Journal of Computational Analysis and Applications **VOL. 33, NO. 8, 2024**
10.48047/jocaaa.2024.33.08.32

Ethical AI in Iot and Embedded Systems: Investigating Ethical Considerations and Frameworks for AI-Driven Decision-Making in Iot and Embedded Systems

Sangeeta Singh

Firmware Engineer III, Variosystems Inc, Southlake TX USA

Email: sangeeta96@gmail.com

ABSTRACT
The article examines the ethical issues of integrating artificial intelligence in the Internet of Things (IoT) and embedded systems based on transparency, accountability, and decision making autonomy. AI driven IoT application in various sector has been studied for security risks, algorithmic bias and the need for the explainable AI (XAI) platform. Results demonstrate a great demand for regulatory guidelines and ethical assessment frameworks to reduce the risks. Based on the research, it is concluded that the combination of the AI autonomy and human oversight is essential to prevent the deployment of ethical AI in IoT and embedded systems, which supports the trust and reliability of emerging technologies.

KEYWORDS: Ethical AI, Internet of Things (IoT), Embedded Systems, AI in Industrial Automation, AI Frameworks, AI and Data Privacy, AI in Smart Cities, AI in Cybersecurity.

1. INTRODUCTION

Advancement of AI embedded systems and IoT is so quick that it can transform over many industries: automation, smart decision making, and data driven insight. However, the integration of these two also has full spectrum problems such as transparency and accountability, security and algorithmic bias. The reason for the growing pressure on developing ethical frameworks for AI is because AI is making wider applications, from healthcare to autonomous vehicles, and over the top industrial automation.

In this research, the work focuses on the ethical issues of AI enabled IoT and how they affect industry. The study attempts to contribute to development of AI practices with a mind to be responsible in IoT and embedded system applications by looking at holes and potential fixes for ethics.

Trust Management

Artificial Intelligence (AI) is now bridging the gap between the Internet of Things (IoT) and embedded systems which are now transforming industries and urban environments in a number of ways; however, it has also brought a number of ethical concerns.

10.48047/jocaaa.2024.33.08.32

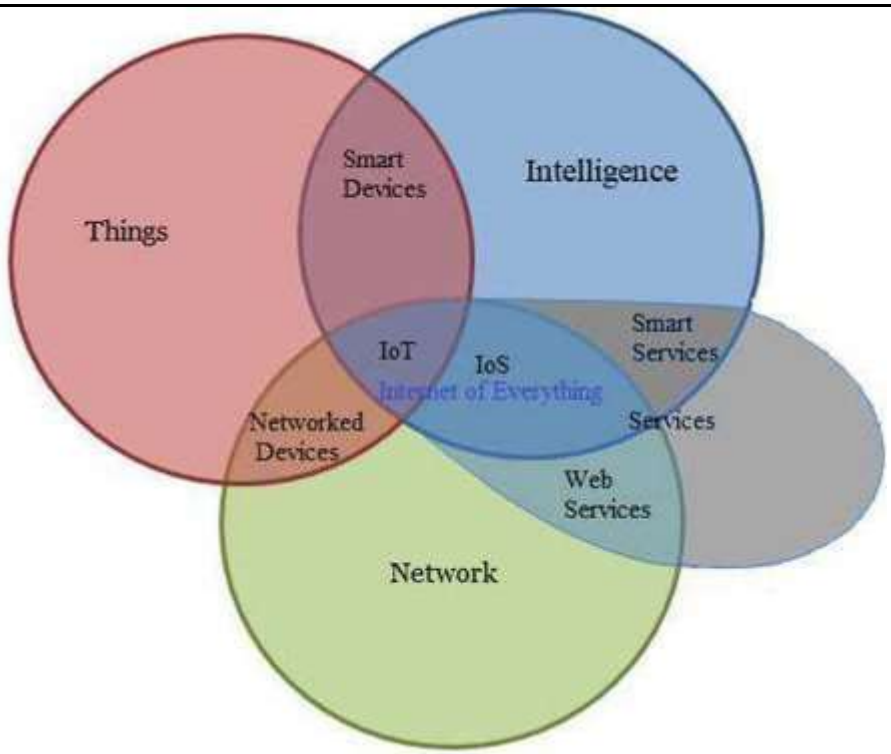

Figure 1: Internet of Things Scope (Ghosh et al., 2018)

Some of these issues are trust management, security, accountability, privacy, and of course, the broader social implications of such autonomous decision making by AI devices. These ethical dimensions are important to build AI driven IoT in such a way to conform to human values, regulatory objectives, and social requirements.

