EAI Endorsed Transactions
on AI and Robotics

Research Article EAI.EU

Security and Privacy in Fog/Cloud-based IoT Systems for AI and Robotics

Prabh Deep Singh[1] and Kiran Deep Singh[2,*]

[1] Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India
[2] Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India

Abstract

Integration of Internet of Things (IoT) systems based on the fog or the cloud with Artificial Intelligence (AI) and Robotics has prepared the way for breakthrough advancements in a variety of different fields of business. However, these cross-disciplinary technologies present significant difficulties in supporting confidentiality and safeguarding data. This article digs into the issues of proving robust security and protecting user privacy in IoT systems based in the fog or the cloud and used for AI and robotics applications. This study gives insights into the possible hazards such interconnected systems meet by conducting an in-depth review of existing security threats, vulnerabilities, and privacy concerns. In addition, the study investigates innovative security mechanisms, encryption approaches, access control strategies, and privacy-preserving solutions that can be used to safeguard data, communications, and user identities. The results of this study highlight the demand for comprehensive security and privacy solutions to support the mainstream deployment of Fog/Cloud-based Internet of Things systems in the field of artificial intelligence and robotics.

Keywords: Security and privacy, Fog/Cloud Computing, Robotics, Artificial Intelligence, Internet of Things

Received on 25 July 2023, accepted on 27 August 2023, published on 28 August 2023

doi: 10.4108/airo.3616

1. Introduction

IoT, AI, and robotics have transformed many industries and aspects of human life due to rapid technological advancement. IoT systems connect physical devices and objects to the internet to collect and exchange data [1],[2]. At the same time, AI and Robotics allow them to intelligently process and analyse the data and act autonomously[3]. IoT, AI, and Robotics have created exciting opportunities in healthcare, transportation, agriculture, smart cities, and industrial automation. AI and robotics Fog/Cloud-based IoT systems face significant security and privacy issues [4].

Fog/Cloud computing is used in IoT architectures due to the rapid growth of IoT devices and data. Fog computing, which extends Cloud services to the network edge near the data source, has enabled real-time data processing, reduced latency, and increased bandwidth efficiency [5]. This paradigm shift has enabled the integration of AI and Robotics into IoT systems, enabling devices to make intelligent decisions and perform tasks without Cloud infrastructure [6]. IoT, AI, and Robotics offer promising opportunities and complex security and privacy issues. Distributed data processing, heterogeneous devices, and wireless communication make Fog/Cloud-based IoT systems vulnerable to attacks [7],[8]. Unauthorized access, data breaches, and cyber-attacks on interconnected devices can cause data theft, service disruption, and even physical harm in critical applications[9].

This paper addresses security and privacy issues related to Fog/Cloud-based IoT systems and AI/Robotics. These technologies must be robustly protected from potential threats as they become more widespread [10], [11]. This research could improve the trustworthiness and reliability of Fog/Cloud-based IoT systems, promoting the widespread adoption of IoT, AI, and Robotics across various domains [12],[13].

*Corresponding author. Email: kdkirandeep@gmail.com

advancement, where interconnected devices, AI, and Robotics are reshaping industries and changing how we interact with our surroundings. IoT systems with Fog and Cloud-based architectures enable real-time data processing, low latency, and scalability for healthcare, transportation, industrial automation, smart cities, and more. This paper examined security and privacy in Fog/Cloud-based IoT systems for AI and Robotics, highlighting their importance, challenges, and practical solutions.

Fog/Cloud-based IoT systems must be secure due to their distributed nature and many connected devices. Security must be strong to prevent cyberattacks. Authentication and access control safeguard the system and sensitive data. IoT devices, Fog nodes, and Cloud data centres send data encrypted and securely. Intrusion Detection and Prevention Systems (IDPS) continuously check network traffic and find suspicious activities to prevent and respond to cyberattacks. Security patches and updates are necessary to fix vulnerabilities and prevent new threats.

Fog/Cloud-based IoT systems must preserve privacy to keep user and stakeholder trust. Anonymization and pseudonymization ensure that sensitive data is de-found during processing. Differential privacy mathematically guarantees individual privacy while allowing meaningful data analysis. Privacy-aware data processing and data minimization reduce data exposure. Privacy policies and user consent management allow users to control and understand data processing.

To be successful, Fog/Cloud-based IoT systems must overcome many challenges and limitations. Limited computational power and energy in Fog nodes may affect system performance and scalability. Balancing local processing efficiency with centralized Cloud capabilities requires careful trade-offs. Due to the diversity of IoT devices and communication protocols, standardization is needed to ensure seamless integration.

