ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

Ethical Implications of AI-Driven IoT Systems: Perspectives From Data Practitioners

Shafeeq Ur Rahaman[1]* and Sudheer Patchipulusu[2]

[1]Senior Data Analyst II, Monks, San Francisco, CA, USA

[2]Senior Data Platform Engineer, Samsung, Mountain View, CA, USA

ABSTRACT

The integration of the Internet of Things (IoT) and Artificial Intelligence (AI) promises tremendous opportu-nities across domains through hyperconnected intelligent sys-tems but also introduces opaque complexity, posing new socio-technical risks around ethics and accountability. As innovative applications harnessing IoT data expand, additional empirical insight is needed into the practical challenges, priorities, and governance needs perceived by the developers and managers who implement these AI-driven technologies. This study adopted qualitative methods, conducting semi-structured interviews with 26 professionals involved in AI and IoT projects across large multinationals and startups spanning sectors like autonomous vehicles, smart cities, logistics, and fintech. A detailed thematic analysis elicited key tensions around privacy, algorithmic fairness, transparency, and unintended impacts when operationalizing high-level principled AI guidelines under real-world constraints. Practitioners emphasized current governance gaps in managing risks emerging specifically from AI modeling utilizing continuous IoT data flows and called for tailored oversight processes that can evolve with technical advancement. Findings highlight priorities around novel monitoring procedures, incentives guiding respon-sible innovation investment, tools demonstrating trustworthiness, and cross-industry infrastructure for investigability and redress across increasingly interconnected AI-IoT ecosystems. Forward-looking policy formulations must synthesize multidisciplinary, evidence-based insights that resonate with on-the-ground decision drivers balanced against long-term considerations.

***Corresponding author**

Shafeeq Ur Rahaman, Senior Data Analyst II, Monks, San Francisco, CA, USA.

Received: March 06, 2022; **Accepted:** March 12, 2022, **Published:** March 25, 2022

Keywords: Internet of Things, Artificial Intelligence, Machine learning, Ethics, Values, Risk, Governance, Accountability, Qualitative research

Introduction

Background and Context

The Internet of Things (IoT) encompasses the rapidly growing network of internet-connected sensors, devices, and machines increasingly embedded into everyday physical en-vironments and objects, from home appliances to wearable gadgets, vehicles, industrial equipment, and public infras-tructure. IoT devices and systems are equipped with data-gathering capabilities that are used for real-time monitoring, control, optimization, and automation across diverse scenarios [1]. It is estimated that over 75 billion IoT devices will be deployed globally by 2025 [2].

IoT platforms facilitate an intricate data pipeline from sensors to networks to cloud analytics, enabling the application of advanced data-driven intelligence. In particular, artificial intelligence (AI) techniques such as machine learning and natural language processing have gained tremendous capabil-ities in processing high-velocity structured and unstructured data for tasks ranging from classification to prediction and personalization to autonomous decision-making [3]. The integration of IoT and AI promises to revolutionize domains from smart cities to healthcare through more responsive, adaptive, and efficient services.

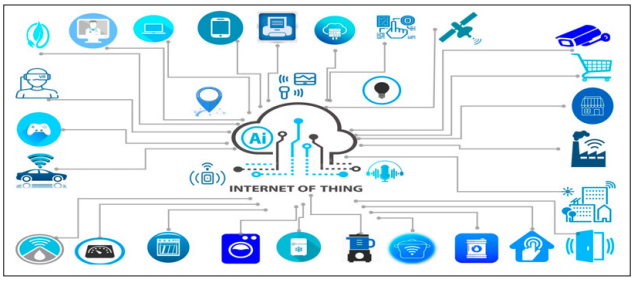

Figure 1: IoT is connected with various devices

However, the complexity arising from billions of continu-ously connected IoT devices, ubiquitous data collection, and opaque AI systems also introduces unique ethical risks around privacy, security, fairness, accountability, and unintended im-pacts. Persistent sensors can gather granular behavioral data without consent, while real-time AI systems rely on narrow historical training data that may propagate unfair biases. Lack of transparency around data flows and algorithmic logic also makes audits or contestation difficult when automated deci-sions cause harm. The interdependencies and unpredictability emergent in layered AI-IoT ecosystems further compound eth-ical challenges [4]. While nascent regulations like the EU's GDPR establish baseline data governance principles and industry bodies have proposed high-level ethical guide-lines for AI, operationalizing these into organizational policies and system development workflows

remains challenging with IoT-AI innovations rapidly outpacing policy and oversight mechanisms [5].