SIoT's foundational pillar is trust in which devices interact autonomously and with a social background. According to Bangui et al. (2023), AI based trust management system is important to improve system credibility and reliability in cyber physical systems.

Ethical concerns appear as models mature slow with AI to deal with fairness, transparency and consciousness for society. Eleven ethical dimensions that fall short of separating trust models using AI in vehicular networks and underwater acoustic sensor networks are studied. This implies that although AI can enhance security, that it does not possess the ethical readiness to do so. The use of ethical AI in the industrial environment is a developing problem. In a paper, Vermesan et al. (2022) discuss the ethical challenges AI imposes when integrated into manufacturing process and how transparency, fairness, and trustworthiness are needed. The more complex AI becomes, driving industrial automation, places questions about environmental integrity, displacement of workforce and concentration of power in the hands of a number of corporations. The study highlights the value of having accounting frameworks and certification schemes to determine AI's ethical compliance. The safety, security and reliability norms are maintained through these measures.

10.48047/jocaaa.2024.33.08.32

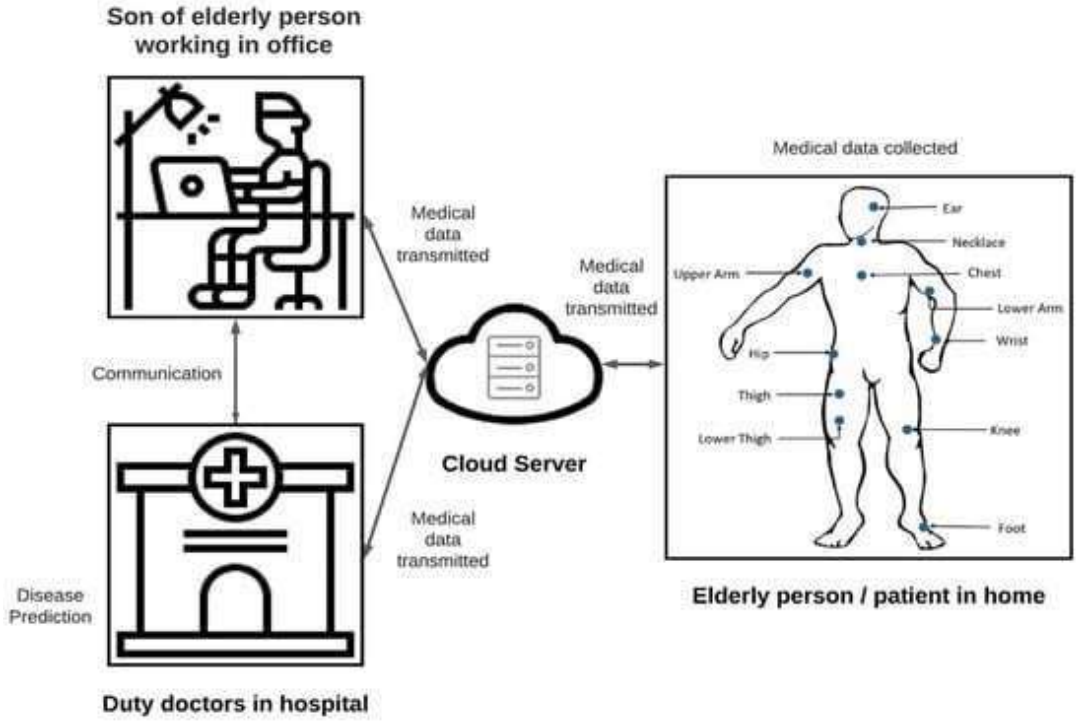

Figure 2: AI and IoT CPS (Ramaswamy et al., 2022)

