Ethical Dilemmas in the system of Internet of Things

Tommy (Kanggeon) Oh
Department of Computing Science
Simon Fraser University
British Columbia, Canada
koa18@sfu.ca

***Abstract*—The Internet of Things (IoT) is one of the growing technologies, along with Artificial Intelligence (AI). IoT devices, such as wearable devices like the Apple Watch, smart thermostats, and smart home speakers like Google Home and Alexa from Amazon, are already integrated into people's lives. IoT devices have revolutionized modern living by providing unparalleled convenience and efficiency through automation and real-time data analytics. However, their widespread adoption raises significant ethical dilemmas, particularly concerning data collection and privacy. This paper examines the moral implications of IoT devices, focusing on critical areas such as privacy, security, access, transparency, and data ownership. The analysis delves into the privacy risks associated with IoT devices, their security challenges, and the complexities of data access and ownership. Additionally, it emphasizes the importance of transparency in data practices to ensure users are fully informed about how their data is collected, used, and shared.**

***Index Terms*—Internet of Things (IoT), Data collection, Data Privacy, Data Security, Data transparency, Ethics**

I. Introduction

The Internet of Things (IoT) is one of the fastest-growing technologies that has arisen with Artificial Intelligence (AI), changing the way that people live. IoT technology simply defines small things that can communicate with any other IoT devices or servers using some kind of connection, such as WiFi or Bluetooth. Already, most people have integrated IoT devices into their lives. There are wearable devices that track healthcare services and smart thermostats that control house temperature. In fact, most medical services are expected to be delivered virtually and diagnosed through IoT devices like wearable devices and phones. Most IoT devices utilize sensors, cameras, monitoring stations, and other devices to collect data [1]. Some of the data can be general, such as temperature. However, most collected data are more sensitive and private, such as user's personal data, location and behaviour [2]. For instance, every phone has Global Positioning System (GPS) sensors, which enable manufacturers to collect data and analyze the information to track or predict people's movements and travel patterns [1]. There is still ongoing controversy as more IoT devices integrate into people's lives and industries grow, thereby increasing the amount of personal information that is collected, stored and used. While IoT devices offer users convenience and efficiency, they raise ethical dilemmas regarding data collection and data privacy. Even though IoT devices collect and store data for improved functions and users' benefit, collecting and using this data without informed consent from users is raising concerns and is unethical.

II. Current Status

A. Current Industries

The current IoT industry is a rapidly expanding and dynamic sector characterized by a proliferation of interconnected devices that span various domains, including smart homes, healthcare, transportation, and industrial automation [3, 4]. It is the technology that can easily link and connect physical devices and items and increase the potential for creativity, automation and efficiency [4]. IoT technology has the potential to revolutionize the healthcare system by allowing remote patient monitoring and, therefore, detecting a mysterious symptom earlier [5]. The adoption of IoT devices promises significant benefits, such as enhanced convenience, improved efficiency, and the ability to make data-driven decisions. It is estimated that IoT industries will grow between $2.7 trillion to $ 6.2 trillion in the world economy [2].

B. Current Protections for Users

Since IoT devices are integrated into people's lives and However, the rapid growth of the IoT industry also brings challenges, particularly regarding interoperability, security, and privacy. IoT devices collect user data that may be personal or private. However, there are not many laws and regulations that are ready to be applied to IoT devices. Current data protection for users in the IoT landscape is shaped by a mix of rules, standards, and industry practices aimed at safeguarding personal information and ensuring user privacy. There are governments that try to regulate data protection. Data Protection Regulation (DPR) has been proposed by the European Union (EU) to support the privacy of data created by new technologies [2]. The DPR mandates that companies obtain explicit consent from users before collecting personal data, ensure data accuracy, provide the right to data access and deletion, and implement robust security measures to protect data from breaches. In the USA, the White House introduced a framework to provide privacy for consumers, especially utilizing the Consumer Bill of Rights to prevent personal data from companies [2]. In order to develop IoT technology, it is

required that government and regulatory agencies create new laws for the safety of IoT devices and ethics [4].

III. Privacy

A. Importance of Privacy

Data that IoT devices collect is one of the controversial areas in the industry. For instance, the information the devices collect may be private, such as GPS or health-related data. IoT devices have access to more private and valuable information without any restriction [2]. Another issue arising from data collection is the raw data that IoT devices collect may be a mixture of other people's data. If the raw data is uploaded into the system, a moral law problem may arise, which is related to the ethics of science [6]. In order to prevent violation of the ethics law, the algorithm that can identify the raw data needs to be implemented, which is a challenging task to finish. Privacy is a fundamental concern in the realm of IoT devices, as these technologies continuously gather and process personal data, often without explicit user consent. The manufacturer may use the data from their users to improve technologies and devices. However, from an ethical point of view, privacy needs to be examined through various ethical theories using Kantianism and Utilitarianism.

