Privacy and Ethical Concerns in Edge Computing

Abstract. As technology continues to advance at a rapid pace, edge computing has emerged as a powerful approach to meet the growing demands of processing data in real-time. By operating closer to the source, this distributed architecture has the potential to unlock new avenues of innovation, enabling everything from self-driving cars to remote healthcare services. However, carrying great power requires great responsibility. In this article, we attempt to supply a balanced perspective on this paradigm and the concerns that may arise from its implementation, regarding privacy and ethics. Come along with us as we explore the exciting domain of edge computing and its impacts on tecnology advancement.

Keywords: Edge Computing · Privacy · Ethics · Internet of Things · Cloud Computing · Healthcare Industry

1 Introduction

The ever-increasing number of connected devices in our everyday lives has created a demand for more efficient and faster data processing. In line with a recent report [1], "Think about devices that monitor manufacturing equipment on a factory floor or an internet-connected video camera that sends live footage from a remote office. (...) Instead of one video camera transmitting live footage, multiply that by hundreds or thousands of devices. Not only will quality suffer due to latency, but the bandwidth costs can be astronomical". This is where edge computing comes in. By bringing data management closer to the source, EC[1] can help companies save money by processing data locally, minimizing the amount of data that needs to be sent to a central location.

In this way, edge computing can support IoT[2] applications, with one of the most important issues being Big Data. The volume of huge amounts of data makes it difficult to control and analyze. From a socio-ethical point of view, determining personal data and distinguishing it from other data is the main privacy issue [2]. Ethical and privacy concerns naturally surface in these systems, where trust and boundaries must be very carefully clarified. In the words of Vincent Cerf, one of the founders of the Internet and creator of the TCP/IP protocol, "Technologies have no ethics. Many systems can be used for both good and ill: Video surveillance may be tremendously helpful in allowing senior citizens stay in their homes longer and parents to monitor their newborns; they can also expose private behavior to unscrupulous viewers and unwanted intrusion" [3].

[1] Edge Computing
[2] Internet of Things

People should control the use of their own data, but this is often a difficult undertaking. These systems know no boundaries, data is used in places where laws are not appropriate [2] or where laws may differ significantly. "Context" is a very important factor related to privacy. Locations, culture, religion, agreements, and so on, can shape context, which can be helpful in designing frameworks for the Internet of Things.

Taking these factors into account, this article aims to define the privacy and ethics issues in edge computing, as well as present some concrete cases and existing solutions that can enable the implementation of EC to meet the growing demand for data processing, without compromising user privacy. "Is the use of edge computing feasible, safe and ethical?" This is the main question that runs throughout the study.

2 Identification and characterization of defining aspects

This section defines the concepts of privacy and ethics in the context of edge computing. As a complement, it explains the motivations, benefits, and functions of this paradigm in order to clarify the article's objects of study. Such definitions and contextualization are important to properly design the proposed solutions.

2.1 Edge Computing

With increasingly real-time applications available, edge computing, a distributed architecture, has emerged as a game-changer in data processing and storage. Given the substantial processing delays that might result from the distance between devices and data centers, traditional computing architectures frequently experience latency[3] problems. By bringing computer resources closer to devices and processing data locally on edge devices, rather than sending it to a remote server [4], edge computing can lower response time, and reduce the consume of energy. For example, instead of depending on a cloud-based service that can take a long time to execute, face recognition algorithms can be processed on an edge server or gateway, or even on a smartphone itself [1].

Despite advances on the Internet, the sheer amount of data generated by billions of devices every day can still cause network congestion. Edge computing, on the other hand, can help mitigate this issue by reducing the amount of data that needs to be transmitted over the network, thereby reducing congestion, and saving bandwidth[4]. This is achieved by deploying data servers at the points where data is generated, allowing many devices to operate over a much smaller and more efficient bandwidth [5]. As a result, companies can not only reduce costs, but also effectively operate many devices with limited bandwidth, increasing the efficiency of the network.

