



# Kahramanmaraş Sutcu Imam University

## Journal of Engineering Sciences



Geliş Tarihi : 07.10.2025  
Kabul Tarihi :20.11.2025

Received Date : 07.10.2025  
Accepted Date : 20.11.2025

### THREATS, VULNERABILITIES AND MEASURES IN ROBOT COMMUNICATION SECURITY: A REVIEW

### ROBOT İLETİŞİM GÜVENLİĞİNDEKİ TEHDİTLER, ZAFİYETLER VE ÖNLEMLER: BİR İNCELEME

Vahdet Cemil ALTUN<sup>1\*</sup> (ORCID: 0000-0001-7792-0380)  
Barış ATA<sup>2</sup> (ORCID: 0000-0003-4773-0564)  
Yavuz CANBAY<sup>1</sup> (ORCID: 0000-0003-2316-7893)

<sup>1</sup> Kahramanmaraş Sutcu Imam University, Faculty of Engineering and Architecture, Computer Engineering Department, Kahramanmaraş  
Türkiye

<sup>2</sup> Cukurova University, Faculty of Engineering, Computer Engineering Department, Adana, Türkiye

\*Sorumlu Yazar / Corresponding Author: Vahdet Cemil ALTUN, vahdetcemilaltun@ksu.edu.tr

#### ABSTRACT

The expansion of networks and the rapid advancement of technology have led to a significant increase in the use of robots across various domains, including robotics, automotive, healthcare, military, and education, thereby bringing numerous security concerns to the forefront. Although it is nearly impossible to completely eliminate security vulnerabilities in robot communication, academia and industry continue to pursue extensive research in this field. This study compiles and organizes recent research in robotics involving network-based, Internet of Things (IoT), Robot Operating System (ROS), and other related approaches, providing a detailed examination of security threats, vulnerabilities, and their conceptual explanations. Furthermore, secure communication protocols, cryptographic methods, and the impact of emerging technologies such as blockchain and edge computing on secure robot communication are discussed. The findings indicate that these evolving technologies hold considerable promise for enhancing the security of robot communications.

**Keywords:** Blockchain, cryptography, IoT, robot communication security, ROS

#### ÖZET

Ağların büyümesi ve teknolojinin hızlı ilerlemesi, robotik başta olmak üzere otomotiv, sağlık, askeri ve eğitim gibi birçok alanda robot kullanımının hızla artmasına yol açmış, bu durum ise çeşitli güvenlik endişelerini gündeme taşımıştır. Robot iletişimindeki güvenlik açıklarını tamamen ortadan kaldırmak neredeyse imkânsız olsa da, akademi ve sektör bu alandaki çalışmalarını aralıksız sürdürmektedir. Bu çalışmada, robotik alanında network, Internet of Things (IoT), Robot Operating System (ROS) ve diğer tabanlı yaklaşımları içeren güncel araştırmalar derlenmiş; robotik sistemlerde karşılaşılan güvenlik tehditleri, zafiyetler ve bunlara ilişkin kavramsal açıklamalar ayrıntılı olarak ele alınmıştır. Ayrıca, güvenli iletişim protokolleri, kriptografik yöntemler ve blockchain ile edge computing gibi güncel teknolojilerin güvenli robot iletişimine etkileri incelenmiştir. Elde edilen bulgular, gelişen teknolojilerin robot iletişiminde güvenliği artırma konusunda umut vadettiğini ortaya koymaktadır.

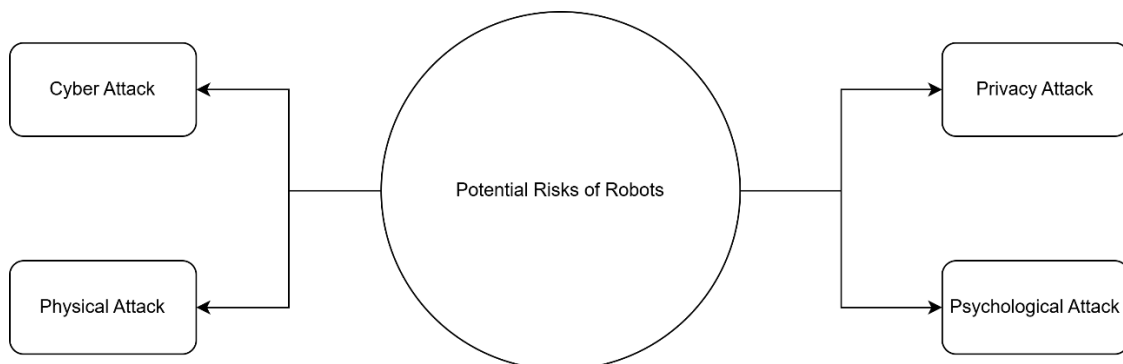
**Anahtar Kelimeler:** Blok zinciri, kriptografi, IoT, robot iletişim güvenliği, ROS

#### INTRODUCTION

A robot is a machine that can automatically perform a series of actions and commands (Abeykoon & Feng, 2017). The rapid advancement of global technology has triggered revolutionary innovations in the field of robotics. Today, robots are widely used in many areas such as industry, health, agriculture, daily life, construction, defense, and service sectors (Abeykoon & Feng, 2017; Yaacoub et al., 2022). According to the 2024 report of the International Federation

of Robotics, there are more than 4 million robots actively working worldwide, and this number has increased by approximately 221% in the last decade (IFR, 2024). The emergence of approaches such as Artificial Intelligence (AI), machine learning, and deep learning has led to significant developments in the field of robotics. Through the application of these technologies, robots sense environmental inputs using sensors or other tools and process them using AI algorithms to form decision-making mechanisms. Thus, robots can adapt to smarter and more dynamic environments and perform tasks effectively (Soori et al., 2023). The advent of Industry 4.0 has enabled smart robots to offer innovative solutions that reduce human labor across various domains, ranging from agricultural operations like irrigation and weeding to critical healthcare tasks such as drug distribution during the COVID-19 pandemic (Javaid et al., 2021).

The recent rapid development of robotics and Internet of Things (IoT) technologies has brought with it some risks, such as cybersecurity risks, privacy risks, psychological risks, and physical risks (Johnson et al., 2020). For example, the hacking of a Jeep Cherokee while driving in 2015 is one of the concrete examples of these risks (Greenberg, 2015). The risk of remote-controlled surgical robots becoming the target of malicious hackers also poses a significant threat. In the event of such a cyber-attack, the seizure of control of the robot can have serious consequences for the physical health of patients. In addition, any manipulation or intervention during surgery can have profound psychological effects on patients and healthcare professionals. These are not the only security risks of robots. For example, if a robot used in elderly care is seized by a hacker, it can be misused by malicious actors. This situation not only disrupts the functionality of the robot, but it can also violate the privacy of the individual and pose a risk of personal information disclosure. Therefore, the security of these robots has become an important research topic today (Fosch-Villaronga & Mahler, 2021). Figure 1 illustrates the potential risks frequently encountered in robotic communication.



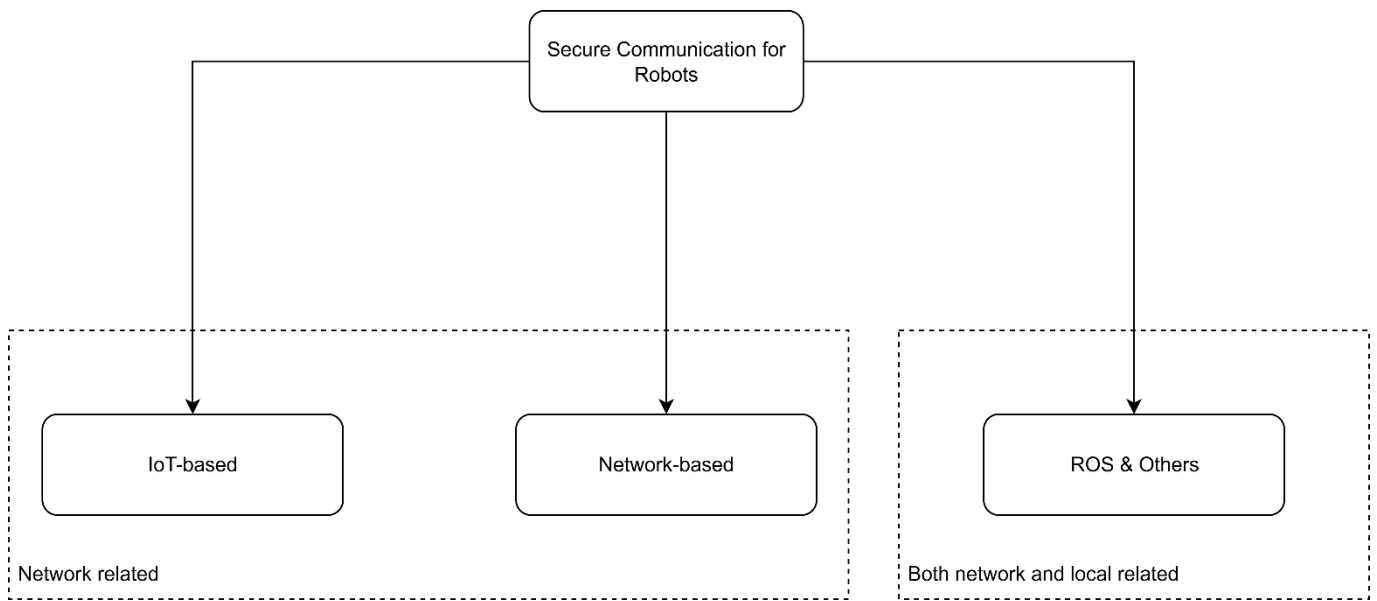
**Figure 1.** Potential Risk Categories Of Robots (Fosch-Villaronga & Mahler, 2021)