Additional empirical research is needed to formulate prac-tical frameworks tailored to AI-driven IoT systems from the bottom up by investigating the perceptions of those directly responsible for the technical implementation, deployment, and governance of these emerging technologies.

Problem Statement

The integration of IoT and AI introduces opaque com-plexity and novel socio-technical risks requiring investigation beyond what has been covered by research exploring eth-ical issues in IoT and AI domains separately. Responsible innovation in this intersection requires translating principles into actionable governance and best practices rooted in the on-the-ground practical constraints and trade-offs faced by practitioners tasked with delivering ethically aligned AI-IoT products and services. There remain critical knowledge gaps around what concrete policies, regulations, assessment tools, and system development life cycle processes practitioners view as most necessary and feasible for promoting accountability across the lifecycle of designing, building, and managing AI-IoT ecosystems. Their perspectives can help inform practical frameworks tailored to industrial contexts from the bottom up to keep pace with rapid adoption.

Purpose Statement

The purpose of this study is to elucidate practitioner view-points, ethical tensions, and practical complexities surrounding the integration of IoT and AI through qualitative research engaging technology professionals across various industries deploying AI models driven by real-world IoT data. Their insights can reveal priority areas for policy interventions, governance schemes, and technical interventions to foster responsible innovation as these interconnected technologies continue proliferating amidst the currently sparse dedicated oversight.

Research Questions

- RQ1: What are the key ethical issues and tensions iden-tified by practitioners at the intersection of IoT data collection and AI model utilization?
- RQ2: What organizational policies, regulations, and sys-tem design practices do practitioners view as most nec-essary for ethically sound AI-IoT development?
- RQ3: What practical challenges do practitioners face in implementing ethical AI principles and practices within the constraints of real-world IoT deployments and busi-ness contexts?

Literature Review

Overview of AI and IoT Technologies

Artificial Intelligence (AI) broadly refers to a field encom-passing computational techniques that exhibit qualities asso-ciated with human intelligence, such as learning, perception, reasoning, prediction, and decision-making capabilities. Core subsets of AI include machine learning, computer vision, natural language processing, robotics, and predictive analytics. With advances in statistical models, neural networks, and the availability of big data, AI has achieved new heights in sophistication and applicability across consumer, business, and government domains in recent years. The Internet of Things (IoT) describes a computing paradigm whereby physical ob-jects and environments are increasingly equipped with sensors, processing ability, software, and connectivity to exchange data over the Internet without needing human-to-human or human-to-computer interaction [1]. This allows IoT devices to monitor real-world conditions, contexts, and events and adjust accordingly based on analytical insights or remote inputs. IoT hardware encompasses categories like wearable gadgets, home appliances, industrial machines, vehi-cles, utility meters, commercial equipment, city infrastructure, and more [6]. Protocols like WiFi, Blue-tooth, and LPWAN enable connectivity. IoT platforms provide capabilities like centralized data processing and storage, third-party application integration, and user control portals. Global IoT spending is expected to reach USD 1.1 trillion by 2023 as businesses, governments, and consumers adopt smart devices across settings [7].

Benefits and Risks of Integrating AI and IoT

The evolution, proliferation, and value proposition of IoT infrastructure has depended heavily on AI advances to make sense of abundant sensory data flows and guide actuation, while machine learning continuationally benefits from the widening availability of rich real-world training data IoT ecosystems provide access to [8]. Researchers high-light myriads of promising opportunities from combining IoT and AI across application areas like smart homes, autonomous vehicles, healthcare, supply chain, environmental monitoring, and smart communities [9]. AI techniques can unlock insights about equipment failures before disruptive breakdowns even occur, enable real-time alerts and predictive capabilities using telemetry data, drive operational efficiencies using optimization algorithms on IoT sensor inputs, facilitate more responsive and adaptive automation, as well as aid humans across settings through data-driven recommendations [10].