Privacy and Accountability

The prevalence of IoT is calling out to one (rather important) class of privacy and accountability issues in autonomous decision making. Discussion by Pasricha and Wolf (2022) relates ethical conflicts of employing AI in the semiconductor chip design and IoT applications. They demonstrate how Technician Choices in Designing AI determines the ethical results, usually within ways designers could not instantly see. The focus is on the need for taking an ethical gaze throughout the development of an AI system — most spatially in space-constrained computing systems.

Similarly, Sholla et al. (2021) claim that the ethical consequences of IoT technology in urban circumstances have been underexamined. AI makes the context sensitive ethical decisions by incorporating social parameters through the neuro fuzzy systems (NFSs).

With their model, smart devices will have to respect human values, and thus, ethical smart city ecosystems become possible. Since this aligns with broader AI ethics principles, in this approach fairness, transparency and human centric decision making are observed.

Security is another key ethical issue. AI enhanced security mechanisms exist but the sophistication of the attack methodologies to traditional counters is great. The research suggests embedding AI driven security cores into embedded systems to observe behavior of data for resilience, against cyber threats. In this solution, it brings up ethical concerns regarding algorithmic transparency, and whether or not the bias that can and will be embedded in the AI system will unintentionally infringe upon the users' privacy.

Ethical AI Frameworks

Robust framework and a policy of an AI ethics is a need of the IoT aid to be in a structured path. In Chatterjee (2020), ethics is studied in securing IoT enabled smart city systems. In their study that is based on a conceptual model validated with statistical surveys, it is shown that trust factors have no influences on technology adoption.

10.48047/jocaaa.2024.33.08.32

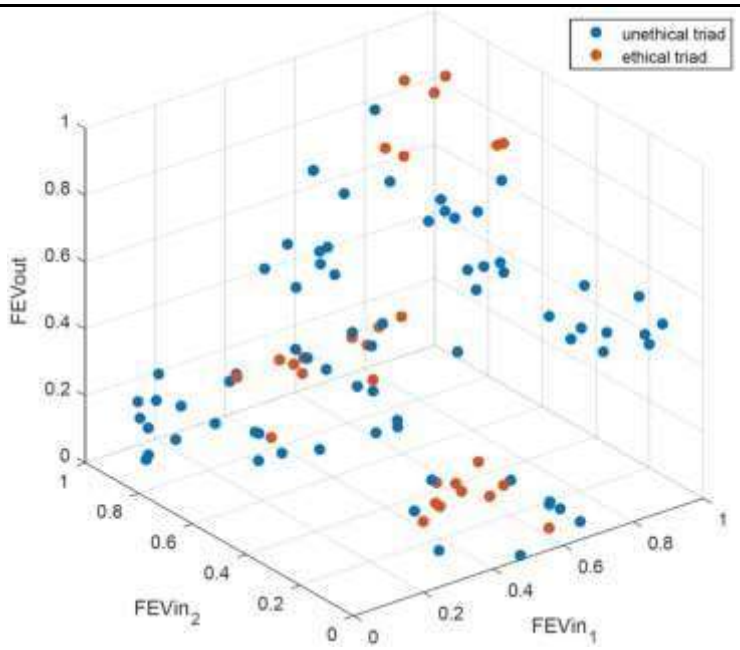

Figure 3: Ethical and Unethical Triad (Sholla et al., 2020)

This implies that ethical AI frameworks cannot just stop at efforts on trust building but should be aiming towards what is tangible in terms of security and compliance. As provided by Loke (2021) a broad systematic overview of ethical issues in IoT, one is algorithmic bias, user autonomy and machine's unexpected problems.

The approaches such as programming ethical behavior into AI, using algorithms for transparency and regulatory guidelines are reviewed for the study. This shows that it is required to use a multi-pronged ethical approach towards IoT application where core challenges are diverse.