B. Ethical Aspect

The Kantian principle mandates that users' privacy must be respected and protected in the context of IoT. Collecting data without informed consent violates the Kantian imperative, as it disregards the autonomy and dignity of the individuals whose data is being harvested. Users should have the right to control their personal information, ensuring that their consent is obtained transparently and respectfully. On the other hand, from a utilitarian perspective, the benefits of IoT devices, such as increased convenience, efficiency, and improved quality of life, must be weighed against the potential harm caused by privacy breaches. If the intrusion into personal privacy results in significant distress, misuse of data, or exploitation, the negative consequences may outweigh the benefits, rendering the practice unethical. Therefore, to align with utilitarian principles, IoT manufacturers must implement robust privacy protections and ensure that the positive outcomes of data collection genuinely enhance overall well-being without causing undue harm to users.

C. Action towards Privacy

Balancing these ethical considerations highlights the need for a comprehensive approach to privacy in the IoT ecosystem. It requires respecting individual rights and autonomy, as emphasized by Kantianism, while also striving to achieve the greatest good, as advocated by Utilitarianism. The one that countries around the world have tried is a data expiration system. The expiration date is set once the data has been added to the system. After the expiration date passes, the data is automatically deleted from the system. As a result, companies can collect and keep their data legally, and users can ensure that their data is safe and secured after the date. This dual approach can guide the development of ethical frameworks and policies that protect user privacy, foster trust, and promote the responsible use of IoT technologies.

IV. Security

A. Importance of Security

Security is a critical concern in the Internet of Things (IoT) ecosystem, as the proliferation of interconnected devices creates numerous vulnerabilities that malicious actors can exploit. Cloud computing plays a significant role in IoT technologies. The application uses cloud computing as a data-processing and storage facility [3]. IoT devices gather massive amounts of data from the world and send it using cloud computing to their endpoints, cloud storage [3]. Cloud storage is an Internet-based storage system that stores raw data on the Internet and allows users to access the data via the Internet [3]. Based on cloud computing, IoT offers a best-connected environment and generates enormous amounts of data. Currently, IoT technologies have identified some security vulnerabilities. Vulnerabilities such as weak default passwords, unsecured connections, and the latest software updates can cause a weak spot in security [4]. If anonymous hackers compromise the system, they can access users' personal data and misuse it later on [8]. In Japan, more than 50 vending machines and delivery trucks utilize IoT devices to send and receive IoT data in real-time [7]. This shows that IoT devices can be implemented in people's lives but also can be vulnerable if the systems get hacked. Ensuring robust security measures is both a technical and ethical imperative. Ethical theories such as Kantianism and Utilitarianism provide valuable frameworks for understanding the moral obligations associated with IoT security.

B. Ethical Aspect

From a Kantian perspective, it emphasizes the importance of treating individuals as ends in themselves and not merely as means to an end. In the context of IoT security, this principle translates into the obligation of manufacturers and service providers to implement stringent security measures that safeguard users' personal data and prevent unauthorized access. Failing to secure IoT devices can lead to data breaches, identity theft, and other forms of harm, violating the Kantian imperative to protect and respect individuals' rights. From a utilitarian perspective, the security of IoT devices is crucial because the potential consequences of security breaches can be severe and widespread. Compromised IoT devices can lead to significant financial losses, personal harm, and disruptions to essential services. Ensuring robust security measures in IoT devices minimizes the risk of such adverse outcomes, thereby enhancing overall well-being. Consequently, investing in solid security protocols aligns with the utilitarian goal of maximizing positive outcomes and minimizing harm to the most significant number of people.

C. Approach towards Security

Balancing these ethical considerations highlights the necessity of comprehensive security measures in the IoT industry.

Kantian ethics demands that companies respect and protect individual rights by securing their devices against potential threats. Simultaneously, utilitarianism underscores the importance of preventing harm and ensuring the most significant good by mitigating the risks associated with IoT security breaches. This dual approach guides the ethical development and implementation of security practices, ensuring that the benefits of IoT technologies are realized without compromising the safety and well-being of users.

V. Transparency

A. Importance of Transparency

Transparency is a fundamental aspect of ethical data practices in the IoT industry, as it directly affects user trust and the integrity of data management processes. Ensuring transparency involves clearly communicating to users what data is being collected, when it is being collected, and how it is being used. Additionally, it addresses the critical question of data ownership and emphasizes the necessity of obtaining informed consent from users before collecting their data.

B. Data Ownership

A vital issue in transparency is the question of data ownership. Once IoT devices have collected data, it often becomes unclear whether the data belongs to the user or the manufacturer. Ethically, the concept of ownership should favour the user, as their personal information is collected, and users need access to their data. However, many manufacturers assert ownership over the data to leverage it for product improvement, marketing, or selling to third parties. Ethical transparency dictates that users should be informed about who owns the data and how it will be used. This principle is supported by the General Data Protection Regulation (GDPR), which mandates that users have the right to access and control their data, emphasizing user ownership and consent [9]. Currently, the concept of ownership is unclear in most national legal systems because of different definitions of ownership [9].