Edge computing can be confusing when compared to cloud computing, but in reality the two paradigms provide different approaches to overcoming the

[3] Time that data takes to transfer across the network.
[4] The maximum volume of data transmitted via network in a specific period of time.

problems of modern computing. First things first, they have complementary architectures: while edge computing offers a distributed infrastructure to process data closer to where it is generated, cloud computing provides a centralized and highly scalable framework that can manage massive volumes of data. However, EC has some unique advantages. The capability of processing in real-time is one of the primary benefits as it allows for instant analysis of data without requiring it to be sent to the cloud. This is crucial for applications where low latency and high bandwidth are essential, such as real-time monitoring, industrial automation, and autonomous cars [6]. Additionally, edge computing can provide better resilience since it can still function even if the connection to the cloud is lost, as well as better data security and privacy as it can process sensitive data without disclosing it to the Internet.

Finally, we must bring attention to one of the most discussed relationships in our study: edge computing for the Internet of Things. Sensors and cameras serve as the primary data sources in IoT applications. These devices generate large amounts of data that must be processed and analyzed in real time to provide useful insights. However, traditional cloud computing architectures are often unable to meet the stringent latency and bandwidth requirements of these applications. Consequently, IoT devices encounter several limitations, including security concerns, limited computational resources, and high energy consumption. Edge computing has emerged as a solution to this problem by providing distributed computational nodes that are closer to end users, reducing network latency and processing time. Each edge node can supply sufficient computing power to meet IoT requirements.

2.2 Privacy

The privacy of an entity is its control over the exposure of its sensitive personal information/data. Privacy is guaranteed in an isolated environment with no contact with outside entities. However, this is not the case in IoT. The flow of information and computing at the periphery of the network (a consequence of EC) leads to a decentralization of data, which is considered more vulnerable than a single cloud [7]. A distributed and decentralized system mandates the data transmission in a secure, integrated, and reliable way.

According to [8], the "inability to establish explicit trust for other devices, and also their inability to establish a trusted connection" make IoT devices targets for security and privacy breaches. In an environment where distrust is prevalent, one way to ensure your anonymity is to not expose your data in the first place. With edge computing, this means not recording information that allows you to link the data to the device it came from, as suggested by [9]. In contrast, the same article discusses that such thing is not feasible in our context because users must be authenticated to participate in these distributed systems.

Authentication is the key concept and one of the most frequently employed in scientific investigations on edge computing privacy. Eight privacy requirements for edge computing are listed in [8]. One of these, along with confidentiality,

integrity, and others, is authenticity. [10] also quotes "data authenticity" as one of the goals of an attractive private data-sharing system in the IoT environment. This criteria helps us be sure about the source of information, and contributes to the identity of participants and trust in the edge of the network. This seems to be a contradiction because it has been discussed that the information cannot be associated with the person who created it, but now we want to give "identity" to strengthen trust between participants. This is the "duel" that privacy must face in EC. How can anonymity and authenticity be guaranteed at the same time?

Sensitive personal information was mentioned in our definition of privacy. But what kind of data is this in the context of our research? In terms of edge computing for social sensing, we are dealing with a huge amount of information periodically collected near the sources, but the metadata gathered from participants may include geolocation and timestamps information [9]. Geolocation is intuitively sensitive, since we do not want everyone to know where our house is. On the other hand, periodic timestamps can indirectly reveal the chronology and steps behind a routine. What could be more harmful than revealing geographic information? Imagine if someone knew exactly your daily steps without even knowing who you are.

In this way, we can summarize privacy protection in EC as the control and protection of the metadata collected at the network's periphery, with anonymous authentication for trust in the participants who will interact with the data.

2.3 Ethical Concerns

The transmission of data over the Internet through countless devices can compromise their security and raise social and ethical issues [11].

In the hospitality sector, IoT implementations have created problems related to user privacy, data collection and usage, responsibility ascription and risk management cost. Such thing is challenging as it involves balancing the convenience and security of IoT systems with customer privacy expectations and regulatory requirements [12]. As highlighted by Zhu and Singh (2019), these expectations can vary depending on individual perceptions, naming time, context and location. Therefore, hotels and IoT application manufacturers need to grant customisable services that allow for flexible consent or refusal. This is often not the case as current user agreements may not provide consumers with sufficient transparency, which can lead to data being collected and used without their full understanding or consent. Since customers may not be aware of the implications of sharing data, ownership rights may become a concern. These applications also lack communication interfaces for users to change security settings, limiting their control over the devices.