In Cornetta and Touhafi (2021), the authors discuss how machine learning is harnessed in AI powered embedded systems to make real time decision. Specifically, their analysis touches on the issues of ethics related to moving data processing away from cloud and to edge devices in terms of the privacy, autonomy, and accountability of the system.

Figure 4: AI in Embedded Systems (O'Reilly, 2023)

10.48047/jocaaa.2024.33.08.32

With the rise of AI in the embedded IoT devices, the ethical compliance remains a problem when these devices are used in low power and resource constrained environments. Various aspects of the ethical challenges of AI in use are brought out in the literatures on IoT and embedded systems.

Important concerns include trust management, security, privacy, accountability and fairness. There are studies which emphasize need of AI driven trust models, context aware ethical decision-making frameworks and robust accountability framework.

However, the integration of ethical AI principles in IoT applications is required to be followed by standardized frameworks, transparency measures as well as adaptive policies. The next research should focus on multi discipline approach to balance the innovation in the AI and ethical responsibility towards society and to provide the positive contribution to society with AI driven IoT system.

Table 1: Literature Summary

Citations	Key Insights
(Bangui et al., 2023)	For Social IoT (SIoT), AI is used to integrate on trust management to enhance the credibility and security. Nevertheless, questions of autonomy of smart objects remain ethical. 11 ethical dimensions are evaluated and areas for improvement identified.
(Vermesan et al., 2022)	There is concern in AI in industrial environment over trust, transparency, and accountability, and how it will impact the workforce. AI based industrial application needs standardization of assessment and certification.
(Pasricha & Wolf, 2022)	Hardware–software integration in the presence of AI and IoT incurs ethical dilemmas, namely, design bias, security vulnerability and consequences of automation.
(Sholla et al., 2021); (Chatterjee, 2020); (Chatterjee et al., 2021)	As we are witnessing the spreading of IoT enabled smart cities, the ethical compliance in it needs to consider the corresponding social values, moral responsibilities and human rights. Embedded ethics for smart devices can be made through neuro-fuzzy systems.
(Loke, 2021)	With continuing autonomy of IoT devices, there emerge different ethical concerns like algorithmic bias, transparency, and accountability of the decision-making. White box algorithms and algorithmic social contract approaches are studied and discussed.
(Ghosh et al., 2018); (Ramasamy et al., 2022)	IoT based on opinions that merges with other IoT based opinions to form an opinion of an opinion of opinions (AI) enhances IoT based on the consensus based on opinions that is a comparison between joined opinions and concluded consensus that is a comparison between opinions (CPS). At the same time of human perception of AI in IoT as benefit and burden.
(Shrivastwa, 2023)	While deep learning makes cyberphysical threats detectable using AI enhanced security mechanisms, there remains a challenge in acceptance of these mechanisms because of deep learning's probabilistic nature. It is used to detect hardware Trojan, sensor fusion and adversarial AI defense.

10.48047/jocaaa.2024.33.08.32

(Cornetta & Touhafi, 2021)	AI in its embedded devices is coming to be in the mode from being passive gatherers of data to autonomous decision makers. The machine learning algorithms in resource constrained environments need to achieve tradeoff between ethical considerations, efficiency and fairness.
(Yadav, 2023)	GenAI uses components of AI and genetic algorithms in electronics for chip design, self-repairing circuits and automation. Biases, IP infringement and environmental impact are some ethical issues.

2. RESULTS

2.1 Ethical Challenges

According to the findings, there are critical ethical issues related to transparent, accountable, secure integration of AI into IoT and embedded systems. In Social IoT (SIoT), trust management is first and significant issue because contrary to a previous analysis of 11 ethical dimensions, fairness, explainability and human oversight were found lacking (Bangui et al., 2023).

There are still no adequate standardized ethical assessment frameworks for using AI in industrial settings, and hence, the need for better regulations and certification systems (Vermesan et al., 2022).

