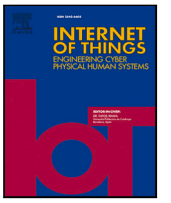
Internet of Things 28 (2024) 101357

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot



Review article

Enhancing security of Internet of Robotic Things: A review of recent trends, practices, and recommendations with encryption and blockchain techniques

Ehsanul Islam Zafir [a], Afifa Akter [a], M.N. Islam [a], Shahid A. Hasib [b], Touhid Islam [a], Subrata K. Sarker [c,*], S.M. Muyeen [d]

[a] Department of Mechatronics Engineering, Rajshahi University of Engineering & Technology, Rajshahi 6204, Bangladesh
[b] Department of Control & Instrumentation Engineering, King Fahd University of Petroleum & Minerals, Dhahran, 31261, Saudi Arabia
[c] School of Electrical and Data Engineering, University of Technology Sydney, Australia
[d] Department of Electrical Engineering, Qatar University, Qatar

ARTICLE INFO

Keywords:
IoRT
Encryption
Cryptography
Cyber security
Security algorithm
Robotics
IoT

ABSTRACT

The Internet of Robotic Things (IoRT) integrates robots and autonomous devices, transforming industries such as manufacturing, healthcare, and transportation. However, security vulnerabilities in IoRT systems pose significant challenges to data privacy and system integrity. To address these issues, encryption is essential for protecting sensitive data transmitted between devices. By converting data into ciphertext, encryption ensures confidentiality and integrity, reducing the risk of unauthorized access and data breaches. Blockchain technology also enhances IoRT security by offering decentralized, tamper-proof data storage solutions. By offering comprehensive insights, practical recommendations, and future directions, this paper aims to contribute to the advancement of knowledge and practice in securing interconnected robotic systems, thereby ensuring the integrity and confidentiality of data exchanged within IoRT ecosystems. Through a thorough examination of encryption requisites, scopes, and current implementations in IoRT, this paper provides valuable insights for researchers, engineers, and policymakers involved in IoRT security efforts. By integrating encryption and blockchain technologies into IoRT systems, stakeholders can foster a secure and dependable environment, effectively manage risks, bolster user confidence, and expedite the widespread adoption of IoRT across diverse sectors. The findings of this study underscore the critical role of encryption and blockchain technology in IoRT security enhancement and highlight potential avenues for further exploration and innovation. Furthermore, this paper suggests future research areas, such as threat intelligence and analytics, security by design, multi-factor authentication, and AI for threat detection. These recommendations support ongoing innovation in securing the evolving IoRT landscape.

* Corresponding author.
E-mail addresses: 1808010@student.ruet.ac.bd (E.I. Zafir), 1808027@student.ruet.ac.bd (A. Akter), nazmulnafim@gmail.com (M.N. Islam), shahidhasib586@gmail.com (S.A. Hasib), 1808007@student.ruet.ac.bd (T. Islam), subratakumar.sarker@student.uts.edu.au (S.K. Sarker), sm.muyeen@qu.edu.qa (S.M. Muyeen).

https://doi.org/10.1016/j.iot.2024.101357
Received 30 April 2024; Received in revised form 9 August 2024; Accepted 30 August 2024
Available online 2 September 2024

1. Introduction

1.1. Background studies

The rapid growth of technology has created a connected world where different systems and devices are readily integrated into every aspect of our lives. The Internet of Robotic Things (IoRT) connects robots and autonomous devices to the Internet so they may communicate, collaborate on data, and carry out tasks more effectively [1]. IoRT has the potential to completely transform a variety of industries, including manufacturing, healthcare, and transportation [2]. However, security issues can lead to the failure of IoRT systems, making them vulnerable, which is true for any internet-connected device. To guarantee the secure and reliable functioning of interconnected robotic systems, the security of IoRT infrastructure must be fortified [3]. Despite the numerous advantages IoRT offers, special attention is required regarding the security measures to safeguard sensitive data from malicious attacks [3]. Fig. 2 illustrates the conceptual model of IoRT with a high-level overview of the key components and functionalities within an IoRT system. It highlights the interconnectedness of smart devices, sensors, robots, and cloud services.

The security of the IoRT is crucially reliant on encryption, and it is a vital layer of defense against unauthorized access and data breaches as IoRT systems become more linked and exchange sensitive data [4]. IoRT encompasses a network of interconnected robotic devices capable of communicating and sharing data with external systems. Security concerns emerge from the potential for malicious actors to intercept or manipulate the data exchanged among these devices, particularly given their proximity [5]. Encryption mitigates these threats while preserving the integrity of data within IoRT systems by transforming data into ciphertext, rendering it incomprehensible without the corresponding decryption keys [6].

Encryption is a vital safeguard against unlawful penetration, interception, and tampering by converting data into ciphertext, rendering it incomprehensible without the corresponding decryption key [6]. Beyond confidentiality, encryption algorithms also verify the authenticity of data to ensure it remains unaltered during transmission. Message authentication codes (MAC) or digital signatures are employed to authenticate the data. This protects against unauthorized access and safeguards the overall functionality and security of IoRT devices by preventing unauthorized users from tampering with critical instructions or altering sensor data. [5]. The encryption process involves applying mathematical operations to plaintext using an encryption algorithm managed by an encryption key.

Decryption, requiring the associated decryption key, reverses the transformation, restoring the ciphertext to plaintext [7]. Asymmetric encryption utilizes a key pair, while symmetric encryption employs the same key for both encryption and decryption [8]. Widely recognized encryption algorithms, such as DES (Data Encryption Standard) [9], RSA (Rivest Shamir Adleman) [10], SHA (Secure Hash Algorithm) [11], AES (Advanced Encryption Standard) [12], Diffie–Hellman [13] and so on.

Blockchain technology, a digital ledger system, ensures data security, transparency, and immutability within a network of users. This system enhances security by employing various processes [14]. Initially, network users validate transactions or data and incorporate them into blocks through consensus mechanisms like proof of work or proof of stake [15]. Each block is cryptographically linked to the preceding one, forming an immutable chain. Encryption methods, such as elliptic curve cryptography, ensure data security and provide cryptographic signatures to authenticate transactions [15].

To maintain data integrity, blockchain security algorithms utilize robust cryptographic hash functions like SHA-256 or Keccak-256 [16]. The decentralized nature of blockchain and consensus protocols protects the network against hacking and unauthorized alterations. Additional security measures include access controls, safeguarding private keys, and conducting smart contract audits [17]. Continuous security audits and updates are essential to address emerging risks and uphold a secure blockchain ecosystem, complementing efforts to fortify IoRT security [18].

The integration of blockchain technology into the IoRT holds the potential to significantly enhance security measures [19]. Blockchain ensures data integrity, decentralizes trust, and facilitates secure communication, aligning with the security objectives of IoRT systems. The tamper-proof and immutable nature of blockchain safeguards the integrity of data transmitted between IoRT devices [20]. This characteristic also deters unwanted tampering and ensures the accuracy of information exchanged, reinforcing the security of IoRT networks. Additionally, blockchain's decentralized architecture mitigates single points of failure, enhancing the resilience of IoRT systems against malicious attacks [21]. Furthermore, blockchain's cryptographic protocols enable the establishment of secure communication channels, ensuring the confidentiality and authenticity of messages exchanged among robotic devices [22]. By integrating blockchain technology, IoRT systems can establish a robust security framework, reducing vulnerabilities and bolstering the overall security posture of networked robotic systems [22].

1.2. Motivations

The IoRT represents a contemporary research frontier, integrating robots and various devices to collaborate and communicate with each other. With the growing volume of data exchanged among these devices, ensuring the security and privacy of this data becomes paramount. Encryption emerges as a vital tool for addressing this need. Through encryption, data transforms, rendering it unreadable to anyone lacking the decryption key. This mechanism ensures that only authorized parties can access the data as it traverses between IoRT devices, shielding it from potential threats such as hackers.

A primary concern in IoRT is safeguarding users' data, encompassing financial details, health records, transaction histories, media files, and personal contacts. Such information can become a vulnerable target if accessed by malicious entities. Given that IoRT comprises interconnected devices, a security breach in a single device could compromise the entire network. Consequently, securing vital information necessitates measures such as encrypting user authentication and fortifying database security.

To safeguard data exchanged among IoRT devices against unauthorized access, encryption stands out as a robust security solution. By encrypting the data, it becomes indecipherable to anyone lacking the decryption key. This means that even if an intruder gains access to the data, they would be unable to make sense of it. Encryption thus serves as a critical component of IoRT's security framework, ensuring that sensitive data remains protected from online threats.

1.3. Research objectives

The research objectives of this work includes:

- To review and analyze the current architectural frameworks for IoRT security.
- To analyze the effectiveness of cryptographic and encryption techniques in enhancing IoRT security.
- To assess the potential application of blockchain technology in IoRT.
- To identify gaps in existing research and propose future research directions for IoRT security.

1.4. Literature review

As encryption is a vital way to provide security to an IoRT system, it is used to perform secure communication between interconnected devices as a result imposter cannot obtain data from the network. It is possible to guarantee that data is delivered safely and cannot be intercepted by unauthorized parties in the IoRT by encrypting the communication links between robots and other devices as seen in [23]. The paper also stresses the key of the legal framework and technical standards as the significant factors that regulate production and utilization of robots, as well as stress that these parameters are necessary to guarantee the safety and security of robots used in the sphere of care. Although the paper promotes the enhancement of linking cybersecurity and safety in care robots, the today's issue of the lack of the sufficient reference guidelines and strategies for stakeholders might not be supplemented with the clear and effective tactics and recommendations.

In healthcare applications such as [34], where private patient data is handled, IoRT devices are being employed more and more. This data can be shielded from online dangers and kept private with the use of encryption. As the distinctive aspect of the study, the paper presents a GDPR compliance auditing procedure and underlines the relevance of the issue of data protection. The paper focuses on GDPR, which is a basic obligation regarding data protection, nevertheless, there may be differences in data protection laws across the districts and compliance standards, so the results might be different in some certain area.

Moreover, as discussed in [35], it can be seen that robots and other equipment need control signals in industrial automation applications to carry out specified duties. To prevent eavesdropping on these control signals and guarantee that the devices only take orders from authorized people, encryption can be utilized. Several uses of encryption in IoRT can be seen over time. Consequently, the paper's results may carry implications for boosting the functionality and definitive credibility of ATM software based upon comprehension originating from wireless sensor networks. This does not consider the proposed algorithm's ability to operate or be modified in a constantly changing network environment which could be a drawback for real life usage. The authors in [36], presented a secure communication protocol for the IoRT that uses encryption to safeguard data transmitted between devices. The system was tested in a simulated environment, confirming its effectiveness in securing the IoRT. The proposal of a workable and efficient method for safeguarding data transmissions between devices makes the paper a significant contribution to the field of IoRT security. The categorization of sensors and actions implemented in IoT-based robots provides recommendations that can be useful to scholars and practitioners providing modifications to the robotic system's sensory and interactive components. It can be used to optimize robots for various situations and roles in various settings and applicational contexts. Surprisingly, there are no special focus on security issues concerning software, messages to be transported and data in most of the surveyed papers. While some papers referred to the usage of secure methods of exchanging messages like the HTTPS, the concept of security was not majorly well-covered. Furthermore, [37] offers a thorough analysis of security concerns related to IoRT, including the usage of encryption as a means of safeguarding data. The authors discuss the suitability of various encryption methods for protecting data sent between IoRT devices and various encryption methods. This paper offers a useful overview of IoRT security as it stands now and suggests areas in which additional study is required to strengthen security measures.

Vermesan, Ovidiu, et al. [38], provided a novel strategy for securing the IoRT by fusing blockchain technology with encryption methods. The authors offer a secure framework that makes use of these technologies' security properties to build a strong security system for the IoRT. The usefulness of their suggested framework is demonstrated in the study by using it in a simulated setting. By merging cutting-edge technologies, this novel solution to IoRT security overcomes the difficulties of protecting a densely interconnected network of robotic devices. Blockchain is also familiar with providing security in the IoRT system. In [18], a secure data-sharing system for the IoRT is proposed. This system makes use of blockchain technology to guarantee the integrity and privacy of data exchanges. The solution uses distributed ledger technology from the blockchain to produce an unchangeable record of data transfers, creating a transparent and reliable environment for data sharing amongst robotic equipment. One of the major issues in the IoRT is addressed by the authors' strategy, which highlights the significance of maintaining data integrity and authenticity. Andronie, Mihai, et al. [27], suggested a blockchain based data exchange mechanism for the IoRT that is safe and scalable. The authors build a secure environment for data sharing between robotic devices using blockchain, while simultaneously ensuring scalability and effective resource use. Blockchain is decentralized and transparent. The suggested approach incorporates elements of blockchain technology to overcome the difficulties associated with effective and safe data sharing in the IoRT.

A blockchain-based architecture for the IoRT is introduced in Ref. [39], creating a safe and scalable platform for data sharing amongst robotic devices. The suggested architecture uses cryptographic protocols and the distributed consensus mechanism of the

Table 1
Different reviews work on IoRT security and their main focuses.

References	Year	Main focus	Algorithm	Limitation
Ref. [24]	2024	This manuscript delves into the utilization of the IoRT to support independent living, particularly within the healthcare sector. It focuses specifically on enhancing autonomy, security, and independence for the elderly and individuals with disabilities (PLWD).	PLWD	Application only in specific field
Ref. [25]	2023	This paper aims to outline the design methodology for a control framework tailored to secure robotic systems and facilitate IoT-Enabled Robotic Communication.	Communication protocol	Mainly work in communication security
Ref. [26]	2023	This article provides a comprehensive analysis of modern approaches to integrating IoT (Internet of Things) and BCT (Blockchain Technology).	BCT	Focused on IoT data sharing
Ref. [27]	2023	This systematic review aimed to investigate IoRT and align its findings with regard to remote large data management tools.	Mapping	Mainly for big data
Ref. [22]	2023	The aim of this systematic review was to assess IoRT and integrate the concepts it presents regarding big data management methodologies.	ML	Only for big data
Ref. [28]	2022	The primary objective of this paper is to comprehend the data exchange process within an IoRT system using standard communication protocols.	Communication protocol	Mainly work in communication security
Ref. [5]	2022	This study reviews the associated approaches, architectures, and capabilities of IoRT.	Architecture	Only discuss on architecture
Ref. [29]	2021	This study examines how the integration of robotic and IoT technologies may enhance the capabilities of both technologies.	Connectivity protocol	Less importance on data security
Ref. [30]	2021	This article delves into the fundamentals of designing multi-role robotic systems for IoRT and explores their application in execution.	Framework evaluation	Focuses solely on definition
Ref. [31]	2021	This study provides an overview of Internet-based robotic solutions aimed at addressing design issues within the IoRT framework.	Architecture security	Mainly focuses on framework
Ref. [32]	2021	This paper conducts a comprehensive evaluation focusing on the imminent security aspects of IoT, including risk assessment for the existing IoT system.	Risk assessment	Mainly focused on identifying the risk
Ref. [33]	2020	This publication discusses state-of-the-art IoRT applications, with a focus on highlighting their impact on various research areas.	Application	Less concerned on security
Ref. [1]	2020	This study investigates IoRT's taxonomy, emphasizing its intelligent connectivity, architectures, interoperability, and trustworthiness framework.	Taxonomy framework	No specific security for data
Current Study	2024	The study conducts an in-depth analysis of the necessity, applicability, and functions of encryption and blockchain within the realm of the IoRT. It thoroughly explores potential outcomes arising from the utilization of these technologies. Additionally, a comprehensive examination of IoRT security implementation is undertaken, with a particular emphasis on future perspectives and contributions.	Encryption & Blockchain	Limited implementation

blockchain to preserve the integrity and confidentiality of data transactions. The authors' strategy highlights the value of security and scalability in the IoRT and suggests a solution that takes advantage of blockchain technology's advantages to address these issues. Here, the research objectives are designed to get over the limitations of the centralized systems by introducing novel architecture based on Blockchain to control IoT. The research focuses on the requirement of strong security in the IoT applications to avoid cybercrimes such as intrusion and data manipulation. Thus, the paper does not disclose substantial details concerning the technical

issues or issues prospective in the resultant IIoT architecture when employing blockchain. Table 1 provides a summary of published review works in the IoRT security domain, highlighting their contributions and main focuses.

1.5. Aim and contribution

In this increasingly interconnected society, the integration of humans and technology has precipitated a significant shift towards robotics, where machines are assuming a multitude of tasks once exclusively performed by humans. However, the efficacy of robots hinges on successful human-machine interaction. To achieve genuine autonomy and long-term viability, the concept of the Internet of Robotic Things (IoRT) has emerged within the robotics domain. IoRT entails the interconnection of specialized devices, forming a network of collaborative robots that work synergistically to achieve comprehensive automation and cultivate a self-sustaining environment for robotics.

IoRT security becomes more complex and dangerous as it combines robots with IoT, providing a considerably different approach to security. While IoRT is centered around real-time decision-making and physical contacts, on the other hand, IoT entails data sharing. This leads to a higher probability of possessing safety-sensitive conditions and possibly even physical injury. Therefore, there is a necessity to incorporate the security measures against any unauthorized access and control signals' interference for IoRT systems to protect both the information and the robotic control. Introducing such complexity is the only way to address those vulnerabilities that are typical for IoRT scenarios while the more advanced security measures, such as the distributed control based on the blockchain, creation of the safe records and the use of the encryption means for safe communication are to be used.

The growing adoption of IoRT in the robotics industry underscores the critical importance of prioritizing user and system security. Given the extensive interconnection of devices and the exchange of sensitive data, robust security measures are imperative. Blockchain technology and encryption have emerged as vital tools for addressing these security challenges. Encryption is increasingly employed to safeguard the confidentiality and integrity of critical information transmitted between IoRT devices. Meanwhile, blockchain technology ensures secure storage of IoRT device data by providing a decentralized and tamper-proof ledger.

By integrating encryption and blockchain into IoRT systems, stakeholders can foster a secure and dependable environment, effectively manage risks, bolster user confidence, and expedite the widespread adoption of IoRT across diverse sectors. Collectively, these efforts contribute to a more efficient and secure future. This paper aims to delve deeper into these themes:

- **Examine the requisites of encryption in IoRT** This study delves into the necessity of employing encryption within IoRT systems to establish a secure technological environment. It thoroughly analyzes the primary security needs driving the utilization of encryption in IoRT, providing a comprehensive perspective on the subject.
- **Exploring scopes of encryption in IoRT** The study introduces research aspects concerning IoRT security, offering valuable insights that can guide future research endeavors in gathering essential information for similar studies. By exploring the potential scopes of encryption within IoRT, this research lays the groundwork for further investigations in this emerging field.
- **Comprehensive analysis of current implementations of IoRT security** Recent implementations of IoRT security measures are meticulously reviewed in this study to extract insights and identify potential use case scenarios. This comprehensive analysis aims to provide valuable output and insights that can pave the way for further exploration and advancements in IoRT security protocols.
- **Recommending future aspects and complications** The study's findings are thoroughly analyzed to extract actionable data that can inform future studies and ensure the continuous progress of research in this field. By synthesizing the identified aspects and challenges, the study underscores the significance of ongoing research and highlights potential avenues for further exploration and innovation.

IoRT necessitates a specific approach of providing security instead of conventional IoT security to perform better in real-time environment. Thus the study focused more on the security techniques specific to IoRT.

This manuscript is valuable for both the engineering and research communities, as it presents a comprehensive investigation into the importance of security enhancement in the IoRT. In the emergence of an interconnected world, the integration of robots into various domains presents unique challenges for ensuring data privacy and system integrity. Addressing these challenges, the study not only provides essential insights for researchers, engineers, and policymakers to comprehend the complexities of IoRT security but also offers practical recommendations for enhancing security measures. By providing comprehensive insights and guidance, this study aims to assist academia, industry practitioners, and policymakers involved in IoRT security efforts. It provides a thorough evaluation of encryption approaches, practices, and recommendations within the realm of IoRT security enhancement, thus contributing to the advancement of knowledge and practice in this emerging field.

Moving on, the rest of the paper is organized based on a process shown in Fig. 1.

1.6. Organization

The rest of the manuscript is organized as follows. In Section 2, various aspects of IoRT privacy and security have been given, which begins with an exploration of the framework, requisites, and scopes of security in IoRT. Section 3 explores encryption methods, possibilities, algorithms, and opportunities for securing IoRT systems. The manuscript examines the role of blockchain technology in enhancing security within IoRT systems in Section 4. In Section 5, current trends and challenges in IoRT security and privacy are discussed, including cryptanalytic assessments, network security, firewall and software security, authentication and access control, malfunction security, and database security. Finally, in Section 6, the manuscript concludes with future recommendations for enhancing security in IoRT systems.

