Multidisciplinary Reviews

CONFERENCE PAPER
Published Online: December 01, 2025
https://doi.org/10.31893/multirev.2025ss0106

Global Challenges, Local Solutions: Engineering, Science, and Technology in Developing Regions

Mechanisms for ensuring the security of collaborative robot systems in industrial settings

Prakhar Goyal[a] | Kothakonda Sairam[b] | Nihar Ranjan Nayak[c] | Sasanka Choudhury[d] | A. Aranganathan[e] | Suneetha K[f] | Gagan Tiwari[g]

[a]Quantum University Research Center, Quantum University, Roorkee, Uttarakhand, India.
[b]Centre for Multidisciplinary Research, Anurag University, Hyderabad, Telangana, India.
[c]Department of Computer Science and Engineering, Presidency University, Bengaluru, Karnataka, India.
[d]Department of Mechanical Engineering, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India.
[e]Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India.
[f]Department of Computer Science and Information Technology, JAIN (Deemed-to-be University), Bangalore, Karnataka, India.
[g]Department of Computer Science, Noida International University, Greater Noida, Uttar Pradesh, India.

Abstract Manufacturing is being revolutionized by Industrial Collaborative Robots (Cobots), which facilitate safe and effective human–machine cooperation. Cobots are flexible, function without physical barriers, and integrate seamlessly into production lines, in contrast to traditional robots. The Industrial Internet of Things (IIoT) and cloud connection are driving their wider use. However, there are serious safety risks associated with this evolution, such as illegal access, data breaches, and operational interruptions. Because cybersecurity principles are not fully integrated into system architecture, cobots are still vulnerable despite progress. Poor IT and OT network segmentation, outdated firmware, a lack of real-time monitoring, and uneven safety standards are some of the main drawbacks. The majority of cobots are ill-equipped to handle complex threats like data poisoning and AI model modification. The purpose of this review is to analyse the security issues that collaborative robot systems are now facing and investigate workable solutions that guarantee operational integrity and safety in networked industrial settings. Cyber-physical vulnerabilities, current attack vectors (such as network spoofing and illegal firmware access), and security best practices are the main topics of the paper's thorough literature assessment. It combines results from industry case studies and scholarly research to pinpoint gaps and suggest solutions. Cobot-related dangers are considerably decreased by important strategies including network segmentation, role-based access control (RBAC), frequent patch management, intrusion detection systems (IDS), and physical security enforcement. Every method has its own benefits, ranging from limiting user permissions and separating risks to stopping malware from spreading and instantly identifying unusual activity. A multilayered protection approach integrating operational, technical, and physical precautions is necessary to secure collaborative robot systems. A proactive, coordinated strategy combining robotics engineers, cybersecurity specialists, and industry stakeholders is crucial to guaranteeing robust and reliable deployments as cobots become increasingly autonomous and integrated with external data sources.

Keywords: industrial internet of things (IIoT), cyber-physical vulnerabilities, role-based access control (RBAC), intrusion

1. Introduction

The ability of various building robotics to replace various production machines has not been extensively investigated in light of the present building machinery replacement scenario. The fundamentals of the task–technology match concept concentrate on project competency traits that develop a theoretical basis for discussing human–task machines within the building industry. Thus, it highlights the existing state of machinery replacement in the construction industry and the growth possibilities of various construction robotics (Ma et al., 2022). The authors presented ways to overcome current issues in soft robotic control, sensing, and actuation by leveraging intrinsic phases. Methods for building fully soft logical components that employ instability to provide soft robotics materials with knowledge and dispersed computational abilities are also reviewed. Such mechanical disturbances offer a novel way to achieve powerful output amplifiers and outstanding actuator rates via quick transitions from structurally stable modes (Pal et al., 2021).

