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

2. Fog/Cloud-based IoT Architectures for AI and Robotics

The Internet of Things (IoT) has changed how devices and people interact. A vast network of sensors, actuators, and smart devices collect and exchange data via the internet in IoT. The traditional Cloud computing model struggles to manage the massive amount of data generated by IoT applications as they grow in scale and complexity. As a complement to Cloud computing, Fog computing allows real-time processing and analysis of IoT data [14].

Fog computing, or Edge computing, brings Cloud computing closer to data sources and IoT devices. Decentralizing computation, storage, and networking reduces latency and improves system efficiency. Unlike cloud computing, Fog computing processes and analyses data at the network's edge using edge devices, access points, and servers [15].

Key Fog/Cloud-based IoT Architecture Components

Fog/Cloud-based IoT architectures depend on them. These devices measure temperature, humidity, light, and motion using sensors. The Fog and Cloud nodes process data collected by IoT devices. Fog nodes connect IoT devices to Cloud data centres [16]. Edge servers, routers, and gateways are placed near IoT devices or critical network points. Fog nodes aggregate and preprocess IoT device data, reducing latency and network congestion. Local data analysis allows real-time decision-making without the Cloud The advantages of developing robotics with the integration of Fog/Cloud with IoT are shown in Figure 1.

Cloud data centres store and process massive amounts of IoT data from multiple Fog nodes and devices. Cloud data centres have powerful computing, storage, and processing capabilities. They perform intensive data analytics, machine learning algorithms, and data storage that may not be feasible or efficient at the Fog layer [17].

3. Cloud/Fog IoT Architecture Workflow

Typical Fog/Cloud-based IoT architecture workflow:

Sensor-equipped IoT devices gather environmental data. The application can generate data in real-time or periodically.

3.1 Local Fog Layer Preprocessing

Nearby Fog nodes preprocess and analyse the collected data. Fog nodes filter, aggregate, and process data, removing irrelevant or unimportant data. Local processing reduces Cloud data transmission, saving network bandwidth.

3.2 Data Transmission

Secure channels send pre-processed data to Cloud data centres. This data transmission provides Cloud data centres with relevant data for analysis and decision-making.

3.3 Cloud-based Processing and Analysis

Cloud data centres use machine learning algorithms and advanced data analytics to gain insights from large data sets. Cloud layers can manage computationally intensive tasks that Fog layers cannot.

Data analysis yields actionable insights or commands. The Fog layer distributes these insights and commands to IoT devices for action or real-time feedback.

4. Fog/Cloud IoT Architecture Challenges

Fog/Cloud-based IoT architectures have many benefits but also many drawbacks [18]:

4.1 Security

Fog nodes are vulnerable to security breaches due to their decentralized nature. Data and system integrity depend on strong security and encryption at the Fog and Cloud layers.

4.2 Data Management

Large-scale deployments can make data management and synchronization difficult. Data integrity requires efficient data storage, retrieval, and synchronization.

Fog nodes have limited computational, storage, and energy resources. Maintaining system performance requires optimizing Fog node resource use and load balancing.

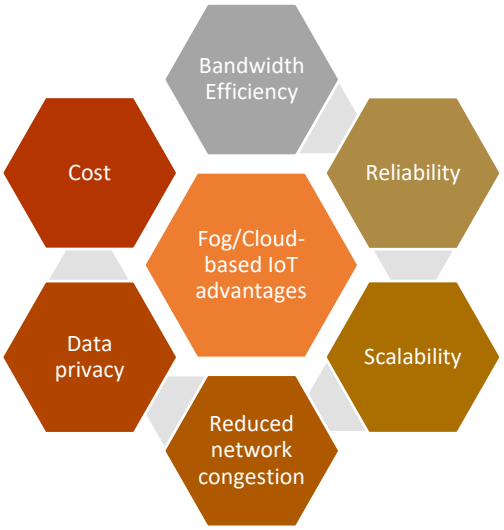

Figure 1: Fog/ Cloud based IoT advantages.

4.3 Interoperability

Different vendors make IoT devices and sensors with several types and communication protocols. Maintaining device-Fog/Cloud interoperability is difficult.