The IoT-based robots collect, process, and share data required for local communication with other devices connected to a network environment, or through the Robot Operating System (ROS) (Rodríguez-Lera et al., 2018; Johnson et al., 2020). However, when such communications are not secure, the risk of data being misused increases. Therefore, the security of robot communication is of great importance. In particular, the use of encryption algorithms such as symmetric, asymmetric, and hash functions has become an important requirement to protect the integrity and confidentiality of data during communication. In addition to encryption algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA), and Hash-based Message Authentication (HMAC), protocols such as Transport Layer Security (TLS), Internet Protocol Security (IPSec), and communication tunneling in robot networks protect against attacks by creating a secure infrastructure for robots to communicate locally or over a network (Breiling et al., 2017; Rodríguez-Lera et al., 2018).

An increasing interest in the integration of security and encryption methods in robot communication is observed when current studies are examined. With the widespread use of robots, especially in critical areas such as healthcare, the need for secure communication comes to the fore. Indeed, according to the PubMed database, there are 12.785 different publications on the importance of security for robot communication in the healthcare sector. Another study on the security of healthcare robots evaluated the importance of cybersecurity on the characteristics, analysis, and ethical issues of the problems in this area (Giansanti & Gulino, 2021). Similarly, comprehensive studies have been conducted on the types of attacks on robots, the protection methods developed against these attacks, and the security vulnerabilities of robots used in different areas, such as industrial, health, or education. Within the scope of these studies, security threats are classified and detailed at the network level, physical layer level, and operating system

level (Botta et al., 2023). The security vulnerabilities of robots used in different industries and for various purposes are discussed in terms of network, data, and remote access (e.g., encryption and security protocols), and various prevention strategies are presented (Tanimu & Abada, 2025).

The main motivation of this study is to evaluate the existing solutions, from various perspectives, for providing secure communication in different areas where robots are widespread. Factors that especially directly affect system performance and information security, such as encryption, delay, secure communication channels, and efficiency, indicate that this area needs to be developed. In this context, the vulnerabilities and weaknesses in robot communication, secure communication paths, data encryption, and secure data transmission are examined in detail and systematically grouped. The security risks encountered are determined by combining the methods and findings of the examined studies, and the potential solutions against these risks are discussed. The general framework of the recent studies in the literature is summarized in Figure 2.



**Figure 2.** General Structure Of Secure Communication For Robots

The purpose of this study is to integrate security and encryption methods in robot communication and to consider the disadvantages encountered in current applications in the literature. Various approaches have been proposed for security solutions in network-based, IoT-based, and local systems such as ROS, but these solutions still have the potential for improvement in important parameters such as efficiency, processing power usage, and latency. Therefore, this study aims to provide the literature with a new perspective in order to systematically analyze the challenges faced by current security methods and evaluate alternative approaches. Thus, a comprehensive analysis is provided to increase security in robot communication.

This paper is structured as follows. Section 2 covers recent literature studies on secure robot communication in networks and platforms such as IoT and ROS. Section 3 examines potential threats and security vulnerabilities commonly encountered in robot communication. Section 4 presents alternative encryption methods and security protocols proposed against these vulnerabilities. Section 5 discusses the impact and security of recent and current technologies on robot communication. Finally, Section 6 summarizes the findings of the previous sections and reveals the research gaps in the literature.

## RELATED WORKS

In this section, current studies in the literature on ensuring security in robot communication have been comprehensively reviewed. These studies cover network-based communication methods, security protocols implemented in IoT-based systems, and encryption, authentication, and access control mechanisms used in the ROS and other local platforms.

### *Network-based Secure Communication Methods*

Shepita et al. (2025) developed a mathematical model to protect a robotic system in the printing industry against various cyberattacks. Attacks such as Distributed Denial of Service (DDoS), Man-in-the-Middle (MITM), data manipulation, and industrial robot vulnerabilities can disable the operation of an active robotic system, thereby negatively affecting its efficiency and performance. In the proposed method, protection was achieved through a model developed in the MATLAB environment. Accordingly, network security monitoring, anomaly detection, and data encryption or TLS techniques were integrated with an AI-based behavioral analysis. The results indicated that DDoS attacks both disabled the system and caused further performance deterioration. However, TLS-based solutions greatly improved the resilience of the network against cyberattacks and demonstrated the crucial importance of data encryption in this domain.

Mwanje et al. (2025) investigated the effects of various attacks, including MITM, spoof packet injection, and data packet manipulation, against Light Detection and Ranging (LiDAR) sensors mounted on autonomous vehicles. The experimental study was carried out on a robotic vehicle platform based on a JetRacer ROS AI Kit running ROS 1. The attackers performed Address Resolution Protocol (ARP) using the arpspoof tool to intercept network traffic between ROS nodes and then decrypted and modified captured Transmission Control Protocol (TCP) packets containing LiDAR data (e.g., laser\_scan messages) through a Python script implemented with the Scapy library. The modified LiDAR sensor data caused the robotic vehicle to fail to detect newly introduced obstacles and exhibit unpredictable behavior, leading to serious malfunctions.

Degirmenci et al. (2023) conducted a study on the effects on the system of Denial-of-Service (DoS) attacks observed in both the transmission and application layers in the ROS environment. The ROSploit, a security testing tool, was used to detect attacks in the ROS environment, and TShark was used for performance analysis in the network environment. ROSploit was used to detect attacks on the application layer by employing methods such as creating signed or multiple subscribers for the transmission layer, while TShark was used to examine performance criteria such as delay and packet loss in various network traffic scenarios. When the experimental results were examined, it was determined that delay measurements provided earlier warnings than packet loss.

In another study, Degirmenci et al. (2023) proposed a network traffic dataset and a new Instruction Detection System (IDS) to improve the security of ROS-based systems. The data consists of a laboratory environment including a controller, robotic arm movements, a recorder, and an attacker device. In addition, each dataset was labeled as either malicious or harmless by monitoring network traffic with the tcpdump tool. The constructed dataset includes unauthorized access, unauthorized subscription, subscriber flood, and DoS attacks. Thus, the ROSIDS23 dataset was introduced to ensure security in the communication of ROS on the network and to develop early attack detection systems.

Jain and Doriya (2022) addressed the security deficiencies in robot communication and data processing processes and developed a new approach to address these issues. It is suggested that data processing causes intensive memory usage and high energy consumption in robots, and a cloud-based, secure communication solution was proposed to overcome this situation. According to this approach, the data received by the robots from sensors is transmitted to a cryptographic server based on Elliptic Curve Cryptography (ECC). The information required for authentication is hashed by a system administrator and updated regularly. In the cryptographic server, the data is encrypted using a public key and a secret key, and then securely stored on another cloud server. Robots must first authenticate with the ECC-based server when requesting data. Then, the requested data is securely transmitted to the relevant robot through the cryptographic server. This approach reduces the processing power usage of the robots by moving the data processing and security processes to a server outside the robot, which has been shown to effectively provide secure communication.

Goerke et al. (2021) examined the security vulnerabilities that may arise in network communication in ROS 1 and ROS 2 systems. The study showed that both systems are vulnerable to network-based attacks in their default settings and analyzed the ways to protect against these vulnerabilities. In particular, attacks such as MITM and ROS node hacking were addressed, and it was stated that methods such as TLS, Datagram Transport Layer Security (DTLS), Secure ROS, AES-DES encryption, Virtual Private Network (VPN), and Internet Protocol Security (IPSec) could be used to increase the security of the system against such threats. These approaches presented the potential to create a secure channel for robot communication.

Diro et al. (2020) proposed a system that addresses the need to provide end-to-end security due to the limited resources of IoT devices and the inadequacy of existing security protocols. It is emphasized that existing methods are not applicable in the IoT environment due to their high processing power, bandwidth, and storage requirements. A lightweight security protocol based on Cipher Block Chaining Message Authentication Code encryption, incorporating ECC and AES in counter mode, was developed to address this problem within the publish-subscribe communication model. The objective was to reduce the storage and processing overheads of the devices by using fog nodes as intermediate agents. The proposed system optimized the bandwidth by reducing the number of handshakes and message sizes compared to the TLS protocol. In addition, its security is enhanced with strong authentication mechanisms and message integrity.