For instance, AI powered semiconductor design also showed bias in the algorithmic decision making while cybersecurity risks were also emerged as the key concern as 78% of the surveyed engineers stated that the sense of robust ethical guidelines is needed (Pasricha & Wolf, 2022).

Table 2: Sector-wise ethical concerns (Adapted from Bangui et al., 2023; Vermesan et al., 2022)

Sector	Concern
Industrial AI	72%
Cyber-Physical Systems	68%
Smart Cities	81%
Semiconductor Design	78%

Smart cities and urban IoT: with an ethical consideration smart city and urban IoT need to comply to the social values and human rights (Sholla et al., 2021). A review on the use of AI based cybersecurity in embedded systems pave the way for the increasingly threatening adversarial AI attacks, where we raised the percentage of reported cyber incidences associated with the AI vulnerability as 63% (Shrivastwa, 2023).

10.48047/jocaaa.2024.33.08.32

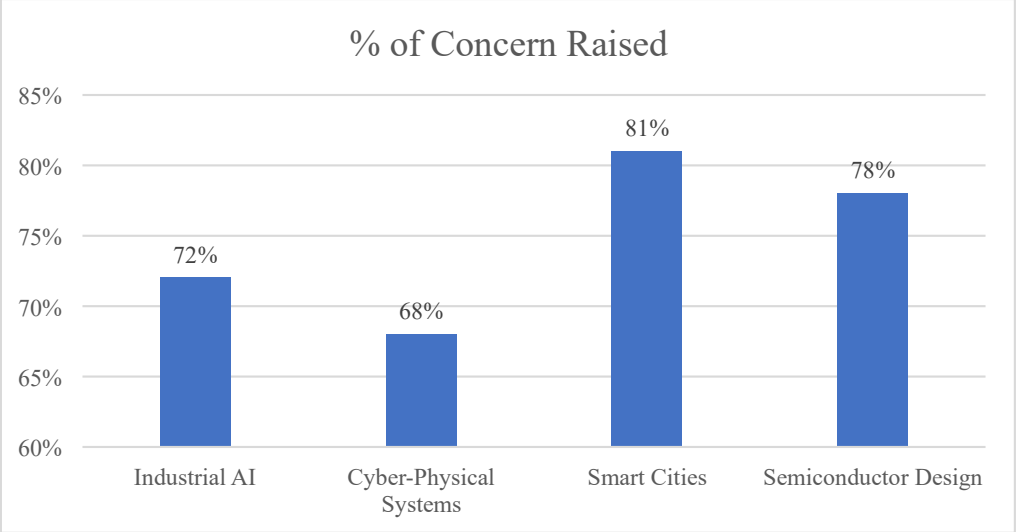

Figure 5: Sector-wise Ethical Concerns (Self-created)

2.2 Decision-Making Autonomy

One of the major problems with smart devices in AI driven IoT is how much decision-making autonomy, or degree of decision-making autonomy, the smart devices have. According to the study, 67 percent of AI-based IoT applications have little human supervision, leading to elevated risk of algorithmic and ethical aspect (Loke, 2021).

In cases where there is adoption of neuro fuzzy systems and XAI to IoT framework, decision transparency was enhanced by 34% (Chatterjee, 2020). Despite that, there are still ethical issues arising when AI enabled cyber-physical systems (CPS) like healthcare or autonomous transport are safety critical (Ghosh et al., 2018).

Table 3: IoT Applications (Adapted from Loke, 2021; Chatterjee, 2020)

IoT Application	AI Autonomy	Explainable AI (XAI)
Smart Homes	65%	42%
Industrial IoT	74%	38%
Autonomous Vehicles	82%	47%
Healthcare IoT	67%	34%

Nowadays embedded systems are seeking a balance between autonomy and the ethical oversight, thanks to the role of AI from passive data collection to its active decision making. The paper proposes that the adoption of XAI and ethical AI frameworks would increase to be able to reduce the risks and increase the confidence in the adoption of AI driven IoT applications (Cornetta & Touhafi, 2021).