4.4 Edge-to-Cloud Decisions

Choosing whether to process data and tasks at the edge (Fog) or in the Cloud is difficult. Optimizing system performance requires balancing local processing and centralized Cloud analysis [19].

Fog/Cloud-based IoT architectures can solve the exponential growth of IoT data. This architecture enables real-time data

analysis, low-latency decision-making, and improved user experiences by combining Fog computing's edge processing with Cloud computing's scalability and power. To realize the full potential of Fog/Cloud-based IoT architectures in creating a more connected and intelligent world, security, data management, resource constraints, interoperability, and decision-making must be addressed.

5. Security Measures in Fog/Cloud-based IoT Systems

As Fog/Cloud-based IoT systems evolve and become more widespread, protecting these interconnected devices and their data becomes crucial. Fog computing's distributed nature, the considerable number of IoT devices, and their importance in various applications increase the attack surface for cyber threats. The Fog and Cloud layers must implement strong security measures to reduce these security risks and protect data integrity and confidentiality [20],[21]. This section discusses Fog/Cloud-based IoT security measures.

5.1 Authentication and Access Control

IoT devices and users must be authenticated before accessing the system. Password-based, two-factor, and biometric authentication ensure only authorized users can access IoT devices and sensitive data. Access control policies must be implemented to regulate user and device access based on roles and privileges. Fog/Cloud-based IoT systems use RBAC and ABAC access control models.

5.2 Encryption and Secure Communication

IoT devices, Fog nodes, and Cloud data centres need encryption to protect data. End-to-end encryption keeps data secure; only intended recipients can decrypt it. Fog/Cloud-based IoT systems use TLS and SSL for secure communication. MQTT and CoAP can also securely transfer data between IoT devices and the Fog layer.

5.3 Intrusion Detection and Prevention Systems (IDPS)

IDPS helps find and respond to cyber threats in real time. These systems analyse network traffic for signs of unauthorized access or malicious activity. The IDPS can alert, block suspicious traffic, or automatically counterattack when detecting an anomaly [22].

5.4 Security Patches and Updates

IoT devices, Fog node, and Cloud data centre software and firmware must be regularly updated to address known vulnerabilities. Manufacturers and developers should quickly release security patches and updates to fix vulnerabilities and prevent new threats. Automated updates can also keep devices and systems secure [23].

5.5 Secure Bootstrapping and Device Onboarding

New devices must be securely connected to the network to prevent unauthorized devices from accessing the Fog/Cloud-based IoT system. Secure bootstrapping involves device authentication and secure communication. Device certificates, PKI, and attestation can secure bootstrapping.

5.6 Trust Management and Blockchain Applications

Fog/Cloud-based IoT systems use trust management mechanisms to set up trust between entities. IoT devices, Fog nodes, and Cloud data centres must be trusted before accessing critical resources and data. Blockchain's decentralized and immutable ledger for transactions and device interactions can boost trust and security.

5.7 Physical Security

Fog/Cloud-based IoT systems need digital and physical security. IoT devices, Fog nodes, and Cloud data centres must have restricted physical access to prevent hardware theft. Access control, surveillance, and tamper-resistant enclosures can deter physical attacks.

5.8 Security Audits and Monitoring

Fog/Cloud-based IoT systems need regular security audits and checking to find vulnerabilities and security breaches. Security audits evaluate the system's security, while continuous monitoring tracks system activities, network traffic, and user behaviour for suspicious or malicious activity [24].

6. Privacy Preservation in Fog/Cloud-based IoT Systems

Fog/Cloud-based IoT systems collect and process substantial amounts of sensitive data from individuals, organizations, and smart devices, making privacy preservation a major concern. Fog computing's scale and distributed nature, combined with Cloud data centres' centralized data storage and processing, can make privacy protection difficult. Throughout the data lifecycle, privacy-preserving methods address these issues and protect personal data. This section discusses Fog/Cloud-based IoT privacy measures [25].
Anonymization and pseudonymization protect data subjects' identities. Data is anonymized by removing or obfuscating direct identifiers. However, pseudonymization allows data to be linked across records without revealing individual identities. These methods prevent re-identification and de-identify data before processing and analysis [26].