Traditional industrial robotic systems call for bulky barrier guards requiring ancillary security apparatuses, which limits adaptability and raises prices and the needed area. However, the present marketplace requires quicker turnaround times and widespread customization. Given that it blends personal judgement, planning, and reaction skills alongside the robot's power and consistency, cooperation factories and colleagues who are both humans and robots are enabled to cooperate to do jobs together side by hand. An enormous number of production robots have been employed to substitute or aid persons in

different tedious and dangerous manufacturing activities. To effectively combine human and robotic abilities, innovative methods for human and robot interaction are essential (Matheson et al., 2019).

It was especially eager to learn about the security criteria, as well as the techniques and difficulties associated with ensuring security. Important functional specifications, collaborative options, standardizations, and security methods will be addressed regarding the current state of the current practice of cobot security monitoring (Bi et al., 2021). A possible way to overcome this limitation is offered by providing safety-rated modification dimensions and determining permissible variants that indicate the maximum changes that can be made to the software or system while still complying with safety standards. According to the abovementioned alteration restrictions, modifications to the framework can be performed without performing a fresh risk evaluation to a model-based technique that is suggested. The proposed approach creates a brand-new security paradigm for collaborative robotic applications that guarantees versatility and upholds security criteria (Brandstötteet et al., 2020). The development and validation of an assortment of rules regarding the creation of the characteristics defining the end product. Enhancing employee protection while operating in a shared location is a key focus (Gualtieri et al., 2022).

Using the most recent ISO standards and manufacturing circumstances, an assortment of security signals and a framework for evaluation were created. To ensure the security of cooperation between humans and robots while preserving the highest level of output, a dynamically adjusted (speeding and spacing measurement) system is given. On a teamwork cell employing a six-degree-of-freedom industry machine, this approach has been empirically proven (Liu et al., 2020).

An evaluation of sensory devices for people identification and recognition of action in workplaces. The creators also presented two examples of concepts for potential collaborative applications of robotics that take advantage of improved perceptions and engagement capacities. In the initial instance, a method for protecting people in jobs involving avoiding collisions or identifying movement objects was suggested. It is related to fixed-base collaborative robots (Bonci et al., 2021).

Collaborative robots—commonly referred to as cobots—are gaining significant traction in advanced manufacturing environments (Levratti et al., 2019). Both industrial applications and academic investigations in this area are evolving at a rapid pace. This review summarizes recent developments in robotics and outlines future directions for cobot integration, particularly within the context of Industry 4.0 and global innovation trends. This study contributes valuable insights, as relatively few publications have addressed the topic of human–robot collaboration in depth. In addition, researchers have proposed two dynamic methods to continuously regulate robot speed within a team-oriented framework, following the speed and separation monitoring (SSM) principle, and assessed their performance. The findings indicated that the proposed methods offered clear benefits over conventional safety mechanisms by enabling faster deployment across various test conditions. The experiments also highlighted multiple factors that should be considered during system design (Byner et al., 2019).

The necessary degree of security throughout the interaction between humans and machines and the essential duties of collaborative machines when carrying out certain tasks systematized the most recent (Kildal et al., 2019). The present study provides a comprehensive examination of the security of modern machines, addresses the use of risk evaluation methods to provide extra security in automated systems, and suggests a roadmap for safety compliance features to be incorporated into artificial system design. To evaluate the important science and technology advancements that concurrently enhance both mental and physical welfare, efficiency, effectiveness, and long-term viability are needed to rapidly adapt the workplace for both humans and cobots. Principles and suggestions to aid innovators in technology in creating systems that put people at the core of the structure and provide a healthy and secure setting, in addition to the technologies (Khalid et al., 2018).

This research aims to examine the security concerns involved in the implementation of collaborative robots within industrial settings. It focuses on addressing major cyber and physical vulnerabilities and evaluates effective security measures—such as applying network segmentation, enforcing strict access controls, and incorporating intrusion detection techniques—to ensure the safe, dependable, and secure operation of cobots in a smart manufacturing environment.

