Scientometric Analysis for Access Control in the Social Robots Era

Jennifer A. Cardenas Castaneda
SMART Lab
University of Alberta
Edmonton, Canada
Jacarden@ualberta.ca

Rafiq Ahmad
SMART Lab
University of Alberta
Edmonton, Canada
Rafiq.ahmad@ualberta.ca

Patrick C. K. Hung
Faculty of Business and IT
Ontario Tech University
Oshawa, Canada
Patrick.Hung@ontariotechu.ca

Yung-Fa Huang
Department of Information and Communication Engineering
Chaoyang University of Technology
Taichung, Taiwan (R.O.C.)
yfahuang@cyut.edu.tw

Abstract— **Social robots are cyber-physical systems consisting of cyber and physical robotic components that connect to Cloud services to improve the ease and productivity of activities through networking, multi-media, and sensory technologies. However, social robots introduce new security threats beyond what a regular computing system may tackle. The International Organization for Standardization (ISO) specifies requirements and guidelines for the inherently safe design and protective measures for personal care robots. However, ISO only covers human-robot types of physical contact applications, not from the data security and privacy perspective. However, while social robots attract new research, security and privacy issues are still thoroughly investigated. This paper provides a scientometric approach to propose research gaps and future trends related to access control and social robot's research.**

*Keywords— **Social robots, social interaction robots, human-robot interaction, access control, privacy protection, authentication systems, blockchain.***

I. Introduction

Social robots have taken an impressive journey from concept to reality. They began as an academic curiosity and have been transitioning to commercial products across different sectors, from hospitals and nursing homes to schools and homes [1]. As media personalities, academics, and legislators discuss the implications of the coming "robot revolution," it is clear that robots are transforming industries ranging from logistics to human services [2]. This "robot revolution" opens not just opportunities but also challenges that need to be addressed.

Human-machine interactions take on an exciting new dimension when social robots are integrated into our surroundings. Nevertheless, with this level of intimacy comes the urge to understand content management in their interactions and conversations becomes critical, highlighting their current lack of such capabilities and privacy awareness [3]. Imagine sharing personal moments, family events, or sensitive information around a device that has the capability to record or interpret data. Moreover, this increasing integration raises concerns about the growing number of personal data they access since the possibility of this data being intercepted or redirected to malicious systems exposes the susceptibility of audio, video, actuator movement, and environmental interaction recordings [4].

The incorporation of technology into daily living increases unnoticed data collection [5]. Every voice command, every gesture, and every interaction become a potential data point. Furthermore, concerns about informational privacy have expanded beyond interactions between users and robots to interactions between individuals assisted by robots. This is particularly relevant when considering scenarios such as robot hacking or instances of espionage permitted by telepresence robots [6].

To face these challenges, solutions to protect user data and assure privacy are being researched. For example, the integration of blockchain-based decentralized systems promises to be a potential strategy, providing more decentralization, transparency, tamper resistance, and traceability [7]. This technology provides a good alternative for developing secure privacy interactions, potentially addressing the privacy problems raised by social robots [8].

While strategies such as blockchain may provide potential solutions, the quickly expanding world of social robots requires constant awareness and research [9]. The integration of robots into human society is not a static process; new concerns and challenges will develop as technology advances. This is one of the main reasons why identifying research gaps and projecting future trends is critical. This study investigates the relationship between social robots and access control to discover research gaps and potential future research scenarios.

II. Research Methodology

A. Data acquisition

The data used for this study was retrieved from Scopus database. A search query was generated to retrieve recent and relevant research papers at the intersection of social robots and access control within specific parameters. This query includes a set of keywords covering various aspects of both areas, including "social robots," "humanoid robots," "robotic systems," "access control," "security mechanisms,". These keywords are coupled with Boolean operators such as "OR," guaranteeing that articles that discuss any of these themes appear in the search results. This resulted in the search query: (TITLE-ABS-KEY ("social robots" OR "humanoid robots" OR "robotic systems" OR "autonomous robots" OR "robotic companions" OR "service robots" OR "social interaction robots" OR "assistive robots" OR "smart robots" OR "intelligent robots" OR "human-robot interaction" OR "robotic applications") AND ("access control" OR "security mechanisms" OR "authentication systems" OR "authorization protocols" OR "identity management" OR "privacy protection" OR "user authentication" OR "biometric access control" OR "physical security" OR "surveillance systems" OR "intrusion detection" OR "security policies" OR "access management")).