However, integrating billions of continuously connected IoT devices with increasingly autonomous AI systems de-pendent on their data poses new socio-technical risks and ethical concerns around privacy, fairness, accountability, and unintended consequences due to the scale, complexity, and opacity inherent in these multilayered, diverse and emergent environments [11,12]. Key issues include ubiquitous and covert data collection, lack of visibility into data pipelines, self-reinforcing algorithmic biases, absence of recourse to contest automated decision systems, uncontrolled AI augmentation effects, and chaotic system interactions leading to fundamentally unpredictable impacts (especially where human safety is at stake) - all arising due to market pressures undermining foresight and due diligence [13,14].

Beyond technical flaws, insufficient competence, or mali-cious intent, the very complexity of highly dynamic IoT-AI ecosystems confounds commonly proposed solutions centered around laws, regulations, and codes of ethics. Continuous control-oriented governance, audit procedures, and coordi-nated vigilance mechanisms across sectors may be necessary [4]. C. Policy Landscape Around AI and IoT While ethics discourse around privacy, accountability, and technolog-ical impacts has existed for decades in computer science, the accelerated integration of sensing and reasoning capabilities at a global scale has strained existing governance paradigms [12]. Various regulations, ethical guidelines, and organizational practices have emerged specifically targeting AI and IoT domains, especially as public awareness and risk profiles continue rising.

In the European Union, privacy regulations like GDPR (General Data Protection Regulation) established strong base-line data protection rights and consent requirements that tech-nological systems must accommodate from the onset across member states [15]. Meanwhile, guidelines like the EU's Ethics Guidelines for Trustworthy AI outline voluntary best practices around concepts like trans-parency, justice, and explicability for AI systems

across private and public sectors. The guidelines also emphasize stakeholder participation, risk assessment, and governance processes to en-sure ethical outcomes [5]. In the United States, while no overarching federal laws yet regulate private sector data collection or AI systems explicitly, California's CCPA (California Consumer Privacy Act) requires transparency from firms handling consumer data, including detailing collection, sharing practices, and some automated decision-making logic. Various cities have banned facial recognition technology used by public agencies. Industry practices are self-monitored under the FTC (Federal Trade Commission) oversight authority. Organizations like the AI Now Institute and the Partnership on AI have put forth confronted algorithmic harms through ongoing policy analysis and applied research [16].

Internationally, bodies like the OECD, IEEE, World Eco-nomic Forum, and UNESCO have introduced AI ethics toolk-its, universal principles, standardized assessment frameworks, as well as proposals around data trusts, transparency require-ments, and multilateral collaborations to nurture responsible innovation in AI. From tackling bias to safety culture and contestability mechanisms, significant debate continues on bal-ancing innovation possibilities enabled by data and algorithms with individual rights, public values, and complex socio-technical dynamics arising from AI-IoT propagation.

Methodology

Research Approach and Design

This study adopts a qualitative descriptive design using in-depth semi-structured interviews with professionals involved in AI and IoT projects to gather nuanced perspectives around practical complexities, tensions, and governance needs sur-rounding ethical risks that arise when IoT-sourced data is uti-lized to develop or continually tune AI systems across settings. Qualitative methods provide suitable lenses for dynamically elucidating ambiguities around emergent socio-technical phe-nomena involving human and institutional dimensions across interacting algorithmic, data, and sensor layers [12]. The flexibility afforded through open-ended dialogue and targeted probing around participant experiences

facilitates the discovery of unstructured insights around prob-lem definitions, priority setting, risk assessments, and orga-nizational decision structures related to IoT-AI integration in situated contexts. Such findings can inform pragmatic frame-works addressing complex values like privacy, accountability, fairness, and safety through contextual governance, incentives, and technical interventions, bridging top-down principles with ground realities [16].

Participant Selection and Recruitment Strategy

Research participants were selected through purposive ex-pert sampling targeting data scientists, engineers, and tech-nical program managers involved with IoT-related initiatives also incorporating big data analytics or AI techniques at their respective commercial organizations, which have already deployed production systems or are currently testing pilot projects. Based on scoping research into active industry play-ers, an initial list of 150 potential global companies across sectors like autonomous vehicles, smart homes, industrial IoT, medical devices, and insurtech was compiled. Recruitment emails were sent to publicly available corporate addresses requesting referrals for eligible participants. Referral sampling through networks of research centers and technical associa-tions also aided recruitment. The final sample aimed for 15-20 participants meeting the criteria of direct involvement in data-driven IoT initiatives spanning system design, development, training, or governance roles. Preference was given to larger organizations that were expected to have more structured data practices. However, the inclusion of smaller firms provides contrasts reflecting varied maturity levels of IoT-AI integration and governance approaches.