Mukhandi et al. (2019) presented the security deficiencies in the network using ROS, emphasized that robots can be exposed to potential cyber threats from malware developers due to communicating over a network, and proposed a new solution against these risks. When a robot communicates over a network, it needs an IP address. If this communication occurs directly on ROS, the robot may become vulnerable to malicious use by hackers due to the weak security of ROS. Therefore, when the robot communicates, a cloud system is accessed via the Message Queuing Telemetry protocol, as it performs many security operations such as lightweight encryption and authentication. Then, the cloud system forwards the incoming data to the intended destination after ensuring authentication and data confidentiality. In this study, data is transmitted over both secure and insecure channels, and their performances are compared. The performance results show a delay increase of approximately 25% to 40% for response times due to the authentication process, over the secure channel, compared to the insecure channel. However, the authors observe a decrease in delay of approximately 80% to 90% after the authentication process is completed. Similarly, a reduction of approximately 0.4% to 1.5% in message efficiency is observed due to the use of authentication and digital certificates when communicating over a secure channel compared to the insecure channel.

Dourado et al. (2019) proposed a hybrid IoT-based and network-based system for positioning and locating mobile robots. Mobile robots use a network infrastructure to transfer images to a cloud-based IoT system. Thus, authentication is applied through HyperText Transfer Protocol Security (HTTPS), and the integrity and security of the data are ensured. On the cloud system, Convolutional Neural Network (CNN) and Transfer Learning approaches are used for feature extraction, training, and prediction from images. After the decision mechanism, the relevant data is transmitted to the robot's navigation system via the cloud-based system. In the study, secure and insecure data transmission channels are compared in terms of performance. Since the authentication process occurs over a secure channel, there is an associated performance overhead ranging from 20% to 35%. However, no communication delays are observed following the completion of authentication. Furthermore, in terms of efficiency, there is no degradation in data transmission performance after the authentication phase.

The studies summarized in Table 1 reveal that the default communication configuration of ROS contains significant security vulnerabilities, particularly in networked environments (Mukhandi et al., 2019; Goerke et al., 2021; Mwanje et al., 2025). The limited computational resources of robotic systems and the resource-intensive nature of secure communication channels, such as encryption, have led to a growing tendency to offload security and computation-intensive processes to cloud-based infrastructures (Mukhandi et al., 2019; Diro et al., 2020; Jain & Doriya, 2022). Methodologically, these approaches differ in terms of the protocols and cryptographic mechanisms they employ, such as standard protocols like HTTPS (Dourado et al., 2019), lightweight protocols such as Message Queuing Telemetry Transport (MQTT) (Mukhandi et al., 2019), or specialized cryptographic solutions like ECC (Diro et al., 2020; Jain & Doriya, 2022). A common limitation of these prevention-based approaches lies in the additional performance overhead introduced by authentication and encryption procedures. However, once the initial setup phase is completed, it has been observed that communication remains secure while system performance returns to normal (Dourado et al., 2019; Mukhandi et al., 2019). In contrast to these prevention-based solutions, research has also addressed detection-oriented methods. For instance, Degirmenci et al. (2023) proposed a novel IDS that automates the detection of anomalies such as network latency during DoS attacks.

### ***IoT-based Secure Communication Methods***

Martin et al. (2025) proposed the ROS 2-based Robotic Instruction Prevention System (RIPS) for mobile robots to perform reliable and secure operations. The RIPS system is a hybrid model that includes both behavioral systems, such as mobility and physical behaviors of robots, and deliberative systems, such as decision-making mechanisms and task planning on objects. This model emphasizes security and reliability. For instance, when an attack is detected,

the robot's camera is disabled, its movement is stopped, laser sensors are turned off, and it is returned to the starting point. Thus, it has been shown that robots operating in social and industrial areas can perform reliable operations. This system test and verification process has been applied to a sample robot, and successful results have been obtained. In addition, it has been stated that RIPS cannot only work as a stand-alone IDS but can also be integrated with other IDSs.

**Table 1.** An Overview Of Network-Based Secure Communication Techniques

Study	Year	Main Topic	Methodology
Shepita et al.	2025	Robotic systems for warehouse assets contain security vulnerabilities in protocols such as DDoS, MITM, and Message Queuing Telemetry Transport (MQTT).	Using MATLAB Simulink and ROS, DDoS and MITM attack scenarios were modeled on a myCobot-280 manipulator. Countermeasures such as IDS, TLS 1.3 encryption, and AI-based behavioral analysis were tested.
Mwanje et al.	2025	Analysis of autonomous vehicle sensors and ROS network security.	During the robotic vehicle's communication, MITM attack, ARP spoofing, and the TCP packets carrying LiDAR data were blocked. Thus, the robotic communication was manipulated.
Degirmenci et al.	2023	Analysis of DoS attacks at transport and application layers in ROS systems	Delay and packet loss measurement under real traffic, data collection with ROSploit and Tshark
Degirmenci et al.	2023	Creation of a multi-class intrusion detection dataset (ROSIDS23) for ROS-based systems	Data collection from real ROS network with pcap, feature extraction with CICFlowMeter, DoS, and unauthorized access scenarios
Jain & Doriya	2022	Security gaps in robot communication and optimising data processing	Cloud-based ECC encryption, authentication
Goerke et al.	2021	Evaluation of security mechanisms in ROS variants	Structured analysis of security requirements; comparison of multiple protection mechanisms
Diro et al.	2020	Providing end-to-end security for devices	ECC and AES-CCM based security protocol, publisher-subscriber model, and fog node usage
Mukhandi et al.	2019	To minimise security vulnerabilities for network communication of robots	Secure MQTT protocol for cloud communication, authentication
Dourado et al.	2019	Localization and navigation of mobile robots via IoT-based and network-based hybrid systems	HTTPS-based authentication for secure cloud communication; CNN and Transfer Learning for feature extraction, training, and prediction

Gao et al. (2022) examined in detail the existing problems related to the security of autonomous vehicles. The study addressed four main issues that threaten the security of autonomous vehicles, namely sensors, operating system security, control mechanisms, and Vehicle-to-Everything (V2X) communication. In terms of sensors, false signal attacks are among the prominent threats, while ROS's insufficient authentication and data encryption features pose problems in operating system security. In the control mechanism, sharing the location information of vehicles in the network environment creates security risks, and threats such as data integrity and identity fraud stand out in V2X communication. The solutions proposed in the study include systems that cross-validate information from different sensor sources, utilizing ROS2's security standards for the operating system, and isolating the developed methods in a modular manner. In terms of control mechanisms, data encryption and authentication methods are proposed, while blockchain-based and anonymous authentication systems are offered as potential solutions for V2X communication.

Liang et al. (2021) proposed a technical solution to the security and authentication issues in IoT-enabled intelligent multi-robot systems. A blockchain-based system that works without the need for a central authority was proposed. The system offers an innovative identity-based authentication model to verify both users and devices. A hash algorithm pool containing algorithms such as Secure Hash Algorithm 256 (SHA256) is used to increase data security. Authentication processes are handled in two stages: (a) user-to-user and (b) user-to-device. The proposed solution enables secure authentication and data exchange by providing a decentralized structure with blockchain technology. In addition, the developed consensus algorithm guarantees secure data processing between all nodes. The advantage

of this system is that it prevents forgery attempts and guarantees the integrity of the data. Experimental analyses showed that the proposed method is effective in terms of processing time, security cost, and storage requirements.

Rishikesh et al. (2021) proposed a secure, robot-based system designed to offer an alternative solution in scenarios such as hostage situations or military espionage. The proposed framework involves the deployment of multiple quadrupeds, lizard-inspired robots capable of executing a variety of tasks, including navigation, live video streaming, location reporting, directed movement, and image transmission. Each robot can be controlled individually or as part of a coordinated group. To reduce operational complexity, each robot is assigned a unique identification number. The control and data transmission for all robots are centralized through a common database. Consequently, ensuring the confidentiality of the information transmitted between each robot and the database is of critical importance. In the study, Rivest Cipher 4 (RC4) encryption is utilized for image-based operations such as video streaming and image transfer, whereas the AES is employed for securing text-based data, including textual information and location data.

**Table 2.** An Overview Of Iot-Based Secure Communication Techniques

Study	Year	Main Topic	Methodology
Martín et al.	2025	RIPS was proposed to provide reliability and security for ROS 2-based mobile robots.	RIPS provides a hybrid security model that includes the robot's behavioral and deliberative systems. It secures the robot in case of an attack. The system has been tested on a real robot and has achieved successful results.
Gao et al.	2022	Analysing security threats in autonomous vehicle systems.	Analyses threats in sensors, operating systems, control mechanisms, and V2X communications. A system based on the blockchain approach is proposed for V2X.
Liang et al.	2021	Addressing security and authentication issues in IoT-enabled multi-robot systems.	A new system for secure data exchange is proposed. This involves a decentralised blockchain system with authentication and SHA256 hashing.
Rishikesh et al.	2021	It includes the search for secure communication paths for robots in military and espionage scenarios.	Lizard-like quadruped robots were built. Furthermore, a mechanism using RC4 for video/image encryption and AES for text/location data was proposed.

The security implications on subfields of the IoT domain, namely mobile systems, autonomous vehicles, and multi-robot systems, are discussed in Table 2. Methodologically, the use of blockchain technology has emerged as a prominent approach to enable decentralized and trustworthy authentication and data exchange (Liang et al., 2021; Gao et al., 2022). Another approach involves the use of encryption techniques such as RC4 and AES to ensure the secure transmission of videos and texts in communication (Rishikesh et al., 2021). Furthermore, these studies not only focus on preventive measures but also explore hybrid detection and response systems, such as RIPS (Martín et al., 2025), which actively manage robot behavior during an attack. Finally, the threat model has been expanded in the context of autonomous vehicles to encompass various components, including sensors, the ROS, and V2X communication (Gao et al., 2022).