A study by Paul Brous et al. [13] suggests that the adoption of IoT in public transportation can lead to unintended consequences, probably constraining individual actions. For example, if IoT is used to control access to public transportation, it can indeed improve the system's efficiency by automating the process of

checking for valid tickets or passes. However, this could also introduce unexpected risks, such as vandalism, because users can be more inclined to damage the IoT infrastructure to bypass the access control system. To mitigate these risks, new measures or protocols may need to be applied. So as an outcome, this might potentially limit the freedom and autonomy of individuals, by subjecting them to increased surveillance or stricter regulations to protect the IoT infrastructure.

The cost of addressing security and privacy issues can be in addition to the capital cost of the technology. For instance, applying security updates may require replacing IoT devices with new ones. Management must make decisions about the level of security and the costs involved to find an optimal point. Moreover, dishonest operators who collect and use data can have some short term advantage over honest business owners.

3 Solutions and Concrete Scenarios

This chapter presents some relevant use cases of edge computing, along with the analysis of articles that propose solutions in the area of ethics and privacy in edge computing. These articles were searched across platforms: Research Gate, Springer Link and IEEE Xplore. The selection of these databases was according to their credibility in the field of scientific dissemination. The initial search string included the keywords "edge computing AND ethical concerns", "edge computing AND privacy". After reading the most attractive articles based on the title and abstract, a criterion to find more concrete scenarios was to consult the "References" and "Related Works" sections of the ones already selected.

3.1 Edge computing usage scenarios

Even though there are inumerous scenarios developed for the domain of edge computing, the following experiments attracted our interest due to the sensitive data implied in the systems. Any finding of leakage or fault can provoke serious damages to the systems participants.

Oil platform In accordance to the report [14], consider a scenario where the operators of an oil drilling platform in the middle of the ocean collect data from sensors like pressure, temperature, and wave height. This data is essential for daily operations, and any delay in processing it could have dangerous consequences. To do this, operators must send the information over the Internet, which is slow and expensive, especially at sea where satellite links are used. Additionally, if a critical component on the platform shows signs of failure, it could take too long to send it to the cloud for processing, delaying the recommended course of action and possibly leading to a disaster. In order to avoid such risks, edge computing provides a solution by placing a data center directly on the oil drilling platform. By processing sensitive data on-site, latency and downtime are reduced, and operators no longer have to wait for critical analysis over a slow

connection. This solution ensures timely response to potential outages, where seconds can make the difference between safety and disaster.

Healthcare industry The healthcare industry is a prime example of how the Internet of Things and edge computing can work together to provide better patient care. Wearables and sensors are increasingly being used to monitor patients remotely, providing doctors and nurses with real time data on vital signs, medication usage and other critical health data. By deploying edge devices at or near the point where the data is generated (e.g. in a patient's home or hospital room), healthcare providers can process the data in real time, reducing response time and improving the overall quality of care. In addition, edge servers can analyze data from multiple edge devices and provide clinicians with a holistic view of a patient's health status. A study by Singh et al. (2022) [15] proposes the use of EC as a middle layer between cloud and user in smart healthcare systems that, in turn, implement IoT technology and cloud infrastructure for data capturing, processing, and healthcare advice.

Our focus remains on the case of healthcare. Monitored data is very personal since it relates to a person's current state of health. It would not be good if such data were spread throughout the network and also associated to a patient. But, how much control can a patient actually have over the data that is collected? Is there a limit to what these systems can do? Trust, anonymity, and logical bases for collecting and processing data were the criteria for finding solutions.

3.2 Solutions in the Privacy Domain - Ring Signatures

The solution aspect Edge computing privacy solutions are described in terms of data encryption and blockchain technology according to [16]. Blockchain technologies have attracted much attention for being a secure data structure maintained by untrusted peers in a decentralized P2P[5] network, characterized by providing transparency, provenance, fault tolerance, and authenticity [17]. The Blockchain technology can assist IoT system, and consequently be crucial for edge computing, in terms of privacy, traceability, and interoperability [10] Furthermore, it is scalable to millions of devices (e.g. bitcoin), is atomic in transactions and without malicious arbitrator (due decentralization).

In terms of data encryption, IoT devices have limited resources and, as a consequence, they are not sufficient to compute traditional cryptographic keys. Therefore, implementing non-invasive and privacy-preserving solutions with edge computing is technically more feasible because edge devices have more computing power than IoT's. However, two limitations must be placed on encryption mechanisms for data anonymity:

- Avoid using third-party providers for encryption and authentication;
- Low required bandwidth, computation, cost, and latency.