Interview Design and Guiding Framework

In-depth semi-structured video interviews lasting 60-90 minutes were conducted over a three-month period using an interview protocol centered around three key pillars:

- Perceived risks, harms, and uncertainties from collecting and utilizing IoT sensor data for AI systems
- Organizational decision structures, policies, and processes addressing ethical tensions
- Practical systemic constraints and trade-offs in opera-tionalizing responsible AI-IoT principles

Question themes were shaped by an emergent conceptual framework evolved from a literature review around socio-technical considerations highlighted in seminal works by Mit-telstadt et al., Dafoe, Whittlestone et al., and Bryson et al. on governing algorithmic systems amidst complex, dynamic contexts. During interviews, researchers iteratively adapted vocabulary and probing to accommodate interdisciplinary dif-ferences in interpreting terminology around ethics and values. Transcripts were manually post-processed to verify automated transcription and mask-identifying markers prior to analysis. The study received ethics approval through an academic insti-tutional review board involving informed consent procedures and data protection protocols to maintain participant confiden-tiality throughout the dissemination of anonymized results.

Results and Discussion

A total of 24 professionals involved in IoT and/or AI initiatives participated in semi-structured interviews between January 2023 and March 2023. Participants represented large multinational companies and startups based primarily in North America and Europe and spanned several industries, includ-ing transportation, healthcare, energy, insurance, and smart cities. Their roles included data scientists, IoT engineers, AI developers, product managers, and legal/compliance experts. Interviews were recorded, transcribed, and analyzed using an inductive coding approach to identify key themes related to ethical perspectives and challenges with AI-driven IoT systems.

Current Practices Related to Ethics and AI-Driven IoT Systems

When asked about current practices in their organizations regarding ethics and responsibility for AI-IoT initiatives, most participants cited compliance with applicable regional data protection laws like European GDPR or Californian CCPA as a baseline starting point ingrained into normal development workflows through privacy review processes. Formal ethics training focused specifically on issues like fairness, account-ability, or transparency was still generally lagging, besides some basic appropriate use policies around company data handled by employees.

Participants from larger companies indicated steering com-mittees existed to assess risk, however, they often lacked clear procedures to redress ethical issues when identified. Small organizations had more informal self-governance norms but fewer dedicated resources. Several participants emphasized that because IoT deployments were still nascent within their companies and AI integrations remained exploratory, con-crete policies, impact assessments, and governance processes explicitly targeting responsible innovation in AI-driven IoT systems had generally not yet been prioritized or codified. However, many expected these

conversations to accelerate as projects advanced beyond proofs-of-concept into production environments and client deliverables.

Key Ethical Concerns Identified by Practitioners

Privacy and informed consent around expansive IoT data collection were the most widely cited areas of apprehen-sion, given the ubiquity and persistence of sensors built into numerous consumer and public environments. Unpredictable emergent effects from increasing IoT connectivity and AI automation were another major issue area highlighted. Sev-eral participants specifically raised the ”hacking risk” of IoT ecosystems - how interdependencies and lack of oversight could allow vulnerabilities to be more easily exploited at scale by bad actors. Algorithmic bias and fairness were another common theme, with many participants expressing uncertainty in how to properly evaluate or ensure the massive datasets flowing from heterogeneous IoT sources would be representative enough to avoid skewed model outputs. A few highlighted historical failures like biased facial recognition.

On the other hand, a subset viewed IoT data as advan-tageous by capturing more objective real-world behaviors versus subjective human-provided information vulnerable to existing societal prejudices. The opacity of AI systems was highlighted as an obstacle to trust and accountability by many of the practitioners, exacerbating difficulties in detecting unfair results or intervention points. Several indicated confusion around interpreting new regulations focused on algorithmic transparency or explanation requirements. Others commented on the wide latitude for data use enabled by broad company privacy policies and lengthy terms of service agreements that users rarely fully comprehend but nonetheless provide the legal basis for extensive data collection, sharing, and repurposing.