### **ROS and Other Secure Communication Methods**

Seo et al. (2025) proposed the memory isolation mechanism ROsec to close the security vulnerabilities of components that run in the same process, which come with the current ROS version. In order to provide flexibility, ROS has a mechanism that allows multiple nodes to work in a distributed manner simultaneously within a single process. However, it has been argued that this approach leads to a loss of memory isolation between nodes and security vulnerabilities. However, a system using ROsec technology, Intel Memory Protection Keys, has been proposed. Thus, instead of each node directly accessing another node, a mechanism has been presented that provides access by assigning a unique key. In particular, it has been stated that this access is at the client level, not the kernel level. Thus, low performance losses and high levels of security have been provided.

Tanadechopon and Kasemsontitum (2023) realized that transmitting data packets in plaintext is a weakness in ROS data transmission and proposed a new framework that ensures the security of data packets by applying a cryptographic algorithm. Data with different resolutions was received from a camera on a robot and converted into ciphertexts by applying a transformation process. These were then encrypted with AES, which rendered the text unreadable when transmitted over a network, thereby providing secure communication. The Central Process Unit (CPU) utilization and average time taken to encrypt and decrypt data were also presented. The results show that there is no increase in CPU utilization for data encryption or decryption. However, there is an increase in the average time since the encryption or decryption process adds additional cost. Nevertheless, it is argued that this delay can be ignored, considering the importance of secure communication.

Mayoral-Vilches et al. (2022) addressed the security shortcomings of ROS 2 by introducing the Security Robot Operating System 2 (SROS 2) framework, which was designed to enhance the security of robotic communication. SROS 2 was presented as a framework that incorporates additional security mechanisms such as authentication, authorization, encryption, and access control for the process graphs within ROS 2. Through the integration of these security tools, the secure transmission of data messages was facilitated within the ROS 2 environment. In the experimental setup, the SROS 2 framework was implemented on a TurtleBot3 robot using ROS 2 packages such as Navigation2 and SLAM Toolbox. As a result, the framework was demonstrated to function as an effective and secure communication mechanism for robotic message exchange and encryption.

Yaacoub et al. (2022) proposed a comprehensive perspective on robot vulnerabilities in the field of cybersecurity, including the classification of attacks and types of robot interactions. Common vulnerabilities in robotic systems were categorized into several groups: Network-based (e.g., spoofing, MITM, sniffing, replay attacks), Platform-based (e.g., outdated systems), Application-level (e.g., coding flaws, software bugs), Malicious (e.g., malware injection), and Management-related (e.g., inadequate policies and procedures). Furthermore, the importance of cryptographic methods such as AES and ECC, along with hashing algorithms, in securing network-based communication was emphasized.

Kim et al. (2018) presented a study addressing the security status of ROS 2, which was developed to overcome the cybersecurity vulnerabilities found in ROS 1. A ROS 2 environment was configured on two separate machines, and network-based analyses were conducted using both Ethernet and Wireless Fidelity (Wi-Fi) networks. The experiments were carried out under three different scenarios: without any additional security policies, with cryptographic techniques, and using a VPN. Each scenario was evaluated based on latency and throughput performance metrics. In the Ethernet network, unencrypted communication resulted in low latency, whereas the use of cryptographic techniques significantly increased latency. In the VPN scenario, latency was reduced by approximately half, thus also providing a secure communication channel. On the Wi-Fi network, cryptographic techniques were shown to negatively affect both efficiency and latency, while VPN usage yielded acceptable results in terms of performance and delay.

Breiling et al. (2017) introduced a more secure communication channel method for ROS. The proposed system was necessary due to the insufficient security measures of ROS1 and the need for more secure communication channels. In the new system proposed for transferring data over TCP and User Datagram Protocol (UDP), many operations such as data encryption, handshake, authorization, TLS, and DTLS data integrity are encapsulated, and data security is achieved. Handshake with the RSA algorithm for authentication and authorization, secure communication with AES-256, and data integrity with MACs are provided. In TCP communication, a TLS handshake is performed after the TCP handshake, and the message header is sent to the publisher in an encrypted form. Similarly, the subscriber sends the encrypted information to the publisher and guarantees the data is transmitted securely. For the UDP, DTLS is preferred for secure communication because it is a connectionless protocol. DTLS is designed to function similarly to TCP and guarantees that the data travels securely. On the other hand, the average handshake time for TLS was 387.7 milliseconds (ms), and for DTLS it was 431.4 ms. As a result, secure ROS communication was achieved with the proposed method.

The studies presented in Table 3 shift the focus beyond network-based and other external solutions to ROS-based communication mechanisms. Methodologically, initial approaches aimed to address the security limitations of ROS 1 by adding standard cryptographic protocols such as TLS and DTLS (Breiling et al., 2017). Following the release of ROS 2, native security frameworks that integrate authentication, authorization, and encryption emerged, such as SROS 2 (Mayoral-Vilches, 2022). However, a recurring theme in all these studies is the need to achieve an optimal balance between security and performance. For example, Kim et al. (2018) showed that encryption increases latency, while the use of VPNs provides an acceptable trade-off between the two parameters. Similarly, Tanadechopon & Kasemsontitum (2023) reported that AES encryption at the application layer increases the average processing time without increasing CPU utilization. An advanced approach is the solution proposed by Seo et al. (2025) that incorporates hardware-level memory isolation. This solution aims to provide high security with minimal performance overhead without requiring kernel-level intervention.

**Table 3.** An Overview Of The ROS And Other Secure Communication Techniques

Study	Year	Main Topic	Methodology
Seo et al.	2025	ROSec memory isolation mechanism mitigates security vulnerabilities in composable nodes sharing the same process in the latest ROS version.	ROSec technology using MPK is proposed, which assigns a unique key to each node and ensures that access is secure without direct access to other nodes. The mechanism operates at the client level, not the kernel level, ensuring low performance overhead and high security.
Tanadechopon & Kasemsontitum	2023	Secure ROS is proposed to prevent security vulnerabilities by encrypting data packets for data communication.	AES encryption was applied to text converted from camera data on an experimental robot, with evaluations of CPU usage, average encryption/decryption times, and power consumption.
Mayoral-Vilches	2022	The SROS 2 framework for secure robot communication has been proposed.	A system was proposed using SROS 2, which integrates additional security methods such as authentication, authorization, encryption, and access control into ROS 2.
Yaacoub et al.	2022	Cyber security vulnerabilities and weaknesses in the field of robotic systems were analysed in detail.	The use and importance of cryptographic algorithms such as AES, ECC, and hashing of vulnerabilities classified into network, platform, application, malware, and management types are presented.
Kim et al.	2018	Performance assessment of ROS 1 cyber vulnerabilities versus ROS 2 security features.	Performance evaluations using latency and throughput metrics showed VPN-based solutions effectively perform on both Ethernet and Wi-Fi networks.
Breiling et al.	2017	Proposed TLS and DTLS-based security framework for securing ROS TCP and UDP communications.	Encapsulated encryption, handshake, and integrity checks using RSA, AES-256, MACs, and handshake protocols for TCP and UDP.

## SECURITY THREATS AND VULNERABILITIES

In this section, potential threats and vulnerabilities affecting robot communication are discussed in detail. Attack vectors encountered on robots, existing vulnerabilities, potential threats, and strategies to minimize these risks are comprehensively evaluated.

In the automation environment of the modern age, security threats and potential vulnerabilities in robot communication and robot systems have become increasingly important. Therefore, today's robots are widely used in various areas, including social spaces, industry, autonomous vehicles, military, and agriculture. One of the greatest advances of the digital age is the integration of AI with these robots to create smarter systems. Almost all robots, from smart ones to commercial robots, include autonomous systems and AI integration. Although this situation significantly eases the workload in most sectors, it also entails a significant disadvantage. The misuse of AI brings with it many concerns, such as cyber threats in robot communication, manipulation of secure communication on robot operating systems, and manipulation of robot control and autonomous systems (Qayyum et al., 2020; Yaacoub et al., 2022).

The idea of machines that can think like humans has become one of the fundamental concepts that bring together AI technologies and robotics today. In this regard, AI has been integrated into many robot systems developed for industrial, military, health, and commercial purposes (Acun et al., 2023). According to a report published by the UK-RAS Network, the number of global investments in AI has risen by over a million in the last eight years (Perez et al., 2017). The emergence of systems such as AI has transformed numerous sectors and has had a direct impact on robotics, facilitating significant advancements, particularly through robotic system integrations that enable a more intelligent and flexible connection between perception and action (Brady, 1985). However, this development also brings with it challenges such as unpredictable threats and security vulnerabilities.