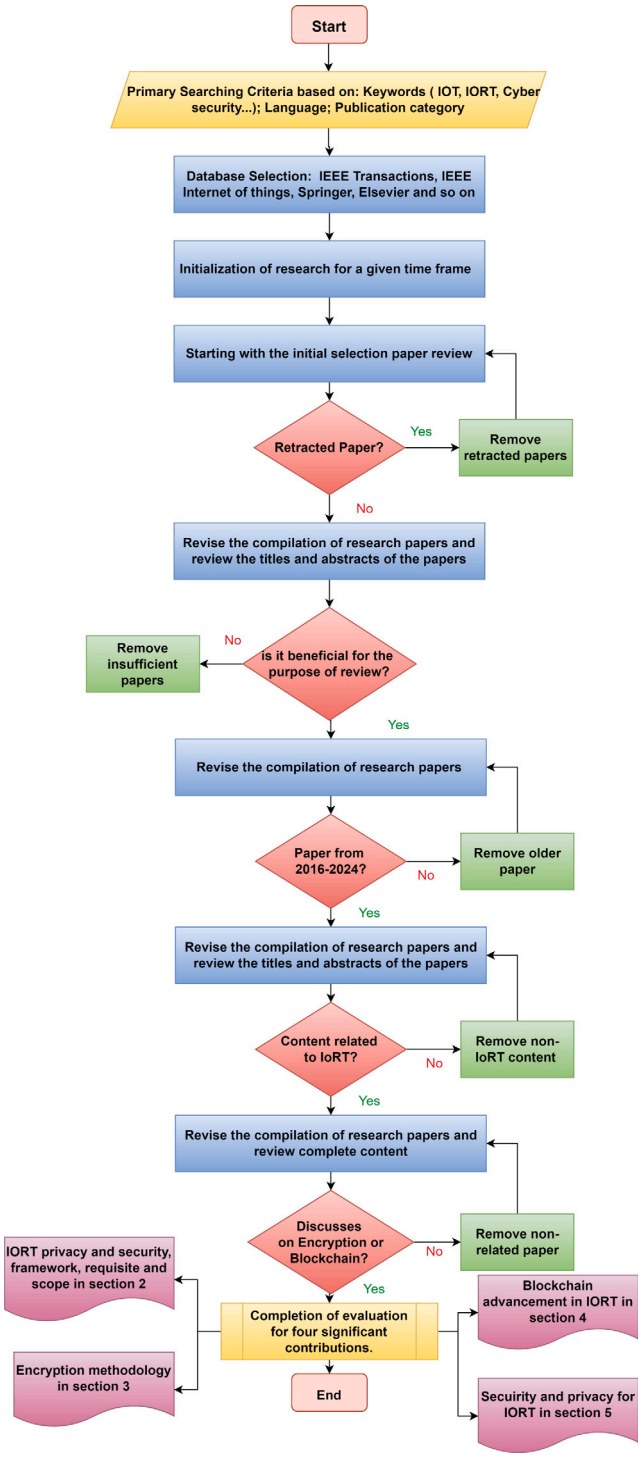


Fig. 1. Literature analysis framework for IoRT.

2. IORT privacy/security: Framework, requisites, and scopes

A cutting-edge technology called the Internet of Robotic Things (IoRT) combines IOT with robotics to enable more autonomous robotics, as shown in Fig. 2. Shortly, it will perform many common manual labor duties. Executing automated work tasks in this highly automated society is crucial when fewer individuals are engaged in operational duties. In the modern day, where machines

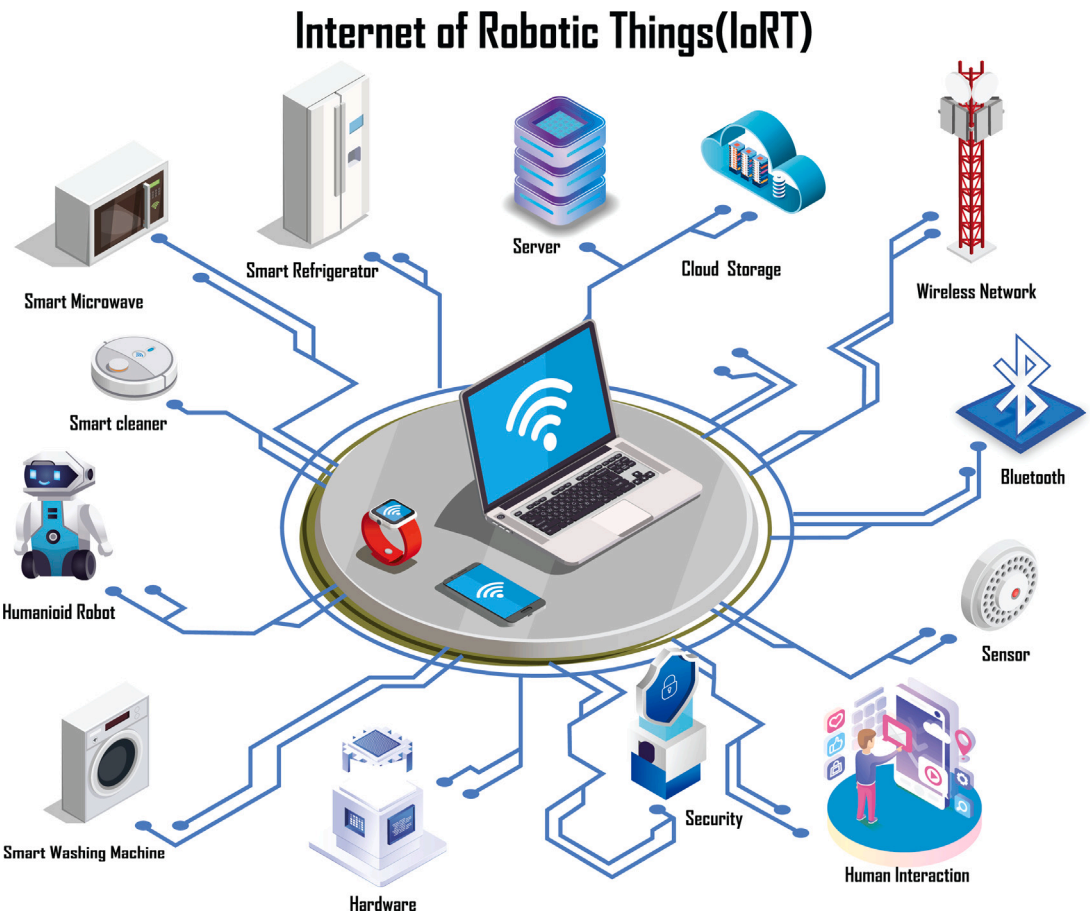


Fig. 2. Internet of Robotic Things(IoRT), The diagram illustrates a conceptual model of the IoRT, a network that integrates robotic devices, sensors, and actuators with cloud computing and internet connectivity.

perform tasks that humans have done for ages, robotics is the most useful area of engineering. Robots are machines that use several mechanical or electrical processes to carry out certain tasks. Real-world items are connected through the IOT process. To control integrated operation synchronization between the system's devices, a global or local network has been employed. The two cutting-edge technologies used in this industrial revolution are combined to form IoRT [3].

The architecture of IORT can be described in various ways. The architectures can be displayed as:

- Network-based authentication Architectures or Operational Architectures
- Layer-based Architectures
  - 3 Layer-based Architecture.
  - 5 Layer-based Architecture.

2.1. IORT framework

2.1.1. Network-based authentication architecture/ operational architecture

IoT devices, including gateways, cloud servers, and network infrastructure, form the backbone of safe and dependable communication in IoRT systems. Network-based authentication is pivotal in ensuring secure access management. Cloud servers centrally manage IoT device data, employing robust authentication procedures. Digital credentials validate users, enhancing security. The architecture, comprising sensing, communication, cloud, management, and service layers, ensures comprehensive functionality. Fig. 3(b), represents the IoRT network-based architecture highlighting the key functional layers and their interactions. It emphasizes the layered approach where data sensing, communication, service provisioning, management, and cloud integration coexist to facilitate network operation and service delivery.

The sensing layer collects data from diverse sensors, while the communication layer safeguards communication among components using encryption and digital certificates. The cloud layer manages and analyzes data, employing strong authentication

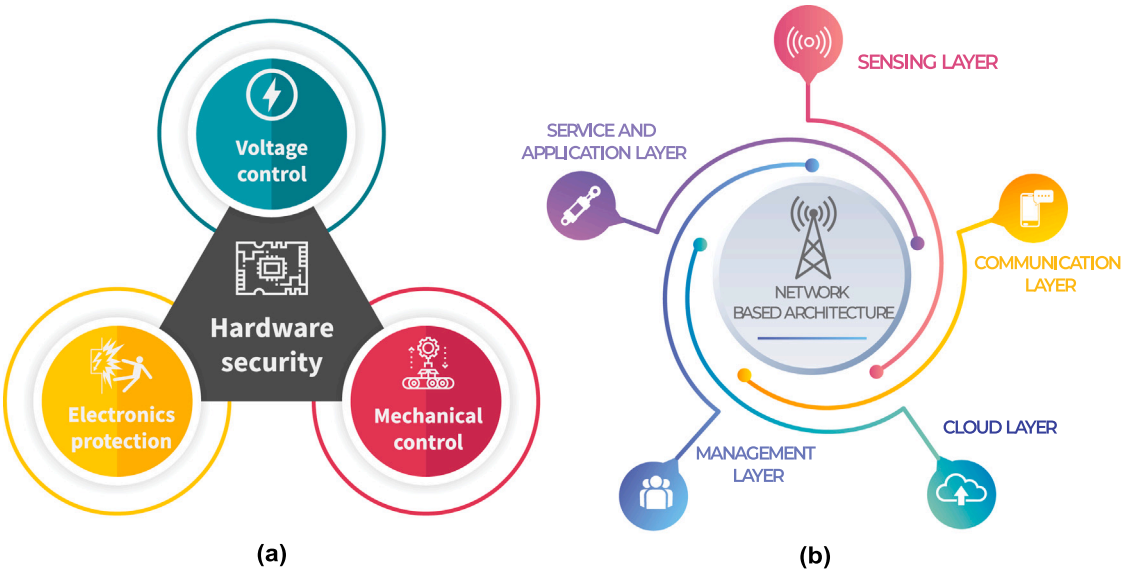


Fig. 3. (a) A simplified model of hardware security, the multifaceted nature of hardware security, encompassing various techniques to protect against electrical issues, environmental threats, and mechanical issues, (b) The core functional components within a network-based architecture for IoRT.

and encryption. The management layer oversees network upkeep, security, and compliance, ensuring effective system operation. The services and application layer facilitates user interaction, offering features like control, visualization, and encryption, enabling seamless integration with other systems. This network-based authentication architecture establishes a secure, efficient IoRT ecosystem, preserving data integrity and user privacy [40]. Table 2 given an illustration of different IoRT frameworks. It gives a comparison among different IoRT architectures.

2.1.2. Layer-based architectures

Layer-based Each operating sector for IORT has processing layers due to the layer-based design. This offers detailed information about each component of the system. It controls the operation split into specific individual tasks, assisting the project in allocating responsibility to engineers. Two traits can be divided out of this. First is the three-layer architecture used to conduct consumer-grade IoRT; the other one is the five-layer architecture used mainly by researchers across the field [41].

3-layer based Architectures: The three-layer architecture of the Internet of Robotic Things (IoRT) provides a foundational framework for understanding system components and operations, enabling efficient development and deployment. The perception layer, the first tier, gathers data from various sensors and conducts preliminary analysis, crucial for informed decision-making and system responsiveness to environmental changes. The network layer facilitates secure communication among system components, employing protocols and technologies to ensure efficient data transmission and confidentiality. Finally, the application layer, the uppermost tier, grants users access to IoRT system features through intuitive interfaces, enabling data analysis and informed decision-making. Together, these layers form a cohesive structure essential for the effective functioning and acceptance of IoRT systems [41].

5-layer based Architectures: While the three-layer design captures the essence of IoRT, its complexity demands further exploration, leading to the development of the five-layer architecture. In this model, the perception and application layers retain their roles, while additional tiers address nuanced aspects of IoRT functionality. The Transport Layer ensures efficient, secure communication among system components across various networks, employing protocols like IP and TCP, along with security measures like SSL and TLS. Routers and gateways enhance integration and provide essential security features. The Middleware Layer acts as a communication bridge between service and network layers, facilitating data sharing, protocol management, and algorithm implementation, ensuring system scalability and reliability. Lastly, the Business Layer offers end users services and applications based on data from lower layers, enabling diverse use cases and integrating third-party services, all while maintaining data security and confidentiality through encryption and authentication procedures. Together, these layers form a comprehensive framework essential for the effective functioning and utilization of IoRT systems [41].

2.2. Requisite for IORT security

The Internet of Robotic Things' (IoRT) security is essential for consumers' protection and privacy and the efficient running of the systems consumers' protection and privacy as well as the efficient running of the systems, the Internet of Robotic Things' (IoRT) security is essential. Some essential requisites for IoRT security include the ones listed below:

Table 2
A comparison among different IoRT frameworks. The distinct functionalities performed at each layer, facilitate data collection, processing, analysis, and service delivery in an IoRT environment.

Reference	Type of architecture	Layer	Feature	Application
[3]	Network-based authentication architecture/ Operational Architecture	Sensing layer	Real-time monitoring of connected objects' physical conditions.	Cameras, Sensors for temperature, Sensors for motion, and GPS units.
		Communication layer	Interacting with other layers.	IoRT devices, Gateways, Cloud servers, and Network infrastructure.
		Cloud layer	Data storage, processing, and analysis.	Cloud computing.
		Management layer	Operating and monitoring other layers.	Cloud management tools.
		Services and application layer	Data collection, data analysis, data visualization, and security.	Applications for mobile devices, Web interface.
[40]	Three layers	Perception layer	Responsible for collecting data from various sensors and devices.	IoRT gadgets, sensors, and actuators.
		Network layer	Connect other intelligent devices, network devices, and Servers.	Satellite, Cellular, and Wi-Fi networks.
		Application layer	Delivering a specific application service to the user.	Smart homes, Smart cities, Intelligent health.
[40]	Five layers	Perception layer	Responsible for collecting data from various sensors and devices.	IoRT gadgets, sensors, and actuators.
		Transport layer	Transfers sensor data.	Bluetooth, Wireless, 3G, LAN (Local area network), NFC, RFID.
		Middleware layer	Store, analyze, and process large quantities of transportation data	Databases, Cloud computing, big data processing modules.
		Application layer	Delivering a specific application service to the user.	Smart homes, Smart cities, Intelligent health.
		Business layer	In charge of managing IoRT system.	Business applications, Business models, User Privacy

2.2.1. Device identification

Ensuring IoRT security hinges on robust device identification protocols. To restrict network access solely to authorized devices, confirming the identity of gadgets seeking entry is imperative. Authentication methods may vary, relying on factors like biometrics, MAC addresses, or digital certificates. Employing cryptographic techniques such as public key infrastructure (PKI) or digital signatures emerges as a popular approach for device authentication, providing a secure means to verify devices and prevent unauthorized access. Effective device identification also serves as a deterrent against threats like device spoofing and man-in-the-middle attacks. Overall, device authentication plays a pivotal role in safeguarding the security and integrity of the IoRT ecosystem [42].

2.2.2. Data encryption and secure communication

IoRT security relies heavily on data encryption and secure communication, as they ensure the confidentiality, integrity, and authenticity of information exchanged between devices, safeguarding it from unauthorized access or tampering. By encoding plaintext using encryption methods and secret keys, data becomes unreadable to unauthorized parties lacking the decryption key. Essential to IoRT systems are encryption protocols like Transport Layer Security (TLS) or Secure Sockets Layer (SSL), which authenticate and encrypt data during transmission, ensuring end-to-end security. To safeguard encryption keys from misuse or

disclosure, robust key management systems are imperative in IoRT systems. This involves securely generating, distributing, and managing keys, as well as promptly revoking and replacing compromised keys. Real-time encryption must be executed seamlessly without compromising system performance. This necessitates hardware or software enhancements to facilitate high-speed encryption and decryption processes. Furthermore, IoRT data encryption strategies must consider secure storage and retrieval methods to ensure data remains protected even during periods of inactivity.

For secure communication, encryption algorithms such as Elliptic Curve Cryptography (ECC) and RSA can be used to safeguard the connection. These algorithms guarantee the confidentiality and security of the transmitted data. Additionally, encrypted messaging methods like MQTT-SN or CoAP can be used to establish secure communication in IoRT. Even in contexts with limited resources, these protocols' use of lightweight message techniques ensures safe and reliable communication. In general, secure communication is essential to guaranteeing the dependability and security of IoRT applications [43] By implementing reliable encryption and secure communication mechanisms, data remains inaccessible to unauthorized parties, bolstering the overall security of the IoRT system. These measures serve as cornerstones in IoRT systems, guaranteeing the security of transmitted and stored data and establishing a foundation for a trustworthy and resilient IoRT ecosystem [44].

2.2.3. Access management

Access management is a crucial part of IoRT security since it makes sure that only authorized people and devices have access to sensitive information and can manage essential functions. Based on variables including user identification, device belongings, network location, and time of access, access control methods employ a variety of techniques to restrict access. The physical device, network, and application layers of the IoRT architecture are only a few of the levels where access control can be applied. A common technique for access control is role-based access control (RBAC), which provides users with unique roles and privileges based on their job duties and access needs. Access management solutions should also offer thorough audit logs so that administrators are informed of any illegal access attempts and may track access attempts and actions. Access management that is properly established can stop malevolent actors from jeopardizing the protection of an IoRT system [3].

2.2.4. Hardware security

A key requirement for guaranteeing the security of IoRT devices is hardware security, which is illustrated in Fig. 3(a). The figure highlights the multifaceted nature of hardware security, encompassing various techniques to protect against electrical issues, environmental threats, and physical intrusion. Defending the device against physical and manipulation threats entails incorporating hardware-level security features. To store and process sensitive data safely, secure hardware uses trusted platform modules (TPMs), secure regions, and hardware security modules (HSMs). These controls make sure that only permitted parties can access the gadget and the data it handles. Voltage control, electronic protection, and mechanical protection are further hardware security methods that stop hackers and other bad actors from accessing and tampering with the hardware. Implementing hardware-based authentication methods like USB tokens, smart cards, or biometric authentication to authenticate people and devices is another aspect of secure hardware. As a result, the equipment and its services are protected from unauthorized access. In addition to ensuring the privacy, reliability, and accessibility of any information they handle, IoRT devices can offer a strong defense against physical and manipulation assaults by adopting secure hardware [45].

2.2.5. Software security

The protection of the IoRT depends on software security. Fig. 4 highlights the unique software security challenges in IoRT due to resource limitations, device heterogeneity, and the potential for physical attacks. It emphasizes the need for robust security solutions tailored to the specific constraints of IoRT systems. It entails putting security mechanisms in place across the entire life cycle of software development to make sure that security is considered during software design, development, testing, and deployment. This covers methods including vulnerability assessments, penetration testing, and code reviews. Access restrictions and encryption are also used in security software to safeguard data and thwart illegal access. Software should be updated and patched often to fix known security flaws. Furthermore, employing secure coding standards and programming languages helps lessen security threats. As a whole, it is essential to have security software to guarantee the availability, confidentiality, and integrity of data in the IoRT [45].

2.2.6. Disaster recovery and incident response

Disaster recovery and incident response are essential elements of IoRT security. A strategy must be in place to deal with any potential security incidents. Processes for identifying and reacting to security breaches, determining the incident's primary cause, and putting corrective measures in place to avoid recurrences should all be part of the incident response plan. Disaster recovery is particularly essential since it requires preparing for and rebounding from unforeseen occurrences that could harm the IoRT system, such as cyberattacks and natural disasters. A disaster recovery strategy should contain instructions on how to quickly resume normal operations after an incident while restoring data, hardware, and software. To guarantee their success in a real-world scenario, response to incidents and recovery strategies must be tested and updated often [46].

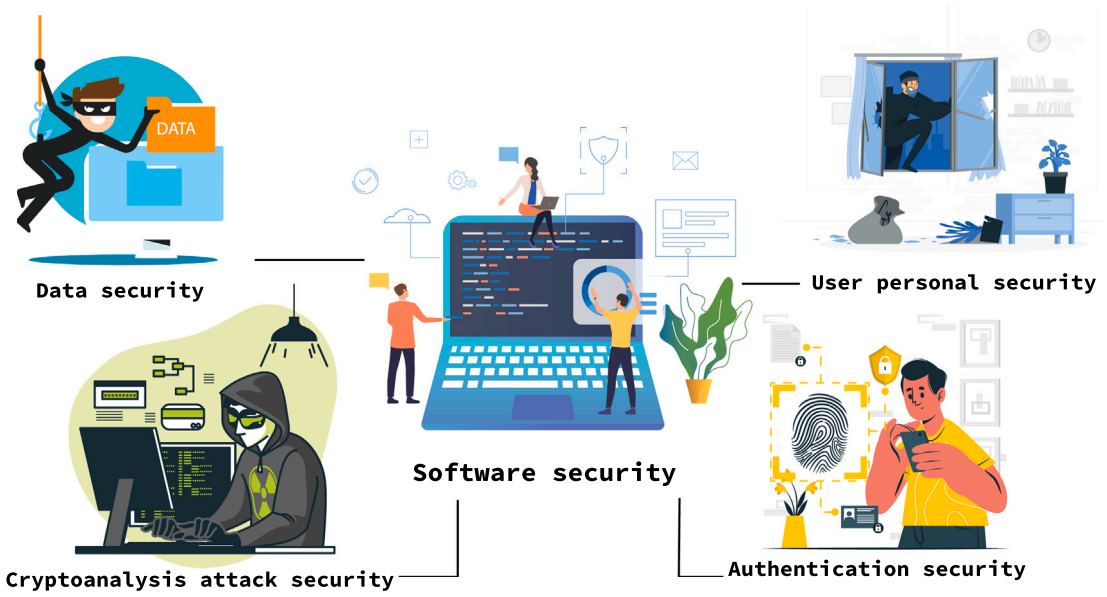


Fig. 4. Software Security Challenges in the IoRT, IoRT integrates robotic devices, sensors, and actuators with internet connectivity and cloud computing, creating a complex system with unique security vulnerabilities.