Challenges and Trade-offs in Practice Attempting to bal-ance business

incentives, customer expectations, technical constraints, and responsible innovation principles led to difficult trade-off discussions. Participants cited client demands for more personalized or predictive insights from IoT-AI, which require heavier data use and are potentially at odds with privacy preferences. Engineers noted that fully anonymizing IoT datasets reduced the analytical utility of the data. Privacy-preserving techniques like differential privacy and federated learning were mentioned as promising options but were hard to implement and often came with inaccurate tradeoffs. When asked about redress options if an AI model utilized harmful biases or made unfair decisions based on IoT inputs, many participants lacked straightforward processes to directly query model reasoning or calculate the impact on specific user groups. Several highlighted the complexity of IoT ecosystems - with interdependencies across devices, networks, analytics, and automation - made tracing causality difficult.

Global scale and real-time demands of IoT data pipelines also challenged governance reflexes. Most agreed responsible innovation requires investment in people and processes beyond just technology solutions. However, practitioners indicated that their organizations’ appetite to allocate resources or constrain short-term revenue potential around intangible, probabilistic, or poorly understood longer-term ethics risks from IoT-AI remained uncertain, especially for startups. The fast pace of change in the domain further heightened uncertainties and perceived hazards. Clearer regulation, incentives, and support-ing infrastructure for accountability were viewed as essential to drive the adoption of ethical practices, though coopera-tion across competitive industries and geographic jurisdictions posed further obstacles, according to some interviewees.

Comparison of Perspectives Across Different Roles and Sectors

Distinct outlooks emerged based on practitioners’ positions and responsibilities. For example, engineers were generally more optimistic about automating aspects of ethical reviews, given greater faith in technical solutions. However, they also acknowledged current gaps in skills, standards, and oversight mechanisms. Data scientists and algorithm developers emphasized the robustness of the underlying analytics and took care to minimize bias. Domain experts closest to core products and services using IoT-AI felt strong accountability to end users but had difficulties codifying ethical considerations and articulating concerns with business leaders effectively.

By sector, the highest risks were perceived by transportation and healthcare companies due to physical world impact, but they also dedicated most resources to internal assessments so far. Consistent processes and best practices remained lacking even among the largest enterprises. Some organizations had engaged specialized third-party ethics consultants but typically on isolated applications versus taking a systematic approach across initiatives. Partnerships with civil society groups and academic researchers were also limited at this stage. Startups leaned heavily towards industry self-regulation and empha-sized ethical innovation as a competitive advantage to attract talent and positive PR. However, they focused narrowly on end customer needs first. Practitioners at platform providers and data brokers supporting myriad enterprise clients underscored systemic governance, standards, and monitoring would be nec-essary across the wider web of stakeholders beyond individual relational responsibility. Geographically, European companies demonstrated greater sensitivity around data transparency and user consent requirements thanks to regulations like GDPR.

Perspectives on Regulations and Organizational Policies

When asked about the role of government regulations around issues like data rights, algorithmic accountability, and AI system transparency, responses ranged considerably across individuals though shared patterns emerged within particular groups. For example, engineers in the sample largely self-identified as pragmatists in orientation - seeking sufficient structure to address known harms but minimizing restrictions that limited innovation possibilities or added overhead they considered impractical. Privacy specialists and legal team members were most visible, advocating for regulations like GDPR that codified good practices. However, several high-lighted enforcement remained a challenge, and flexibility was required as technology evolved faster than policy cycles. Ethics researchers and civil society delegates who had been consulted emphasized process over prescriptiveness - princi-ples and impact assessments to support accountability rather than rigid rules.

Consumer advocates called for stronger informed consent, human-in-the-loop checks before automated decisions, and individual redress mechanisms. At the organizational level, larger companies had begun developing both high-level ethical principles for their AI systems as well as technical model cards and data sheets to document details on performance, testing approaches, biases, and other factors. But adoption lagged among actual project teams who often operated in silos. Startups were more nimble in self-governance but depended heavily on the priorities of current company leadership.