Systems such as AI require large amounts of data to operate effectively and efficiently (Doğan & Özyurt, 2025). However, storing this data securely is crucial to mitigate risks, especially when considering situations such as personal information being disclosed through malicious software (Canbay & Utku, 2024). In this sense, the role of AI-based customized robotic systems in ensuring personal data security is quite important. For instance, a healthcare

robot may be at risk of exposing the personal information of patients during the transmission of data processed by AI tools. In addition, the bias or incompleteness of the data sets on which AI algorithms are trained is another important problem that directly affects the decision-making processes of intelligent robot systems (Karaferis et al., 2024).

A primary factor adversely affecting the development of robotic systems is the presence of cybersecurity vulnerabilities in network-based communication and the lack of a Zero Trust Architecture (ZTA). Robotic communication channels are vulnerable to spoofing, DoS, and MITM attacks, which can lead to financial losses, data breaches, and even consequences that threaten human life. A striking example demonstrating the severity of these threats is the Stuxnet worm. Stuxnet, a malicious software capable of causing not only software disruptions but also physical damage to equipment, clearly exposed the vulnerability of robotic systems to cyber-physical attacks (Stuxnet, 2017). Also, the non-adoption of the ZTA in many robotic networks further weakens security. In existing architectures built upon implicit trust assumptions, malicious actors who gain unauthorized access following a network breach can manipulate internal data or disrupt communication (Alquwayzani & Albuali, 2024).

The primary threats encountered in robot communication are remote monitoring of robots, data transmission over network infrastructures, and the security vulnerabilities of wired or wireless communication protocols used. Robots typically employ short-range communication technologies such as Bluetooth, Ultra-Wideband (UWB), Zigbee, and Wi-Fi (802.11 networks) when interacting with other systems. Additionally, for long-distance communication, satellite links and cellular networks are utilized (Abed et al., 2023). These communication protocols are susceptible to various categories of attacks and vulnerabilities. For instance, jamming attacks target wireless communication, disrupting the robot's interaction with its environment and causing communication loss. The absence of integrity checks or the use of insecure communication protocols can lead to interception, manipulation of transmitted data, or exposure to DoS attacks. Vulnerable firmware versions may result in security weaknesses at both the physical and software levels of the robot (Tanimu & Abada, 2025).

From another perspective, one of the potential threats in robot communication is a social engineering attack. Data flows occurring in robot-to-robot and robot-to-human interactions can lead to significant security vulnerabilities if proper authentication processes are not enforced. The transmission of passwords in plaintext, the unencrypted transfer of sensitive system operation information, and the insufficient measures to ensure data integrity can be easily exploited by malicious actors using social engineering techniques (Alsharif et al., 2022). Such vulnerabilities create opportunities for more advanced attacks. For example, in an MITM attack, an attacker can eavesdrop on and manipulate data exchanged between two robotic units or communication nodes. Similarly, Meet-in-the-Middle attacks target encryption methods such as 2-DES or 3-DES. In this type of attack, brute-force techniques are employed to compromise the encrypted communication (Abed et al., 2023).

Another security problem encountered in robot communication is data manipulation. While performing the given tasks, robots receive data from various hardware parts such as sensors, process the data, and transform it into decision-making mechanisms (Khalid et al., 2018). The interception or modification of data by unauthorized persons during data traffic allows the robot to make incorrect decisions and perform incorrect actions. Robotic systems that lack additional security methods, such as authentication, payload encryption, and data integrity provided by secure data communication protocols, make it easier for attackers to obtain this information and invite data modification and manipulation (Vilches et al., 2021). In such a case, robots may be directed to the wrong targets, exhibit abnormal behavior, or cause systemic and financial damage (Brady, 1985; Khalid et al., 2018; Vilches et al., 2021). Table 4 summarizes the findings, providing a general perspective on security vulnerabilities observed in robot communication.

## **TECHNICAL MEASURES: CRYPTOGRAPHIC TECHNIQUES AND PROTOCOLS**

The cryptographic techniques and communication protocols employed in robotic systems are explored in this section. Fundamental security components such as data confidentiality, authentication, data integrity, and overall communication security in robotic environments were examined.

Various cryptographic techniques and protocols are used to ensure secure robot communication and data transmission. Data confidentiality, data integrity, authentication, and encryption are among the elements that ensure secure communication in the field of robotics (Breiling et al., 2017; Yaacoub et al., 2022). However, in systems based on open-source platforms such as ROS and Pixhawk Extended 4 (PX4), these security measures are inadequately

implemented. Survey results reveal that only 36% of robotic systems use special cryptographic solutions, and security is largely limited to network perimeter measures (Mayoral-Vilches, 2022).

**Table 4.** List Of Security Vulnerabilities And Threats in Robot Communication

Threads	Type of Vulnerability	Definiton
Misuse of AI	Manipulation of robot control and communication	Malicious use of AI could lead to manipulation of robot control and communication systems, resulting in unpredictable behavior or cyber threats.
Lack of Zero Trust Architecture	Architectural & Trust Model Vulnerability	This architectural approach, rooted in an implicit trust model, inherently facilitates movement and system compromise by threat actors who, having breached the perimeter, can operate without subsequent authentication.
Biased decision-making	Biased or insufficient training datasets	Bias in training data can lead to faulty decision-making processes in intelligent robots.
Network-based attacks	Lack of communication infrastructure	Robot systems connected to the Internet or local networks are vulnerable to spoofing, DoS, and MITM attacks.
Protocol and firmware exploitation	Lack of secure communication protocols	Protocol and firmware exploitation occur when insecure communication protocols and outdated firmware expose software and hardware layers to vulnerabilities, enabling attackers to intercept, alter, or block communications.
Unauthorized access	Lack of authentication mechanisms	A weak authentication mechanism allows robot communication to be hijacked or manipulated.
Credential theft	Transmission of authentication information in plaintext	Transmitting authentication credentials in plaintext creates a vulnerability to social engineering attacks.
Communication disruption	Jamming attack	Wireless protocols such as Bluetooth and Wi-Fi can be blocked, leading to interruption of communication.
Social manipulation	Social engineering attack	Weak authentication policies expose robot-to-human and robot-to-robot communications to spoofing attacks.
Weak encryption	Weak encryption methods	Weak algorithms like 2-DES or 3-DES are vulnerable to brute-force attacks like MITM.
Data Falsification	Data manipulation	Unauthorized access to sensor data can result in robots making false decisions or behaving abnormally.

Data confidentiality ensures that transmitted data is accessible only to authorized persons, while data integrity confirms that the data has not been altered and is accurate (Mukhandi et al., 2019). Authentication is a security process that is performed to verify whether a user, system, or device truly has the identity it claims. Encryption is a cryptographic technique that transforms data or information into a complex form so that it can only be read by authorized persons (Diro et al., 2020).

Cryptography is fundamentally divided into symmetric and asymmetric types (Rodríguez-Lera et al., 2018; Goerke et al., 2021; Yaacoub et al., 2022; Dere & Ülkü, 2023). Both forms are used for different purposes in different components of robotic systems. Symmetric encryption, also known as secret key encryption, uses the same key for both encrypting and decrypting the plaintext, and the data is encrypted in blocks. The plaintext is encrypted with a secret key created by the sender of the message, and the encrypted text is sent to the recipient. The recipient decrypts the encrypted text with the same key to view the plaintext again. One of the biggest advantages of this encryption method is that it is easy and fast to manage since the same key is used when encrypting and decrypting. It is also much faster than other encryption methods, such as asymmetric methods. In this respect, it is quite suitable in cases where the communication speed is high, the computational cost is low, and it is efficient. The algorithms commonly used for symmetric encryption are mainly DES, AES, and 3DES. DES encrypts or decrypts data in 64-bit blocks. DES is quite cost-effective; 3DES involves encrypting the data blocks three times using DES. AES is an advanced symmetric encryption algorithm that encrypts and decrypts in 128-bit blocks. Although AES is not as costly as DES, despite offering high security, it provides high security (Zhang, 2021).

Symmetric encryption in robot communication offers significant advantages due to its low energy consumption and fast processing power. Therefore, it is preferred by mobile systems or embedded system robots limited power and resources (Yaacoub et al., 2022). Symmetric encryption algorithms require less computational power because they perform both encryption and decryption with the same key. This increases energy efficiency in robot systems where

battery life is critical. However, one of the biggest challenges of symmetric encryption is secure key sharing. Therefore, it is often used in conjunction with a secure key exchange protocol to ensure communication security (Rodríguez-Lera et al., 2018; Zhang, 2021; Goerke et al., 2021).

Asymmetric encryption, also known as public key encryption, is a secure encryption method that uses a public key and a private key. In this method, security is based on mathematical problems that are quite difficult to solve. The data to be sent is encrypted using the recipient's public key and transmitted over the network. This encrypted data can only be decrypted with the recipient's private key, thus allowing the recipient to access the data securely. There is a complex mathematical relationship between the public and private keys (Lalem et al., 2023). Asymmetric encryption supports not only data confidentiality but also security services such as authentication and integrity. For example, in the digital signing process, the sender signs the text with his private key, and the receiver verifies this signature with the sender's public key, ensuring both the integrity of the data and the identity of the sender (Zhang, 2021; Lalem et al., 2023).