2.2.7. Execution and regulations

The security of IoRT systems is critically dependent on execution and regulations. Organizations must abide by the regulations and standards established by various regulatory agencies and standards bodies to ensure the privacy and security associated with their IoRT systems. In particular, the General Data Protection Regulation (GDPR) requires businesses to safeguard customers' personal information confidentiality. The National Institute of Standards and Technology (NIST) has also released recommendations for protecting IoT systems and devices, such as IoRT. Organizations may guarantee they comply with best practices and reduce the risk of breaches of information and other security-related events by adhering to such standards and guidelines. Corporations can demonstrate their dedication to security as well as responsibility by following execution and regulatory regulations, which helps to foster confidence with customers, collaborators, and other stakeholders [47].

2.2.8. Risk control

To guarantee the security of the IoRT, risk control is an essential aspect. It entails the discovery, evaluation, and prioritization of potential hazards to the integrity of IoRT systems, as well as the creation of plans to reduce or remove those dangers. In IoRT, risk management entails determining the dangers present at each tier of the architecture, including the perception, network, and application levels, and taking the necessary precautions to lessen those dangers. This entails performing routine risk assessments, putting security controls in place, and checking in on their efficiency. To preserve the safety, integrity, and accessibility of information and infrastructure in IoRT and to ensure that the potential advantages of IoRT become apparent while limiting risks, efficient risk control is essential [48].

2.2.9. Continuous surveillance and analysis procedure

An IoRT system's continuous surveillance and analysis procedure must be ensured by constant monitoring and assessment. This entails regularly monitoring the system's performance, spotting any risks or weaknesses, and putting in place the necessary measures to reduce the risk. To guarantee that the infrastructure remains compatible with security rules and regulations, evaluations should be carried out regularly. To identify any aberrant or suspicious activity, continuous monitoring involves gathering and evaluating security-related data from numerous sources, including networking logs, system records, and security alerts. This data can be monitored and analyzed by automated technologies, which can assist in identifying and stopping safety incidents before they happen. To ensure that they continue to be efficient and follow industry requirements and standards, this evaluation entails assessing the safety measures, procedures, and controls for the IoRT system regularly. This entails routinely checking the effectiveness of the system's safety controls, such as firewall and intrusion detection systems. To be adaptable and open to alterations in the IoRT's surroundings, such as the introduction of new hardware or software, a continuous surveillance and analysis procedure should be created. To provide prompt and efficient responses to any security issues, it ought to be coupled with incident handling and disaster recovery plans [49].

Overall, IoRT deployment demands a thorough understanding of these prerequisites and their efficient integration to build a secure and functional IoRT system.

2.3. Security scopes for IORT

As IORT is a combination of various electronic devices, it can pose several security hazards. Security hazards can be divided into various sectors [6]. The sectors can be:

2.3.1. Hardware security

i. Voltage control: A key component of hardware security in the IoRT is voltage control. It entails controlling the hardware components' voltage levels to make sure they run within safe parameters and do not become exposed to various types of attacks. Voltage malfunctioning and voltage failure injection are two attack methods that take advantage of voltage flaws to induce system failures, get over security measures, or steal private information. Hardware safety precautions must be put in place to reduce the hazards brought on by voltage attacks [50]. The utilization of sophisticated voltage regulatory bodies, capacitors that store energy, and other hardware elements that defend against voltage-based attacks are a few examples of these. Furthermore, voltage tracking and evaluation techniques can be applied to detect anomalous voltage behavior and perform corrective steps. It also serves to prevent voltage-based attacks from leveraging hardware flaws and jeopardizing the protection of IoRT systems. In the end, good voltage regulation is critical for guaranteeing the security and stability of hardware elements in IoRT systems, particularly as these structures become increasingly sophisticated and interconnected [51].

ii. Electronics Protection: Hardware security in the IoRT also needs to consider electronics protection. It entails putting protective measures in place to shield electronic components from many types of assaults, including power surges, EMI, and electrostatic discharge (ESD). By interfering with electronic components with electromagnetic waves, attackers can take advantage of EMI vulnerabilities to bring about system crashes or data damage. Attacks using electrostatic discharge (ESD) have the potential to break or destroy delicate electronic components [52]. Hardware safety precautions must be put in place to guard against these dangers, including the use of EMI and ESD insulation, surge-preventing devices, and grounded systems. These steps aid in ensuring the reliable operation of electronic components and preventing damage from environmental causes. Also, choosing the right electronic components is essential for assuring hardware security. Devices must be selected based on their ability to withstand voltage swings, other types of interference, and their sensitivity to EMI and ESD. The security and dependability of the electronic parts in IoRT systems must be guaranteed, and this is where electronic protection comes into play. Strong defense measures can stop attackers from taking advantage of electronic flaws and aid in maintaining the reliability of IoRT platforms in the context of different types of attacks [53].

iii. Mechanical control: A further vital part of hardware security in the IoRT is mechanical protection. It entails defending physical elements from harm brought on by physical strain, collisions, and vibrations. Sensors, actuators, and various other mechanical components can be put under physical stress in IoRT systems, which can lead to failure or malfunction. This may lead to data loss, system outages, and security breaches. Shock absorbers, protective enclosures, and vibrating damping devices must be used as defenses against these dangers. By taking these precautions, components are protected from physical stress that could harm them and are maintained reliably. To offer mechanical protection, suitable design and installation techniques are also crucial. To avoid components getting loose or misaligned during installation, components must be built to resist the forces that will be present. All things considered, mechanical protection is crucial for guaranteeing the security and dependability of hardware parts in IoRT systems. The functionality of IoRT systems may be maintained in the face of varied stresses and impacts with the aid of effective protective measures, which can also avoid physical damage [54].

2.3.2. Software security

i. Data security: Data security is crucial in the IoRT to prevent unintentional manipulation and data leaks. A key tool for protecting IoRT networks and information is encryption, which can be used in a variety of ways to improve data security. User authentication employs encryption to confirm the identity of devices and guarantees that only authorized devices can access the system, while communication encryption encrypts data exchanged between devices connected to the internet and cloud-based servers to prevent unauthorized interception. When data is kept on connected gadgets or cloud servers, it is encrypted to prevent unwanted access in the event of theft or breach of security. The safety and confidentiality of sensitive data are further ensured by the advanced encryption technology known as homomorphic authentication, which allows arithmetic to be carried out on data that has been encrypted without decryption. IoRT systems can maintain the privacy and integrity of data by applying efficient encryption techniques, defending against probable security risks, and ensuring the safe and secure processing of information [53].

ii. User personal security: User privacy is highly valued by the IoRT, and encryption is a key tool for safeguarding private data. For example, encryption is an option that can secure user data such as login credentials and private information, as it is transferred between connected devices and cloud-based servers. To prevent sensitive information from being intercepted or viewed without authorization, this is essential. Encryption can be used to protect user privacy by securing the data generated by connected gadgets, such as surveillance cameras or voice-controlled assistants, and preventing illegal access to it. By using encryption in IoRT systems, users can have more confidence in the privacy and security of their information while lowering the risk of data loss, identity theft, and other security threats. IoRT systems must always place a heavy emphasis on user security and employ robust encryption mechanisms to ensure the confidentiality and integrity of user data [55].

iii. Cryptoanalysis attack security: Attacks on cryptoanalysis represent a serious risk to the encryption security of the IoRT. In these types of attacks, encrypted data is examined to determine the key used for encryption or to decrypt the content itself. IoRT systems should use resilient encryption techniques, such as elliptic curve cryptography (ECC) and advanced encryption standards (AES), to defend against cryptoanalysis attacks [51]. These techniques are resistant to well-known cryptoanalysis assaults.

Additionally, as weak or compromised keys might make it simpler for attackers to decode data, key management is essential to preventing cryptoanalysis attacks. To reduce this danger, machines can securely share encryption keys using key exchange protocols like Diffie–Hellman key exchange. To defend against brand-new and developing cryptoanalysis assaults, it is also crucial to make sure that encryption methods are correctly applied and kept up-to-date. IoRT systems can lower the danger of cryptoanalysis attacks and guarantee the security and confidentiality of sensitive data by employing an integrated strategy for encrypting and key management [56].

iv. Authentication security: The IoRT places a high priority on authentication security, and encryption plays a vital role in protecting authentication mechanisms. Digital signatures, utilizing asymmetric encryption to confirm the identification of devices and guarantee only devices with authorization can access the system, are some of the frequently used authentication techniques in IoRT systems. Data can be authenticated using digital signatures to ensure that it is not fiddled with during transit [57]. To prevent unauthorized access or interception, encryption can also be used to safeguard authentication information, such as passwords or communication tokens, during transfer across devices and cloud servers. To ensure the authenticity of the software and firmware operating on devices and prevent unauthorized modification or tampering, secure boot is another authentication security mechanism. Organizations can prevent unwanted access and data intrusions by deploying efficient encryption mechanisms for identification protection in IoRT systems and ensuring that only permitted users and devices can access the system [58].

3. Encryption methodology: Practices, algorithms and opportunities

3.1. Practice encryption method in IoRT

A crucial part of protecting IoRT devices and data is encryption. With the Internet of Things, there are numerous encryption options, including:

3.1.1. Symmetric encryption

The same secret key is used for both data encryption and decryption in symmetric encryption, a cryptographic technique. A series of bits known as the key is shared by the two parties engaged in communication. During encoding a message, the shared key and the plaintext are processed by an algorithm that uses symmetric encryption to create the ciphertext. The same key is utilized to undo the operation and retrieve the original plaintext to decrypt the ciphertext. Data privacy, reliability, and authentication are just a few security applications where symmetric encryption is frequently utilized. The Advanced Encryption Standard (AES), a block cipher that utilizes fixed-length plaintext blocks and a variable-length key, is one of the most well-known symmetric encryption methods. Triple DES (Data Encryption Standard) and Blowfish are two further symmetric encryption techniques. The key needs to be kept secret and shielded from unauthorized access for symmetric encryption to function securely. Symmetric encryption relies heavily on key management, and best practices call for often changing the key, employing strong keys, and safely storing the key [59].

To add more security layers, symmetric encryption can also be used in conjunction with other cryptographic tools like digital signatures and hashing. One of symmetric encryption's key benefits is how quickly and effectively it can encrypt and decrypt huge volumes of data. The fact that both parties must share the same key, which might be risky whenever the key is compromised, is a major drawback of symmetric encryption. As a result, symmetric encryption is frequently employed when the key can be securely shared between the communicating parties or when the key is only ever needed briefly. Symmetric encryption is a strong method for protecting the safety of sensitive data across a range of applications, and it is frequently employed in sectors like healthcare, finance, and government [60].

3.1.2. Asymmetric encryption

Asymmetric encryption, commonly referred to as public-key cryptography, uses two distinct keys for encryption and decoding. The drawbacks of symmetric encryption, which employs one key as the secret for decryption as well as encryption, led to the development of this strategy. Asymmetric encryption uses two keys: the public key, which is used for encryption, and the private key, which is used for decryption. While the owner keeps the private key a secret, the public key is accessible to everyone. Regardless of whether the public key gets intercepted, it is unable to be utilized to decipher the data that has been encrypted without the private key [61].

Asymmetric encryption offers an exceptionally high degree of security. This is so that the public key may only be employed for encryption and never for decryption. Because both the decryption and encryption keys are kept by different parties, asymmetric encryption is frequently used for safe communication between two parties. RSA, which is based on the challenge of factoring big prime numbers, is one of the most popular asymmetric encryption methods. Algorithms like Diffie–Hellman, ElGamal, and DSA are also frequently utilized [62]. To offer security and efficiency, asymmetric encryption is frequently used in conjunction with symmetric encryption. In this method, the symmetric key is generated using the recipient's public key after the data has been encrypted using a symmetric encryption technique. The data can then be decrypted by the recipient using their password to decrypt the symmetric key.

Asymmetric encryption is much more secure than symmetric encryption, but it also takes up more time and resources. Because of this, it is frequently used for the exchange of keys and digital signatures instead of encrypting huge volumes of data. With uses ranging from securing online transactions to safeguarding government communications, asymmetric encryption has emerged as a crucial part of contemporary cybersecurity. Blockchain technology uses asymmetric encryption as well, and it depends on cryptographic methods to safeguard transactions and thwart fraud. Researchers are continuously creating new encryption methods to stay in front of potential attacks, but as computational power continues to grow, new vulnerabilities may arise [60].

3.1.3. Transport Layer Security (TLS)

A cryptographic protocol called Transport Layer Security (TLS) is intended to offer secure network communication. Instant chat, email, web traffic, and other forms of online communication are frequently secured using it. TLS, which acts at the transport layer of the OSI model and provides end-to-end security between applications, is a replacement for SSL (Secure Sockets Layer). To protect the transmission, TLS employs both symmetric and asymmetric encryption. The symmetric session key is produced as part of the TLS handshake and is used to encrypt and decode data [63]. The client can only decrypt the session key using its private key after it has been encrypted using the server's public key and transmitted back to the server. Security, integrity, and authentication are only a few of the security characteristics offered by TLS. It secures the data transmitted between the client and server by encrypting it. Additionally, it guarantees data integrity by preventing data tampering during transmission.

Different encryption suites, which are mashups of methods used for message encryption, authentication of messages, and key exchange, are supported by TLS. The TLS connection's security and efficiency are impacted by the cipher suite selection. It is crucial to select a secure and effective encryption suite that works with the program and its users. TLS has developed over time to solve known security flaws and shortcomings in earlier versions. To make sure that the TLS implementation is utilizing the most recent security features and updates, it is crucial to keep it updated. Accessing the internet, email, and messaging services are just a few of the many uses of TLS. It is crucial for preventing unauthorized access to and interception of sensitive information, including login passwords, monetary transactions, and personal data [64].

3.1.4. Data-at-rest encryption

Data-at-rest encryption is an encryption method that encrypts data while it is being kept or at rest rather than in use or transit. Given that devices frequently store sensitive data, including passwords or private details, on local storage, this is a crucial security issue for the IoRT. If the device is physically stolen or there is a data breach, data-at-rest encryption can stop unwanted access to this information. Data-at-rest encryption techniques include file-level encryption and whole disk encryption, which encrypt the contents of the entire storage device as well as specific files [65]. To avoid unauthorized access, encryption keys ought to be carefully controlled and kept in a different location from the encrypted material. To remain ahead of potential threats, it is also critical to routinely upgrade encryption algorithms and techniques. Due to the processing costs that encryption and decryption might impose, implementing data-at-rest encryption necessitates an agreement between security and performance. As a result, it is critical to thoroughly assess the processing speed and memory capacity of IoRT devices to make sure they are capable of handling encryption without suffering significantly from performance reduction. Last but not least, it is crucial to make certain that data-at-rest encryption does not clash with other security measures like emergency recovery and backup procedures, which could require access to unencrypted data [66].

3.1.5. Homomorphic encryption

Homomorphic encryption is a form of encryption that dispenses with the need to first decrypt the ciphertext to perform calculations on it. In other words, data can continue to be encrypted while still enabling relevant actions to be carried out on it. Although homomorphic encryption is still a young field and is still in its infancy, it has enormous potential for safe data processing across a range of industries, including cloud computing, healthcare, and finance [67]. There are two varieties of homomorphic encryption: fully homomorphic encryption and partially homomorphic encryption. While completely homomorphic encryption permits both addition and multiplication to be performed on ciphertext, partially homomorphic encryption only permits one of these operations (addition or multiplication) [68].

Mathematical algorithms and a lot of computing power are used in the intricate process of homomorphic encryption. While there is research being done to make it more effective, it has not yet proven as effective as conventional encryption techniques. Homomorphic encryption's potential to protect cloud computing, in which data is preserved and analyzed on remote servers, is one of its key benefits. Homomorphic encryption's high mathematical and processing demands, which might be a bottleneck in practical applications, are one of its key drawbacks. Homomorphic encryption can also be vulnerable to assaults like chosen-ciphertext attacks and side-channel attacks, which might jeopardize the system's security. Despite these difficulties, homomorphic encryption has the power to revolutionize data security and privacy across a range of industries, particularly as the need for secured cloud computing and data processing grows. The effectiveness and safety associated with homomorphic encryption are anticipated to increase in the future as a result of ongoing research and development [69].

In general, the selection of an encryption technique will be based on the particular needs of the IoT application, such as the required level of security, the available computational resources, and the type of data being sent or stored.

3.2. Encryption algorithms

3.2.1. Data Encryption Standard (DES)

The National Institute of Standards and Technology (NIST) published the Data Encryption Standard (DES), a symmetric-key block cipher. A 64-bit block of plaintext is converted into a 64-bit block of ciphertext using the DES algorithm with a 56-bit key. A 128-bit key requires 10 rounds in the DES process, a 192-bit key requires 12, and so forth. The number of rounds is dependent on the key size. In DES, the same private key is used for both encryption and decryption, and each recipient and sender must be aware of and use the same key. In the past, DES was the preferred symmetric key technique for encrypting electronic data. DES is a block cipher that uses substitution and transposition along with a secret key to encrypt data in 64-bit blocks. The DES algorithm uses 16 rounds of encryption and has four different operating modes [70].

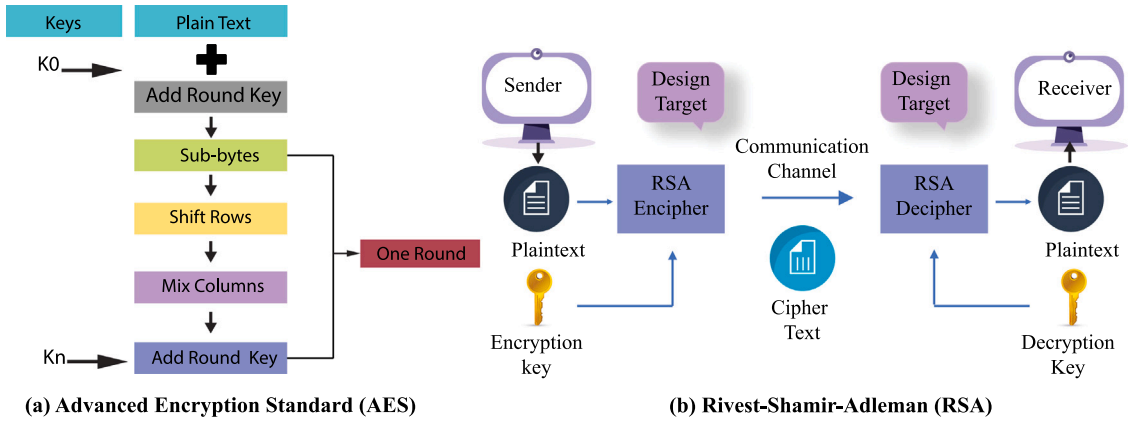


Fig. 5. (a) Advanced Encryption Standard (AES), "Add Round Key" step in AES encryption process (b) Rivest-Shamir-Adleman (RSA), Process of Sending and Receiving a Text Message with RSA Encryption.

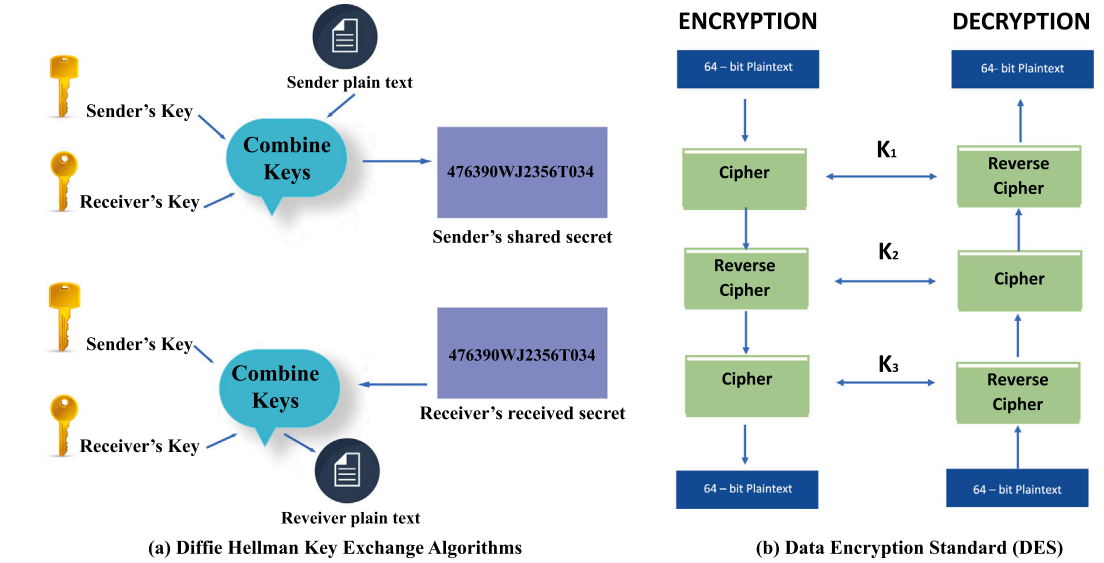


Fig. 6. (a) Diffie Hellman Key Exchange Algorithms, a method for securely establishing a shared secret key over an insecure communication channel. (b) Data Encryption Standard (DES), The process of encrypting data using the Data Encryption Standard (DES) algorithm.