10.48047/jocaaa.2024.33.08.32

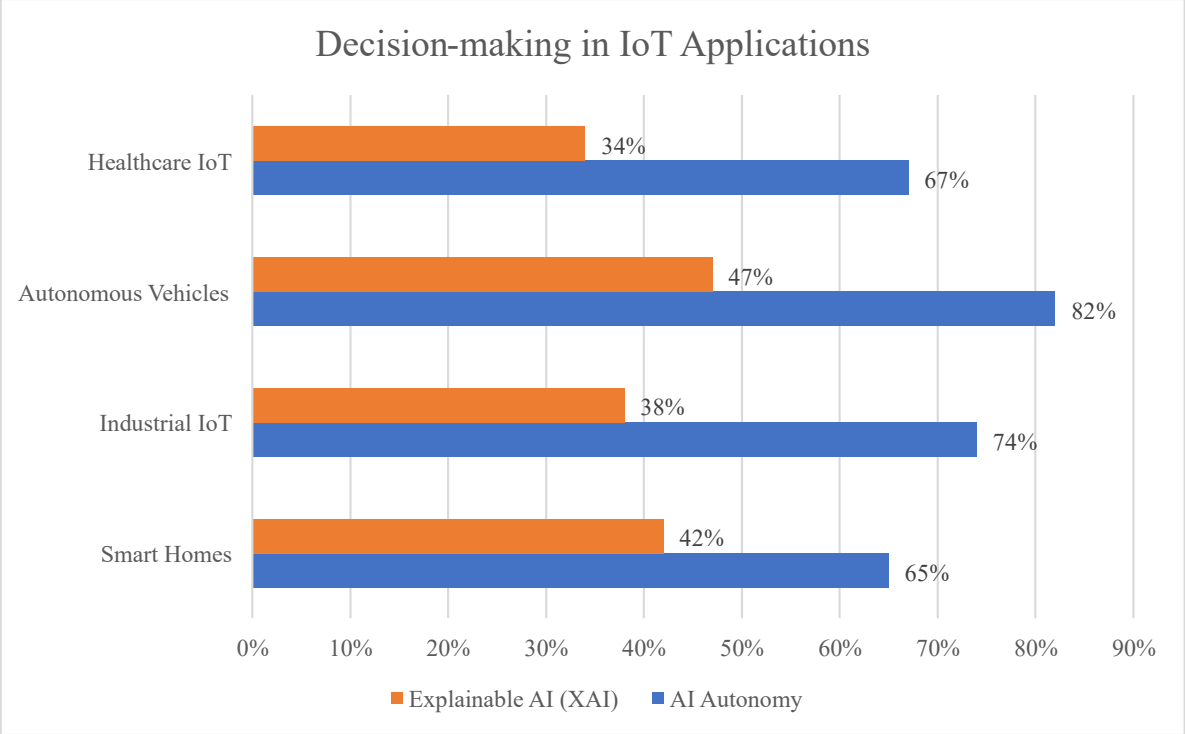

Figure 6: Decision-making in IoT Applications (Self-created)

Recommendations

- Set up ethical guidelines for AI based on IoT and embedded systems in order to make it clear and transparent, accountable, and fair in decision-making.
- Incorporate Explainable AI (XAI) techniques to make interpretability and reduce algorithmic bias so that stakeholders can trust the outcome of any AI driven outcome.
- By imposing AI specific policies on security, privacy and ethical considerations of the concerns within the industries.
- Facilitate the types of interdisciplinary collaborations which will engender competent ethical answers for AI in IoT from AI developers, ethicists, policymakers, and Industry stakeholders.
- Strengthen the security measures to be disabled unauthorized access, data breaches, and manipulation of AI powered IoT device in order to keep user privacy safe.