The subject areas were limited to "Computer Science," "Engineering," and "Social Sciences," which are most likely to provide relevant studies in this context. Moreover, the dates of the publications were limited from 2013 to 2023. Furthermore, Conference Papers" (cp) and "Articles" (ar) were selected for the type of document to be retrieved and lastly, English was selected as the language for the documents.

B. *Scientometric analysis methodology*

The VOSViewer software program is used in the scientometric study to examine the research landscape thoroughly [10]. This methodology identifies patterns and trends in research outputs as well as connections between terms and authors by mapping keyword co-occurrence, author co-citation, and other data. This procedure provides a wide view of the state of the subject and helps in identifying the key areas of research, channels of communication, and patterns of impact. The knowledge gathered from this analysis contributes to the identification of current challenges and potential directions for future research by providing an in-depth understanding of the dynamics of the field [11].

III. Scientometric analysis results

In this section, we present the results of our scientometric analysis. This analysis provides a structured overview of the research landscape regarding social robots and access control. Through detailed mappings, we aim to illustrate key trends, influential works, and critical intersections in the domain. These findings provide insights into the current state of research and point to potential directions for future research.

A. *Keywords co-occurrence analysis*

The keywords co-occurrence mapping analysis used a full counting method to show connections between keywords. With a threshold of 14 occurrences per keyword, 58 keywords were considered out of 4877. The resulting map displayed 1125 links and a total link strength of 3902, offering a clear picture of keyword relationships in the context of social robots and access control. This map highlights key research themes and potential directions for future exploration.

Referring to Fig. 1, Cluster 1 (red color) of the scientometric study indicates a network of interconnected terms related to robotics, security, and technology. The keywords "robots" with 262 occurrences, 48 links and 714 total link strength, and "intelligent robots" with 170 occurrences, 48 links and 493 total link strength, are the main ones of the cluster, creating a main central node, highlighting the importance of the development of robots with advanced cognitive capabilities. Moreover, "access control" with 28 occurrences, 35 links and 97 total link strength, is connected to "network security," with 44 occurrences, 45 links and 162 total link strength, demonstrating the importance of security methods and mechanisms in regulating access to networks and systems.

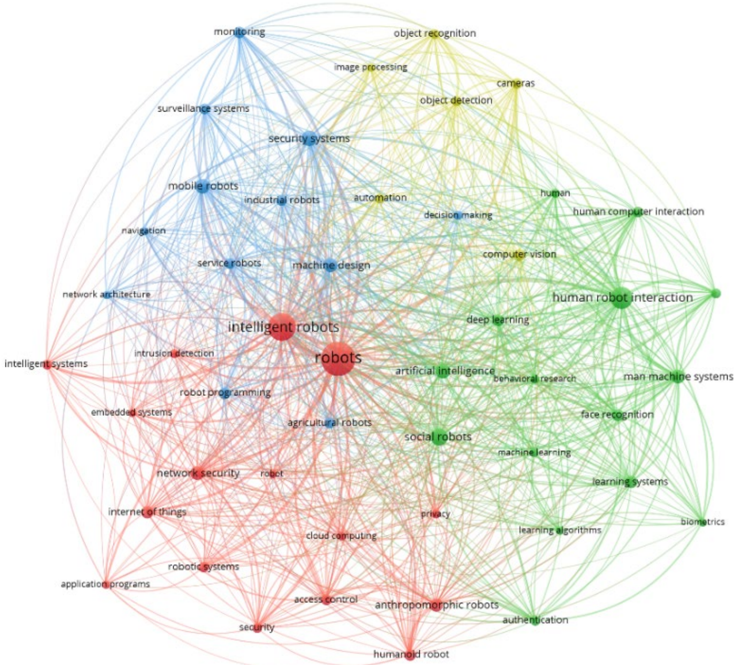

Fig. 1. Keyword co-occurrence network map.

Additionally, the occurrence and link values show a relationship between "cloud computing," with 28 occurrences, 64 links and 19 total link strength; and "embedded systems," with 17 occurrences, 32 links and 68 total link strength; and "humanoid robots," with 29 occurrences, 34 links and 96 total link strength; indicating the integration of cloud technology into embedded systems. Finally, another important connection to highlight is between "anthropomorphic robot," with 39 occurrences, 35 links and 134 total link strength, showing the interest in designing and developing robots that resemble the appearance and behavior of humans. The interconnectivity between these two suggests that these two terms are explored together, showing their common goal of developing robots with human-like features.