DES also provides reverse interoperability and can generate random numbers. With DES, weaker encryption requirements can also be satisfied, and Triple DES, a new DES variation, is made using it. Electronic financial transfers, email encryption, and VPNs are just a few of the applications that use it extensively for confidential communication and data protection. The way DES works is to divide the data into 64-bit blocks and use an assortment of replacement and permutation operations to encrypt and decode the data throughout 16 rounds. Despite having a lengthy history of use, stronger encryption algorithms like the Advanced Encryption Standard (AES) have essentially taken the place of DES. Yet, it continues to play a significant role in the history of cryptography and is still employed in old systems where performance and compatibility are crucial [9]. This algorithm is illustrated in Fig. 6(b). The diagram illustrates the process of encrypting data using the Data Encryption Standard (DES) algorithm. It highlights the use of a shared secret key, the Feistel function as the core operation, and the permutation and substitution stages that contribute to data scrambling.

3.2.2. Advanced Encryption Standard (AES)

A symmetric-key encryption method that is frequently used to protect electronic data is called the Advanced Encryption Standard (AES). The Data Encryption Standard (DES), which had reached the end of its useful life, was replaced by AES by Belgian cryptographers Joan Daemen and Vincent Rijmen in the late 1990s. Since the U.S. government adopted the method in 2001, it has been the de facto norm for protecting sensitive data. AES is a block cipher that uses keys of 128, 192, or 256 bits to encrypt data in fixed-size blocks of 128 bits. Security is one of AES's main advantages. Researchers in the field have thoroughly examined

and tested the algorithm, and it is regarded as being quite secure [71]. AES can swiftly encrypt and decode data while using little processing power, making it quick and effective. The adaptability of AES is another asset. The technique is adaptable to a variety of hardware and software platforms and is simple to implement on both.

AES is also quite adaptable and may be used for a wide range of applications, such as secure communications, network security, and file encryption. The basis of AES is a substitution-permutation network (SPN) structure, which is made up of rounds that perform mathematical operations on the input data. SubBytes, ShiftRows, MixColumns, and AddRoundKey are the four key operations that make up an AES round. The key size, which controls the algorithm's number of rounds, is what determines the security of AES. AES-128 employs a 128-bit key and 10 rounds, whereas AES-192 and AES-256 use 192- and 256-bit keys with 12 and 14 rounds, respectively. Applications for AES include the encryption of files and emails, the security of confidential information in databases, and the protection of online transactions. Along with government and military uses, financial and banking organizations also frequently use it [12]. The process can be seen in Fig. 5(a). The figure depicts a single round of the Advanced Encryption Standard (AES) algorithm, focusing on the "Add Round Key" step. AES, where a symmetric block cipher, is utilized for both encryption and decryption of electronic data.

3.2.3. Message-Digest Algorithm 5 (MD5)

A common cryptographic hash algorithm, MD5 (Message-Digest Algorithm 5), produces hash values of 128 bits. The MD5 algorithm converts a message with a variable length into a hash with a fixed length. It is frequently employed in data integrity checks, digital signatures, and other security-related applications. As an upgrade to MD4, Ron Rivest created MD5 in 1991. The Merkle-Damgard construction, a prominent technique for creating cryptographic hash functions, is the foundation of the MD5 hash function. The input message's hash value is calculated using a string of message blocks [72].

The message is broken up into 16 32-bit words by MD5 and processed in 512-bit blocks. It has been demonstrated that MD5 has several flaws, including the capacity to induce collisions, which allows various input messages to yield an identical hash value. The use of MD5 in cryptographic tasks where conflict resistance is crucial is no longer advised because of these flaws. However, some non-cryptographic applications like checksums and fingerprinting still employ MD5. Additionally, it serves as a checksum in protocols like IPv6 and SSH to ensure the accuracy of the data. It has also been used in a few password storage systems, though this usage is no longer advised because of how simple it is to create collisions with current computational power. Furthermore, MD5 has some helpful applications, but it is crucial to use it carefully and take into account any potential security hazards before doing so. For cryptographic applications, it is typically advised to utilize more recent and secure hash algorithms like SHA-256 or SHA-3 [73].

3.2.4. Secure Hash Algorithm (SHA)

The Secure Hash Algorithm (SHA) family of cryptographic hash functions was created by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) of the United States. There are various hash functions in the SHA family, with SHA-1 and SHA-2 being the most popular. While SHA-1 generates hash values of 160 bits, SHA-2 generates hash values of 224, 256, 384, and 512 bits. A more recent member of the SHA family, SHA-3, was introduced in 2015 and is built differently than SHA-2. Since SHA is a one-way function, it is simple to calculate a hash value from a message, however, it is nearly hard to recover the actual message from the hash value [74]. As a result, SHA may be used to check the consistency of a message because even a little modification to the originating message will produce a significantly different hash value. SHA is frequently employed in many different contexts, including key elaboration, message authentication, and digital signatures. It is also frequently used to store passwords, with the original password being replaced with the password's hash value. In this manner, the actual passwords remain hidden if the database holding password hashes is breached. SHA-1 is no longer regarded as secure due to advances in computer power, and SHA-2 and SHA-3 are suggested for new uses [11].

3.2.5. Rivest-Shamir-Adleman (RSA)

The first public description of RSA (Rivest-Shamir-Adleman) was released in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman of the Massachusetts Institute of Technology. Clifford Cocks developed a public key mechanism in 1973, but the British intelligence agency GCHQ kept it a secret until 1997. Asymmetric cryptography uses the RSA algorithm. Asymmetric implies that it utilizes both the public and private keys, which are two separate keys [10]. The Public Key is distributed to all, as the name implies, while the Private Key is kept secret. The RSA key encryption system can encrypt data with either the private or public key. If the material is encrypted using the public key, it must be decrypted using the private key. Even if the data were intercepted en route, only the intended receiver may decrypt it. In this illustration, the sender uses their private key to encrypt the data before sending it as well as their public key to the recipient.

The data might be intercepted and read in transmission using this method, but the real goal of the encryption is to establish the sender's identity. Two numbers — one among which is the combination of two sizable prime numbers — are used to construct the public and private RSA keys [75]. It is very challenging to factor that number back into the original prime numbers. RSA keys typically have lengths of 1024 or 2048 bits, which makes them very challenging to factor. Internet communication, including electronic mail, internet banking, and e-commerce transactions, is frequently secured with RSA. Additionally, it is utilized for key exchange protocols, digital signatures, and secure authentication. It is simple to implement RSA encryption in a variety of applications since it is extensively supported by well-known computer languages and cryptographic libraries. With a required key length of at least 2048 bits, RSA is thought to be secure. However, if a private key is misplaced or taken, the system's security may be jeopardized. RSA is a key component of contemporary cryptography and has several uses in the field of information security [10]. The Process of RSA Encryption can be seen in Fig. 5(b). The diagram illustrates the process of sending and receiving a text message, secured with RSA encryption. RSA is an asymmetric cryptographic algorithm that uses a public key for encryption and a private key for decryption.

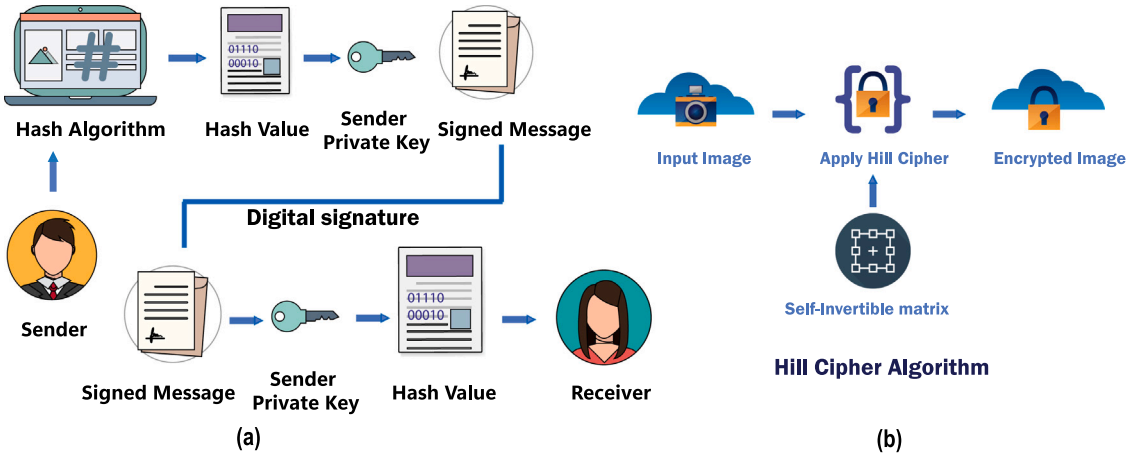


Fig. 7. (a) The process of digital signing using a public-key cryptography system. Digital signatures are used to ensure the authenticity and integrity of a message or document. (b) The process of encrypting a message using the Hill cipher, a classic polygraphic substitution cipher. The Hill cipher operates on blocks of letters, applying a mathematical matrix operation to transform the plaintext into ciphertext.

3.2.6. Diffie Hellman key exchange algorithms

Public-key cryptography is carried out via a method called elliptic curve cryptography, which is based on the algebraic structure of elliptic curves with finite fields. For the Diffie Hellman key exchange algorithms, it serves as the basis. The Diffie Hellman key exchange algorithms were created in 1976 by Whitefield Diffie and Martin Hellman to address the key agreement and exchange problem. To communicate with one another, it enables the two parties to create a symmetric key — a key that can be used for both encryption and decryption — together. Advances in Security and Privacy Protection: The Hellman key exchange algorithm can only be used for key exchange; neither encryption nor decryption is supported. The method is built on mathematical ideas [76].

A shared secret value can be agreed upon by two principals A and B over a public network using authenticated Diffie–Hellman key exchange. The so-called authenticated key exchange with "implicit authentication" is one of the protocols created to address this issue and assure that no other principals besides A can discover any data about this value. To create a secret key that is shared between two parties, Diffie–Hellman key exchange is frequently used in internet safety mechanisms including SSL, TLS, SSH, and IPsec. Additionally, it is utilized in encrypted email and Virtual Private Network (VPN) connections. Because it provides a safe transmission of information by enabling participants to reach an agreement with a secret key without disclosing it to prospective listeners, Diffie–Hellman is crucial for protecting online conversations. In addition, it is utilized in several other cryptographic tasks where both parties must create a shared secret key, including secure conversations, video conferencing, and others [13]. The steps for the Diffie–Hellman key exchange algorithm are illustrated in Fig. 6(a). The diagram illustrates the Diffie–Hellman key exchange algorithm, a method for securely establishing a shared secret key over an insecure communication channel. It highlights that even though the communication channel is insecure, both parties can establish a shared secret key that is only known to them.

3.2.7. Digital signature

A method for confirming the legitimacy and integrity of a digital document, message, or piece of data is known as digital signature encryption. It includes creating a special digital signature that can only be produced by the original sender and authenticated by the receiver using a mathematical method. The Digital Signature Standard, a standard for digital signature encryption, was released by the National Institute of Standards and Technology (NIST) in 1991. (DSS). This standard helped make digital signature encryption a commonly used technique for guaranteeing the authenticity and integrity of digital data by outlining the requirements for creating and validating digital signatures [76]. A one-way function is used to hash the message into a fixed-length value, which is then encrypted with the sender's private key to create a digital signature. The message can then be forwarded to the recipient with the resulting encrypted signature attached.

The digital signature can be decrypted and the original hash value can be obtained by the recipient using the sender's public key after they get the message. To confirm that the message was not altered and that it was sent by the stated sender, they can then recompute the hash of the received message and compare it with the decrypted hash result. Because the distinctive digital signature can only be generated by the original sender and authenticated by the receiver, digital signature encryption offers a mechanism to ensure that messages cannot be altered or falsified. Secure communication protocols like HTTPS, S/MIME, and PGP frequently employ it [77]. Fig. 7(a) illustrates the core steps involved in creating and verifying a digital signature using public-key cryptography. It highlights the importance of hash functions, private keys for signing, and public keys for verification.

3.2.8. Hill cipher algorithm

Lester Hill, an American mathematician, created the Hill cipher in 1929. The American Mathematical Monthly published Hill's article, "Cryptography in an Algebraic Alphabet", in which he described his strategy for using matrix algebra to encrypt and decrypt

messages. One of the first symmetric encryption algorithms that could be utilized for telegraph communication at the time of its creation was the Hill cipher. Hill cipher still serves as a teaching tool in cryptography classes and still finds use in low-security encryption and cryptanalysis, although high-security applications do not frequently employ it nowadays [78]. The Hill cipher works using blocks of plaintext that have a set number of letters in each one. The plaintext is initially transformed into a matrix of numbers, where each letter is given a numerical value based on its place in the alphabet (for example, A=0, B=1, C=2, and so on). A secret matrix known as the encryption key is then multiplied by the matrix, and the resulting matrix is then transformed using modular arithmetic back into ciphertext letters [78]. The size of the square matrix of numbers that makes up the Hill cipher's encryption key defines how many letters are in each block of plaintext. The recipient must be aware of the decryption key, which is the inverse of the encryption key, to decipher the ciphertext. The ciphertext matrix is multiplied by the decryption key matrix during the decryption process, and the resulting matrix is then transformed back into plaintext characters [78]. The size of the key matrix and the block size affect the security of the Hill cipher. More security is provided by larger key matrices and blocks, but the algorithm becomes more computationally difficult as a result. The Hill cipher is susceptible to known plaintext attacks, in which the key can be determined by the attacker by knowing the associated plaintext and ciphertext combinations.

Hill cipher is still employed as a teaching tool today to demonstrate the concepts of symmetric encryption and linear algebra, despite its flaws. Moreover, it is occasionally a part of more sophisticated encryption techniques [79]. The steps of this algorithm are illustrated in Fig. 7(b). The diagram illustrates the process of encrypting a message using the Hill cipher, a classic polygraphic substitution cipher. The Hill cipher operates on blocks of letters, applying a mathematical matrix operation to transform the plaintext into ciphertext.

4. Blockchain advancement in IoRT

Blockchain is a decentralized, digital ledger that keeps track of transactions openly and securely. It is a distributed database, which means that a network of computers, rather than a single entity, manages it. It was first developed as a technology to support the well-known cryptocurrency Bitcoin [19]. Nakamoto first put forth the idea for Bitcoin in 2008, and it was implemented in 2009 [80]. Despite the technology was initially created for the Bitcoin virtual currency, it has subsequently been modified for a variety of other uses, such as supply chain management, digital identity verification, and smart contracts [24].

The blockchain keeps a permanent and irrevocable record of all transactions that have taken place on the network by recording numerous transactions in each block and connecting each block to the one before it in a chain. Cryptography, which is used to safeguard the information in each block and to confirm the veracity and integrity of the transactions, ensures the security of the blockchain. The data in a block and the hash of the block before it in the chain are used to create a unique cryptographic signature, or hash, for each block in the chain [58].

The transparency of the ledger and the decentralized structure of the blockchain make it an excellent platform for secure and effective record-keeping that is also impervious to hacking and manipulation. It is also a trustless system, which means that parties can conduct business with one another without the use of middlemen like banks or governments. Blockchain technology has a wide range of potential applications, including Cryptocurrencies and digital payments, Supply chain management, Digital identity verification, Smart contracts, Healthcare, Voting systems, and Real estate [80]. The uses of this important sector are shown in Fig. 8. highlights the key components of blockchain technology, including blocks, transaction data, hashing, mining, the peer-to-peer network, and the public ledger aspect. It emphasizes the immutability and transparency provided by the blockchain architecture.

4.1. Blockchain in database security of IoRT

The distributed and immutable ledger that blockchain technology offers for storing transactions and data has the potential to improve database security. Blockchain networks protect against fraud and preserve data integrity by using consensus methods and cryptographic algorithms [58]. As a result, it is the perfect solution for protecting sensitive data in sectors including healthcare, banking, and government. Smart contracts can also automate complicated corporate procedures and lessen the need for middlemen, increasing efficiency and transparency. Although they are nevertheless in the early phases of development, blockchain-based database security solutions show great potential for the future of reliable and secure data management [1]. Listed below are a few justifications for using blockchain in database security:

4.1.1. Deterministic archive

A deterministic archive, which offers an effective remedy for data integrity and transparency, is a potent utilization of blockchain in database security. It assures that every modification to the database is permanently stored and tamper-proof by utilizing the permanent nature and transparency aspects of blockchain technology. The integrity of the data is established by this immutable record, which also enables accessible examination and authentication by auditors and regulatory bodies [19].

Since there is no longer a need for a centralized authority due to the decentralized structure of the blockchain, participants are more trustworthy and accountable. Organizations can have a trustworthy and reliable transaction history with a deterministic archive, safeguarding against unwanted changes and guaranteeing the reliability and accuracy of recorded data. For trustworthy and safe databases, the deterministic archive acts as the structural layer that enhances data security, compliance, and accountability [81].

Fig. 8. A simplified conceptual model of blockchain technology, a distributed ledger system designed for secure and transparent recording of transactions.

4.1.2. Decentralization

Blockchain technology offers many advantages and improves data protection when used for database security. Decentralization is key. The first benefit of decentralization is the elimination of the possibility of one single point of failure, providing the database more resistant to attacks and guaranteeing high availability. Secondly, decentralized blockchain systems disperse data processing and storage over some nodes, lessening the risk of data breaches and unwanted access.

Additionally, the decentralized blockchains' consensus algorithms, including Proof of Work or Proof of Stake, offer a trustless setting where database transactions are verified by a network of participants, preserving the accuracy of the data. Decentralization also improves privacy since it spreads out sensitive data around the network rather than keeping it concentrated in one place. Additionally, blockchain-based decentralized databases enable accessible and verified data management, allowing users to confirm the legitimacy and authenticity of the stored data. Organizations can improve data privacy, strengthen database security, and reduce vulnerabilities that accompany centralized systems by embracing decentralization [82].

4.1.3. Data encryption

An essential component of using blockchain for reliable database security is encryption. Encoding sensitive data in a form that is inaccessible that can only be decoded with the right decryption key, ensures its confidentiality and privacy. Data saved on the blockchain is secure thanks to encryption, even in the event of illegal access. The distributed nature of blockchain technology combined with encryption methods adds an extra degree of protection because data is dispersed over numerous nodes, making it very difficult for attackers to obtain all of the information. Before being placed on the blockchain, the data is encrypted using encryption methods like AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman), making it virtually hard for malevolent parties to decode without the accompanying decryption key. Organizations may protect sensitive information, adhere to data protection laws, and create a secure and reliable data environment by utilizing encryption in the blockchain that relies on database security [83].

4.1.4. Transparency

Using blockchain technology to secure databases has several benefits, but transparency stands out because it increases responsibility and visibility. Blockchain by default offers a transparent and verifiable trace of each transaction and database modification. Because it enables the confirmation and verification of data integrity, this transparency fosters trust among participants. Users can independently confirm the legitimacy and correctness of data saved thanks to the instantaneous inspection of the transaction history provided by the distributed ledger of the blockchain.

On top of that, blockchain's decentralized structure does away with the necessity for a single authority, lowering the possibility of fraud or manipulation. Because the auditors and authorities can easily observe and assess database transactions, the transparency offered by blockchain also improves regulatory compliance. Organizations may encourage confidence, enhance data integrity, and advance a secure and accountable data environment by using transparency in blockchain-based database security [84].

4.1.5. Smart contracts

A vital part of using blockchain for strong database security is smart contracts. When particular conditions are satisfied, these self-executing contracts, which are stored in the blockchain, automatically carry out predetermined activities. Smart contracts can be used to improve database security in several ways. Initially, smart contracts make it possible to automate contractual arrangements, doing away with the need for middlemen and lowering the possibility of mistakes made by humans or manipulation.

Additionally, smart contract trades are stored in a tamper-proof way because of blockchain's transparency and immutability, which improves data integrity. Furthermore, smart contracts make it possible for authorized parties to share data in an auditable, safe manner while maintaining access control and data privacy. The use of smart contracts also makes it possible to implement established rules and permissions, prohibiting illegal changes to the database. Organizations may improve computerization, assurance, and integrity while reducing the risks related to conventional contract management systems by utilizing smart contracts based on database security [85].

In conclusion, blockchain technology can offer a very transparent and safe platform for database administration, which can have a big impact on data privacy, security, and efficiency.

4.2. Implementation steps of blockchain in IoRT

The creation of a linked ecosystem entails integrating robotic equipment, instruments, and IoT technologies as part of IoRT deployment. To enhance processes and boost productivity, it makes use of real-time data collecting, analysis, and automation. Robotic devices can complete tasks independently thanks to IoRT's simultaneous interaction, coordination, and collaboration capabilities [19]. Benefits include higher production, improved safety, and lower expenses. The installation of IoRT needs careful planning, including data management, device integration, and security considerations. Organizations may unleash the full capabilities of IoT and robotics by effectively applying IoRT, revolutionizing sectors, and spurring innovation [40]. The following general IoRT blockchain implementation steps are:

4.2.1. Determine the use case

A critical first step in implementing the IoRT is determining the use case. It entails determining operational difficulties and assessing robotic automation's possibilities. Examining tasks that are repetitive, hazardous, time-consuming, or need high precision is one factor to take into account [58]. It is also crucial to consider whether IoRT is appropriate for tasks like managing materials, assembly, inspection, or surveillance. Identification of the use case requires a thorough understanding of the industry- or organization-specific requirements. Organizations can identify the most efficient use case for leveraging robotic technology to improve productivity, efficiency, security, and general performance by matching IoRT capacities with the identified difficulties and tasks [86].