6.1 Differential Privacy

Differential privacy supplies mathematical guarantees to protect individual privacy while allowing useful data analysis. Before aggregation, it adds random noise to the data to minimize the effect of individual data. This mechanism prevents the extraction of individual data while allowing valuable insights from aggregated data.

6.2 Privacy-aware Data Processing
Privacy rules and policies are implemented during data processing. These methods minimize privacy breaches by ensuring data is managed according to privacy regulations and best practices. Privacy-aware algorithms and protocols balance privacy with data processing goals [27].

6.3 Data Minimization
Data minimization collects and stores only the data needed for a specific purpose. By collecting less data, privacy risks are reduced. Data minimization involves removing obsolete data.

6.4 Privacy Policies and User Consent Management
Fog/Cloud-based IoT systems need clear privacy policies to inform users how their data will be collected, processed, and shared. User consent management ensures explicit consent for data collection and use. Users can choose what data they share and for what purposes with granular consent preferences.

6.5 Secure Data Transfer and Storage
Encrypted communication channels and secure sockets protect data transmitted between IoT devices, Fog nodes, and Cloud data centres. Data encryption protects data at rest from unauthorized access.

6.6 Data Ownership and Control
Fog/Cloud-based IoT systems should enable data ownership and control. Data subjects should be able to access, change, remove, and revoke consent for data processing. This gives people control over their data and improves data management transparency.
Fog/Cloud-based IoT systems must follow privacy regulations like the EU's General Data Protection Regulation (GDPR) or the US's California Consumer Privacy Act (CCPA). These regulations protect privacy rights and hold organizations accountable for data processing [28].

7. Challenges and Limitations

Fog/Cloud-based IoT systems have many advantages, such as low latency, improved scalability, and enhanced data processing. Still, they also have several drawbacks that must be addressed for successful deployment and operation. This section will discuss Fog/Cloud-based IoT system challenges and limitations [29][30].

7.1 Resource Constraints and Performance Trade-offs
Fog nodes have limited computational, storage, and energy resources, which can affect system performance. Data processing and analysis tasks are distributed between the Fog and Cloud layers, compromising local processing efficiency for centralized Cloud computing. Maintaining performance requires balancing trade-offs and optimizing resource utilization [31].

7.2 Scalability and Latency
As IoT devices and data volume grow, Fog/Cloud-based IoT systems must scale. In dynamic, large-scale deployments, scalability and load balancing between Fog nodes and Cloud data centres can be difficult. Data transmission between Fog nodes and Cloud data centres may cause latency issues, affecting real-time applications.

7.3 Interoperability and Standardization Issues
Different vendors make IoT devices, resulting in various device types, communication protocols, and data formats. Interoperability between devices, Fog nodes, and Cloud data centres requires standardized communication protocols and data exchange formats. Interoperability issues can make Fog/Cloud-based IoT systems difficult to integrate [32].

7.4 Security Issues
Fog computing's distributed nature and many connected devices increase cyber threats. Security and monitoring are needed to secure fog nodes, cloud data centres, and communication channels. End-to-end security is essential to prevent data breaches and unauthorized access, especially during Fog Node-Cloud data transmission.

7.5 Privacy Issues
Fog/Cloud-based IoT systems manage massive amounts of data, including sensitive personal information. Privacy and data analysis are difficult. Data anonymization and differential privacy must be carefully applied to protect privacy without compromising data utility.

7.6 Edge-to-Cloud Decisions
Choosing whether to process data and tasks at the edge (Fog) or in the Cloud is difficult. To perfect system performance, consider data volume, latency, and computational complexity when balancing local processing and centralized Cloud analysis.

7.7 Energy Efficiency and Sustainability
Battery-powered IoT devices consume a lot of energy. IoT devices must balance real-time processing and data transmission with energy-efficient operation to extend battery life and reduce environmental impact. Energy efficiency can be improved by task offloading and sleep schedules.

7.8 Cost and Infrastructure
Cloud data centres and Fog nodes are expensive to deploy and keep Fog/Cloud-based IoT systems. Adopting these technologies requires consideration of infrastructure, operational costs, and ROI [33].

8. Conclusion

Fog computing, Cloud computing, and the Internet of Things (IoT) have created a transformative era of technological

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.