[5] Peer-to-Peer

According to [9], edge computing systems are compromised when collusion occurs between the trusted party and the server, justifying the first constraint. As a complement, SSEC[6] applications typically support hundreds or thousands of devices, requiring a scalable solution, justifying the second constraint.

In short, besides to what has been said, in a data sharing environment idealized by the IoT, for which EC is key, it is necessary to model a system that guarantees anonymity (sensing data may contain a lot of body information regarding its owner), data authenticity (a trusted method to verify the shared data), rewarding (to promote the exchange of confidential information) and access control [10].

Proposed Solutions Considering the solutions' limiting factors, let us examine the one proposed by [9] in more detail. By doing so, the main goal we are looking for mustn't be forgotten: to make the data collected by the edge nodes unlinkable from the generating source, so that a leak in the edge devices does not compromise its anonymity. The solution in this paper aims to maintain the authentication necessary for SSEC to work, while preserving the devices privacy (i.e., the unlinkability of the metadata) in a matter that is controlled and managed by the edge. In opposition to traditional individual authentication schemes (API keys), the idea behind this scheme is based on group certification mechanisms, on the context of the ring signature formalized by [18].

The ring signature – Figure 1 – is a form of digital signature that, in some way, confirms our stated desire to authenticate a participant by giving them a verified "identity". It differs from individual signature strategies because, when validating the authentication of a "message", the verifier can only tell that the message came from a certain group of participants, not which one in particular.

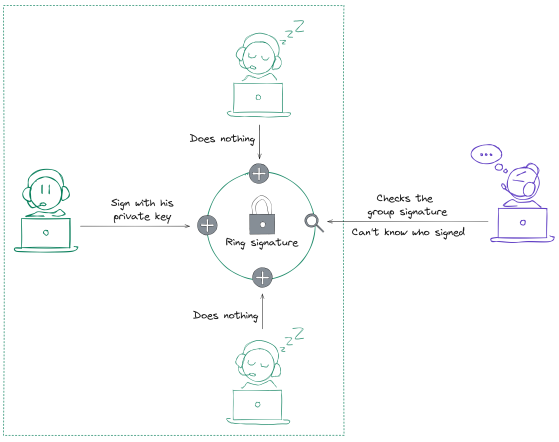

Fig. 1: Ring Signature Structure

[6] Social Sensing Edge Computing

Ring signature concept is widely used in financial concepts, where "privacy" must be one criterion of ideal electronic cash, which means "the relationship between the user and his purchases must be untraceable by anyone" [17]. In other words, "for each incoming transaction all possible senders are equiprobable" and to satisfy the untraceability, ring signatures schemes were implemented. Famous privacy-preserving blockchain systems, like Monero [19] – a confidential and decentralized cryptocurrency, use ring signatures.

According to [18], "These are simplified group signature schemes which have only users and no managers. Group signatures are useful when the members want to cooperate, while ring signatures are useful when the members do not want to cooperate." The author said that people say "ring signatures" instead of "group signatures" because rings are geometric regions with uniform periphery and no center. But, if you look closely at it, you see that the algorithm itself has a ring shape, which is kind of poetic. The signing member uses his private key with the public key of the other ring members to sign his message. This data is combined so that the verifier can prove whether or not the message is from a ring member. This mechanism does not use third parties for authentication and does not require the cooperation of ring members or a coordinating agent that could manipulate operations. This was exactly what we were looking for. Due to the complexity of the algorithm behind ring signatures, it would take too long to explain it in this document. However, as a relevant topic, we have created an additional support article just to explain how such subscriptions function. This paper was designed with the idea of making this term easily accessible to the general public. It can be found in this Repository.