4.2.2. Selection of a suitable blockchain platform

To execute the IoRT, choosing an appropriate blockchain platform is essential. It entails comparing various blockchain platforms' features, scalability, security, interoperability, and consensus procedures scalability, capacity, safety, interoperability, and consensus procedures of various blockchain platforms. The platform's capacity to manage the huge amount and rapid pace that information produced by IoRT devices is another factor to take into account [58]. It is important to evaluate the integration potential and compatibility with current systems. For long-term success, it is also critical to evaluate the platform's developer ecosystem, documentation, and community support. Organizations may assure smooth integration, accuracy of data, and trustworthiness among IoRT devices by carefully assessing and choosing the correct blockchain platform, enabling safe and open communication, data exchange, and automated transactions inside the IoRT ecosystem [40].

4.2.3. Specify the data schema

One of the most important steps in putting the IoRT into practice is defining the data structure. It entails specifying the organization and structure of the data that IoRT devices produce. The sorts of data to be gathered, including sensor readings, equipment status, location data, or operational metrics, are factors to take into account. Determining the data properties, methods of measurement in order and any other metadata is also crucial. The schema ought to be in line with the particular use case and the required analytics or processing. The compatibility and interoperability of data between various IoRT systems and devices must be ensured. Organizations may effectively safeguard, analyze, and extract valuable insights from the data produced by IoRT devices by defining an established data schema, allowing for informed decision-making and system optimization overall [87].

4.2.4. IoRT device integration with blockchain

Deploying the IoRT requires integrating IoRT devices with blockchain technology. It entails setting up the hardware so that it can communicate with the platform for blockchain technology using protocols and APIs. In addition to providing procedures for the validation of data and consensus, considerations include maintaining the safety of the device, restricting access, and data privacy. To facilitate the seamless sharing of data and communication, the combining process should also guarantee interoperability among various hardware and software platforms [58]. Organizations may assure data immutability, openness, and confidence within the IoRT ecosystems by connecting blockchain with IoRT devices, enabling safe and systematic transactions and interactions between devices. The development of decentralized apps and services that make use of the two IoRT and blockchain-based technologies may also be made possible by this connection [86].

Table 3
Critical Evaluation of Decentralized Database with Blockchain Viability in IoRT.

Feature	Decentralized Database [1]	Blockchain [90]
Data Integrity	High, with proper security measures	Very high, immutable
Data Availability	High, with redundancy	High, distributed across nodes
Scalability	Generally good, depends on architecture	Can be challenging, especially for high transaction volume
Complexity	Moderate to high, depending on the architecture	High, due to consensus algorithms and cryptography
Use Cases in IoRT	Centralized data management, analytics, and storage	Secure data sharing, provenance tracking, and tamper-proofing

4.2.5. Deploy smart contracts

The IoRT implementation process must include the deployment of smart contracts. On the blockchain platform, self-executing contracts must be programmed and deployed. The contract logic, circumstances, and behaviors that IoRT devices should carry out on their own should all be taken into account. In IoRT, smart contracts can simplify processes like device coordination, resource distribution, or payment settlements. To avoid unlawful access or malicious activity, smart contracts' security and dependability must be guaranteed. Organizations may automate device interactions, build trust, and enable smooth transparent fulfillment of contractual obligations by implementing smart contracts in IoRT. As a result, the IoRT ecosystem's activities may be made more effective, accurate, and efficient, leading to increased autonomy and improved general efficiency of linked devices [86].

4.2.6. Monitor and maintain the blockchain network

To successfully implement the IoRT, it is essential to monitor and manage the blockchain network. To assure the network's reliability, security, and efficiency, it involves ongoing network monitoring. The condition of blockchain nodes is tracked, together with the rate of transactions being processed and the consensus mechanism's validity [58]. Additionally, proactive steps like periodic updates, modifications, and audits of security should be conducted to resolve vulnerabilities and guarantee the reliability of the network. To support the increasing number of IoRT devices, organizations need also to keep an eye on how well the network is using its resources and how easily it can expand. Organizations may ensure uninterrupted functioning, accurate information, and trustworthiness among IoRT devices by carefully tracking and upholding the blockchain network. This will help to create a dependable and secure environment for autonomous operations, exchange of information, and interactions [40].

4.3. Blockchain consensus protocols

The set of guidelines and procedures known as blockchain consensus protocols enable nodes in a decentralized network to concur on the blockchain's current state. Blockchain technology uses a variety of consensus mechanisms, each of which has advantages and disadvantages [88]. Table 4 compares various consensus mechanisms suitable for IoRT applications. It highlights the key features, founding year, classification (public vs. private), and potential use cases within IoRT for each mechanism.

4.4. Critical evaluation of blockchain viability in IoRT

Decentralized databases, like InterPlanetary File System (IPFS) and Apache Cassandra, offer robust solutions for data storage and retrieval in distributed systems. These databases excel in environments where high availability, fault tolerance, and horizontal scalability are critical. They are designed to handle large volumes of data efficiently and ensure data consistency across distributed nodes [89]. A comprehensive analysis on the two topic has been portrait in Table 3.

While blockchain offers significant advantages in certain scenarios, it is not a one-size-fits-all solution. The choice between blockchain and other decentralized solutions should be based on specific application requirements. For instance, if the primary need is high-speed data processing with complex queries, decentralized databases might be more suitable. Conversely, if the focus is on ensuring data integrity, transparency, and operating in a trustless environment, blockchain is the preferred choice [91].

In conclusion, integrating blockchain into IoRT provides unique benefits that complement the capabilities of decentralized databases. A hybrid approach, leveraging both technologies based on their strengths, could offer the most comprehensive solution for securing and optimizing IoRT networks [92].

4.4.1. Efficiency concerns

One of the primary concerns regarding the use of blockchain technology in IoRT is its efficiency. Blockchain networks, especially those using proof-of-work (PoW) consensus mechanisms, can be resource-intensive, leading to concerns about scalability and energy consumption. These efficiency concerns are critical in IoRT applications, where real-time data processing and minimal latency are often required [91,92].

4.4.2. Scalability

Traditional blockchains, such as Bitcoin and Ethereum, have limited throughput capabilities, processing a relatively small number of transactions per second. This limitation can be problematic for IoRT applications that require high transaction volumes and low latency [24]. The time required to confirm transactions on a blockchain network can be significant. In IoRT, where immediate data processing and response are crucial, such delays can impact the system's performance and reliability [93].

4.4.3. Energy consumption

PoW-based blockchains are known for their high energy consumption, which is unsuitable for many IoRT applications, particularly those involving resource-constrained devices [94]. The substantial energy requirements of PoW blockchains raise concerns about their environmental impact. As IoRT systems often aim to be sustainable and efficient, alternative consensus mechanisms or solutions may be preferred [94].

4.4.4. Significance of blockchain in IoRT

In scenarios where security and data integrity are paramount, such as in healthcare robots handling sensitive patient data, blockchain's immutable ledger ensures that data cannot be tampered with once recorded. This feature is critical for maintaining trust and compliance with regulations [51]. Blockchain is particularly advantageous in environments where multiple parties need to interact without mutual trust. For example, in industrial IoRT applications involving various stakeholders, blockchain can provide a secure and transparent platform for data sharing and transaction verification without a central authority [90].

Blockchain's smart contract functionality enables automated and self-executing contracts based on predefined conditions. This capability is beneficial for IoRT applications requiring automated billing, access control, and maintenance scheduling, enhancing operational efficiency and reducing human intervention. Blockchain technology presents certain efficiency challenges, its unique advantages in terms of security, data integrity, and decentralization can justify its use in specific IoRT applications. By adopting more efficient consensus mechanisms and hybrid approaches, IoRT systems can leverage blockchain's strengths while mitigating its limitations. The choice to use blockchain should be based on a thorough evaluation of the specific requirements and constraints of the IoRT application in question [90].

5. Security and privacy for IoRT: Recent trends and challenges

5.1. Recent trends of IoRT security

The IoRT security landscape is quickly changing, with recent advancements focusing on blockchain and encryption technology. More and more IoRT devices are using encryption to safeguard sensitive data exchanged between them, assuring data security while in transit [106]. It is also being investigated if blockchain technology can offer safe and unhackable storage for data produced by IoRT devices, utilizing the distributed ledger's immutability to improve data security. Blockchain-based decentralized identification solutions are also being looked into as a way to protect access to IoRT devices and data. These patterns indicate an increased understanding of the significance of IoRT devices and data security in warding off online dangers and preserving user security and privacy. To ensure the continuous development of the IoRT ecosystem, researchers and industry players must continue to discover and deploy cutting-edge security solutions [40].

The trends can be sorted into different segmentations like risk analysis, network security, firewall and software security, authentication, and access control, security malfunction, and database security.

5.1.1. Cryptanalytic assessment

The assessment of cryptanalytic attacks for IoRT security entails determining the strengths and weaknesses of cryptographic systems based on blockchain that is used in IoRT devices and networks. It seeks to pinpoint potential attack points and assess how well blockchain or encryption defenses work to thwart unwanted access and data breaches. To find weaknesses in encryption or blockchain algorithms and protocols, this examination makes use of a variety of methodologies, including mathematical and algorithmic analysis, as well as real-world attacks. Understanding the possible impact of cryptanalytic attacks on IoRT security and developing mitigating techniques using blockchain or encryption technology are the main goals. Organizations can strengthen the security of their IoRT systems, protect sensitive data, and guarantee secure and dependable communication inside the IoRT by carrying out a thorough cryptanalytic attack assessment [107].

5.1.2. Network security

The IoRT network security strategy focuses on securing communication networks and the data transferred between IoRT devices and networks. It includes guarding against unwanted access, data breaches, and malicious assaults on network components. Blockchain and encryption technologies are essential for enhancing IoRT network security. While data is being transmitted, encryption maintains its secrecy and integrity, and blockchain offers decentralized, tamper-proof data storage and verification. These technologies are used to protect sensitive information, authenticate devices, secure network protocols, and create secure communication channels. IoRT systems can reduce risks of unwanted access, data interception, and manipulation by utilizing encryption and blockchain in network security measures, resulting in a robust and secure environment for IoRT operations [5].

Table 4
Consensus mechanisms suitable for Internet of Robotic Things (IoRT) applications.

Ref	Name of consensus	Feature of consensus	Founding year	Classification	Use in IoRT	Energy Consumption	Resource Requirements
[95]	Proof-of-work (PoW)	i. Solving computational puzzles, ii. Significant consumption of energy.	2008	Both public and private.	i. Validating transactions, ii. Ensuring the accuracy of data, iii. Protecting communications between robotic devices.	High	High computational power
[96]	Proof of Stake (PoS)	i. Selection based on stakes, ii. Energy-saving.	2012	Both public and private.	i. Secured robotic communications and transactions, ii. Conserving energy.	Low	Moderate network connectivity
[97]	Delegated Proof of Stake (DPoS)	i. Quick block confirmation, ii. Delegated voting.	2014	Both public and private.	i. Coordinating robotic network governance, ii. Safeguarding transactions, iii. Achieving effective consensus.	Low	Moderate network connectivity
[98]	Proof of Authority (PoA)	i. Centralized control, ii. Legitimacy based on identity.	2017	Private	i. Secured robotic network, ii. Ensuring the validity of robotic devices.	Low	High trust in validators
[99]	Byzantine Fault Tolerance (BFT)	i. Consensus in failures and resistance to rogue or malfunctioning nodes.	1999	Both public and private.	i. Robotic device consensus, ii. Building trust, iii. IoRT security.	Moderate	High communication overhead
[100]	Practical Byzantine Fault Tolerance (PBFT)	i. Low latency in turn, ii. Resilience to malfunctioning.	1999	Private	i. Establishing trust, ii. Preventing malevolent conduct in robotic networks.	Moderate	High communication overhead
[101]	Proof-of-Activity (PoA)	i. PoW and PoS combined, ii. Conservation of energy.	2014	Public	i. IoRT activities require little energy.	Moderate	Combination of PoW and PoS
[102]	Proof-of-Elapsed-Time (PoET)	i. Verified time to wait, ii. Stochastic leader selection.	2016	Both public and private.	i. Election of the leader, ii. Time-sensitive operations.	Low	Trusted execution environments
[102]	Proof-of-Capacity (PoC)	i. Integrates the available storage.	2013	Both public and private.	i. Storage-based tasks, ii. Effective consensus.	Low	Significant storage space
[103]	Proof-of-Space-and-Time (PoST)	i. Use time and storage space measurements.	2013	Public	i. Activities based on storage, ii. Operations based on time.	Low	Significant storage space and time sync
[104]	Proof of Storage (PoStorage)	i. Implements storage space for consensus.	2017	Both public and private.	i. IoRT data storage and integrity checks.	Low	Significant storage space
[105]	Proof-of-burn (PoB)	i. Burning of the digital currency tokens, ii. Supply minimization.	2012	Both public and private.	i. Distributing tokens, ii. Eradicating unused tokens, iii. Creating legitimacy in IoRT systems.	Low	Currency Tokens

5.1.3. Firewall and software security

Protecting IoRT devices and networks from unauthorized access and harmful activity requires a firewall and software security. To stop illegal connections and potential risks, firewalls act as protective barriers, monitoring and filtering network traffic. By encrypting data packets and enabling secure communication channels between IoRT devices and the firewall, encryption, and blockchain improve firewall security. Operating systems, apps, and firmware must all be protected for software to be secure. Encryption protects

sensitive data, and blockchain offers a tamper-proof method for secure software upgrades. IoRT systems may efficiently defend against unauthorized access, data breaches, and software vulnerabilities by integrating encryption and blockchain into the firewall and software security mechanisms, thereby assuring the integrity and security of the IoRT ecosystem [108].

5.1.4. Authentication and access control

The IoRT security relies heavily on authentication and access control to validate user identities and manage user access to devices and systems. Access control decides what users may do, while authentication makes sure that only authorized parties can interact with IoRT devices. By protecting authentication credentials and communication channels and maintaining the confidentiality and integrity of sensitive data, encryption improves authentication and access control. Blockchain technology enables secure and transparent authentication by providing decentralized and tamper-resistant identity management. IoRT systems can protect against illegal access, reduce the danger of identity spoofing, and create a secure and reliable IoRT ecosystem by utilizing encryption and blockchain in authentication and access control [51].

5.1.5. Malfunction security

Malfunction security, which focuses on avoiding and treating device failures that could result in operational disruptions or safety issues, is an essential component of IoRT security. It entails taking prompt action to identify problems, isolate them, and repair the damage they cause. Blockchain and encryption technologies are essential for improving IoRT malfunction security. To maintain the integrity and confidentiality of IoRT operations, encryption is used to protect important orders, data, and communication channels. The decentralized and unchangeable record of device behavior provided by blockchain makes it easier to identify and spot any flaws. IoRT systems can reduce risks, improve reliability, and maintain a secure and resilient IoRT environment by utilizing encryption and blockchain in malfunction security techniques [109].

5.1.6. Database security

To protect the integrity, confidentiality, and accessibility of the data stored in IoRT databases, database security is a crucial component of IoRT security. It entails putting precautions in place to prevent unwanted access, data breaches, and the alteration of sensitive data. Data is protected even in the case of a database intrusion thanks to encryption, which encrypts data both in transit and at rest. By providing decentralized and impermeable data storage and verification processes, blockchain technology can be used to increase database security. IoRT systems may efficiently safeguard sensitive data, avoid unwanted access, uphold data integrity, and guarantee thorough security across the IoRT ecosystem by utilizing encryption and blockchain in database security measures [5].

5.2. Implementation challenges

Implementing security in IoRT devices could come with a lot of perks. It is important to acknowledge the challenges that come up with the advantages of security in IoRT. The use of additional security features comes up with the issues of the requirement of large server storage, high computational power, high network bandwidth, increased device size, being less cost efficient and hard to implement [5]. All the perks are discussed below:

5.2.1. Large server storage

The IoRT requires particular specifications for significant server storage to provide encryption. Due to the additional security measures, encrypted data has a bigger storage capacity than unencrypted data, needing a significant number of storage resources in large server networks. Additionally, extra storage space and specialized hardware or software are needed for efficient key management when keeping encryption keys safe. The storage capacity must be expandable and quickly adaptive to meet changing needs as the IoRT grows. Furthermore, it is crucial to have a well-thought-out storage architecture that guarantees data confidentiality, integrity, and high-performance levels. Additional storage space and specific storage solutions may also be required to meet compliance and regulatory requirements. To address the important needs for big server storage, leading to safe and scalable storage solutions, encryption implementation in the IoRT necessitates careful study [110].

5.2.2. High computational power

High processing power is required for encryption implementation in the context of the IoRT. Intricate mathematical calculations are needed for the encryption and decryption operations, which use a lot of processing power. Robotic machines may not be able to complete these calculations due to their low processing capability, necessitating the utilization of external computing resources. Additionally, the processing needs for encryption and decryption may rise as the IoRT generates more data. As a result, high-performance computing platforms with the capacity to handle massive data quantities and quickly complete complicated calculations are needed to implement encryption in the IoRT. Making sure that the available computational resources are sufficient and used to their fullest potential is essential to overcoming the problem of fulfilling the high computational power needs in the IoRT [6].

Table 5
Summary of the implementation challenges.

Ref	Resource	Encryption	Decryption	Impact on IoRT
[6]	Computational Power	High	High	Requires external computing resources; IoRT devices may have insufficient processing capability
[110]	Memory/Storage	Large	Large	Needs significant server storage; encrypted data requires more space than unencrypted data
[111]	Network Bandwidth	High	High	Increased data transmission capacity needed; may cause bottlenecks and higher latency

5.2.3. High network bandwidth

High network bandwidth is necessary to implement encryption in the IoRT. Due to the increased encryption overhead, encrypted data requires more data transmission capacity than unencrypted data. As a result, data flow between devices may experience bottlenecks, which can impair network performance and increase latency. Additionally, as the IoRT continues to grow, the amount of data generated and exchanged between devices will rise, further escalating the need for network capacity. A network architecture that can handle the increased data volume and transmission overhead is required to deploy encryption in the IoRT. To ensure effective and secure communication between devices, it should have enough bandwidth and minimal latency. To ensure that the network infrastructure is properly planned and optimized for high-performance data transmission, it is necessary to carefully evaluate the difficulty of fulfilling the high network bandwidth needs in the IoRT [111].

5.2.4. Device size

The IoRT requires greater device hardware to implement encryption. To function effectively, encryption methods and procedures require additional hardware resources, such as greater memory, processing power, and specialized hardware modules. As a result, hardware with low resources may not be able to accomplish the required encryption duties, necessitating the employment of more potent and substantial hardware. Additionally, as the IoRT generates more data, the hardware resources required for encryption and decryption may increase as well. Therefore, to implement encryption in the IoRT, more robust hardware devices that can handle the higher processing and memory needs are needed. Careful consideration is required to ensure that the hardware devices are appropriate and optimized for optimal use given the issue of achieving the higher device hardware size requirements in the IoRT [43].

5.2.5. Less cost efficient

The cost-effectiveness of implementing encryption in the IoRT can be a problem. This is because running encryption processes and algorithms require more hardware and software resources. Devices utilized in the IoRT may cost more due to the specialized hardware components, greater memory, and computing power required to carry out encryption functions. Further investments in specialized software and hardware may be necessary to manage the encryption keys to preserve the system's security through encryption. The overall cost may increase if the network infrastructure needs to be upgraded to handle the increased bandwidth needs of encrypted traffic. The careful balancing of security and cost, as well as the choice of cost-effective hardware and software solutions, are therefore necessary if encryption is to be implemented in the IoRT while being cost-efficient [43].

5.2.6. Hard to implement physically

Due to its complexity and difficulty, implementing encryption in the IoRT offers a significant hurdle. Implementation of encryption techniques and procedures is difficult and requires a thorough understanding of cryptography as well as specific hardware and software. Furthermore, the IoRT's enormous and complex network of devices creates additional difficulties for uniformly deploying encryption across all devices and maintaining safe communication between them. The importance of ensuring that encryption is implemented effectively and completely is highlighted by the fact that any flaw or error during the implementation process could jeopardize the security of the entire system. It is necessary to carefully consider the knowledge and resources needed to implement encryption effectively and securely, as well as the selection of suitable encryption solutions that can be seamlessly integrated into the existing IoRT infrastructure, to overcome the challenge of hard-to-implement encryption in the IoRT [110]. The research trends in IoRT are given in Tables 6–11. This table summarizes recent research trends in IoRT security, including various security challenges and proposed solutions in IoRT systems. It showcases the increasing exploration of techniques like Federated Learning, Blockchain, and lightweight encryption algorithms for securing data and communication within IoRT environments.

Table 5 provides a summary of the implementation challenges faced for encryption and decryption.

A comprehensive review of IoRT security studies from 2016 to 2024 (Tables 6–11) reveals significant advancements and emerging trends across various domains. The integration of federated learning and blockchain technology has gained prominence, offering robust defense mechanisms and decentralized security solutions. However, these technologies face challenges in terms of computational complexity and scalability that warrant further investigation. Encryption techniques have evolved considerably, with researchers exploring advanced methods such as multi-keyword-based ciphertext retrieval, chaotic encryption, and quantum

Table 6
Recent Research Trends in IoRT Security (2016–2024).