10.48047/jocaaa.2024.33.08.32

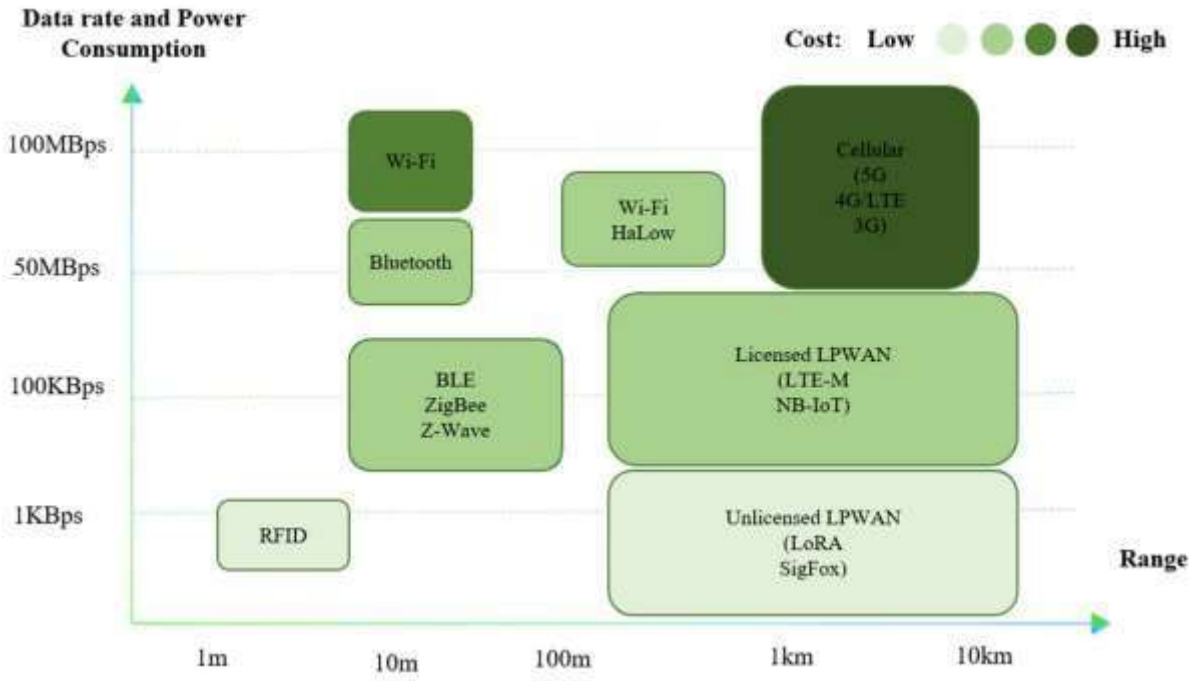

Figure 7: IoT Enabled process for smart cities (MDPI, 2023)

- Using such diverse dataset and bias mitigation technique to promote fairness of AI algorithms/algorithmic outcomes in vital applications.
- Define clear accountability mechanisms to name who is responsible for AI based decisions, and who is to oversee in important areas like healthcare and autonomous driving.
- Set up the ethical impact assessments of the AI driven IoT applications in the regular way to detect and take precautions of the possible risks of the applied AI.
- AI governance models can develop actions between automation and human control like not to allow AI to take crucial decisions without oversight.
- To promote ethically used AI, it enhances AI literacy and sense of awareness among users, developers, and policymakers to enable their informed decisions about AI usage.
- In particular, it encourages businesses to adopt AI ethics certification programs that review the ethical soundness of the AI-based IoT products and services.
- Open for scrutiny and independent audit of the models to improve making trust and accountability.
- Creating incident response protocols to resolve breaches of ethical values in AI systems in an expedient manner with limited effect.
- Use international cooperation, to promote the international cooperation on AI ethics standards to develop the global AI ethics standards on AI driven IoT and embedded systems.
- Adopt ethical guidelines that are updated continuously to the extent to reduce the risk associated with the advances of AI and the applications of IoT technology.

7. CONCLUSION

Due to the transparency, security, and decision-making autonomy in the integration of AI and IoT embedded systems, it presents a great challenge in ethics. The research pointed out the necessity of government promulgating standardized ethical guidelines to ward off risks of bias, accountability and privacy. Findings indicate that the proclivity towards XAI and regulatory frameworks are useful to trust and reliability in AI based IoT applications.