Two commonly used asymmetric algorithms are RSA and ECC. RSA is an encryption algorithm based on the difficulty of factoring large prime numbers. It is often preferred in areas such as digital certificates and private area networks. ECC is an encryption method based on elliptic curve mathematics and uses shorter key lengths than RSA. This method is often preferred in situations where processing resources are limited, such as robotics (Ma, 2021).

Modern robots usually connect to a server or to each other over a wired or wireless network and transfer data. These networks are usually insecure and require additional security measures such as authentication and encryption. The direct use of asymmetric encryption in end-to-end encryption is a major disadvantage, due to the complex mathematical calculations and limited resources of the robots. In contrast, symmetric encryption involves a single key, and the fact that this key can be obtained by an attacker is also a serious security problem. Therefore, a hybrid version that includes the advantages of asymmetric and symmetric encryption is often preferred in robot communication. In the hybrid system, a handshake is performed to verify the other party, and the identity is confirmed before the robot sends data. While the process of verifying the identity of the recipient involves asymmetric encryption steps, symmetric encryption is used in data exchanges after authentication (Yfantis & Fayed, 2014).

Advanced robotic systems employ secure communication protocols to mitigate various types of attacks, including those targeting inter-robot communication, data manipulation in communications with central control units, and identity spoofing. However, TCP and UDP do not inherently provide security features (Rescorla & Modadugu, 2012). Therefore, TLS or Datagram Transport Layer Security (DTLS) working on the transport layer is preferred. These protocols support confidentiality, integrity, and encryption in data transmission. Thus, data security is ensured (Breiling et al., 2017). Moreover, MQTT over TLS is widely preferred, especially in IoT-based robot systems, due to its lightweight structure and secure connection feature (Singh et al., 2015). In new-generation architectures such as ROS 2, security layers are integrated into publish/subscribe mechanisms via the Data Distribution Service (DDS) protocol. This structure enables security services such as authentication, authorization, and data encryption in communication. Applications such as SROS are among the fundamental examples of this approach (White et al., 2019). Technical cryptographic approaches for secure robot communication, the protocols used, and information, including the security services and definitions offered by these protocols, are specified in Table 5.

## EFFECTS OF NEW TECHNOLOGIES ON THE SECURITY OF ROBOT COMMUNICATION

The effects of emerging technologies on the security of robot communication are analyzed in this section. Contemporary technologies such as AI, edge computing, blockchain, Large Language Models (LLMs), and 5G connectivity were examined in terms of their potential to both enhance and compromise communication security within robotic systems.

Advancements in contemporary technology, along with the opportunities offered by emerging innovations, have led humanity to continuously engage in various efforts to ensure the rapid transmission of information. The development of emerging technologies such as AI, IoT, and 5G has fundamentally transformed the communication infrastructure of robotic systems. These technologies provide robots with faster, more autonomous, efficient, and flexible interaction with their environment. However, the advancement of technology also brings certain disadvantages in terms of security and cost. The use of fiber-optic cables for high-speed communication significantly increases costs.

Moreover, extensive network coverage and high data transmission speeds result in increased energy consumption. Additionally, the misuse of AI or incidents of cyberattacks pose significant risks to data privacy, representing another critical drawback in this field (Qiao et al., 2021; Ramavath et al., 2025).

**Table 5.** Technical Cryptographic Approaches For Secure Robot Communication

Protocols and Approaches	Definition
Data confidentiality	It ensures that communication between robots or servers can only be accessed by authorized units. For example, robots in the healthcare sector contain sensitive information such as patient data. Therefore, this data must be protected.
Data Integrity	Verifies that the message received is the same as the one sent. Protects against possible manipulation during data transmission.
Authentication	It verifies identity in multi-communication situations such as robot-robot and robot-human. It prevents identity fraud.
Symmetric encryption	It uses the same secret key for encryption and decryption. It offers high speed and low processing costs. It is used in robots with limited energy and processing power.
Asymmetric encryption	It uses a mathematically related pair of public and private keys. This method is used in methods such as secure key exchange and digital signature verification.
Hybrid encryption	It combines asymmetric encryption for secure key exchange and symmetric encryption for efficient data transfer. Therefore, it is the preferred model for robot communication.
TLS	Provides encrypted, authenticated, and integrity-protected communication in robot systems
DTLS	It is a TLS protocol for UDP-based communication. It is preferred in real-time and latency-sensitive robotic systems.
MQTT over TLS	It is a lightweight messaging protocol that uses a publish-subscribe model and provides efficient communication in unstable network conditions, such as low bandwidth.

The proliferation of IoT technology has enabled robots to communicate through sensors, control units, and cloud services. While this infrastructure has made robotic systems more accessible, it has also increased the vulnerability of low-memory connected devices to cyber-attacks, which is a significant concern for new technologies like autonomous machines (Mazhar et al., 2023). These developments, while creating significant opportunities, have also revealed security vulnerabilities and various attack vectors that threaten the confidentiality, integrity, and availability of systems (Ramavath et al., 2025). However, as demonstrated by studies showing its effectiveness in mitigating such vulnerabilities through real-time threat detection and advanced network security in IoT environments, technologies like Software-Defined Networking (SDN) offer a potential solution by providing centralized control and dynamic management (Hamad et al., 2024).

LLMs are being increasingly integrated into robotic systems. Natural language processing plays a critical role in robot communication, decision-making, and interaction with their surroundings. However, the cloud-based operation of LLMs, their accessibility via exposed Application Programming Interfaces (APIs), and their handling of user identities introduce vulnerabilities that pose risks to both security and the privacy of personal data (W. Zhao et al., 2024).

The low latency and high bandwidth offered by 5G technology enable real-time synchronized operation of robotic systems (Ramavath et al., 2025; Lin et al., 2025). Similarly, alternative communication technologies such as Wi-Fi 6 and the next-generation 6G can support these functions by offering high data transmission speeds and low latency. However, due to high data traffic and centralized structures, these systems can create vulnerabilities concerning data privacy and personal data protection. Data leakage or misuse during the transmission of sensitive data can lead to privacy violations and legal compliance issues in industrial robot applications. Therefore, secure communication protocols (e.g., TLS 1.3, IPsec) and advanced cryptographic methods play a crucial role in enhancing the reliability of these technologies (Y. Zhao et al., 2021; Ramezanzpour et al., 2022; Saeed et al., 2025).

Blockchain has emerged as an innovative and robust technological paradigm for ensuring secure and decentralized communication management within the domain of robotics. In particular, the secure exchange of robotic data and algorithms through the implementation of smart contracts effectively mitigates the risk of data manipulation. Beyond enabling autonomous mobility of robotic systems, this technology substantially enhances data integrity and transparency. The storage of sensitive data acquired by robots as immutable blocks offers considerable advantages in terms of regulatory compliance and auditability. Consequently, blockchain possesses the potential to serve as a

foundational infrastructure for the secure, accountable, and efficient operation of future robotic systems (Srinivas Aditya et al., 2021).

Edge computing architecture enables local processing of data in robotic systems, reducing latency and limiting certain security threats (Shi et al., 2016). It enables data processing locally on embedded devices or network edge nodes, rather than solely on remote cloud infrastructures. It significantly reduces communication latency, improving real-time responsiveness. This local processing not only optimizes bandwidth utilization but also limits certain cybersecurity risks by reducing the amount of sensitive data transmitted over potentially insecure networks. Edge computing is becoming an innovative and enabling element for the secure, efficient, and autonomous operation of next-generation robotic systems (Mao et al., 2017; Bentayeb et al., 2025).

## CONCLUSION AND FUTURE DIRECTIONS

The rapid advancement of technology and network infrastructures has led to a transformative revolution in the field of robotics, as in many other domains. With Industry 4.0, robots are no longer limited to performing pre-defined tasks; they also utilize advanced communication methods involving human-robot and robot-robot interactions. Furthermore, robotic systems integrated with telecommunications and AI technologies play a crucial role not only in process management but also in the execution of fast and effective decision-making mechanisms. These communication frameworks, implemented through network-based platforms or local system architectures, ensure that tasks are completed with high speed and efficiency.

Although technological advancements in the field of robotics have significantly facilitated daily life, every system possesses potential security vulnerabilities. For instance, malicious software developers may gain access to a robot's data during its communication processes, potentially taking control of the system. Such breaches can lead to substantial financial losses for organizations. Therefore, both academic research and industry initiatives have focused on developing potential solutions to address these issues. Among these efforts, considerable attention has been given to various methods for ensuring secure data transmission, including encryption techniques, access control mechanisms, and secure communication protocols, aimed at preventing security threats and vulnerabilities.

This study provides a comprehensive review of contemporary research aimed at ensuring the security of data communication among robots. It details the security threats and potential risks that may emerge during robot-human, robot-robot, and robot-machine interactions. The study further examines cryptographic approaches and secure communication protocols employed to mitigate these risks. Particular emphasis is placed on the critical role of encryption techniques within the context of fundamental principles such as data confidentiality, integrity, and authentication. Moreover, the study explores the contributions of advanced technologies, including LLMs, Long Term Evolution (LTE), and 5G telecommunications and wireless networks, blockchain, and edge computing in enhancing the security of data transmission in robotic communication.