The organization of the research involves 5 sections. Phase 2 involves security threats in the Cobots system. Phase 3 contains the key solutions that overcome the threats for the effective cobot system. Phase 4 contains a discussion of the research, and Phase 5 includes the conclusion.

2. Security challenges and vulnerabilities in industrial collaborative robot systems

This section describes how cobasics have transformed and improved industrial processes through the use of cyber- or physical security threats. As cobots are becoming increasingly integrated with IoT technologies and cloud systems, the risks of unauthorized access or data breaches and undesirable interactions are rapidly emerging. It is vital to have a cohesive and coordinated approach to ensure the safety of their operation in smart environment systems.

Cobots are revolutionizing industrial processes by working with human operators without the use of physical barriers. Cobots differ from conventional robots because they are safe in terms of design, flexible, and easy to integrate, enabling a wide variety of applications, such as assembly, packaging, quality control, and material handling. Because they tend to be small, easy to program, and flexible, even small manufacturers can easily realize the benefits of automation. With the

expansion of Industry 4.0, cobots are increasingly being connected in IoT networks and cloud systems to facilitate real-time data sharing, remote monitoring, and performance enhancement. The connectivity opens up considerable cybersecurity and operational integrity questions that need to be addressed for robust and dependable implementation (Pizoń et al., 2022).

Most industrial system cobots, known as cyber- or physical security threats, have been identified. Cobots are connected devices that are vulnerable to being breached in several different ways and exposed to cyberattacks such as unauthorized access, data interception, and command spoofing (Ananias et al., 2022). A compromised cobot behaves in ways that are not planned. Physical threats such as universal serial bus (USB) insertion or reprogramming cooperate with their integrity, undermining the safety measures in place to control robot actions. Additionally, cobots reliant upon third-party software or open-source libraries might incorporate security flaws into the software itself or its application. Increased knowledge of hazards can help build the security layers necessary to safeguard the physical integrity and functional capacity of cobot systems.

One of the key challenges in securing collaborative robot systems is their susceptibility to network-based attacks (Tasooji & Marquez, 2022). The growing use of wireless communication, remote access, and cloud connectivity has increased the exposure of cobots to data breaches, injected unauthorized commands, and software tampering. Industrial settings often lack stringent segmentation between operational technology (OT) and information technology (IT) systems, making it easy for potential lateral attacks to occur. In addition, outdated software, unpatched vulnerabilities, and default access controls expose cobots to risks. Detecting unusual behavior without sophisticated detection mechanisms is challenging, and responses to such threats that are late might cause disruptions to operations, safety events, or long-term damage to industrial infrastructure.

The secure deployment of cobots is made more uncertain by physical and operational vulnerabilities. These systems, by the very nature of their purpose, often operate in open or semiopen spaces and therefore can be influenced or manipulated by unauthorized access (Taesi et al.,2023). Facilities that do not have adequate surveillance or access control protocols will be more exposed to physical tampering (theft or deliberate sabotage). Human error or malicious activity provided by elements such as configuration errors or modified firmware access can also compromise a system's integrity. In addition, inconsistent application of minimum safety standards has led to hazardous human–cobot interactions. Finally, the absence of real-time monitoring or fail-safes could create risk when a system experiences dangerous operation, even if it is impervious to access by human interference.

As cobots become more autonomous and networked, they are exposed to more advanced security threats (Manikandan et al., 2025). The dependence on external data, AI decision-making algorithms, and machine learning creates new potential vulnerabilities such as data poisoning, model tampering, and decision-making mistakes. Most existing cobot systems do not integrate cybersecurity into their development, so they are not geared to handle sophisticated attacks. Failure to collaborate among IT administrators, cybersecurity experts, and robotics developers can cause defenses to be fragmented. Furthermore, the pace of technological innovation tends to be much faster than that of setting up broad policies and security protocols. Unless there is a unified and proactive effort, cobots are vulnerable in the overall landscape of intelligent manufacturing.