Due to the increased attack surface, security measures must be strengthened to keep up with evolving cyber threats. Fog/Cloud-based IoT systems must apply privacy-enhancing techniques and follow privacy regulations to protect personal data without compromising data utility. Edge-to-Cloud decision-making requires intelligent task allocation between Fog and Cloud layers, considering data volume, latency, and computational complexity.

Battery-powered IoT devices must be energy efficient and sustainable to reduce environmental impact and energy consumption. Fog/Cloud-based IoT systems can perfect resource use and budget allocation, but the cost must be considered.

References

[1] P. Singh and K. D. Singh, “Fog-Centric Intelligent Surveillance System: A Novel Approach for Effective and Efficient Surveillance,” in *2023 International Conference on Advancement in Computation \& Computer Technologies (InCACCT)*, 2023, pp. 762–766.

[2] K. D. Singh, “Securing of Cloud Infrastructure using Enterprise Honeypot,” in *Proceedings - 2021 3rd International Conference on Advances in Computing, Communication Control and Networking, ICAC3N 2021*, 2021, pp. 1388–1393. doi: 10.1109/ICAC3N53548.2021.9725389.

[3] G. Aceto, V. Persico, and A. Pescapé, “Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0,” *J. Ind. Inf. Integr.*, vol. 18, 2020, doi: 10.1016/j.jii.2020.100129.

[4] S. S. Kang, K. D. Singh, and S. Kumari, “Smart antenna for emerging 5G and application,” in *Printed Antennas*, CRC Press, 2022, pp. 249–264.

[5] K. D. Singh, “Particle Swarm Optimization assisted Support Vector Machine based Diagnostic System for Dengue prediction at the early stage,” in *Proceedings - 2021 3rd International Conference on Advances in Computing, Communication Control and Networking, ICAC3N 2021*, 2021, pp. 844–848. doi: 10.1109/ICAC3N53548.2021.9725670.

[6] 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,” *J. Netw. Comput. Appl.*, vol. 196, p. 103245, 2021, doi: 10.1016/j.jnca.2021.103245.

[7] S. Meng, X. He, and X. Tian, “Research on Fintech development issues based on embedded cloud computing and big data analysis,” *Microprocess. Microsyst.*, vol. 83, 2021, doi: 10.1016/j.micpro.2021.103977.

[8] H. Goumidi, Z. Aliouat, and S. Harous, “Vehicular Cloud Computing Security: A Survey,” *Arab. J. Sci. Eng.*, vol. 45, no. 4, pp. 2473–2499, 2020, doi: 10.1007/s13369-019-04094-0.

[9] K. D. Singh and P. Singh, “A Novel Cloud-based Framework to Predict the Employability of Students,” in *2023 International Conference on Advancement in Computation \& Computer Technologies (InCACCT)*, 2023, pp. 528–532.

[10] P. Dhiman *et al.*, “A novel deep learning model for detection of severity level of the disease in citrus fruits,” *Electronics*, vol. 11, no. 3, p. 495, 2022.

[11] S. Tiwari, S. Kumar, and K. Guleria, “Outbreak Trends of Coronavirus Disease-2019 in India: A Prediction,” *Disaster Med. Public Health Prep.*, vol. 14, no. 5, pp. e33–e38, 2020, doi: 10.1017/dmp.2020.115.

[12] J. Venkatesh *et al.*, “A Complex Brain Learning Skeleton Comprising Enriched Pattern Neural Network System for Next Era Internet of Things,” *J. Healthc. Eng.*, vol. 2023, 2023.

[13] P. R. Kapula, B. Pant, B. Kanwer, D. Buddhi, K. V. D. Sagar, and S. Sinthu, “Integration of AI in implementation of Wire-less Webbing: A detailed Review,” in *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, 2023, pp. 983–989.

[14] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, “Security and privacy in 6G networks: New areas and new challenges,” *Digit. Commun.*

Networks, vol. 6, no. 3, pp. 281–291, 2020, doi: 10.1016/j.dcan.2020.07.003.

[15] G. Yang *et al.*, "Homecare Robotic Systems for Healthcare 4.0: Visions and Enabling Technologies," *IEEE J. Biomed. Heal. Informatics*, vol. 24, no. 9, pp. 2535–2549, 2020, doi: 10.1109/JBHI.2020.2990529.

[16] A. Martinetti, P. K. Chemweno, K. Nizamis, and E. Fosch-Villaronga, "Redefining Safety in Light of Human-Robot Interaction: A Critical Review of Current Standards and Regulations," *Front. Chem. Eng.*, vol. 3, 2021, doi: 10.3389/fceng.2021.666237.