Back in the context of edge computing, [9] states: "It is desirable to make the ring as large as possible to achieve greater anonymity (i.e., a larger number of devices are indistinguishable from each other). Under the standard ring signature protocol, though, where signatures are not linkable, three operations scale linearly with ring size: signature creation, signature verification, and network overhead. While larger ring sizes would be desirable to promote greater anonymity, a latency-tolerant application must impose a maximum ring size that forces devices to be split into multiple rings". However, as the same article shows later, the existence of multiple rings can be a problem if the choice of ring members is poorly made. The problem of poor choice is that participants become distinguishable by extracted patterns in their choice of rings. The "distinguishable" problem, focused on cryptocurrency transaction issues, is also mentioned in [17]. It discusses the fragility of the ring signature scheme through the "chain reaction" analysis, where infering the coins spent is possible by leveraging traffic flow and recognizing common patterns. This implies that the currency spent has a high risk of being detected, jeopardizing anonymity.

The major contribution of [9] is the idea of picking rings on the basis of the metadata similarity of the ring members. The ring whose participant has the most identical metadata is then selected, using clustering principles and identifying the nearest centroid. In this way, it is tougher to identify the participant since it is "cloaked" among the other ring members' highly comparable data.

What's curious to note is that the suggested solution in [17] revolves around the same concept. They conclude that, for any two currencies, the ring signature must produce observations with "similar" distributions. To ensure that differentiating the money spent is hard, the term "similar distribution" refers to the notion of currency indistinguishability.

In short, [9] brings together a ring signature and a ring negotiation system inside the framework of a blockchain system, where blockchain serves as a mechanism of participant coordination. The edge device claims an activity from the task pool, authenticates it using a ring signature, and when it's finished, the server starts a payout of incentives through an anonymous currency system. (e.g., Monero). On top of that, we have managed to achieve a decentralized and distributed model that permits unidentified authentication in an edge computing system by handling multiple rings to control their size – which guarantees the scalability of the solution, and the mechanism behind the signatures per ring – which contributes to the decoupling of the data source).

3.3 Solutions in Ethical Domain - Boolean Algebra

Quick overview of solutions The ethical issues raised by IoT in the hospitality industry can be addressed through various solutions. For instance, a study by Tomislav et al. [20] emphasizes the importance of clear privacy policies and user agreements related to data privacy and security, in order to better understand customer needs and provide personalized services with opt-in and opt-out flexibility. They suggest that data management is well governed by setting clear and transparent policies for data collection, usage, and access. To ensure security, data is encrypted and made available only to authorized individuals.

Another implementation of an ethical aware system is exposed by [21]. This article presents a computational model of moral decision making regarding social and ethical judgment on design, which is highly inspired by theories and models developed in cognitive neuroscience. This research deepens the architecture behind a moral decision considering the brain functioning itself. Even though our research does not explore this subject, we intend to emphasize the implementation of ethical theories in a computational logic approach, capable of generating well-defined evidence mechanisms.

The proposed mechanisms convey a logical based solution. The methodology covered in [22] maximizes the probability of a robot behaving ethically in a complex environment that mandates such conduct for human safety. Another alternatives for behavior are only actions that can be proven as morally permissible in a human-selected deontic logic. This paper is of interest since it offers a logical approach to engineering ethically correct judgments, as opposed to non-logicist ways, for instance neural networks. This is significant because the consensus of decisions on ethical questions depends critically on the presence of a formal proving mechanism, transparent to human comprehension. Following [23] as a reference, we intend to discuss in more detail a novel solution based on

Boolean algebra, that enables a machine to exhibit a variety of ethical behavior by employing the concept of ethics categories and modes.

Boolean method solution According to a study by Sahil Sholla et al. (2019), a Boolean method can be used to implement ethics in smart devices [23]. They first specify propositional variables that capture the Essential Operating Principles of the device, using these propositions to identify different scenarios that could occur between the device and its environment. Instead of a binary decision, five categories are used to determine the ethical status of a scenario: Forbidden, Disliked, Permissible, Recommended, and Obligatory. Resorting to a 5-bit register called ESR[7], where each bit represents one of the previous five, the category of a given scenario is defined by setting the corresponding bit, while the others are initialized to 0. In addition, to decide whether the scenario is accepted or not, another register called EMR[8] (with the same syntax as ESR) is used to indicate which ethics mode is applicable in a machine: Mild, Default, Strong and Stringent. A value of 1 for the ethics bit means that the scenario is allowed, whereas a value of 0 means that the scenario is denied.