3. Key security techniques to overcome risks in collaborative robot systems

Network segmentation refers to the practice of dividing a larger network into multiple independent zones, which helps regulate data flow and restrict the spread of potential cyberattacks. In the context of collaborative robot systems, segmentation creates a clear separation between operational technology (OT), including robots, sensors, and controllers, and broader information technology (IT) infrastructures such as office networks or cloud-based services. This separation reduces the likelihood of lateral intrusion if one segment is breached. For example, even if an attacker compromises the IT network through a phishing attempt, they face significant barriers in reaching the control environment for cobots. Establishing dedicated communication layers and limiting outside connectivity enables threats to be contained, maintains stability in production activities, and protects the time-sensitive functions that are vital for cobot operations (Mhaskar et al., 2021).

Role-based access control (RBAC) determines the level of access that users have to access rights on the basis of the user's role or other duties and responsibilities. RBAC helps prevent users from accessing, changing, or controlling cobot settings without proper access. For example, a floor worker may have operational control access only, whereas a system administrator may have access to configure or even update the firmware. RBAC reduces the potential risk of unintentional misconfiguration or malicious acts by insiders, and it prohibits privilege escalation. The real use of RBAC limits users from accessing or making changes to firmware or command swaps, which may have direct negative safety consequences, subverted commands, or unintended reprogramming. Using RBAC enables additional avenues for control, audit capability, and accountability from all access points that may be deployed as part of an industrial robot system (Muppalaneni et al., 2025).

Outdated firmware and software are typical attack points for cyberattacks. Periodic software updates and patching ensure the closing of known security loopholes in cobot systems. Producers normally supply updates to correct bugs, optimize performance, or address patch security vulnerabilities. Without timely updates, cobots can run with known

vulnerabilities that can be attacked via malware or remote code execution. Patch management keeps cobots and associated systems up to date everywhere in a facility with the same security baseline. Automated update schedules, centralized management platforms, and update verification mechanisms ensure integrity and reduce downtime. This method is critical for protecting against zero-day attacks and keeping cobot systems robust in a changing threat environment (Mugarza et al., 2020).

Intrusion detection systems (IDSs) inspect network traffic and system activity to identify malicious events. In cobot environments, IDS tools can recognize anomalies such as unauthorized access attempts, unexpected data flows, or unanticipated command sequences. These tools typically employ behavior analysis and machine learning to differentiate between known and unknown actions. For example, if during off-hours a cobot is suddenly issued movement commands, the IDS can mark or stop the activity for inspection. IDS further helps in detecting threats early, such as command spoofing or DoS attacks; thus, intervention is prompt before harm occurs. Through real-time alerts and audit trails, IDSs improve the visibility and security posture of connected cobot systems (Diana et al., 2025).

Despite their technological sophistication, cobots are still physical machines and can be tampered with, stolen, or sabotaged. Physical security technologies such as access-restricted areas, CCTV cameras, biometric locking systems, and tamper-evident tape secure the physical components of cobots. An example is blocking unauthorized personnel from plugging USB sticks into cobot ports to prevent malware infection. Similarly, controlling access to robot control panels prevents anyone but trained individuals from reprogramming or changing operations. Physical barriers and surveillance lessen the likelihood of insider threats—purposeful or unintentional. Combined with operational procedures such as visitor logging and employee training, physical security strengthens the overall robustness of cobot deployments and stops breaches at the hardware level (Fausto et al., 2021).