One important connection that can be found in Cluster 2 (green color) is between Artificial Intelligence (AI), with 52 occurrences, 43 links and 178 total link strength, "deep learning," with 29 occurrences, 43 links and 139 total link strength; and machine learning. AI is the general term for deep learning and machine learning, subfields focused on building algorithms and models that allow computers to learn and make autonomously predictions or judgments[12]. This close connection suggests their importance for research and development.

Another important connection to highlight within Cluster 2, is between "Human-Computer Interaction (HCI)," with 28 occurrences, 35 links and 117 total link strength, and "Human-

Identify applicable funding agency here. If none, delete this text box.

Robot Interaction (HRI)," with 107 occurrences, 44 links and 386 total link strength. HCI studies the interaction between humans and computers, whereas HRI studies the interaction between humans and robotics. These terms share several similarities since they are both focused on the interfaces, usability, and communication channels between humans and technical systems [13]. This connection demonstrates that understanding the design, usability, and effectiveness of human-robot interfaces and interactions is critical.

Cluster 3 (blue color) shows an important interconnectivity between "service robots," with 28 occurrences, 36 links and 115 total link strength; "machine design," with 46 occurrences, 41 links and 176 total link strength; "industrial robots," with 25 occurrences, 33 links and 83 total link strength. This cluster suggests several elements of robotics, with "machine design," playing an important role in the creation of both industrial and service robots. Moreover, another important connection to highlight is between "surveillance systems," with 27 occurrences, 35 links and 104 total link strength; "monitoring," with 31 occurrences, 31 links and 126 total link strength; "navigation," with 16 occurrences, 28 links and 61 total link strength; and "network architecture," with 16 occurrences, 25 links and 57 total link strength. This suggests that monitoring and navigation are closely associated with surveillance systems, emphasizing the key role of these components in ensuring effective surveillance. Additionally, "network architecture," implies the integration of networked surveillance systems.

Automation is one of the key core keywords found in cluster 4 (yellow color) with 21 occurrences, 32 links and 65 total link strength; and is the use of technology to accomplish activities automatically, hence reducing the need for human intervention [14]. Within this cluster, automation is connected to "cameras" and "computer vision". Cameras are used as input devices for computer vision systems, gathering visual data that is then processed using image analysis techniques, including "object detection" and "object recognition" [15].

B. Countries citation analysis

In this research study, a citation-based analysis was conducted with countries as the unit of analysis. The analysis employed specific thresholds for inclusion, requiring a minimum number of documents (5) and a minimum number of citations (7) from each country. Out of the total 81 countries examined, 23 met these threshold criteria. Further analysis revealed that 19 of these countries were interconnected within the network. As a result, these 19 countries were selected for the mapping visualization, providing a focused representation of the research landscape.

The data illustrated in Fig. 2 includes 19 countries, among which the United States and China emerged as the main players with 94 documents and 2075 citations, resulting in a total link strength of 27 and China with 106 documents and 1562 citations. Germany also demonstrated significant research activity, producing 27 documents with 579 citations, resulting in a total link strength of 25. Austria, with 6 documents and 133 citations, exhibited a high total link strength of 18, indicating strong research collaboration.

Italy and Spain also displayed notable research performance, with Italy contributing 25 documents and 547 citations and Spain contributing 20 documents and 224 citations.

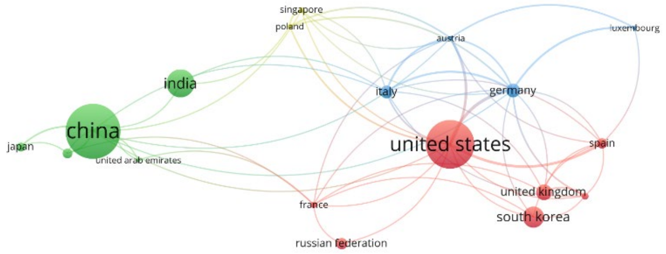

Fig. 2. Citation countries network map.