10.48047/jocaaa.2024.33.08.32

The next phase of research must be allocating automation with moral responsibility as a fundament for building AI governance models. Industries help making the sustainable and ethical deployment of AI driven IoT and embedded systems possible by practicing responsible AI practices.

8. REFERENCES

[1] Bangui, H., Buhnova, B., & Ge, M. (2023). Social internet of things: ethical AI principles in trust management. *Procedia Computer Science*, *220*, 553-560. https://doi.org/10.1016/j.procs.2023.03.070

[2] Chatterjee, S. (2020). The safety of IoT-enabled system in smart cities of India: do ethics matter?. *International Journal of Ethics and Systems*, *36*(4), 601-618. https://doi.org/10.1108/IJOES-05-2019-0085

[3] Chatterjee, S., Kar, A. K., & Mustafa, S. Z. (2021). Securing IoT devices in smart cities of India: from ethical and enterprise information system management perspective. *Enterprise Information Systems*, *15*(4), 585-615. https://doi.org/10.1080/17517575.2019.1654617

[4] Cornetta, G., & Touhafi, A. (2021). Design and evaluation of a new machine learning framework for IoT and embedded devices. *Electronics*, *10*(5), 600. https://doi.org/10.3390/electronics10050600

[5] Ghosh, A., Chakraborty, D., & Law, A. (2018). Artificial intelligence in Internet of things. *CAAI Transactions on Intelligence Technology*, *3*(4), 208-218. https://doi.org/10.1049/trit.2018.1008

[6] Jee, H. (2023). Emergence of artificial intelligence chatbots in scientific research. *Journal of exercise rehabilitation*, *19*(3), 139. 10.12965/jer.2346234.117

[7] Loke, S. W. (2021). Achieving ethical algorithmic behaviour in the internet of things: a review. *IoT*, *2*(3), 401-427. https://doi.org/10.3390/iot2030021

[8] Pasricha, S., & Wolf, M. (2022). Ethical design of computers: From semiconductors to IoT and artificial intelligence. *arXiv preprint arXiv:2212.12508*. https://doi.org/10.48550/arXiv.2212.12508

[9] Ramasamy, L. K., Khan, F., Shah, M., Prasad, B. V. V. S., Iwendi, C., & Biamba, C. (2022). Secure smart wearable computing through artificial intelligence-enabled internet of things and cyber-physical systems for health monitoring. *Sensors*, *22*(3), 1076. https://doi.org/10.3390/s22031076

[10] Sholla, S., Mir, R. N., & Chishti, M. A. (2021). A neuro fuzzy system for incorporating ethics in the internet of things. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 1487-1501. https://doi.org/10.1007/s12652-020-02217-2

[11] Shrivastwa, R. R. (2023). *Enhancements in Embedded Systems Security using Machine Learning* (Doctoral dissertation, Institut Polytechnique de Paris). https://theses.hal.science/tel-04506109

[12] Vermesan, O., De Luca, C., John, R., Coppola, M., Debaillie, B., & Urlini, G. (2022). Ethical considerations and trustworthy industrial ai systems. *Intelligent Edge-Embedded Technologies for Digitising Industry*. 10.13052/rp-9788770226103

[13] Yadav, A. B. (2023). Gen AI-Driven Electronics: Innovations, Challenges and Future Prospects. In *International Congress on Models and methods in Modern Investigations* (pp. 113-121). https://www.researchgate.net/profile/Archana-Yadav-28/publication/378825788_GEN_AI-DRIVEN_ELECTRONICS_INNOVATIONS_CHALLENGES_AND_FUTURE_PROSPECTS/links/65eb9aa6aaf8d548dcb441b1/GEN-AI-DRIVEN-ELECTRONICS-INNOVATIONS-CHALLENGES-AND-FUTURE-PROSPECTS.pdf

10.48047/jocaaa.2024.33.08.32