4. Discussion

The integration of collaborative robots into manufacturing environments has greatly increased productivity, flexibility, and safety. However, the development of connected and smart cobots provides an intricate scenario of security and physical risks. As previously stated, threats include unauthorized access, command spoofing, physical tampering, and data poisoning. The implementation of methods such as segmenting networks, RBAC, intrusion prevention, and patch management demonstrates an emerging understanding and proactive approach to these issues. However, their implementation varies substantially by manufacturing and remains reactive in most cases. One key takeaway is that security-by-design strategies must be developed and implemented immediately. Furthermore, comprehensive collaboration across sectors among IT, OT, and security functions is needed to develop robust frameworks. Additional advancements in AI-based threat identification and predictive maintenance are expected to improve Cobot's security. As a result, integrated, proactive, and adaptable security must be at the center of sustainable development in smart manufacturing ecosystems. The research is limited to a specific industrial case, with results dependent on the chosen vision system and panel type, which may reduce generalizability to other manufacturing environments (Magalhaes and Ferreira, 2022). The research findings are derived from a controlled laboratory setting and a digital twin model, which may not fully capture the complexities of real-world production environments. The proposed guidelines were validated only with non-expert manufacturing engineers, so their applicability to diverse industries, varying team expertise levels, and dynamic assembly conditions require further investigation before broad implementation of these methods can be achieved (Gualtieri et al., 2022).

5. Conclusion

Cobots are sophisticated robotic platforms that safely coexist with people in industry without physical separation. Their main function is to perform repetitive, dangerous, or precision-based operations such as assembly, packaging, and inspection to increase productivity, safety, and operational flexibility. With cobots integrated into Industry 4.0 systems via the IoT and cloud connectivity, these systems have become vulnerable to a variety of security risks. These consist of cyber threats, including unauthorized access, data compromise, command spoofing, and physical threats such as firmware corruption. To address these challenges, critical solutions, including network segmentation, role-based access control, intrusion detection systems, timely software patches, and physical security controls, are paramount. However, some limitations remain in the form of mixed security standards, immature policy development, and a lack of integrated security in the design of cobots. Subsequent research will aim at AI-based threat prediction, uniform security measures, and interdisciplinary collaboration to develop adaptive and robust cobot security systems for smart manufacturing.

Ethical Considerations

Not applicable.

Conflict of Interest

The authors declare no conflicts of interest.

Funding

This research did not receive any financial support.

References

Ananias, E., & Gaspar, P. D. (2022). A low-cost collaborative robot for science and education purposes to foster the Industry 4.0 implementation. *Applied System Innovation, 5*(4), 72.

Bi, Z. M., Luo, C., Miao, Z., Zhang, B., Zhang, W. J., & Wang, L. (2021). Safety assurance mechanisms of collaborative robotic systems in manufacturing. *Robotics and Computer-Integrated Manufacturing, 67*, 102022. https://doi.org/10.1016/j.rcim.2020.102022

Bonci, A., Cen Cheng, P. D., Indri, M., Nabissi, G., & Sibona, F. (2021). Human-robot perception in industrial environments: A survey. *Sensors, 21*(5), 1571. https://doi.org/10.3390/s21051571

Brandstötter, M., Berns, K., & Görges, D. (2020). Versatile collaborative robot applications through safety-rated modification limits. In K. Berns & D. Görges (Eds.), *Advances in service and industrial robotics. RAAD 2019. Advances in Intelligent Systems and Computing* (Vol. 980, pp. 485–493). Springer. https://doi.org/10.1007/978-3-030-19648-6_50

Byner, C., Matthias, B., & Ding, H. (2019). Dynamic speed and separation monitoring for collaborative robot applications–concepts and performance. *Robotics and Computer-Integrated Manufacturing, 58*, 239–252. https://doi.org/10.1016/j.rcim.2018.11.002

Diana, L., Dini, P., & Paolini, D. (2025). Overview of intrusion detection systems for computer networking security. *Computers, 14*(3), 87. https://doi.org/10.3390/computers14030087

Fausto, A., Gaggero, G. B., Patrone, F., Girdinio, P., & Marchese, M. (2021). Toward the integration of cyber and physical security monitoring systems for critical infrastructures. *Sensors, 21*(21), 6970. https://doi.org/10.3390/s21216970

Gualtieri, L., Rauch, E., & Vidoni, R. (2022). Development and validation of guidelines for safety in human-robot collaborative assembly systems. *Computers & Industrial Engineering, 163*, 107801. https://doi.org/10.1016/j.cie.2021.107801

