unauthorized access, malware attacks, data breaches, and denial-of-service attacks can negatively impact operational continuity, data integrity, and physical safety [17][18][20]. Therefore, implementing robust cybersecurity measures including strong authentication, encryption, continuous monitoring, software updates, and secure network architectures is essential for ensuring the reliability and resilience of robotic systems.

Future research should focus on the development of intelligent cybersecurity frameworks specifically designed for autonomous robotic environments. Emerging technologies such as blockchain-based security mechanisms, AI-driven threat detection systems, digital twins, and self-healing cyber-physical systems offer promising opportunities for enhancing robotic security and operational reliability. Additionally, experimental studies and real-world industrial case analyses are needed to evaluate the effectiveness of these approaches in dynamic and large-scale deployment environments.

In conclusion, robotics and automation will continue to play a critical role in shaping the future of smart industries, healthcare, transportation, agriculture, and service sectors. With continuous technological advancements and stronger cybersecurity integration, intelligent robotic systems are expected to become more autonomous, secure, and capable of supporting sustainable industrial growth in the coming years.

REFERENCES

[1] G. Bekey, Robotics: State of the Art and Future Challenges. World Scientific, 2008.

[2] B. Siciliano and O. Khatib, Springer Handbook of Robotics, Springer, 2016.

[3] J. J. Craig, Introduction to Robotics: Mechanics and Control, Pearson, 2018.

[4] .M. P. Groover, Automation, Production Systems, and CIM, Pearson, 2015.

[5] Asimov, I, Robot, Doubleday, 1950.

[6] J. J. Craig, Introduction to Robotics: Mechanics and Control, 4th ed. Boston, MA, USA: Pearson, 2018.

[7] R. Siegwart, I. R. Nourbakhsh, and D. Scaramuzza, Introduction to Autonomous Mobile Robots, 2nd ed. Cambridge, MA, USA: MIT Press, 2011

[8] M. Ben-Ari and F. Mondada, Robots and Their Applications, Springer, 2018

[9] T. B. Sheridan, Humans and Automation: System Design and Research Issues. New York, NY, USA: Wiley, 2002.

[10] S. Y. Nof, Ed., Handbook of Industrial Robotics, 2nd ed. Hoboken, NJ, USA: Wiley, 2017.

[11] K. Schwab, The Fourth Industrial Revolution. Geneva, Switzerland: World Economic Fo-rum, 2016.

[12] G. Salvendy, Handbook of Human Factors and Ergonomics, 4th ed. Hoboken, NJ, USA: Wiley, 2012.

[13] International Federation of Robotics, “World Robotics Industrial Robots,” IFR, Frankfurt, Germany, 2022.

[14] R. C. Arkin, Behavior-Based Robotics, MIT Press, 1998.

[15] G. N. DeSouza and A. C. Kak, “Vision for mobile robot navigation: A survey,” IEEE Trans-actions on Pattern Analysis and Machine Intelligence, vol. 24, no. 2, pp. 237–267, Feb. 2002.

[16] K. Goldberg and M. Kehoe, “Cloud robotics and automation: A survey of related work,” IEEE Robotics & Automation Magazine, vol. 20, no. 2, pp. 22–35, Jun. 2013.

[17] Humayed, J. Lin, F. Li, and B. Luo, “Cyber-physical systems security—A survey,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[18] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82, 2015.

[19] E. Byres and J. Lowe, “The myths and facts behind cyber security risks for industrial control systems,” VDE Kongress, 2004.