Future research should focus on developing agile and context-aware security frameworks for robotic systems. Rather than depending on a fixed set of protocols, such systems ought to possess the capability to dynamically adapt their encryption mechanisms and security policies in response to contextual threat assessments. For example, a robot engaged in a mission-critical operation within a hostile network environment could autonomously escalate its encryption scheme to a more robust yet computationally demanding algorithm, while reverting to a lightweight configuration for routine tasks conducted in trusted environments. Machine learning techniques could be employed to intelligently evaluate threat levels and facilitate this real-time adaptation.

### Artificial Intelligence Contribution Statement

We declare that this article was written, edited, analyzed, and prepared without the assistance of any artificial intelligence tool. This statement confirms that all content, including the text, data analysis, and figures, was created solely by the authors.

## REFERENCES

Abed, M. S., Al-Doori, Q. F., Abdullah, A. T., & Abdallah, A. A. (2023). Security Vulnerabilities and Threats in Robotic Systems: A Comprehensive Review. *International Journal of Safety and Security Engineering*, 13(3), 555–563. <https://doi.org/10.18280/ijssse.130318>

- Abeykoon, I., & Feng, X. (2017). A Forensic Investigation of the Robot Operating System. *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 851–857. <https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.131>
- Acun, M. F., Daldal, M., & Avci, K. (2023). STM32F407 ve Nodemcu ESP8266 Kartları Kullanarak Kablosuz Çok Yönlü Kontrollü Robotik Araç Sisteminin Geliştirilmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Mühendislik Bilimleri Dergisi*, 26(4), 1030–1049. <https://doi.org/10.17780/ksujes.1351636>
- Alquwayzani, A. A., & Albuali, A. A. (2024). A Systematic Literature Review of Zero Trust Architecture for Military UAV Security Systems. *IEEE Access*, 12, 176033–176056. <https://doi.org/10.1109/ACCESS.2024.3503587>
- Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering*, 40(3), 1153–1166. <https://doi.org/10.32604/csse.2022.019938>
- Bentayeb, Y., Chaoui, K., & Badir, H. (2025). Integrating Blockchain and Edge Computing: A Systematic Analysis of Security, Efficiency, and Scalability. *International Journal of Advanced Computer Science and Applications*, 16(1). <https://doi.org/10.14569/IJACSA.2025.0160160>
- Botta, A., Rotbei, S., Zinno, S., & Ventre, G. (2023). Cyber security of robots: A comprehensive survey. *Intelligent Systems with Applications*, 18, 200237. <https://doi.org/10.1016/j.iswa.2023.200237>
- Brady, M. (1985). Artificial intelligence and robotics. *Artificial Intelligence*, 26(1), 79–121. [https://doi.org/10.1016/0004-3702\(85\)90013-X](https://doi.org/10.1016/0004-3702(85)90013-X)
- Breiling, B., Dieber, B., & Schartner, P. (2017). Secure communication for the robot operating system. *2017 Annual IEEE International Systems Conference (SysCon)*, 1–6. <https://doi.org/10.1109/SYSCON.2017.7934755>
- Canbay, Y., & Utku, A. (2024). A Comparative Study for Privacy-Aware Recommendation Systems. *Gazi University Journal of Science Part A: Engineering and Innovation*, 11(1), 68–79. <https://doi.org/10.54287/gujsa.1393692>
- Degirmenci, E., Kirca, Y. S., Yolaçan, E. N., & Yazıcı, A. (2023). An Analysis of DoS Attack on Robot Operating System. *Gazi University Journal of Science*, 36(3), 1050–1069. <https://doi.org/10.35378/guj.976496>
- Degirmenci, E., Sabri Kirca, Y., Özçelik, İ., & Yazıcı, A. (2023). ROSIDS23: Network intrusion detection dataset for robot operating system. *Data in Brief*, 51, 109739. <https://doi.org/10.1016/j.dib.2023.109739>
- Dere, N., & Ülkü, E. E. (2023). QUANTUM KEY DISTRIBUTION IN SMART HOME SYSTEMS. *Kahramanmaraş Sütçü İmam Üniversitesi Mühendislik Bilimleri Dergisi*, 26(4), 932–942. <https://doi.org/10.17780/ksujes.1325805>
- Diro, A., Reda, H., Chilamkurti, N., Mahmood, A., Zaman, N., & Nam, Y. (2020). Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication. *IEEE Access*, 8, 60539–60551. <https://doi.org/10.1109/ACCESS.2020.2983117>
- Doğan, N., & Özyurt, F. (2025). IOT DESTEKLİ HAVA DURUMU VERİLERİ İLE YAPAY ZEKÂ TABANLI HAVA TAHMİN SİSTEMİNİN GELİŞTİRİLMESİ. *Kahramanmaraş Sütçü İmam Üniversitesi Mühendislik Bilimleri Dergisi*, 28(1), 524–535. <https://doi.org/10.17780/ksujes.1528386>
- Dourado, C. M. J. M., Da Silva, S. P. P., Da Nóbrega, R. V. M., Barros, A. C. S., Sangaiah, A. K., Rebouças Filho, P. P., & De Albuquerque, V. H. C. (2019). A new approach for mobile robot localization based on an online IoT system. *Future Generation Computer Systems*, 100, 859–881. <https://doi.org/10.1016/j.future.2019.05.074>
- Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law & Security Review*, 41, 105528. <https://doi.org/10.1016/j.clsr.2021.105528>
- Gao, C., Wang, G., Shi, W., Wang, Z., & Chen, Y. (2022). Autonomous Driving Security: State of the Art and Challenges. *IEEE Internet of Things Journal*, 9(10), 7572–7595. <https://doi.org/10.1109/JIOT.2021.3130054>
- Giansanti, D., & Gulino, R. A. (2021). The Cybersecurity and the Care Robots: A Viewpoint on the Open Problems and the Perspectives. *Healthcare*, 9(12), 1653. <https://doi.org/10.3390/healthcare9121653>

- Goerke, N., Timmermann, D., & Baumgart, I. (2021). Who Controls Your Robot? An Evaluation of ROS Security Mechanisms. *2021 7th International Conference on Automation, Robotics and Applications (ICARA)*, 60–66. <https://doi.org/10.1109/ICARA51699.2021.9376468>
- Greenberg, A. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway—With Me in It [Security]. *Hackers Remotely Kill a Jeep on the Highway—With Me in It*. <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
- Hamad, D., Yalda, K., Tapus, N., & Okumus, I. T. (2024). Enhancing IoT scalability and security through SDN. *Revista Română de Informatică Şi Automatică*, 34(2), 113–126. <https://doi.org/10.33436/v34i2y202409>
- IFR. (2024). *Record of 4 Million Robots in Factories Worldwide* (pp. 1–4) [Press Report]. IFR International Federation of Robotics. <https://ifr.org/ifr-press-releases/news/record-of-4-million-robots-working-in-factories-worldwide>
- Jain, S., & Doriya, R. (2022). Security framework to healthcare robots for secure sharing of healthcare data from cloud. *International Journal of Information Technology*, 14(5), 2429–2439. <https://doi.org/10.1007/s41870-022-00997-8>
- Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2021). Substantial capabilities of robotics in enhancing industry 4.0 implementation. *Cognitive Robotics*, 1, 58–75. <https://doi.org/10.1016/j.cogr.2021.06.001>
- Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. W. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. *PLOS ONE*, 15(1), e0227800. <https://doi.org/10.1371/journal.pone.0227800>
- Karaferis, D. C., Balaska, D., & Pollalis, Y. (2024). Artificial Intelligence and Robotics: Catalysts or Threats in the Development of Healthcare. *Biostatistics and Biometrics Open Access Journal*, 11(5), 14. <https://doi.org/10.19080/BBOAJ.2024.11.555825>
- Khalid, A., Kirisci, P., Khan, Z. H., Ghairi, Z., Thoben, K.-D., & Pannek, J. (2018). Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry*, 97, 132–145. <https://doi.org/10.1016/j.compind.2018.02.009>
- Kim, J., Smereka, J. M., Cheung, C., Nepal, S., & Grobler, M. (2018). *Security and Performance Considerations in ROS 2: A Balancing Act* (No. arXiv:1809.09566). arXiv. <https://doi.org/10.48550/arXiv.1809.09566>
- Lalem, F., Laouid, A., Kara, M., Al-Khalidi, M., & Eleyan, A. (2023). A Novel Digital Signature Scheme for Advanced Asymmetric Encryption Techniques. *Applied Sciences*, 13(8), Article 8. <https://doi.org/10.3390/app13085172>
- Liang, W., Ning, Z., Xie, S., Hu, Y., Lu, S., & Zhang, D. (2021). Secure fusion approach for the Internet of Things in smart autonomous multi-robot systems. *Information Sciences*, 579, 468–482. <https://doi.org/10.1016/j.ins.2021.08.035>
- Lin, Y., Chen, Y., Qin, Y., Sun, Y., Xu, R., Yang, Y., Zhang, Z., Chen, J., Tian, Y., Cao, Y., Chai, X., Chen, H., Qi, H., & Pang, X. (2025). *AI in the 5G-A Era: Scenarios, Key Technologies, and Evolution Trends*. Huawei. Retrieved August 6, 2025. <https://www.huawei.com/en/huaweitech/future-technologies/5ga-scenarios-key-technologies-evolution-trends>
- Ma, M. (2021). Comparison between RSA and ECC. *2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*, 642–645. <https://doi.org/10.1109/AINIT54228.2021.00129>
- Mao, Y., You, C., Zhang, J., Letaief, K. B., & Huang, K. (2017). A Survey on Mobile Edge Computing: The Communication Perspective. *ResearchGate*. <https://doi.org/10.1109/COMST.2017.2745201>
- Martín, F., Soriano-Salvador, E., Guerrero, J. M., Guardiola Múzquiz, G., Manzanares, J. C., & Rodríguez, F. J. (2025). Towards a robotic intrusion prevention system: Combining security and safety in cognitive social robots. *Robotics and Autonomous Systems*, 190, 104959. <https://doi.org/10.1016/j.robot.2025.104959>
- Mayoral-Vilches, V. (2022). Robot Cybersecurity, a Review. *International Journal of Cyber Forensics and Advanced Threat Investigations*, 0, Article 0. <https://doi.org/10.46386/ijcfati.crossmarkpolicy>