Khalid, A., Kirisci, P., Khan, Z. H., Ghrairi, Z., Thoben, K. D., & Pannek, J. (2018). Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry, 97*, 132–145. https://doi.org/10.1016/j.compind.2018.02.009

Kildal, J., Martín, M., Ipiña, I., & Maurtua, I. (2019). Empowering assembly workers with cognitive disabilities by working with collaborative robots: A study to capture design requirements. *Procedia CIRP, 81*, 797–802. https://doi.org/10.1016/j.procir.2019.03.202

Levratti, A., Riggio, G., Fantuzzi, C., De Vuono, A., & Secchi, C. (2019). TIREBOT: A collaborative robot for the tire workshop. *Robotics and Computer-Integrated Manufacturing, 57*, 129–137. https://doi.org/10.1016/j.rcim.2018.11.001

Liu, Z., Wang, X., Cai, Y., Xu, W., Liu, Q., Zhou, Z., & Pham, D. T. (2020). Dynamic risk assessment and active response strategy for industrial human-robot collaboration. *Computers & Industrial Engineering, 141*, 106302. https://doi.org/10.1016/j.cie.2020.106302

Ma, X., Mao, C., & Liu, G. (2022). Can robots replace human beings?—Assessment of the developmental potential of construction robots. *Journal of Building Engineering, 56*, 104727. https://doi.org/10.1016/j.jobe.2022.104727

Magalhaes, P., & Ferreira, N. (2022). Inspection application in an industrial environment with collaborative robots. *Automation, 3*(2), 258–268. https://doi.org/10.3390/automation3020013

Manikandan, B., Ganesh Kumar, G., Kanakaprabha, S., Vijaya Kumar Reddy, R., & Janani, R. (2025). Blockchain technology for the cobot's cybersecurity issues. In *Intelligent robots and cobots: Industry 5.0 applications* (pp. 377–399). Wiley. https://doi.org/10.1002/9781394198252.ch18

Matheson, E., Minto, R., Zampieri, E. G., Faccio, M., & Rosati, G. (2019). Human–robot collaboration in manufacturing applications: A review. *Robotics, 8*(4), 100. https://doi.org/10.3390/robotics8040100

Mhaskar, N., Alabbad, M., & Khedri, R. (2021). A formal approach to network segmentation. *Computers & Security, 103*, 102162. https://doi.org/10.1016/j.cose.2020.102162

Mugarza, I., Flores, J. L., & Montero, J. L. (2020). Security issues and software update management in the industrial Internet of Things (IoT) era. *Sensors, 20*(24), 7160. https://doi.org/10.3390/s20247160

Muppalaneni, R., Inaganti, A. C., Ravichandran, N., & Nersu, S. R. K. (2025). AI-powered role-based access control (RBAC): Automating policy enforcement in enterprise environments. *Journal of Advanced Computing Systems, 5*(2), 1–12.

Pal, A., Restrepo, V., Goswami, D., & Martinez, R. V. (2021). Exploiting mechanical instabilities in soft robotics: Control, sensing, and actuation. *Advanced Materials, 33*(19), 2006939. https://doi.org/10.1002/adma.202006939

Pizoń, J., Cioch, M., Kański, Ł., & Sánchez-García, E. (2022). Cobots implementation in the era of Industry 5.0 using modern business and management solutions. *Advances in Science and Technology Research Journal, 16*(6), 166–178. https://doi.org/10.12913/22998624/156222

Taesi, C., Aggogeri, F., & Pellegrini, N. (2023). COBOT applications—recent advances and challenges. *Robotics, 12*(3), 79. https://doi.org/10.3390/robotics12030079

Tasooji, T. K., & Marquez, H. J. (2022). A secure decentralized event-triggered cooperative localization in multi-robot systems under cyber attack. *IEEE Access, 10*, 128101–128121. https://doi.org/10.1109/ACCESS.2022.3227076