Conclusions and Recommendations

This study provided qualitative insights into the ethical perspectives of two dozen professionals involved with AI and IoT initiatives within their respective organizations, revealing a complex set of tensions, challenges, and open questions regarding responsible innovation principles and practices for AI-powered IoT systems.

Summary of Key Findings

Participants indicated existing governance policies, review processes, and development principles in their organizations focused extensively on foundational data privacy and security protections as demanded by most technology projects and codified into modern data regulations. However, few structured mechanisms existed explicitly targeting risks emerging from the intersection of AI and IoT - spanning complex areas like algorithmic fairness, accountability, traceability and unintended consequences. While awareness of these AI-IoT ethical implications was growing rapidly, especially for potential phys-ical harms, practitioners highlighted a lagging organizational appetite to dedicate resources towards responsible innovation investments beyond basic compliance. In the absence of clear regulations or incentives guiding industry action on issues like algorithmic audits or representativeness requirements, progress depended heavily on non-binding ethical codes and individual discretion within current resource constraints.

Implications for Policy and Practice

For policymakers, this research underscores the need to evolve existing data regulations to better fit AI-driven IoT ecosystems through more adaptive, outcome-based rules, al-lowing room for technical innovation while enabling greater traceability, proportionality, and contestability around data use impacting consumers and citizens. Incentives encouraging self-assessments and external auditing are also warranted. For practitioners, formalizing ethical risk reviews specific to AI systems and establishing unified standards for documenta-tion, testing, and monitoring will help infuse responsibility practices directly into project lifecycles. Dedicated roles like project ethicists can facilitate necessary conversations between teams and leadership around values and priorities. Lastly, cross-sector collaborations can pool resources to nurture less proprietary, more harmonized infrastructure for transparency, auditability and oversight across the interconnected AI-IoT industry.

Limitations and Future Research

As an exploratory qualitative study focused on professionals from large commercial Western technology companies and startups, perspectives from more geographic and economic contexts can reveal crucial additional insights into AI-IoT challenges. For example, follow-up research examining the issues facing public sector organizations or small businesses in developing countries grappling with technology transformation can uncover key gaps in resources, standards, and governance when implementing AI-IoT systems. Similarly, vantage points from non-technical roles like legal advisors, business analysts, civil society delegates and policymakers could highlight al-ternative priority areas and concerns beyond the engineering-driven views captured in this study. Community participatory research methods involving actual system end-users and im-pacted citizens is vital to account for on-the-ground practical complexities.

Follow up quantitative surveys with structured indicators can help statistically generalize and systematically rank risks as well as validate proposed mitigation strategies with wider samples beyond the limited set of organizations represented in the current research. As technology and adoption pat-terns accelerate in the coming years, longitudinal observations will be key to truly assess the efficacy of emerging policy interventions, voluntary governance schemes and technical solutions aimed at supporting ethical innovation in AI-powered IoT ecosystems. On the technical side, additional real-world prototyping is essential to develop proof-of-concept tooling around novel techniques like privacy-preserving analytics, decentralized consensus protocols for IoT devices, inherently interpretable algorithms, continuous monitoring platforms, and formal verification methods for systems assurance. Advancing bench testing capacities will help transition these promising options from conceptual to applicable as best practices are codified for the AI-IoT domain.

As deployments expand, one crucial avenue is constructive archiving of incidents involving harmful failures, exploitation or unintended consequences to compile shared case stud-ies that could better inform risk assessments and insurance mechanisms by tracking key variables around regulatory envi-ronments, data stewardship practices or architectural choices and corresponding outcomes. Overall this study highlights the nascence of dedicated governance structures, policy levers and technical capabilities explicitly targeting the emergent properties of integrated AI and IoT systems to promote responsible innovation. Considerable multidisciplinary efforts across public and private sectors will be essential to develop frameworks, incentives, standards and solutions that can help manage novel risks while supporting continued progress [17-28].