C. Bibliographic coupling sources

In this section, a bibliographic coupling analysis was employed, with sources serving as the unit of analysis. The counting method used was total counting, which ensured the comprehensive inclusion of relevant citations. The threshold for inclusion required a minimum of three citations for each document. Among the 350 sources considered, 30 met this threshold criterion. A subset of 27 sources was identified as interconnected within the network to facilitate networking visualization, providing a focused representation of the relationships among these sources.

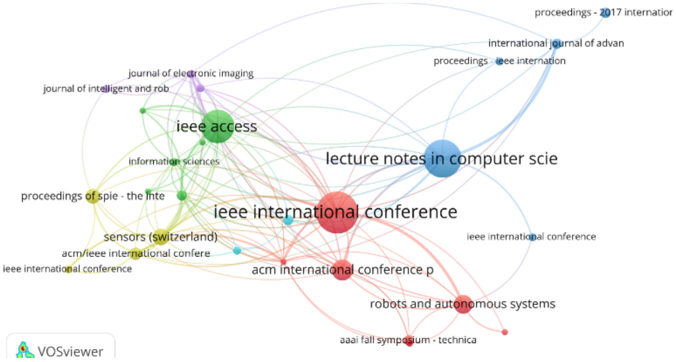
proceedings - 2017 internatior
international journal of advan
proceedings · ieee internation
journal of electronic imaging
journal of intelligent and rob
ieee access
lecture notes in computer scie
information sciences
proceedings of spie - the inte
ieee international conference
sensors (switzerland)
ieee international conference
acm/ieee international confere
ieee international conference
acm international conference p
robots and autonomous systems
aaai fall symposium - technica
VOSviewer

Fig. 3. Bibliographic coupling sources network map.

Considering the research focus on social robots and access control, the bibliographic coupling analysis using VOSviewer provides valuable insights into the most relevant and influential sources in this specific research area. Among the identified sources, "IEEE International Conference on Intelligent Robots and Systems" and "IEEE Access" emerge as the leading contributors with 20 and 16 documents, respectively, and substantial citation counts of 361 and 405, respectively. These sources exhibit strong total link strengths of 49 and 45, signifying their significant influence and interconnectedness with other publications in the field.

Moreover, "Journal of Electronic Imaging" and "Sensors (Switzerland MDPI)" show a considerable total link strength of 38, suggesting their relevance and impact in the context of social robots and access control. The findings from this analysis offer essential guidance to researchers and practitioners in the domain, helping them identify significant references and sources that shape the development and understanding of social robots and access control systems.

D. *Authors co-authorship analysis*

Understanding cooperation patterns among authors is critical in academic research. The co-authorship mapping, shown by VOSviewer, provides insight into these trends by connecting researchers based on shared authorship of papers [11]. For the analysis, co-authorship analysis was conducted with authors as the unit of analysis. The analysis employed specific thresholds for inclusion, requiring a minimum number of documents (e.g., 3) and a minimum number of citations (e.g., 3) for each author. Of the total 1970 authors considered, 52 met these threshold criteria. However, not all of these 52 authors were interconnected within the network. The mapping visualization focused on the largest set of connected authors, which consisted of 32 authors. This visualization provides an insightful representation of the collaborative relationships among this subset of authors in the research network.

The use of VOSviewer for co-authorship analysis offers insight into authors' collaborative patterns and influence in the realm of social robotics and access control. Wang Y. emerges as a significant contributor, co-authoring 9 documents and receiving 47 citations, resulting in a total link strength of 8. Similarly, Yang J. demonstrates substantial research influence with 4 documents and 75 citations, leading to a total link strength of 7. Li Y., Sun 1., and Li J. exhibit notable collaboration and citation impact, with total link strengths of 6, 6, and 5, respectively [16]–[18].

Furthermore, other authors, such as Li Z., Wang S., and Wu H., show strong collaborative connections, contributing to a total link strength of 5. Zhang Y., Yang G., and Wang W. also display significant research collaboration and impact. Overall, this co-authorship study reveals significant researchers in the field of social robots and access control and highlights their collaborative efforts [18].