Ethics category	ESR
Forbidden	10000
Disliked	01000
Permissible	00100
recommended	00010
Obligatory	00001

Fig. 2: ESR values for various ethics categories [23]

Ethics mode	EMR
Mild	01111
Default	00111
Strong	00011
Stringent	00001

Fig. 3: EMR values of ethics modes [23]

Imagine a medical device that measures a patient's health condition and sends health status messages to close relatives and friends [23]. Instead of checking if the recipient is authorized to receive the message, the device assumes so, but while notifying the friend(s) is only suggested, informing the relative(s) is mandatory in case of an emergency. Although it is recommended not to disturb them unnecessarily, it can also relay health status messages to both groups.

During the device's functioning, different scenarios may occur over a period of time, represented by three Boolean variables in a MATLAB context table – Figure 4, that indicates the ethical status of each scenario. As explained before, the simulation uses a 5-bit Boolean variable to represent the scenario status and another 5-bit variable to indicate the applicable ethics mode. For each scenario, an ethics bit is calculated by performing a logical 'AND' operation of the set bit in the ethics category with the corresponding bit position in the ethics mode. Depending on the type of application, some scenarios can be denied or allowed by default by setting the default ethics to deny or allow respectively.

[7] Ethics Status Register
[8] Ethics Mode Register

Scenario	e	r	m	Meaning	Ethical Status
1	0	0	0	no emergency, recipient is friend, no message	R
2	0	0	1	no emergency, recipient is friend, send message (health status update to friend in case of no emergency)	P
3	0	1	0	no emergency, recipient is relative, no message	R
4	0	1	1	no emergency, recipient is relative, send message (health status update to relative in case of no emergency)	P
5	1	0	0	emergency, recipient is friend, no message (not informing friend in emergency)	D
6	1	0	1	emergency, recipient is friend, send message (informing friend in emergency)	R
7	1	1	0	emergency, recipient is relative, no message	F
8	1	1	1	emergency, recipient is relative, send message	O

e - health emergency occurred

r - recipient is relative of patient

m - send heath status message

Fig. 4: Context table for the healthcare device [23]

4 Challenges and Benefits of a Secure Edge Computing Structure

In a first analysis, without considering the solutions proposed earlier, edge computing structures bring some challenges that enterprises must acknowledge beforehand. For one, implementing an edge infrastructure can be complex and expensive, requiring careful planning and the deployment of additional equipment and resources. For example, organizations may need to invest in edge servers, network devices and other hardware and software to support this paradigm. Another challenge is data loss, since edge computing can only handle subsets of information. Companies must carefully choose which data to process at the edge and which to send to central servers to avoid losing critical data. They must also ensure that data processing at the edge is accurate and reliable to avoid errors [5]. In addition, because data processing outside the network can be exposed to potential attacks, the necessary measures must be taken to ensure that the edge infrastructure is adequately secured. This includes implementing robust security protocols and encryption methods to protect data both in transit and at rest. Additionally, organizations must regularly monitor and update their edge computing devices to protect against new threats and vulnerabilities [4].

In truth, setting up a blockchain system with ring signatures and a participation reward service is no easy task. The reward system must be impartial, balanced, and free from manipulation. The conclusion is that not only financial resources for edge computing equipment, but also a qualified technical team must be taken into account (which can be a problem for institutions with very limited resources). In contrast, the proposed studies, offer the advantage of addressing solutions even in the event of system failures. The solutions investigated are based on the “indistinguishability” of user data, , so even when in possession of data from edge computing servers, it is impossible to attribute the data from

the generating sources. This is excellent because confidence in these services will increase if solutions are envisaged for data leakage scenarios.

When confronting ethical challenges linked to IoT in the hospitality industry, the emphasis on clear and open policies concerning data privacy and security is one benefit of the solutions presented in Section 3.3. This can help to foster customer trust in IoT systems. A logical-based strategy for designing morally sound decisions can also increase decision-making transparency. Meanwhile, these techniques are not liberated from flaws. For instance, using encryption and anonymization might hinder the ability to share and analyze data. Moreover, the complexity of ethical decision-making can limit the scope of the logical-based approach, calling for more nuanced and context-specific methods.