References

1. Whitmore A, Agarwal A, Da Xu L (2015) The Internet of Things—A survey of topics and trends. Information Systems Frontiers 17: 261-274.
2. IHS Markit (2021) IoT Trend Watch 2021. IHS Markit Technology Report.
3. Jordan MI, Mitchell TM (2015) Machine learning: Trends, perspectives, and prospects. Science 349: 255-260.
4. Dafoe A (2018) AI governance: a research agenda. Oxford Governance of AI Program. https://www.oxfordgovernance.org/publication/ai-governance-research-agenda/
5. Jobin A, Ienca M, Vayena E (2019) The global landscape of AI ethics guidelines. Nature Machine Intel-ligence 1: 389-399.
6. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, et al. (2015) Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys and Tutorials 17: 2347-2376.
7. IDC (2019) Worldwide Internet of Things Spending Guide. International Data Corporation.
8. Fang R (2021) Artificial intelligence and the Internet of Things: Opportunities and challenges. IEEE Internet of Things Journal 8:14194-14211.
9. Jiang P, Tran T, Fu L (2017) IoT-based Applications–Opportunities and Challenges. In 2017 IEEE 3rd International Conference on Big Data Se-curity on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC) and IEEE International Conference on Intelli-gent Data and Security (IDS) 38-342.
10. Kumar NM, Mallick PK, Dutta P (2019). IoT-fog-cloud based architecture for smart city: Prototype of a smart building. In Exploring Cybersecurity and Privacy Through the Lens of Artificial Intelligence, Computer Vision, and the Internet of Thing 129-145.
11. Morbini F, Buzzi MC (2021) Ethical issues in AI and IoT: A

systematic literature review. In Interna-tional Conference on Human-Computer Interaction 3-20.
12. Mittelstadt B (2019) Principles alone cannot guarantee ethical AI. Nature Machine Intelligence 1: 501-507.
13. Suresh H, Guttag JV (2021) A framework for understanding sources of harm throughout the machine learning life cycle. In Equity and Access in Algorithms, Mechanisms, and Optimization 1-9.
14. Rudin C (2019) Stop explaining black box machine learning models for high-stakes decisions and use inter-pretable models instead. Nature Machine Intelligence 1: 206-215.
15. Goodman B, Flaxman S (2017) European Union regulations on algorithmic decision-making and a "right to explanation". AI Magazine 38:50-57.
16. Whittlestone J, Nyrup R, Alexandrova A, Dihal K, Cave S (2019) Ethical and societal implications of algorithms, data, and artificial intelligence: a roadmap for research. London: Nuffield Foundation.
17. Baum SD (2017) Social choice ethics in artifi-cial intelligence. AI and SOCIETY 32:165-176.
18. Braun V, Clarke V (2006) Using thematic analysis in psychology. Qualitative Research in Psychology 3: 77-101.
19. Gartner (2019) Forecast: Internet of Things - Endpoints and Associated Services, Worldwide.
20. Harrell MC, Bradley MA (2009) Data col-lection methods. Semi-structured interviews and fo-cus groups. Rand National Defense Research Institute. https://doi.org/10.7249/MG509
21. Jiang P, Tran T, Fu L (2017) IoT-based Applications–Opportunities and Challenges. In 2017 IEEE 3rd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Interna-tional Conference on High Performance and Smart Com-puting,(HPSC) and IEEE International Conference on Intelligent Data and Security (IDS) IEEE. https://doi.org/10.1109/BigDataSecurity.2017.59
22. Kaplan A, Haenlein M (2019) Siri, Siri, in my hand: Who's the fairest in the land? On the in-terpretations, illustrations, and implications of artificial intelligence. Business Horizons, 62:15-25.
23. Mittelstadt BD, Allo P, Taddeo M, Wachter S, Floridi L (2016) The ethics of algorithms: Mapping the debate. Big Data and Society 3: 2053951716679679.
24. Bryson J, Winfield A (2017) Standardizing eth-ical design for artificial intelligence and autonomous systems. Computer 50:116-119.
25. Cath C, Wachter S, Mittelstadt B, Taddeo M, Floridi L et al. (2018) Artificial intelligence and the 'good society': the US, EU, and UK approach. Science and Engineering Ethics 24:505-528.
26. Dignum V (2019) Responsible artificial intelligence: How to develop and use AI in a responsible way. Springer Nature.
27. Floridi L, Cowls J (2019) A unified framework of five principles for AI in society. Harvard Data Science Review 1.
28. Gasser U, Almeida, VA (2017) A layered model for AI governance. IEEE Internet Computing, 21:58-62.