Paper	Year	Security type	Algorithm	Trend	Technical details	Limitations
[53]	2024	Federated learning	"FedMTD" shuffling-based moving target defense strategy	Heterogeneous cross-silo IoRT environments	Shuffling-based moving target defense for federated learning	High computational complexity, communication overhead
[112]	2024	Security attacks within the robotics domain	Dedicated Short Range Communication (DSRC)	Wireless communication	Dedicated communication protocol for low-latency, secure comms	Limited range, potential for interference
[113]	2023	Data Sharing security	Glowworm swarm optimization (GSO)	Network security	Optimization technique based on glowworm swarming behavior	May not scale well with network size
[114]	2023	Assess cybersecurity vulnerability	Nmap and OpenVAS	Security malfunction	Network scanning and vulnerability assessment tools	False positives/negatives, high resource usage
[115]	2023	Hacking protection	Blockchain	Database security	Decentralized ledger technology for secure, immutable records	Scalability, energy consumption
[116]	2023	Fog computing-based data security	Multi-keyword-based ciphertext retrieval scheme	Cryptanalytic assessment	Advanced encryption scheme for secure fog computing environments	High computational complexity
[117]	2023	Communication protocol by random key generation	Key Generation Center (KGC) protocol	Encryption facilities	Centralized key generation protocol for secure communications	Single point of failure, trust issues
[26]	2023	Complete security infrastructure	Blockchain Technology	Network security	Decentralized network for robust security infrastructure	Scalability, energy consumption
[25]	2023	Secure control frame-work design	Network architecture	Firewall and software Security	Comprehensive network design for enhanced security	Complexity, potential bottlenecks
[118]	2023	Communication protocol design	Quantum computing based encryption	Network security	Utilizing quantum cryptography for ultra-secure communication	High cost, complex implementation
[119]	2023	Cloud security	Blockchain Technology	Database security	Decentralized ledger for secure cloud storage	Scalability, energy consumption
[120]	2023	Server security	HPCchain	Database security	High-performance blockchain for secure server operations	Resource intensive, complex management
[121]	2023	Network and storage Security	Blockchain	Database security, Network security	Decentralized ledger for securing network and storage	systems Scalability, energy consumption
[122]	2023	Secure network system activity	Blockchain distributed consensus	Network security	Blockchain for secure and incentivized network activities	Scalability, energy consumption
[123]	2023	DDOS protection	Lightweight privacy-preserving and (LPP) scheme	Firewall and software security	Lightweight scheme for protecting against DDOS attacks	Limited to specific attack vectors
[124]	2023	Framework decentralization	Privacy-Perceiving Asynchronous Federated Learning (PPAFL)	Firewall and software security	Asynchronous federated learning for decentralized privacy	Communication overhead, implementation complexity
[125]	2023	Transmission security	Chaotic encryption	Network security	Using chaotic systems for secure data transmission	Complexity, potential vulnerabilities
[126]	2023	Database protection for healthcare IoRT	Private blockchain	Database security	Private ledger for secure healthcare data storage	Trust management, scalability issue

computing-based encryption. While these approaches promise enhanced data security, their high implementation costs and complexity remain obstacles to widespread adoption. The application of machine learning and artificial intelligence in cybersecurity

Table 7
Recent Research Trends in IoRT Security (2016–2024).

Paper	Year	Security type	Algorithm	Trend	Technical Details	Limitations
[127]	2023	Authentication, integrity protection	ES-SECS/GEM	Authentication and access control	Enhanced secure scheme for robust authentication	Implementation complexity, performance overhead
[128]	2023	Predicts and prevent possible cyber-attack	Blockchain, Machine learning	Database security	Using blockchain and ML for predictive cybersecurity	Scalability, data quality issues
[129]	2022	Server authentication	AES	Authentication and access control	Symmetric encryption for secure server authentication	Key management, potential for brute force attacks
[130]	2022	To reduce the overhead of microcomputers and to have strong encryption of data	Chaos-Based Lightweight Encryption	Cryptanalytic assessment	Lightweight encryption using chaotic maps	Limited security, key management
[131]	2022	To implement monitoring solutions based on IoRT	LoRaWAN	Malfunction security	Low power wide area network for IoRT monitoring	Range limitations, security issues
[132]	2022	Data peer security	Blockchain	Database security	Decentralized ledger for peer-to-peer data security	Scalability, energy consumption
[133]	2022	Integration of Command-and-Control systems	Coalition Warrior Interoperability Exercise	Firewall and software security	Framework for secure integration of C2 systems	Complexity, interoperability issues
[109]	2022	Big data IoT security	Federated Learning	Database security	Federated learning for secure big data handling	Communication overhead, model complexity
[134]	2022	Enables patching vulnerable modules	iRECOVer	Malfunction security	Framework for recovering and patching IoT systems	Implementation complexity, coverage issues
[135]	2022	Authorizing protocol	CoAP and MQTT	Authentication and access control	Lightweight protocols for secure IoT communication	Security vulnerabilities, scalability
[107]	2022	Security attacks within the robotics domain	AES	Cryptanalytic assessment	Symmetric encryption for securing robotic communications	Key management, potential for brute force attacks
[136]	2022	IoT cyber-attacks	Forensics and antiforensics methods	Cryptanalytic assessment	Techniques for identifying and countering cyber-attacks	Complexity, potential for false positives
[137]	2021	Cloud computing database	AES, DES	Database security	Symmetric encryption for secure cloud database storage	Key management, potential vulnerabilities
[138]	2021	Railway transportation security	Fog computing	Network security	Decentralized computation for secure railway communication	Latency, resource management
[139]	2021	Data Security and Privacy	SDN-based Federated Learning	Database security	Combining software-defined networking with federated learning	Complexity, scalability
[140]	2021	V2G communication security	V2G protocols	Network security	Secure communication protocols for vehicle-to-grid systems	Implementation complexity, interoperability
[141]	2021	IOT security enhancement	Fake system frameworks (ANNs) and inherited computations	Firewall and software security	Using ANNs for anomaly detection in IoT systems	Complexity, false positives

Table 8
Recent Research Trends in IoRT Security (2016–2024).

Paper	Year	Security type	Algorithm	Trend	Technical details	Limitations
[142]	2021	Secure framework design	FSM	Firewall and software security	Finite state machines for secure system operations	Complexity, potential for state explosion
[143]	2021	Communication Protocols security	Communication Protocol	Network security	Secure communication protocols for IoRT	Implementation complexity, potential vulnerabilities
[144]	2021	IoRT Framework security	RCNN ResNet 101	Firewall and software security	Deep learning models for anomaly detection in IoRT	High computational requirements
[145]	2021	Verification and authentication security	STM, UML	Authentication and access control	Modeling languages for secure system verification	Complexity, learning curve
[146]	2021	Digitization security	Firewall architecture	Firewall and software security	Comprehensive firewall design for digital systems	Performance overhead, potential bottlenecks
[147]	2021	Service framework security	CoAP, DTLS	Firewall and software security	Lightweight protocols for secure IoT service communication	Security vulnerabilities, scalability
[148]	2021	Network control framework	FNC	Firewall and software security	Framework for secure network control in IoRT	Complexity, potential bottlenecks
[108]	2021	Framework security	SDN, CPS	Firewall and software security	Combining SDN with cyber–physical systems for enhanced security	Complexity, scalability
[149]	2021	SCADA security	AI based algorithm	Firewall and software security	Using AI for secure SCADA system operations	Complexity, potential for false positives
[150]	2021	Privacy breach security	Model driven, blockchain	Database security	Model-driven design combined with blockchain for privacy protection	Implementation complexity, scalability
[151]	2021	Data transmission security	POMDP	Network security	Partially Observable Markov Decision Process (POMDP) for making decisions in uncertain environments	Complexity in solving POMDP problems and high computational overhead
[152]	2021	Military robot security	AI and ML based algorithm	Firewall and software security	Utilizes Artificial Intelligence (AI) and Machine Learning (ML) to enhance security measures for military robots	Requires significant training data and computational resources, potential for adversarial attacks
[153]	2021	Big data security	ML based algorithm	Database security	Machine Learning algorithms to secure big data systems	Data dependency and vulnerability to adversarial attacks
[154]	2021	Performance improvement	Blockchain and AI based algorithm	Database security	Combining blockchain technology with AI to enhance performance and security	High energy consumption, complexity in implementation, and scalability issues
[155]	2021	Automation security	ROS framework, blockchain	Database, firewall and software security	Integrating Robot Operating System (ROS) with blockchain for secure automation	Scalability issues and high computational cost
[156]	2021	Optimal network, Data, transmission security	UV and IOT protocol, Node architecture	Network security	Uses UV communication and IoT protocols for secure data transmission	Complexity in implementation and potential for high latency

Table 9
Recent Research Trends in IoRT Security (2016–2024).

Paper	Year	Security type	Algorithm	Trend	Technical details	Limitations
[157]	2021	Protocol security	Designed communication protocol	Network, firewall and software security	Custom communication protocols designed for enhanced security	May not be compatible with existing systems and can be resource-intensive
[1]	2020	Framework design	Encryption and framework algorithms	Firewall and software security	Utilizes encryption and comprehensive security frameworks for enhanced protection	Complexity in integration and potential performance overhead
[158]	2020	Network virtual system design	NVS	Network security	Network Virtualization Systems (NVS) for creating secure network environments	Complexity in implementation and management
[159]	2020	FC network security	Fog-assisted method, SAT, CBF, ECC	Network security	Uses fog computing, SAT solvers, and Cryptographic Boolean Functions (CBF) along with Elliptic Curve Cryptography (ECC) for network security	High computational and resource requirements
[160]	2020	Privacy framework	UCI, HAR	Firewall and software security	Utilizes User-Centric Identity (UCI) and Human Activity Recognition (HAR) for privacy protection	Complexity in managing user identities and potential for false positives/negatives
[161]	2020	Framework method design	Fog computing method	Firewall and software security	Uses fog computing to distribute data processing and enhance security	Latency issues and complexity in resource management
[162]	2020	Signal strength and security	ML based method	Malfunction security	Machine Learning methods to monitor and enhance signal strength security	Data dependency and susceptibility to adversarial attacks
[163]	2020	Intelligence application	CI, AIS, SI, GA	Artificial intelligence based security	Computational Intelligence (CI), Artificial Immune System (AIS), Swarm Intelligence (SI), Genetic Algorithm (GA) enhance security by simulating biological processes	High computational costs and complexity
[161]	2020	Transmission security	Framework design	Network security	Secure framework for data transmission	Implementation complexity and high overhead
[40]	2019	Optimal secure framework design	Umbrella and architecture protection	Firewall and software security	Comprehensive security framework for IoRT systems	Difficult to scale and integrate with existing systems
[164]	2019	Communication security	AES	Network security	Standard encryption algorithm for secure communication	Susceptible to advanced cryptographic attacks
[165]	2019	Network communication enhancement	ML based algorithm	Network security	Uses machine learning to improve network security	Data dependency and complexity in training models
[166]	2019	Communication security	NOMA	Network security	Allowing multiple users to share communication resources simultaneously	High complexity in signal processing, potential interference issues

Table 10
Recent Research Trends in IoRT Security (2016–2024).

Paper	Year	Security type	Algorithm	Trend	Technical details	Limitations
[167]	2019	Architecture security	Physical layer security	Firewall and software security	Securing the physical layer to prevent eavesdropping and tampering	Susceptibility to physical attacks, complex implementation
[168]	2019	TCP/IP security	MQTT	Network security	Ensuring secure TCP/IP communication in IoT environments	Vulnerable to DoS attacks, requires proper configuration
[169]	2019	Operational security	ML based algorithm	Malfunction security	Monitoring and securing operational processes using ML	Data dependency, vulnerability to adversarial attacks, high computational requirements
[170]	2019	Digital twin security	Architectural layer design	Firewall and software security	Ensuring data integrity and protection in digital twin technologies	Complex implementation, integration challenges
[171]	2019	Optimal security	ML based algorithm	Cryptanalytic assessment, Network security, Firewall and software security	Using ML for optimal security configurations and assessments	High computational cost, large dataset requirements, potential for adversarial attacks
[172]	2019	Automation security	Encryption, mining algorithm	Cryptanalytic assessment, authentication and access control	Combining encryption with data mining for enhanced security	Computationally intensive, complex algorithm integration
[173]	2019	Physical layer security	Authentication	Firewall and software security	Implementing secure authentication mechanisms at the physical layer	Complexity in implementation, potential performance overhead
[174]	2019	Database encryption	Blockchain	Database security	Using blockchain for secure database encryption and integrity	Scalability issues, high energy consumption, complex key management
[175]	2018	Address localization	Dijkstra's algorithm	Network security	Optimal routing and address localization in networks	High computational complexity for large networks, potential routing inefficiencies
[176]	2018	Architecture security	Framework	Firewall and software security	Implementing comprehensive security frameworks	Complexity in deployment, potential performance impact
[177]	2018	Optimal security	Server encryption/blockchain	Database security	Combining server-side encryption with blockchain	Scalability challenges, high resource consumption, complex implementation
[178]	2018	Data secure method	DE4MHA	Database security	Encrypting data for multiple heterogeneous architectures	Managing heterogeneous systems complexity, potential performance overhead
[179]	2017	ResDac security	CPT	Cryptanalytic assessment, database security	Using cryptographic protection techniques for research data archives	Complexity in cryptographic management, potential performance impact
[180]	2017	Firewall protection	DMA, PCI	Firewall and software security	Using DMA, PCI technologies enhancing firewall protection	Vulnerability to hardware attacks, complexity in configuration
[181]	2017	Physical layer security	Burke's rhetoric	Firewall and software security	Applying Burke's rhetorical principles for securing physical layer	Abstract concept, difficult to implement practically
[182]	2017	Optimal security	Infrastructure security algorithm	Firewall and software security	Designing algorithms for securing infrastructure	High complexity, potential scalability issues

Table 11
Recent Research Trends in IoRT Security (2016–2024).

Paper	Year	Security type	Algorithm	Trend	Technical Details	Limitations
[183]	2017	Data collection security	TFAA	Database security	Using TFAA for secure data collection and storage	Complexity in implementation, potential performance overhead
[184]	2017	ROS security	Peer-to-peer communication	Network security	Implementing peer-to-peer communication for secure ROS environments	Vulnerable to peer-to-peer network attacks, requires robust validation
[185]	2017	Communication channel security	Peer-to-peer	Network security	Using peer-to-peer techniques for secure communication channels	Potential for network congestion, security risks in peer-to-peer networks
[186]	2016	Server authorization	RSA	Authentication and access control	Using RSA for secure server authorization	Computationally intensive, requires secure key management
[187]	2016	Medical IOT security	Architecture design	Firewall and software security	Designing secure architecture for medical IoT devices	Complexity in integration, high regulatory requirements
[188]	2016	Automation security	AES	Malfunction security	Standard symmetric encryption for secure automation	Vulnerable to side-channel attacks
[189]	2016	Modeling security	AES	Firewall and software security	Ensures model integrity with encryption	High computational load and key management issues
[190]	2016	Wireless security	AES	Network security	Secures wireless communication	Performance degradation under high load
[191]	2016	Data protection technique	AES	Database security	Encrypts data to prevent unauthorized access	Challenges in key management
[192]	2016	Communication security	AES	Network security	Standard encryption for secure data exchange	Vulnerable to advanced cryptographic attacks
[193]	2016	Configuration security	AES	Firewall and software security	Securing configuration data, ensuring data integrity and confidentiality	Susceptible to side-channel attacks, requires secure key management practices
[194]	2016	Communication security	AES	Network security	Providing robust encryption for securing communication channels, protecting data in transit	Vulnerable to advanced cryptographic attacks, requires proper implementation to avoid potential weaknesses
[195]	2016	Optimal IOMT security	AES	Firewall and software security	Securing Internet of Medical Things (IoMT) devices, ensuring secure data storage and communication	High computational load for resource-constrained devices, key management challenges

has become increasingly sophisticated, particularly in vulnerability assessment and anomaly detection. These technologies offer optimized security measures but raise concerns regarding data quality and computational demands that must be addressed. Secure communication protocols and frameworks, including Dedicated Short Range Communication (DSRC) and Key Generation Center (KGC), have proven critical for low-latency, secure communication in IoRT environments. However, range limitations and trust issues continue to pose challenges for researchers and practitioners alike. To address privacy concerns, lightweight privacy-preserving schemes and decentralized frameworks have emerged as promising solutions. While these approaches offer efficient and secure alternatives, they often grapple with implementation complexity and communication overhead. Notably, sector-specific security measures for healthcare IoRT, military robotics, and railway transportation underscore the need for tailored solutions. Common challenges across these domains include scalability, resource management, and regulatory compliance, highlighting the importance of interdisciplinary research in developing robust, context-specific security measures. This analysis emphasizes the critical balance between advanced security techniques and practical implementation considerations. As the field of IoRT security continues to evolve, researchers and stakeholders must navigate this complex landscape, making informed decisions about technology adoption and future research directions. Further studies are needed to address the identified challenges and to explore the potential of emerging technologies in enhancing IoRT security.

6. Future recommendations

IoRT is one of the state-of-the-art emerging technologies and so it is going to evolve in recent future. To ensure a safe sustainable use of this product security will be a matter of concern for everyone. In near time several new terms could be introduced to provide security in this valuable sector of technology. Some of the mentions are:

6.1. Threat intelligence and analytics

IoRT devices can be improved by ensuring intelligence and analytics on threats. The demand for comprehensive threat intelligence and analytics is increasing as IoRT networks and devices continue to develop. Processing large amounts of data and identifying new dangers, abnormalities, and real-time patterns need the use of machine learning, artificial intelligence, and big data analytics. The adoption of security measures at the appropriate times and quick responses to potential threats are made possible by this proactive approach.

6.2. Security by design

In the future, security can be prioritized as a fundamental component from the very beginning of the design of IoRT systems. Security considerations can be seamlessly included in the design and development phases, including secure protocols, strong authentication systems, and the use of secure coding techniques. Potential vulnerabilities can be reduced, significantly reducing the chance of security breaches, by implementing security by design principles.

6.3. Blockchain for security

The use of blockchain technology has the potential to greatly improve IoRT system security. It is possible to create immutable and transparent transaction records, safe lines of communication, and decentralized identity management by utilizing distributed ledger technology and cryptographic components. Within IoRT contexts, blockchain can successfully address issues with data integrity, device authentication, and secure peer-to-peer communication.

6.4. Multi-factor authentication

Traditional username and password-based authentication techniques might not be sufficient to protect IoRT devices and networks. Future IoRT security measures should incorporate multi-factor authentication methods, which include biometrics like fingerprint and facial recognition, hardware-based authentication like smart cards and tokens, and behavioral patterns like typing and mouse movement. These additional authentication layers could significantly improve the security of robotic systems if they are used.

6.5. Security orchestration and automation

The issue of controlling security across the ecosystem grows more challenging as IoRT devices proliferate. Tools for security orchestration and automation are emerging as significant resources to meet this problem. They allow for streamlined security operations, automated threat detection and response, and centralized management of security policies and upgrades. By utilizing such technologies, businesses can effectively track and respond to security events across all of their IoRT deployments, increasing the effectiveness of security management as a whole.

6.6. Secure over-the-air (OTA) updates

IoRT security can always require over-the-air (OTA) updates. To ensure the quick and secure distribution of crucial security patches, firmware updates, and bug fixes, future IoRT systems should prioritize the creation of resilient and secure OTA procedures. The integrity and validity of OTA updates can be protected by the use of encryption, digital signatures, and secure boot procedures, adding another layer of security to the IoRT ecosystem.

6.7. Artificial intelligence (AI) for threat detection

AI algorithms have a great deal of potential for identifying and reducing security issues in IoRT situations. Continuous analysis of IoRT network traffic, device activity, and aberrant patterns is made possible by utilizing AI-based threat detection systems, allowing the discovery of potential security breaches or malicious activities. Adaptive security measures can also be made possible by AI, giving systems the ability to automatically respond to attacks and dynamically change their security setups.

6.8. Standardization and certification

It is crucial to establish industry-wide standards and specific certification processes for IoRT security. With these standards, manufacturers, developers, and users have access to comprehensive guidelines, best practices, and benchmarks that help to assure an increased level of security throughout all IoRT implementations. Programs for certification make additional contributions by confirming the security capabilities of IoRT systems and devices and fostering confidence in their resiliency.

6.9. Federated learning

The future potential for federated learning to enhance the IoRT blockchain and encryption security is quite bright. Federated learning has great promise for supporting dynamic threat response, collaborative threat intelligence, safe blockchain consensus, privacy-preserving data analysis, and decentralized key management. The IoRT can achieve higher levels of security, privacy protection, and adaptive defense mechanisms by utilizing the power of federated learning. This will help to cultivate a more robust and resilient ecosystem for carrying out encrypted data analysis, managing cryptographic keys, and carrying out blockchain-based transactions.

7. Conclusion

This review paper comprehensively examines the privacy and security aspects of the Internet of Robotic Things (IoRT), highlighting the evolving landscape of security challenges and solutions in this domain. Through a thorough exploration of existing literature, the manuscript identifies key frameworks, requisites, and scopes for ensuring the confidentiality, integrity, and availability of data within IoRT systems.

The importance of encryption methods, including symmetric and asymmetric encryption, Transport Layer Security (TLS), and data-at-rest encryption, in safeguarding sensitive information exchanged among IoRT devices is discussed. Furthermore, various encryption algorithms and their applications in securing data transmission and storage within IoRT networks are explored.