Transparency also involves disclosing what specific data is being collected. IoT devices can gather a wide range of information, from usage patterns and location data to personal preferences and biometric information publicly [10]. Users should be clearly informed about the scope of data collection so they can make informed decisions about their privacy. The timing of data collection is another crucial aspect. Users need to know when their data is being collected – whether it is continuous, periodic, or event-based. This knowledge allows users to understand the extent of the surveillance and make informed choices about their interaction with the device. However, ownership questions who owns the data and involves four elements: control, protection, valuation, and allocation of a resource [9]. Transparency demands that users are informed about how their data is being used. This includes whether the data is used to improve device functionality, for marketing purposes, shared with third parties, or sold. In order to prevent the issue of data ownership, the controversy of transparency needs to be discussed.

C. Approach to Ownership in IoT

Several approaches to data ownership exist in the IoT ecosystem, each involving critical elements such as ownership, control, and protection of personal data. Control and protection of personal data are the essential concepts of transparency.

Control of personal data refers to the ability of users to manage how their data is collected, used, and shared. Ownership allows users to use their personal data, such as access, store, and share, and it also enables users to destroy their data responsibly [9]. Effective control mechanisms ensure that users can give informed consent and make decisions about their data usage. The GDPR emphasizes user control, requiring explicit consent for data collection and providing users with the ability to withdraw consent at any time. Ensuring user control helps maintain privacy and trust in IoT devices.

Protection of personal data encompasses the security measures implemented to safeguard data from unauthorized access, breaches, and misuse. Since privacy issues perplex the ownership of personal data, transparency is closely related [9]. Robust data protection involves encryption, secure data storage, regular security updates, and incident response plans. Legal frameworks like the GDPR mandate stringent data protection standards, requiring organizations to implement appropriate technical and organizational measures. Adequate data protection is essential for preventing data breaches, ensuring compliance with legal requirements, and maintaining user trust.

VI. Conclusion

In conclusion, while the proliferation of IoT devices in smart homes offers unparalleled convenience and efficiency, it also raises significant ethical concerns regarding data privacy and security. The extensive data collection by these devices often occurs without explicit user consent, posing threats to individual privacy and autonomy. Addressing these issues through robust transparency, security measures, and clear data ownership policies is essential. Ethical frameworks such as Kantianism and Utilitarianism highlight the necessity of respecting user autonomy and maximizing overall well-being, guiding the development of ethical IoT practices.

Despite the progress made, there is still much to be done to enhance data protection and user privacy in the IoT ecosystem. The industry needs to develop more comprehensive and harmonized global standards that ensure consistent data protection across different regions. This includes stricter enforcement of existing regulations like the GDPR and the creation of new policies that address emerging threats and technological advancements.

Possible solutions to these challenges include the implementation of advanced security technologies such as blockchain and AI-driven threat detection, which can enhance the protection of user data and prevent unauthorized access. Additionally, promoting user education and awareness about data privacy and security can empower individuals to make informed decisions about their data. Providing clear and accessible information about data collection practices, ownership, and

usage, as well as obtaining explicit consent from users, are critical steps in fostering transparency and trust.

As the IoT industry continues to evolve, it is imperative to balance technological advancements with ethical considerations. Prioritizing user privacy, security, and transparency will not only address the ethical challenges but also foster user trust and promote sustainable growth in smart home technologies. The ongoing dialogue among stakeholders, including manufacturers, regulators, and users, will shape the future of IoT, ensuring that it benefits society without compromising ethical principles.

REFERENCES

[1] C. Phillips and J. Jiao, "Artificial Intelligence & Smart City Ethics: A systematic review," *2023 IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS)*, May 2023.

[2] A. Shahraki and O. Haugen, "Social Ethics in internet of things: An outline and review," *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, May 2018.

[3] P. Singh, N. Singh, P. R. Luxmi, and A. Saxena, "Artificial Intelligence for smart data storage in cloud-based IOT," *Transforming Management with AI, Big-Data, and IoT*, pp. 1–15, 2022.

[4] K. K. Gautam, R. Kumar, R. Yadav, and P. Sharma, "Investigation of the internet of things (IOT) security and privacy issues," *2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA)*, Aug. 2023.

[5] M. Lal *et al.*, "Enhancing patient care and monitoring through AI and IOT in Healthcare," *2023 IEEE International Conference on Computer Vision and Machine Intelligence (CVMI)*, Dec. 2023.

[6] A. N. Gorodishcheva, Y. V. Paskhalskaya, A. V. Gorodishchev, A. I. Vinogradova and G. P. Kovalev, "IoT Ethic In Scientific Communications," *2021 Communication Strategies in Digital Society Seminar (ComSDS)*, St. Petersburg, Russia, 2021, pp. 136-140.

[7] Y. Shoji, K. Nakauchi, W. Liu, Y. Watanabe, K. Maruyama and K. Okamoto, "A Community-Based IoT Service Platform to Locally Disseminate Socially-Valuable Data : Best effort local data sharing network with no conscious effort?," *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, Limerick, Ireland, 2019, pp. 724-728.

[8] K. P. Singh, V. Rishiwal and P. Kumar, "Classification of Data to Enhance Data Security in Cloud Computing," *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Bhimtal, India, 2018, pp. 1-5.

[9] V. Janeček, "Ownership of personal data in the internet of things," *Computer Law & Security Review*, vol. 34, no. 5, pp. 1039–1052, Oct. 2018.

[10] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: Threats andchallenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, Jun. 2013.