- Mazhar, T., Talpur, D. B., Shloul, T. A., Ghadi, Y. Y., Haq, I., Ullah, I., Ouahada, K., & Hamam, H. (2023). Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. *Brain Sciences*, 13(4), Article 4. <https://doi.org/10.3390/brainsci13040683>
- Mukhandi, M., Portugal, D., Pereira, S., & Couceiro, M. S. (2019). A novel solution for securing robot communications based on the MQTT protocol and ROS. *2019 IEEE/SICE International Symposium on System Integration (SII)*, 608–613. <https://doi.org/10.1109/SII.2019.8700390>
- Mwanje, M. D., Bhagwat, G. P., Kaiwartya, O., Maladkar, R., & Sadiq, A. S. (2025). Cyber Security Risks in Connected and Autonomous Vehicles-An Experimental Demonstration. *CCGridW*, 109–116. <https://doi.org/10.1109/CCGridW65158.2025.00024>
- Perez, J. A., Deligianni, F., Ravi, D., & Yang, G.-Z. (2017). *UK-RAS Network* (UK-RAS White Paper Series on Robotics and Autonomous Systems (RAS), p. 56) [Whitepaper]. Artificial Intelligence and Robotics (White Paper). Engineering and Physical Sciences Research Council (EPSRC). <http://doi.org/10.31256/WP2017.1>
- Qayyum, A., Usama, M., Qadir, J., & Al-Fuqaha, A. (2020). Securing Connected & Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and the Way Forward. *IEEE Communications Surveys & Tutorials*, 22(2), 998–1026. <https://doi.org/10.1109/COMST.2020.2975048>
- Qiao, L., Li, Y., Chen, D., Serikawa, S., Guizani, M., & Lv, Z. (2021). A survey on 5G/6G, AI, and Robotics. *Computers and Electrical Engineering*, 95, 107372. <https://doi.org/10.1016/j.compeleceng.2021.107372>
- Ramavath, S., Samal, U. C., Patra, P. K., Sunil, P., Appasani, B., Ramavath, S., Samal, U. C., Patra, P. K., Sunil, P., & Appasani, B. (2025). 5G and Beyond: Advancements in Wireless Communications for IoT and Smart Cities. In *Advanced Wireless Communications and Mobile Networks—Current Status and Future Directions*. IntechOpen. <https://doi.org/10.5772/intechopen.1009925>
- Ramezanpour, K., Jagannath, J., & Jagannath, A. (2022). *Security and Privacy vulnerabilities of 5G/6G and WiFi 6: Survey and Research Directions from a Coexistence Perspective* (No. arXiv:2206.14997). arXiv. <https://doi.org/10.48550/arXiv.2206.14997>
- Rescorla, E., & Modadugu, N. (2012). *Datagram Transport Layer Security Version 1.2* (Request for Comments No. RFC 6347). Internet Engineering Task Force. <https://doi.org/10.17487/RFC6347>
- Rishikesh, Bhattacharya, A., Thakur, A., Banda, G., Ray, R., & Halder, R. (2021). Secure Communication System Implementation for Robot-based Surveillance Applications. *2021 International Symposium of Asian Control Association on Intelligent Robotics and Industrial Automation (IRIA)*, 270–275. <https://doi.org/10.1109/IRIA53009.2021.9588788>
- Rodríguez-Lera, F. J., Matellán-Olivera, V., Balsa-Comerón, J., Guerrero-Higuera, Á. M., & Fernández-Llamas, C. (2018). Message Encryption in Robot Operating System: Collateral Effects of Hardening Mobile Robots. *Frontiers in ICT*, 5, 2. <https://doi.org/10.3389/fict.2018.00002>
- Saeed, M. M., Saeed, R. A., Hasan, M. K., Ali, E. S., Mazha, T., Shahzad, T., Khan, S., & Hamam, H. (2025). A comprehensive survey on 6G-security: Physical connection and service layers. *Discover Internet of Things*, 5(1), 28. <https://doi.org/10.1007/s43926-025-00123-7>
- Seo, J., Kayondo, M., Kang, J., Lee, K., Kwon, D., & Paek, Y. (2025). ROsec: Intra-Process Isolation for ROS Composition With Memory Protection Keys. *IEEE Transactions on Automation Science and Engineering*, 22, 10546–10559. <https://doi.org/10.1109/TASE.2024.3525050>
- Shepita, P., Durnyak, B., Petriv, Y., & Yasinskyi, M. (2025). Cybersecurity of robotic sorting systems of warehouse assets of a printing company. *The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS 2025)*, 3963, 299–313. <https://ceur-ws.org/Vol-3963/paper24.pdf>
- Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*, 3(5), 637–646. <https://doi.org/10.1109/JIOT.2016.2579198>
- Singh, M., Rajan, M. A., Shivraj, V. L., & Balamuralidhar, P. (2015). Secure MQTT for Internet of Things (IoT). *2015 Fifth International Conference on Communication Systems and Network Technologies*, 746–751. <https://doi.org/10.1109/CSNT.2015.16>

- Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *Cognitive Robotics*, 3, 54–70. <https://doi.org/10.1016/j.cogr.2023.04.001>
- Srinivas Aditya, U. S. P., Singh, R., Singh, P. K., & Kalla, A. (2021). A Survey on Blockchain in Robotics: Issues, Opportunities, Challenges and Future Directions. *Journal of Network and Computer Applications*, 196, 103245. <https://doi.org/10.1016/j.jnca.2021.103245>
- Stuxnet Definition & Explanation*. (2017, September 13). [CyberSecurity Blogs]. Stuxnet Explained: What It Is, Who Created It and How It Works. <https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet>
- Tanadechopon, T., & Kasemsontitum, B. (2023). Proposed Technique for Data Security with the AES Algorithm in Robot Operating System (ROS). *2023 27th International Computer Science and Engineering Conference (ICSEC)*, 153–156. <https://doi.org/10.1109/ICSEC59635.2023.10329645>
- Tanimu, J. A., & Abada, W. (2025). Addressing cybersecurity challenges in robotics: A comprehensive overview. *Cyber Security and Applications*, 3, 100074. <https://doi.org/10.1016/j.csa.2024.100074>
- Vilches, V. M., Kirschgens, L. A., Calvo, A. B., Cordero, A. H., Pisón, R. I., Vilches, D. M., Rosas, A. M., Mendia, G. O., Juan, L. U. S., Ugarte, I. Z., Gil-Uriarte, E., Tews, E., & Peter, A. (2021). *Introducing the Robot Security Framework (RSF), a standardized methodology to perform security assessments in robotics* (No. arXiv:1806.04042). arXiv. <https://doi.org/10.48550/arXiv.1806.04042>
- White, R., Caiazza, G., Christensen, H., & Cortesi, A. (2019). SROS1: Using and Developing Secure ROS1 Systems. In A. Koubaa (Ed.), *Robot Operating System (ROS)* (Vol. 778, pp. 373–405). Springer International Publishing. [https://doi.org/10.1007/978-3-319-91590-6\\_11](https://doi.org/10.1007/978-3-319-91590-6_11)
- Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, 21(1), 115–158. <https://doi.org/10.1007/s10207-021-00545-8>
- Yfantis, E. A., & Fayed, A. (2014). Authentication and Secure Robot Communication. *International Journal of Advanced Robotic Systems*, 11(2), 10. <https://doi.org/10.5772/57433>
- Zhang, Q. (2021). An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption. *2021 2nd International Conference on Computing and Data Science (CDS)*, 616–622. <https://doi.org/10.1109/CDS52072.2021.00111>
- Zhao, W., Khazanchi, V., Xing, H., He, X., Xu, Q., & Lane, N. D. (2024). Attacks on Third-Party APIs of Large Language Models (No. arXiv:2404.16891). arXiv. <https://doi.org/10.48550/arXiv.2404.16891>
- Zhao, Y., Zhai, W., Zhao, J., Zhang, T., Sun, S., Niyato, D., & Lam, K.-Y. (2021). A Comprehensive Survey of 6G Wireless Communications (No. arXiv:2101.03889). arXiv. <https://doi.org/10.48550/arXiv.2101.03889>