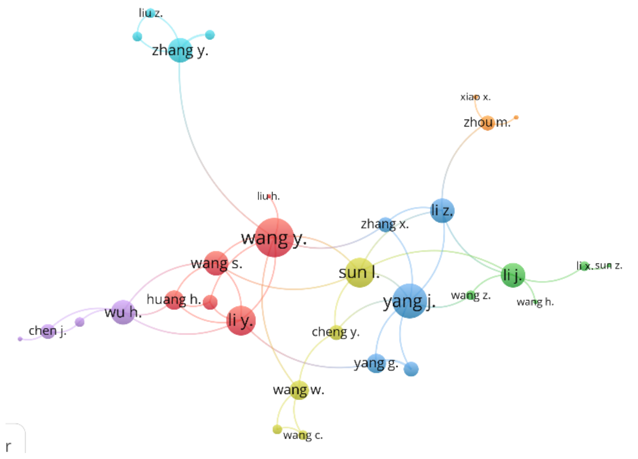

Fig. 4. Authors co-authorship network map.

E. *Research gaps*

1. **Lack of integration of cloud computing in access control**
The analysis found that "access control" had a lower occurrence and link strength than other keywords, such as "robots" and "intelligent robots." This points to a possible research gap in studying and creating effective access control systems customized specifically for social robots to provide secure and controlled interactions in a variety of applications.
2. **Limited focus on access control in social robots**
While the terms "cloud computing" and "embedded systems" were discovered to be related, there appears to be little research on cloud-based access control solutions for social robots. Future research could investigate the benefits and drawbacks of using cloud technology in access control systems for social robots.
3. **Need for in-depth research on human-robot interaction**
"Human computer interaction (HCI)" and "human robot interaction (HRI)" are highlighted as interconnected keywords in the study. However, a research gap may exist in understanding the specific problems and opportunities for building successful and intuitive human-robot interaction interfaces and experiences, particularly in the context of access control applications [19].

F. *Future trends*

4. **Increasing interdisciplinary collaboration**
The interconnection of several research areas and keywords, such as "cloud computing" and "embedded systems," indicates a growing trend of combining multiple technologies to improve the capabilities of social robots and access control systems.
5. **Advancement in AI for social robots**
The strong link between "artificial intelligence (AI)," "deep learning," and "machine learning" suggests that AI-based algorithms are being developed to improve the cognitive capacities of social robots, potentially leading to more intelligent and context-aware access control systems.
6. **Integration of security and surveillance in social robots**
The connection between "network security," "surveillance systems," and "access control" suggests a future trend of exploring comprehensive security frameworks for social robots, which include surveillance features to assure safe and secure operations in a variety of situations.
7. **Human-like features and anthropomorphic design**
The association between "anthropomorphic robot" and "humanoid robots" suggests an increasing interest in creating social robots with human-like appearances and behavior. Future trends may include advancements in anthropomorphic design to produce robots that can interact and communicate with humans

more effectively while access control methods maintain proper interactions.

8. **Application of social robots in different industries** The connection between "service robots," "machine design," and "industrial robots" implies a potential trend of investigating the application of social robots in industries other than traditional contexts. Future research might focus on developing access control techniques specific to certain industrial requirements and use cases.

G. Conclusions

The scientometric study provides important insights. Keyword co-occurrence research highlights keywords such as "robots" and "intelligent robots," while exposing weaknesses in cloud computing integration into access control. The citation-based mapping analysis of countries emphasizes the important roles of the United States and China in shaping the research landscape. Bibliographic coupling analysis underscores the significance of sources like the "IEEE International Conference on Intelligent Robots and Systems" and "IEEE Access."

Identified research gaps point to opportunities for future investigations, including the exploration of cloud-based access control solutions for social robots and the development of intuitive human-robot interaction interfaces. Looking ahead, interdisciplinary collaborations, advancements in AI, integration of security and surveillance, and the pursuit of human-like features in anthropomorphic design are expected trends in the field of social robots and access control. Additionally, the application of social robots in diverse industries and the development of tailored access control techniques are anticipated areas of research focus.

References

[1] A. van Wynsberghe, "Social robots and the risks to reciprocity," *AI Soc*, vol. 37, no. 2, pp. 479–485, 2022, doi: 10.1007/s00146-021-01207-y.

[2] P. Share and J. Pender, "Preparing for a Robot Future? Social Professions, Social Robotics and the Challenges Ahead," *Irish Journal of Applied Social Studies*, vol. 18, no. 1, p. 4, 2018, doi: 10.21427/D7472M.