Moreover, the paper underscores the significant role of blockchain technology in enhancing security and transparency in IoRT systems. By leveraging features such as decentralization, data encryption, and smart contracts, blockchain offers a robust framework for securely managing and verifying transactions across distributed networks of IoRT devices.

Additionally, implementation steps and challenges associated with integrating blockchain technology into IoRT systems are outlined, providing insights into best practices for deploying and maintaining blockchain networks in real-world scenarios.

Again, the examination of current trends and challenges in IoRT security underscores the need for continuous innovation and collaboration in addressing emerging threats and vulnerabilities. From cryptanalytic assessments to network security measures, the IoRT ecosystem requires comprehensive strategies and solutions to mitigate risks and protect sensitive data from malicious actors.

With a focus on encryption techniques, recommendations, and best practices, this manuscript addresses the security of the Internet of Robotic Things. The requirements and scopes of IoRT's fundamental structure have been addressed. Then, through a brief discussion, the range of encryption approaches in IoRT security was studied and presented.

Furthermore, by providing the following helpful information, this study can aid researchers and practitioners.

- Demonstrated the core tenets of IoRT that may motivate academics to spend more time working in this field.
- Explored several IoRT security architectures, scopes, and requirements, providing details that could serve as the basis for future research.
- Highlighted the blockchain-based IoRT security that may encourage greater research in this area.
- Presented a summary of current IoRT security and privacy trends across a range of applications, allowing researchers to follow the development of IoRT security in this area.
- Identified a few implementation issues with IoRT security and potential future study topics where academics might carry out their future research regarding them.

In light of these findings, several recommendations for future research and practice in IoRT security are offered. These include the adoption of threat intelligence and analytics, the integration of security by design principles, the utilization of blockchain technology for enhanced data integrity and auditability, and the implementation of multi-factor authentication mechanisms to strengthen access controls.

CRediT authorship contribution statement

Ehsanul Islam Zafir: Writing – original draft, Resources, Project administration, Methodology, Conceptualization. **Afifa Akter:** Writing – original draft, Visualization, Methodology, Formal analysis, Conceptualization. **M.N. Islam:** Writing – original draft, Conceptualization. **Shahid A. Hasib:** Writing – review & editing, Writing – original draft, Validation, Supervision, Project administration, Methodology, Formal analysis, Conceptualization. **Touhid Islam:** Writing – original draft. **Subrata K. Sarker:** Writing – review & editing, Writing – original draft, Validation, Supervision. **S.M. Muyeen:** Writing – review & editing, Supervision.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Subrata K. Sarker reports was provided by School of Electrical and Data Engineering, University of Technology Sydney, Australia. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgment

The open-access funding of this work will be covered by the University of Technology Sydney through the institutional agreement.

References

[1] O. Vermesan, R. Bahr, M. Ottella, M. Serrano, T. Karlsen, T. Wahlstrøm, H.E. Sand, M. Ashwathnarayan, M.T. Gamba, Internet of robotic things intelligent connectivity and platforms, Front. Robotics AI 7 (2020) 104.
[2] H. Singh, V. Veeraiah, H. Khan, D.K. Singh, V. Talukdar, R. Anand, N. Sindhwani, Investigating scope and applications for the internet of robotics in industrial automation, in: Robotics and Automation in Industry 4.0, CRC Press, 2024, pp. 132–151.
[3] P.P. Ray, Internet of robotic things: Concept, technologies, and challenges, IEEE Access 4 (2016) 9489–9500.
[4] H. Kabir, M.-L. Tham, Y.C. Chang, Internet of robotic things for mobile robots: concepts, technologies, challenges, applications, and future directions, Digit. Commun. Netw. (2023).
[5] A. Sayeed, C. Verma, N. Kumar, N. Koul, Z. Illés, Approaches and challenges in internet of robotic things, Future Internet 14 (9) (2022) 265.
[6] A. Alamer, S. Basudan, Security and privacy of network transmitted system in the internet of robotic things, J. Supercomput. 78 (16) (2022) 18361–18378.
[7] W. Easttom, Modern Cryptography: Applied Mathematics for Encryption and Information Security, Springer, 2022.
[8] B. Sankhyan, A. Baliyan, A. Kumar, Review on symmetric and asymmetric cryptography, 2024.
[9] D. Coppersmith, The Data Encryption Standard (DES) and its strength against attacks, IBM J. Res. Dev. 38 (3) (1994) 243–250.
[10] G.R. Blakley, I. Borosh, Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages, Comput. Math. Appl. 5 (3) (1979) 169–178.
[11] D. Eastlake 3rd, P. Jones, US Secure Hash Algorithm 1 (SHA1), Technical Report, 2001.
[12] S. Heron, Advanced encryption standard (AES), Netw. Secur. 2009 (12) (2009) 8–12.
[13] N. Li, Research on Diffie-Hellman key exchange protocol, in: 2010 2nd International Conference on Computer Engineering and Technology, Vol. 4, IEEE, 2010, pp. V4–634.
[14] S. Terzi, I. Stamelos, Architectural solutions for improving transparency, data quality, and security in eHealth systems by designing and adding blockchain modules, while maintaining interoperability: the eHDSI network case, Health Technol. (2024) 1–12.
[15] E.U. Haque, A. Shah, J. Iqbal, S.S. Ullah, R. Alroobaea, S. Hussain, A scalable blockchain based framework for efficient IoT data management using lightweight consensus, Sci. Rep. 14 (1) (2024) 7841.
[16] T. Koroglu, R. Samet, Can there be a two way hash function? IEEE Access (2024).
[17] A.K. Jakhar, M. Singh, R. Sharma, W. Viriyasitavat, G. Dhiman, S. Goel, A blockchain-based privacy-preserving and access-control framework for electronic health records management, Multimedia Tools Appl. (2024) 1–35.
[18] M. Hajiabbasi, E. Akhtarkavan, B. Majidi, Cyber-physical customer management for internet of robotic things-enabled banking, IEEE Access 11 (2023) 34062–34079.
[19] E. Fazel, M.Z. Nezhad, J. Rezazadeh, M. Moradi, J. Ayoade, IoT convergence with machine learning & blockchain: A review, Internet Things (2024) 101187.
[20] X. Wang, Q. Guo, Z. Ning, L. Guo, G. Wang, X. Gao, Y. Zhang, Integration of sensing, communication and computing for metaverse: A survey, ACM Comput. Surv. (2024).
[21] O. Vermesan, M. Coppola, M.D. Nava, A. Capra, G. Kornaros, R. Bahr, E.C. Darmois, M. Serrano, P. Guillemin, K. Loupos, et al., New waves of IoT technologies research–transcending intelligence and senses at the edge to create multi experience environments, Internet Things–Call Edge. Everything Intell. Everywhere (2020).
[22] M. Andronie, G. Lăzăroiu, M. Iatagan, I. Hurloiu, R. Ştefănescu, A. Dijmărescu, I. Dijmărescu, Big data management algorithms, deep learning-based object detection technologies, and geospatial simulation and sensor fusion tools in the internet of robotic things, ISPRS Int. J. Geo-Inf. 12 (2) (2023) 35.
[23] E. Fosch-Villaronga, T. Mahler, Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots, Comput. Law Secur. Rev. 41 (2021) 105528.
[24] M. Sandhu, D. Silvera-Tawil, P. Borges, Q. Zhang, B. Kusy, Internet of robotic things for independent living: Critical analysis and future directions, Internet Things (2024) 101120.
[25] R. Raman, Z. Gupta, S.V. Akram, L. Thakur, B.G. Pillai, M.K. Chakravarthi, Network security concerns for designing robotic systems: A review, in: 2023 International Conference on Artificial Intelligence and Smart Communication, AISC, IEEE, 2023, pp. 661–665.
[26] H.D. Zubaydi, P. Varga, S. Molnár, Leveraging blockchain technology for ensuring security and privacy aspects in Internet of Things: A systematic literature review, Sensors 23 (2) (2023) 788.

[27] M. Andronie, G. Lăzăroiu, O.L. Karabolevski, R. Ştefănescu, I. Hurloiu, A. Dijmărescu, I. Dijmărescu, Remote big data management tools, sensing and computing technologies, and visual perception and environment mapping algorithms in the internet of robotic things, Electronics 12 (1) (2023) 22.
[28] N. Koul, N. Kumar, A. Sayeed, C. Verma, M.S. Raboca, Data exchange techniques for internet of robotic things: Recent developments, IEEE Access (2022).
[29] P. Simoens, M. Dragone, A. Saffiotti, The internet of robotic things: A review of concept, added value and applications, Int. J. Adv. Robot. Syst. 15 (1) (2018) 1729881418759424.
[30] S. Khalid, Internet of robotic things: A review, J. Appl. Sci. Technol. Trends 2 (03) (2021) 78–90.
[31] A.K. Rana, S. Sharma, S. Dhawan, S. Tayal, Towards secure deployment on the internet of robotic things: architecture, applications, and challenges, Multimodal Biom. Syst. (2021) 135–148.
[32] Rachit, S. Bhatt, P.R. Ragiri, Security trends in Internet of Things: A survey, SN Appl. Sci. 3 (2021) 1–14.
[33] L. Romeo, A. Petitti, R. Marani, A. Milella, Internet of robotic things in smart domains: Applications and challenges, Sensors 20 (12) (2020) 3355.
[34] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, C. Patsakis, Security and privacy analysis of mobile health applications: the alarming state of practice, IEEE Access 6 (2018) 9390–9403.
[35] K. Islam, W. Shen, X. Wang, Wireless sensor network reliability and security in factory automation: A survey, IEEE Trans. Syst. Man Cybern. C 42 (6) (2012) 1243–1256.
[36] A. Kamilaris, N. Botteghi, The penetration of Internet of Things in robotics: Towards a web of robotic things, J. Ambient Intell. Smart Environ. 12 (6) (2020) 491–512.
[37] D. Villa, X. Song, M. Heim, L. Li, Internet of robotic things: Current technologies, applications, challenges and future directions, 2021, arXiv preprint arXiv:2101.06256.
[38] O. Vermesan, A. Bröring, E. Tragos, M. Serrano, D. Bacciu, S. Chessa, C. Gallicchio, A. Micheli, M. Dragone, A. Saffiotti, et al., Internet of Robotic Things: Converging Sensing/actuating, Hypoconnectivity, Artificial Intelligence and IoT Platforms, River Publishers, 2017.
[39] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, Z. Zou, A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things, J. Ind. Inf. Integr. 21 (2021) 100190.
[40] I. Afanasyev, M. Mazzara, S. Chakraborty, N. Zhuchkov, A. Maksatbek, A. Yesildirek, M. Kassab, S. Distefano, Towards the internet of robotic things: Analysis, architecture, components and challenges, in: 2019 12th International Conference on Developments in ESystems Engineering, DeSE, IEEE, 2019, pp. 3–8.
[41] R.S. Batth, A. Nayyar, A. Nagpal, Internet of robotic things: driving intelligent robotics of future-concept, architecture, applications and technologies, in: 2018 4th International Conference on Computing Sciences, ICCS, IEEE, 2018, pp. 151–160.
[42] Y. Meidan, M. Bohadana, A. Shabtai, J.D. Guarnizo, M. Ochoa, N.O. Tippenhauer, Y. Elovici, ProfilIoT: A machine learning approach for IoT device identification based on network traffic analysis, in: Proceedings of the Symposium on Applied Computing, 2017, pp. 506–509.
[43] K.U. Bhat, N. Kumar, N. Koul, C. Verma, F.M. Enescu, M.S. Raboaca, Intelligent communication for internet of things (IoRT), in: Proceedings of International Conference on Recent Innovations in Computing: ICRIC 2022, Volume 2, Springer, 2023, pp. 313–328.
[44] R. Bhandari, V. Kirubanand, Enhanced encryption technique for secure iot data transmission, Int. J. Electr. Comput. Eng. 9 (5) (2019) 3732.
[45] T. Xu, J.B. Wendt, M. Potkonjak, Security of IoT systems: Design challenges and opportunities, in: 2014 IEEE/ACM International Conference on Computer-Aided Design, ICCAD, IEEE, 2014, pp. 417–423.
[46] P.P. Ray, M. Mukherjee, L. Shu, Internet of things for disaster management: State-of-the-art and prospects, IEEE Access 5 (2017) 18818–18835.
[47] M. Maroufi, R. Abdolee, B.M. Tazekand, On the convergence of blockchain and internet of things (iot) technologies, 2019, arXiv preprint arXiv:1904.01936.
[48] P. Radanliev, D. De Roure, S. Cannady, R.M. Montalvo, R. Nicolescu, M. Huth, Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance, 2018.
[49] W. Huifeng, S.N. Kadry, E.D. Raj, Continuous health monitoring of sportsperson using IoT devices based wearable technology, Comput. Commun. 160 (2020) 588–595.
[50] C. Ma, Smart city and cyber-security; technologies used, leading challenges and future recommendations, Energy Rep. 7 (2021) 7999–8012.
[51] S.-H. Chang, C.-H. Hsia, W.-Z. Hong, A secured internet of robotic things (IoRT) for long-term care services in a smart building, J. Supercomput. 79 (5) (2023) 5276–5290.
[52] M. Wan, Z. Zhang, Y. Zhang, Z. He, H. Gu, K. Dai, X. Zou, A chip-PCB hybrid SC PUF used for anti-desoldering and depackaging-attack protection, IEEE J. Solid-State Circuits (2024).
[53] Z. Zhou, C. Xu, S. Yang, X. Zhang, H. Li, S. Huang, G.-M. Muntean, Safeguarding privacy and integrity of federated learning in heterogeneous cross-silo IoRT environments: A moving target defense approach, IEEE Netw. (2024).
[54] R. Salama, S. Alturjman, F. Al-Turjman, A survey of issues, possibilities, and solutions for a blockchain and AI-powered internet of things, in: Computational Intelligence and Blockchain in Complex Systems, Elsevier, 2024, pp. 13–24.
[55] B.A. Devi, M.D. Choudhry, Effective hybrid video denoising and blending framework for internet of remote things (IoRT) environments, Automatika 65 (2) (2024) 510–522.
[56] P. Bothra, R. Karmakar, S. Bhattacharya, S. De, How can applications of blockchain and artificial intelligence improve performance of Internet of Things?–A survey, Comput. Netw. 224 (2023) 109634.
[57] P.P. Darode, S.P. Tagde, S.F.A. Warsi, P. Jaipurkar, Monitoring and controlling robot using IOT.
[58] M.D. Xames, T.G. Topcu, A systematic literature review of digital twin research for healthcare systems: Research trends, gaps, and realization challenges, IEEE Access (2024).
[59] W. Lan, K. Chen, J. Cao, Y. Li, N. Li, Q. Chen, Y. Sahni, Security-sensitive task offloading in integrated satellite-terrestrial networks, 2024, arXiv preprint arXiv:2404.15278.
[60] E. Fujisaki, T. Okamoto, Secure integration of asymmetric and symmetric encryption schemes, in: Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings, Springer, 1999, pp. 537–554.
[61] V. Padmapriya, K. Thenmozhi, M. Hemalatha, V. Thanikaiselvan, C. Lakshmi, N. Chidambaram, A. Rengarajan, Secured IIoT against trust deficit-A flexi cryptic approach, Multimedia Tools Appl. (2024) 1–28.
[62] B. Nourdine, S. Demba, Design of fast cramer-shoup scheme into elliptic curve cryptosystem, JP J. Algebra Number Theory Appl. 63 (2) (2024) 169–184.
[63] D.D. Kumar, J.D. Mukharzee, C.V.D. Reddy, S.M. Rajagopal, Safe and secure communication using SSL/TLS, in: 2024 International Conference on Emerging Smart Computing and Informatics, ESCI, IEEE, 2024, pp. 1–6.
[64] T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2, Technical Report, 2008.
[65] M.R. Ali, D. Pal, A. Das, D.R. Chowdhury, HARPOCRATES: An approach towards efficient encryption of data-at-rest, IEEE Trans. Emerg. Top. Comput. (2024).
[66] V. Sidorov, W.K. Ng, Transparent data encryption for data-in-use and data-at-rest in a cloud-based database-as-a-service solution, in: 2015 IEEE World Congress on Services, IEEE, 2015, pp. 221–228.
[67] K. Zhu, Z. Wang, D. Ding, H. Dong, C.-Z. Xu, Secure state estimation for artificial neural networks with unknown-but-bounded noises: A homomorphic encryption scheme, IEEE Trans. Neural Netw. Learn. Syst. (2024).
[68] S. Gupta, R. Cammarota, T. Šimunić, Memfhe: End-to-end computing with fully homomorphic encryption in memory, ACM Trans. Embedded Comput. Syst. 23 (2) (2024) 1–23.

[69] A. Acar, H. Aksu, A.S. Uluagac, M. Conti, A survey on homomorphic encryption schemes: Theory and implementation, ACM Comput. Surv. (Csur) 51 (4) (2018) 1–35.
[70] C. BOURA, Appendix 1: Data encryption standard (DES), Symmetr. Cryptogr. 1: Des. Secur. Proofs (2024) 195–203.
[71] M.R. Rabtsani, A. Triayudi, G. Soepriyono, Combination of AES (advanced encryption standard) and SHA256 algorithms for data security in bill payment applications, SAGA: J. Technol. Inf. Syst. 2 (1) (2024) 175–189.
[72] K. Nistrina, R. Rustiyana, R. Rosmalina, N.S. Rahayu, R.P. Permana, MD5 in a web-based population data management application to improve account security, J. Mantik 8 (1) (2024) 45–54.
[73] R. Rivest, The MD5 Message-Digest Algorithm, Technical Report, 1992.
[74] O.E. Famous, S.E. Adewunmi, V. Yemi-Peters, A comparative review of five leading document management systems based on information security, 2024.
[75] R. Rahul, S. Geetha, S. Priyatharsini, K. Mehata, T.S. Perumal, N. Ethiraj, S. Sendilvelan, Cybersecurity Issues and Challenges in Quantum Computing, Wiley Telecom, 2024.
[76] K. Sasikumar, S. Nagarajan, Comprehensive review and analysis of cryptography techniques in cloud computing, IEEE Access (2024).
[77] R.C. Merkle, A certified digital signature, in: Advances in Cryptology—CRYPTO'89 Proceedings, Springer, 2001, pp. 218–238.
[78] R. Mathews, D.V. Jose, Hybrid homomorphic-asymmetric lightweight cryptosystem for securing smart devices: A review, Trans. Emerg. Telecommun. Technol. 35 (1) (2024) e4866.
[79] B. Acharya, S.K. Panigrahy, S.K. Patra, G. Panda, Image encryption using advanced hill cipher algorithm, Int. J. Recent Trends Eng. 1 (1) (2009) 663–667.
[80] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: A survey, Int. J. Web Grid Serv. 14 (4) (2018) 352–375.
[81] A. O'Neill, Deterministic public-key encryption revisited, Cryptol. ePrint Arch. (2010).
[82] P. De Filippi, The interplay between decentralization and privacy: the case of blockchain technologies, J. Peer Prod. (7) (2016).
[83] L. Guo, H. Xie, Y. Li, Data encryption based blockchain and privacy preserving mechanisms towards big data, J. Vis. Commun. Image Represent. 70 (2020) 102741.
[84] J. Sunny, N. Undralla, V.M. Pillai, Supply chain transparency through blockchain-based traceability: An overview with demonstration, Comput. Ind. Eng. 150 (2020) 106895.
[85] L.W. Cong, Z. He, Blockchain disruption and smart contracts, Rev. Financ. Stud. 32 (5) (2019) 1754–1797.
[86] U.S. Aditya, R. Singh, P.K. Singh, A. Kalla, A survey on blockchain in robotics: Issues, opportunities, challenges and future directions, J. Netw. Comput. Appl. 196 (2021) 103245.
[87] M. Albonico, A. Rohling, J. Santos, P. Varela, Mining evidences of Internet of Robotic Things (IoRT) software from open source projects, in: 15th Brazilian Symposium on Software Components, Architectures, and Reuse, 2021, pp. 71–79.
[88] C. Cachin, M. Vukolić, Blockchain consensus protocols in the wild, 2017, arXiv preprint arXiv:1707.01873.
[89] T. Wang, K. Chen, Z. Zheng, J. Guo, X. Zhao, S. Zhang, PrivShieldROS: An extended robot operating system integrating ethereum and interplanetary file system for enhanced sensor data privacy, Sensors 24 (10) (2024) 3241.
[90] A. Echikr, A. Yachir, C.A. Kerrache, Z. Sahraoui, Exploring the potential of blockchain in internet of robotic things: Advancements, challenges, and future directions, in: 2023 International Conference on Networking and Advanced Systems, ICNAS, IEEE, 2023, pp. 1–6.
[91] N. Kathirvel, S. Bharat, A. Kathirvel, C. Maheswaran, Artificial General-Internet of Things (AG-IOT) for robotics of automation, Syst. Anal. 2 (1) (2024) 59–76.
[92] T. Zhukabayeva, A. Buja, M. Pacolli, Evaluating security mechanisms for wireless sensor networks in IoT and iIoT, J. Robot. Control (JRC) 5 (4) (2024) 931–943.
[93] A.L. López, D.B. Jaramillo, P.D. Salgado, B.S. Muñoz, L.J. Montaño, Integration of emerging technologies in the industrial internet of things to improve efficiency, Nanotechnol. Percept. (2024) 62–72.
[94] T. Huang, Z. Fang, Q. Tang, R. Xie, T. Chen, R. Zhang, F.R. Yu, Integrated computing and networking for LEO satellite mega-constellations: Architecture, challenges and open issues, IEEE Wirel. Commun. (2024).
[95] A. Gervais, G.O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, S. Capkun, On the security and performance of proof of work blockchains, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 3–16.
[96] C.T. Nguyen, D.T. Hoang, D.N. Nguyen, D. Niyato, H.T. Nguyen, E. Dutkiewicz, Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities, IEEE Access 7 (2019) 85727–85745.
[97] F. Yang, W. Zhou, Q. Wu, R. Long, N.N. Xiong, M. Zhou, Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism, IEEE Access 7 (2019) 118541–118555.
[98] S. Alrubei, E. Ball, J. Rigelsford, Securing IoT-blockchain applications through honesty-based distributed proof of authority consensus algorithm, in: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA, IEEE, 2021, pp. 1–7.
[99] Y. Li, L. Qiao, Z. Lv, An optimized byzantine fault tolerance algorithm for consortium blockchain, Peer-to-Peer Netw. Appl. 14 (2021) 2826–2839.
[100] S. Gao, T. Yu, J. Zhu, W. Cai, T-PBFT: An EigenTrust-based practical Byzantine fault tolerance consensus algorithm, China Commun. 16 (12) (2019) 111–123.
[101] M. Kaur, M.Z. Khan, S. Gupta, A. Noorwali, C. Chakraborty, S.K. Pani, MBCP: Performance analysis of large scale mainstream blockchain consensus protocols, IEEE Access 9 (2021) 80931–80944.
[102] S. Aggarwal, N. Kumar, Cryptographic consensus mechanisms, in: Advances in Computers, vol. 121, Elsevier, 2021, pp. 211–226.
[103] M.A. Alrowaily, M. Alghamdi, I. Alkhazi, A.B. Hassanat, M.M.S. Arbab, C.Z. Liu, Modeling and analysis of proof-based strategies for distributed consensus in blockchain-based peer-to-peer networks, Sustainability 15 (2) (2023) 1478.
[104] F. Chahal, D. Gaiti, H. Fouchal, Consensus algorithms in cryptocurrency and V2X-IoT: Preliminary study, in: Innovations for Community Services: 22nd International Conference, I4CS 2022, Delft, The Netherlands, June 13–15, 2022, Proceedings, Springer, 2022, pp. 63–74.
[105] G.A.F. Rebello, G.F. Camilo, L.C. Guimaraes, L.A.C. de Souza, G.A. Thomaz, O.C.M. Duarte, A security and performance analysis of proof-based consensus protocols, Ann. Telecommun. (2021) 1–21.
[106] A. Sękala, T. Blaszczyk, K. Foit, G. Kost, Selected issues, methods, and trends in the energy consumption of industrial robots, Energies 17 (3) (2024) 641.
[107] J.-P.A. Yaacoub, H.N. Noura, O. Salman, A. Chehab, Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations, Int. J. Inf. Secur. (2022) 1–44.
[108] A. Singh Rajawat, P. Bedi, S. Goyal, P.K. Shukla, A. Zaguia, A. Jain, M. Monirujjaman Khan, Reformist framework for improving human security for mobile robots in industry 4.0, Mob. Inf. Syst. 2021 (2021) 1–10.
[109] S. Yarradoddi, T.R. Gadekallu, Federated learning role in big data, jot services and applications security, privacy and trust in jot a survey, in: Trust Secur. Priv. Big Data, CRC Press, 2022, pp. 28–49.
[110] S. Hong, Y. Hwang, Design and implementation for iort based remote control robot using block-based programming, Issues Inf. Syst. 21 (4) (2020) 317–330.
[111] A. Alamer, A secure anonymous tracing fog-assisted method for the internet of robotic things, Libr. Hi Tech 40 (4) (2022) 1081–1103.
[112] M. Siergiejczyk, K. Krzykowska-Piotrowska, P. Olearnik, Companion robot communication with road infrastructure as part of iort, Internet Technol. Lett. (2024) e500.