[17] Y. Chen, Y. Ping, Z. Zhang, B. Wang, and S. Y. He, "Privacy-preserving image multi-classification deep learning model in robot system of industrial IoT," *Neural Comput. Appl.*, vol. 33, no. 10, pp. 4677–4694, 2021, doi: 10.1007/s00521-020-05426-0.

[18] N. A. Angel, D. Ravindran, P. M. D. R. Vincent, K. Srinivasan, and Y. C. Hu, "Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies," *Sensors*, vol. 22, no. 1, 2022, doi: 10.3390/s22010196.

[19] F. Bademosi and R. R. A. Issa, "Factors Influencing Adoption and Integration of Construction Robotics and Automation Technology in the US," *J. Constr. Eng. Manag.*, vol. 147, no. 8, 2021, doi: 10.1061/(asce)co.1943-7862.0002103.

[20] H. Goumidi, Z. Aliouat, and S. Harous, "Vehicular Cloud Computing Security: A Survey," *Arab. J. Sci. Eng.*, vol. 45, no. 4, pp. 2473–2499, Apr. 2020, doi: 10.1007/s13369-019-04094-0.

[21] Y. Chen, Y. Ping, Z. Zhang, B. Wang, and S. Y. He, "Privacy-preserving image multi-classification deep learning model in robot system of industrial IoT," *Neural Comput. Appl.*, vol. 33, no. 10, pp. 4677–4694, May 2021, doi: 10.1007/s00521-020-05426-0.

[22] E. Fosch-Villaronga and C. Millard, "Cloud robotics law and regulation: Challenges in the governance of complex and dynamic cyber–physical ecosystems," *Rob. Auton. Syst.*, vol. 119, pp. 77–91, 2019, doi: 10.1016/j.robot.2019.06.003.

[23] S. Chatterjee, R. Chaudhuri, and D. Vrontis, "Usage Intention of Social Robots for Domestic Purpose: From Security, Privacy, and Legal Perspectives," *Inf. Syst. Front.*, 2021, doi: 10.1007/s10796-021-10197-7.

[24] S. Jain, C. Nandhini, R. D.-W. P. Communications, and undefined 2021, "ECC-based authentication scheme for cloud-based robots," *Springer*.

[25] A. K. Tanwani, R. Anand, J. E. Gonzalez, and K. Goldberg, "RILaaS: Robot Inference and Learning as a Service," *IEEE Robot. Autom. Lett.*, vol. 5, no. 3, pp. 4423–4430, 2020, doi: 10.1109/LRA.2020.2998414.

[26] J. Wan, J. Li, M. Imran, and D. Li, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Trans. Ind. Informatics*, vol. 15, no. 6, pp. 3652–3660, 2019, doi: 10.1109/TII.2019.2894573.

[27] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," *Int. J. Inf. Secur.*, vol. 21, no. 1, pp. 115–158, 2022, doi: 10.1007/s10207-021-00545-8.

[28] E. Fosch-Villaronga and T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," *Comput. Law Secur. Rev.*, vol. 41, 2021, doi: 10.1016/j.clsr.2021.105528.

[29] Y. Xianjia, J. P. Queralta, J. Heikkonen, and T. Westerlund, "Federated Learning in Robotic and Autonomous Systems," *Procedia Comput. Sci.*, vol. 191, pp. 135–142, 2021, doi: 10.1016/j.procs.2021.07.041.

[30] A. K. Tanwani, N. Mor, J. Kubiatowicz, J. E. Gonzalez, and K. Goldberg, "A Fog Robotics Approach to Deep Robot Learning: Application to object recognition and grasp planning in surface decluttering," *Proc. - IEEE Int. Conf. Robot. Autom.*, vol. 2019-May, pp. 4559–4566, 2019, doi: 10.1109/ICRA.2019.8793690.

[31] W. Liang, Z. Ning, S. Xie, Y. Hu, S. Lu, and D. Zhang, "Secure fusion approach for the Internet of Things in smart autonomous multi-robot systems," *Inf. Sci. (Ny).*, vol. 579, pp. 468–482, 2021, doi: 10.1016/j.ins.2021.08.035.

[32] S. Chatterjee, R. Chaudhuri, and D. Vrontis, "Usage Intention of Social Robots for Domestic Purpose: From Security, Privacy, and Legal Perspectives," *Inf. Syst. Front.*, 2021, doi: 10.1007/s10796-021-10197-7.

[33] S. Jain, C. Nandhini, and R. Doriya, "ECC-Based Authentication Scheme for Cloud-Based Robots," *Wirel. Pers. Commun.*, vol. 117, no. 2, pp. 1557–1576, Mar. 2021, doi: 10.1007/s11277-020-07935-6.