[3] B. Tang, D. Sullivan, B. Cagiltay, V. Chandrasekaran, K. Fawaz, and B. Mutlu, "CONFIDANT: A Privacy Controller for Social Robots," Jan. 2022, [Online]. Available: http://arxiv.org/abs/2201.02712

[4] J. Miller, A. B. Williams, and D. Perouli, "A Case Study on the Cybersecurity of Social Robots," in *ACM/IEEE International Conference on Human-Robot Interaction*, IEEE Computer Society, Mar. 2018, pp. 195–196. doi: 10.1145/3173386.3177078.

[5] C. Lutz and A. Tamò, "RoboCode-Ethicists - Privacy-friendly robots, an ethical responsibility of engineers?" in *Proceedings of the 2015 ACM Web Science Conference*, Association for Computing Machinery, Inc, Jun. 2015. doi: 10.1145/2786451.2786465.

[6] E. Fosch-Villaronga, C. Lutz, and A. Tamò-Larrieux, "Gathering Expert Opinions for Social Robots' Ethical, Legal, and Societal Concerns: Findings from Four International Workshops," *Int J Soc Robot*, vol. 12, no. 2, pp. 441–458, May 2020, doi: 10.1007/s12369-019-00605-z.

[7] V. Vasylkovskyi, S. Guerreiro, and J. S. Sequeira, "BlockRobot: Increasing Privacy in Human Robot Interaction by Using Blockchain," in *Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 106–115. doi: 10.1109/Blockchain50366.2020.00021.

[8] E. C. Ferrer, O. Rudovic, T. Hardjono, and A. Pentland, "RoboChain: A Secure Data-Sharing Framework for Human-Robot Interaction," Feb. 2018, [Online]. Available: http://arxiv.org/abs/1802.04480

[9] U. S. P. Srinivas Aditya, R. Singh, P. K. Singh, and A. Kalla, "A Survey on Blockchain in Robotics: Issues, Opportunities, Challenges and Future Directions," *Journal of Network and Computer Applications*, vol. 196, p. 103245, Dec. 2021, doi: 10.1016/j.jnca.2021.103245.

[10] D. O. Oyewola and E. G. Dada, "Exploring machine learning: a scientometrics approach using bibliometrix and VOSviewer," *SN Appl Sci*, vol. 4, no. 5, May 2022, doi: 10.1007/s42452-022-05027-7.

[11] N. Jan van Eck and L. Waltman, "VOSviewer Manual," 2022.

[12] J. Ghahremani Nahr, H. Nozari, and M. E. Sadeghi, "Artificial intelligence and Machine Learning for Real-world problems (A survey)," 2021. [Online]. Available: www.ijie.ir

[13] W. Huang and V. Tech, "When HCI Meets HRI: the intersection and distinction," 2015. [Online]. Available: https://www.researchgate.net/publication/302092478

[14] G. Tsafnat, P. Glasziou, M. K. Choong, A. Dunn, F. Galgani, and E. Coiera, "Systematic review automation technologies," *Systematic Reviews*, vol. 3, no. 1. BioMed Central Ltd., Apr. 12, 2014. doi: 10.1186/2046-4053-3-74.

[15] D. M. Ramík, C. Sabourin, R. Moreno, and K. Madani, "A machine learning based intelligent vision system for autonomous object detection and recognition," *Applied Intelligence*, vol. 40, no. 2, pp. 358–375, Mar. 2014, doi: 10.1007/s10489-013-0461-5.

[16] X. Zhang, P. Zhang, X. Zeng, Y. Wang, and C. hung Chi, "sAuth: a hierarchical implicit authentication mechanism for service robots," *Journal of Supercomputing*, vol. 78, no. 14, pp. 16029–16055, Sep. 2022, doi: 10.1007/s11227-022-04472-w.

[17] W. K. Wong, S. Ye, H. Liu, and Y. Wang, "Effective Mobile Target Searching Using Robots," *Mobile Networks and Applications*, vol. 27, no. 1, pp. 249–265, Feb. 2022, doi: 10.1007/s11036-020-01628-x.

[18] Y. Wang, W. Wang, D. Liu, X. Jin, J. Jiang, and K. Chen, "Enabling edge-cloud video analytics for robotics applications," in *Proceedings - IEEE INFOCOM*, Institute of Electrical and Electronics Engineers Inc., May 2021. doi: 10.1109/INFOCOM42981.2021.9488801.

[19] A. Castro, F. Silva, and V. Santos, "Trends of human-robot collaborat metrics," *Sensors*, vol. 21, no. 12, Jun. 2021, doi: 10.3390/s21124113.