[113] P. Selvaraj, V.K. Burugari, S. Gopikrishnan, A. Alourani, G. Srivastava, M. Baza, An enhanced and secure trust-aware improved GSO for encrypted data sharing in the Internet of Things, Appl. Sci. 13 (2) (2023) 831.
[114] B. Yankson, T. Loucks, A. Sampson, C. Lojano, Robots security assessment and analysis using open-source tools, in: International Conference on Cyber Warfare and Security, Vol. 18, No. 1, 2023, pp. 449–456.
[115] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, S. Moussa, Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective, Sustainability 15 (4) (2023) 3317.
[116] B. Wang, J. Li, Efficient ciphertext retrieval in Internet of Things based on fog consumption computing system, in: Proceedings of the World Conference on Intelligent and 3-D Technologies (WCI3DT 2022) Methods, Algorithms and Applications, Springer, 2023, pp. 169–181.
[117] A.K. Mishra, N. Tripathi, P. Bagla, N.K. Pandey, S. Mittal, D.S. Rana, Optimize a novel integrated solutions to analyses privacy persevering of the Internet of Things, in: 2023 6th International Conference on Information Systems and Computer Networks, ISCON, IEEE, 2023, pp. 1–6.
[118] D. Chawla, P.S. Mehra, A survey on quantum computing for Internet of Things security, Procedia Comput. Sci. 218 (2023) 2191–2200.
[119] H. Sakly, M. Said, A.A. Al-Sayed, C. Loussaief, R. Sakly, J. Seekins, Blockchain technologies for Internet of Medical Things (BIoMT) based healthcare systems: A new paradigm for COVID-19 pandemic, in: Trends of Artificial Intelligence and Big Data for E-Health, Springer, 2023, pp. 139–165.
[120] K. Qian, Y. Liu, X. He, M. Du, S. Zhang, K. Wang, HPCchain: A consortium blockchain system based on CPU-FPGA hybrid PUF for industrial Internet of Things, IEEE Trans. Ind. Inform. (2023).
[121] H. Xue, D. Chen, N. Zhang, H.-N. Dai, K. Yu, Integration of blockchain and edge computing in Internet of Things: A survey, Future Gener. Comput. Syst. 144 (2023) 307–326.
[122] M. Shen, A. Gu, J. Kang, X. Tang, X. Lin, L. Zhu, D. Niyato, Blockchains for artificial intelligence of things: A comprehensive survey, IEEE Internet Things J. (2023).
[123] A.M.A. Alamer, S.A.M. Basudan, P.C. Hung, A privacy-preserving scheme to support the detection of multiple similar request-real-time services in IoT application systems, Expert Syst. Appl. 214 (2023) 119005.
[124] X. Zhou, W. Liang, I. Kevin, K. Wang, Z. Yan, L.T. Yang, W. Wei, J. Ma, Q. Jin, Decentralized P2P federated learning for privacy-preserving and resilient mobile robotic systems, IEEE Wirel. Commun. 30 (2) (2023) 82–89.
[125] C.-Y. Lin, S.-C. Wu, P.-H. Kuo, M.-J. Huang, S.-W. Hong, H.-T. Yau, Application of chaotic encryption and decryption in wireless transmission from sensory toolholders on machine tools, IEEE Sens. J. (2023).
[126] B.S. Egala, A.K. Pradhan, P. Dey, V. Badarla, S.P. Mohanty, Fortified-chain 2.0: Intelligent blockchain for decentralized smart healthcare system, IEEE Internet Things J. (2023).
[127] S.U.A. Laghari, S. Manickam, A.K. Al-Ani, M.A. Al-Shareeda, S. Karuppayah, ES-SECS/GEM: An efficient security mechanism for SECS/GEM communications, IEEE Access 11 (2023) 31813–31828.
[128] S. Sarowa, V. Kumar, B. Bhanot, M. Kumar, Enhancement of security posture in smart farming: Challenges and proposed solution, in: 2023 International Conference on Device Intelligence, Computing and Communication Technologies, DICCT, IEEE, 2023, pp. 1–5.
[129] S.-H. Chang, C.-H. Hsia, W.-Z. Hong, A secured internet of robotic things (IoRT) for long-term care services in a smart building, J. Supercomput. (2022) 1–15.
[130] H.E. Kiran, A. Akgul, O. Yildiz, A new chaos-based lightweight encryption mechanism for microcomputers, in: 2022 10th International Symposium on Digital Forensics and Security, ISDFS, IEEE, 2022, pp. 1–5.
[131] M. Finochietto, R.M. Santos, S.F. Ochoa, R. Meseguer, Reducing Operational Expenses of Lorawan-Based Solutions that Connect Urban and Rural Areas, Available at SSRN 4181570.
[132] L. Sapra, A. Mathani, G. Bhatnagar, A thorough analysis of blockchain's potential for internet of things applications in precision agricultural networks, Math. Stat. Eng. Appl. 71 (4) (2022) 4141–4159.
[133] W. ten Brink, B. Vasilache, K. Wrona, N. Suri, Towards integration of command and control systems with Internet of Things, Procedia Comput. Sci. 205 (2022) 157–166.
[134] U. Maroof, A. Shaghaghi, R. Michelin, S. Jha, iRECOVer: Patch your IoT on-the-fly, Future Gener. Comput. Syst. 132 (2022) 178–193.
[135] A. Keerthana, Performance assessment of IoMT services and protocols, in: The Internet of Medical Things (IoMT) Healthcare Transformation, Wiley Online Library, 2022, pp. 173–186.
[136] J.-P.A. Yaacoub, H.N. Noura, O. Salman, A. Chehab, Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations, Internet Things (2022) 100544.
[137] M. Darbandi, A.F. Alrasheedi, K.A. Alnowibet, D. Javaheri, A. Mehbodniya, Integration of cloud computing with the internet of things for the treatment and management of the COVID-19 pandemic, Inf. Syst. e-Bus. Manag. (2022) 1–30.
[138] P. Singh, Z. Elmi, V.K. Meriga, J. Pasha, M.A. Dulebenets, Internet of Things for sustainable railway transportation: Past, present, and future, Clean. Logist. Supply Chain 4 (2022) 100065.
[139] R. Uddin, S. Kumar, SDN-based federated learning approach for satellite-IoT framework to enhance data security and privacy in space communication, in: 2022 IEEE International Conference on Wireless for Space and Extreme Environments, WiSEE, IEEE, 2022, pp. 71–76.
[140] M. Zhdanova, Security and Trust in Safety Critical Infrastructures, Technische Universität Darmstadt, 2022.
[141] N. Ambika, Enhancing security in IoT instruments using artificial intelligence, in: IoT and Cloud Computing for Societal Good, Springer, 2022, pp. 259–276.
[142] V. Dutta, T. Zielińska, Cybersecurity of robotic systems: Leading challenges and robotic system design methodology, Electronics 10 (22) (2021) 2850.
[143] T. Anusha, M. Pushpalatha, Enhancements in communication protocols that powered IoRT, Human Commun. Technol.: Internet Robot. Things Ubiquitous Comput. (2021) 193–217.
[144] B. Ramalingam, T. Tun, R.E. Mohan, B.F. Gómez, R. Cheng, S. Balakrishnan, M. Mohan Rayaguru, A.A. Hayat, Ai enabled IoRt framework for rodent activity monitoring in a false ceiling environment, Sensors 21 (16) (2021) 5326.
[145] S.G. Devi, C. Nalini, Automated verification and validation of IoRT systems, Human Commun. Technol.: Internet Robot. Things Ubiquitous Comput. (2021) 55–89.
[146] Y. Masuda, A. Zimmermann, S. Shirasaka, O. Nakamura, Internet of robotic things with digital platforms: Digitization of robotics enterprise, in: Human Centred Intelligent Systems, Springer, 2021, pp. 381–391.
[147] A. Kumar, S. Sharma, Internet of robotic things: Design and develop the quality of service framework for the healthcare sector using CoAP, IAES Int. J. Robot. Autom. 10 (4) (2021) 289.
[148] V.A. Kokovin, A.A. Evsikov, V.I. Diagilev, V.V. Skvortsov, S.U. Uvaysov, A.S. Uvaysova, Design of functional networking components as elements of an industrial ecosystems, in: 2021 International Seminar on Electron Devices Design and Production, SED, IEEE, 2021, pp. 1–5.
[149] R. Krishnamoorthy, T. Bikku, V. Priyalakshmi, M. Amina Begum, S. Arun, A concept of internet of robotic things for smart automation, in: Emergence of Cyber Physical System and IoT in Smart Automation and Robotics, Springer, 2021, pp. 83–102.
[150] A. Siriweera, K. Naruse, Internet of cross-chains: Model-driven cross-chain as a service platform for the internet of everything in smart city, IEEE Consum. Electron. Mag. (2021).
[151] M. Debbah, H. Zhang, W. Saad, L. Song, Guest editorial: Special issue on internet of UAVs over cellular networks, IEEE Internet Things J. 8 (12) (2021) 9774–9775.
[152] R. Sawant, A. Shaikh, C. Singh, A. Aggarwal, S.A. Wagle, A Bibliometric Perspective Survey of IoT controlled AI based Swarm robots.

[153] Y. Cai, D. Li, Y. Wang, Intelligent crime prevention and control big data analysis system based on imaging and capsule network model, Neural Process. Lett. 53 (4) (2021) 2485–2499.
[154] P. Bothra, R. Karmakar, S. Bhattacharya, S. De, How can applications of blockchain and artificial intelligence improve performance of Internet of Things?–A survey, 2021, arXiv preprint arXiv:2111.14018.
[155] M. Arduengo, L. Sentis, The robot economy: Here it comes, Int. J. Soc. Robot. 13 (5) (2021) 937–947.
[156] M. Salhaoui, et al., Smart IoT monitoring and real-time control based on autonomous robots, visual recognition and cloud/edge computing services, 2021.
[157] A. Kumar, S. Sharma, A. Singh, A. Alwadain, B.-J. Choi, J. Manual-Brenosa, A. Ortega-Mansilla, N. Goyal, Revolutionary strategies analysis and proposed system for future infrastructure in Internet of Things, Sustainability 14 (1) (2022) 71.
[158] A. Vick, C. Krause, J. Krüger, Networked visual servoing as use-case for cloud-based industrial robot control, in: IECON 2020 the 46th Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2020, pp. 763–768.
[159] A. Alamer, A secure anonymous tracing fog-assisted method for the internet of robotic things, Libr. Hi Tech (2020).
[160] Z. Alsulaimawi, A privacy filter framework for internet of robotic things applications, in: 2020 IEEE Security and Privacy Workshops, SPW, IEEE, 2020, pp. 262–267.
[161] N. El Menbawy, H. Arafat, M. Saraya, A.M. Ali-Eldin, Studying and analyzing the fog-based internet of robotic things, in: 2020 21st International Arab Conference on Information Technology, ACIT, IEEE, 2020, pp. 1–8.
[162] K. Yang, Y. Shi, Y. Zhou, Z. Yang, L. Fu, W. Chen, Federated machine learning for intelligent IoT via reconfigurable intelligent surface, IEEE Netw. 34 (5) (2020) 16–22.
[163] J. Shreyas, A. Jumnal, S.D. Kumar, K. Venugopal, Application of computational intelligence techniques for internet of things: an extensive survey, Int. J. Comput. Intell. Stud. 9 (3) (2020) 234–288.
[164] A. Kaknjo, M. Rao, E. Omerdic, T. Newe, D. Toal, Real-time secure/unsecure video latency measurement/analysis with FPGA-based bump-in-the-wire security, Sensors 19 (13) (2019) 2984.
[165] A. Omidkar, S.A. Roudi, R. Abbas, J. Lam, IoT and satellite based 5G network security, 2019.
[166] Z. Yin, M. Jia, W. Wang, N. Cheng, F. Lyu, Q. Guo, X. Shen, Secrecy rate analysis of satellite communications with frequency domain NOMA, IEEE Trans. Veh. Technol. 68 (12) (2019) 11847–11858.
[167] B. Li, Z. Fei, C. Zhou, Y. Zhang, Physical-layer security in space information networks: A survey, IEEE Internet Things J. 7 (1) (2019) 33–52.
[168] N. Aguirre, N. Aranda, N. Balich, Seguridad en el envío de mensajes mediante protocolo MQTT en IoT, Innova Untref (2019).
[169] Z. Zhang, Applied Machine Learning for Multi-Sensory Robot Perception, Colorado School of Mines, 2019.
[170] X.V. Wang, L. Wang, Digital twin-based WEEE recycling, recovery and remanufacturing in the background of Industry 4.0, Int. J. Prod. Res. 57 (12) (2019) 3892–3902.
[171] K. Raveendranathan, Future directions: Iot, robotics and AI based applications, in: Modern Optimization Methods for Science, Engineering and Technology, IOP Publishing, 2019.
[172] L. Cui, Complex industrial automation data stream mining algorithm based on random internet of robotic things, Automatika: čas. Autom. Mjerenje Elektroniku Računarstvo Komunikacije 60 (5) (2019) 570–579.
[173] A.A. Jaafar, K.H. Sharif, M.I. Ghareb, D.N. Jawawi, Internet of Thing and smart city: State of the art and future trends, Adv. Comput. Commun. Comput. Sci. (2019) 3–28.
[174] S. Bartling, Blockchain for science and knowledge creation, in: Gesundheit Digital, Springer, 2019, pp. 159–180.
[175] S. Babu, S. Markose, IoT enabled robots with QR code based localization, in: 2018 International Conference on Emerging Trends and Innovations in Engineering and Technological Research, ICETIETR, IEEE, 2018, pp. 1–5.
[176] S.G. Tzafestas, The Internet of Things: A conceptual guided tour, Eur. J. Adv. Eng. Technol. 5 (10) (2018) 745–767.
[177] V. Loscrì, Toward Interoperability of Heterogeneous Self-organizing (Smart) Things (Ph.D. thesis), University of Lille 1, 2018.
[178] K.A. Kessel, A.W. Lee, S.M. Bentzen, B. Vikram, F. Nuesslin, S.E. Combs, Data-Based Radiation Oncology–Design of Clinical Trials, Frontiers Media SA, 2018.
[179] K. Vu, B. Miller, J. Vander Molen, S. Otieno, Single-fraction vs multifraction radiation therapy for palliative bone metastases., Radiat. Ther. 26 (2) (2017).
[180] J. Yao, V.J. Zimmer, S. Zeng, A Tour Beyond BIOS: Using IOMMU for DMA Protection in UEFI Firmware, Technical Report, 2017, Retrieved 2021-08-16 from https://firmware.intel.com/sites/default/files....
[181] J.P. Zappen, Digital rhetoric and the Internet of Things, in: Theorizing Digital Rhetoric, Routledge, 2017, pp. 55–67.
[182] V. Kouh Daragh, A heterogeneous communications network for smart grid by using the cost functions, 2017.
[183] V.A. Zamora, Cross-Layer Design Applied to Small Satellites for Data Collection (Ph.D. thesis), Université Montpellier, 2017.
[184] B. Breiling, B. Dieber, P. Schartner, Secure communication for the robot operating system, in: 2017 Annual IEEE International Systems Conference, SysCon, IEEE, 2017, pp. 1–6.
[185] B. Dieber, S. Kacianka, S. Rass, P. Schartner, Application-level security for ROS-based applications, in: 2016 IEEE/RSJ International Conference on Intelligent Robots and Systems, IROS, IEEE, 2016, pp. 4477–4482.
[186] H. Hellaoui, M. Koudil, A. Bouabdallah, Energy-efficient mechanisms in security of the Internet of Things: A survey, Comput. Netw. 127 (2017) 173–189.
[187] J. White, The Proceedings of ACRO 2016, Springer.
[188] G. Hägele, D. Söffker, Fall-back layer concept for autonomous or semi-autonomous systems and processes: requirements, concepts, and first tests, in: 2016 IEEE International Conference on Systems, Man, and Cybernetics, SMC, IEEE, 2016, pp. 000916–000921.
[189] C. Cadena, A.R. Dick, I.D. Reid, Multi-modal auto-encoders as joint estimators for robotics scene understanding., in: Robotics: Science and Systems, vol. 5, no. 1, 2016.
[190] B.L. Harper, Nyxbot Robotic System: The Investigation of the Feasible Design of a CCC/C3 System for the Secured Wireless Control of a Remote Controlled Robot (Ph.D. thesis), Alabama Agricultural and Mechanical University, 2016.
[191] M.M. Chen, F.C. Holsinger, Morbidity and mortality associated with robotic head and neck surgery: an inquiry of the food and drug administration manufacturer and user facility device experience database, JAMA Otolaryngol.-Head Neck Surg. 142 (4) (2016) 405–406.
[192] F. Fuertes-Guiró, A program of telementoring in robotic bariatric surgery, in: EDULEARN16 Proceedings, IATED, 2016, pp. 5747–5750.
[193] D. Godfrey, J. Bannock, O. Kuzmina, T. Welton, T. Albrecht, A robotic platform for high-throughput electrochemical analysis of chalcopyrite leaching, Green Chem. 18 (7) (2016) 1930–1937.
[194] J.M. Carson III, F. Amzajerdian, G.D. Hines, T.V. O'Neal, E.A. Robertson, C. Seubert, N. Trawny, COBALT: A GN&C payload for testing ALHAT capabilities in closed-loop terrestrial rocket flights, in: AIAA Space 2016 Conference, No. JSC-CN-35512, 2016.
[195] L.G. Morris, R.J. Wong, R.M. Tuttle, Ethical considerations when counseling patients with thyroid cancer about surgery vs observation, JAMA Otolaryngol.-Head Neck Surg. 142 (4) (2016) 406–407.