The Boolean technique is another suggestion and it has advantages and disadvantages of its own. While many ethics categories and modes can accommodate various ethical views and priorities, the usage of a 5-bit register can aid in systematizing ethical decision-making. Unfortunately, it might not be suitable for every IoT system types since it necessitates a great deal of adaption. [23] itself says that the ethics categories are inspired by Islamic jurisprudence – called 'fiqh' in the Arabic language, which classifies actions into five groups based on their ethical status. But the system could not be fully dependent in only one moral theory. [24] lists and discusses some benefits and harms of existing alternative moral theories. Despite that, the possibility of combining various ethical theories to solve certain problems is mentioned. For example, taking risks in radiation exposure combines the three main ethical theories of: virtue (referred to as justification); utilitarianism (as optimization); and deontologicalism (as individual dose limits). Additionally, depending on Boolean logic could oversimplify moral judgment and miss the depth and breadth of ethical difficulties encountered in real-world situations.

5 Conclusion

Once in possession of the necessary resources, we conclude that the state of the art in anonymous authentication is advanced enough to ensure the privacy of edge computing system participants. In contrast, the development of ethical issues in data collection and usage remains at a very early stage. This is normal, as this area is subjective and context-dependent. We, therefore, conclude, in a global point of view, that the use of edge computing is not yet sufficiently established to be considered feasible, secure, and ethical.

On the other hand, with a more specialized approach, in systems with properly bounded limits (i.e., coherent and defined laws and ethical systems), it is already possible to bring data processing closer to the end users. However, such a scenario is found precisely in specialized environments, perhaps in systems that are intended to be used only in a particular country, making it not feasible to extend to multicultural domain.

References

1. Jon Gold and Keith Shaw. What is edge computing and why does it matter? Website, 2022.
2. Amin Shahraki and Øystein Haugen. Social ethics in Internet of Things: An outline and review. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, pages 509–516, 2018.
3. Nir Kshetri and Jeffrey Voas. Social and ethical behavior in the internet of things. *Communications of the ACM*, 60(2):70–80, 2017.
4. Sachchidanand Singh. Optimize Cloud Computations using Edge Computing . *International Conference on Big Data, IoT and Data Science, Vishwakarma Institute of Technology, Pune*, 2017.
5. What Is Edge Computing: Definition, Characteristics, and Use Cases. Website, 2023.
6. Vijay Prakash Soni, Alex Williams, Lalit Garg, and Claudio Savaglio. Cloud and Edge Computing-Based Computer Forensics: Challenges and Open Problems. *Electronics*, 2021.
7. John Edwards. Edge Computing Security: Dos and Dont's. *Network Computing*, November 2018. [Online; accessed 21-March-2023].
8. Muktar Yahuza, Mohd Yamani Idna Bin Idris, Ainuddin Wahid Bin Abdul Wahab, Anthony T. S. Ho, Suleman Khan, Siti Nurmaya Binti Musa, and Azni Zarina Binti Taha. Systematic Review on Security and Privacy Requirements in Edge Computing: State of the Art and Future Research Opportunities. *IEEE Access*, 8:76541–76567, 2020.
9. Nathan Vance, Daniel Zhang, Yang Zhang, and Dong Wang. Privacy-Aware Edge Computing in Social Sensing Applications Using Ring Signatures. pages 755–762, 2018.
10. Tian Li, Huaqun Wang, Debiao He, and Jia Yu. Blockchain-Based Privacy-Preserving and Rewarding Private Data Sharing for IoT. *IEEE Internet of Things Journal*, 9(16):15138–15149, 2022.
11. Francine Berman and Vinton G. Cerf. Social and Ethical Behavior in the Internet of Things. *Communications of the ACM*, 60:6–7, 2017.
12. Suat Mercan, Kemal Akkaya, Lisa Cain, and John Thomas. Security, Privacy and Ethical Concerns of IoT Implementations in Hospitality Domain. *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, pages 198–203, 2020.
13. Paul Brous, Marijn Janssen, and Paulien Herder. The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management*, 51, 2020.
14. An Introduction to Edge Computing Architectures. Website, Oct, 2021.
15. Ashish Singh and Kakali Chatterjee. Edge computing based secure health monitoring framework for electronic healthcare syste. *Cluster Computing*, 26:1205–1220, 2022.
16. Naif Almusallam, Daniyal M Alghazzawi, Mustafa M Alobaidli, Abdulaziz Almutairi, Abdulaziz Alharbi, and Nouf Aljaffan. Analysis of Privacy-Preserving Edge Computing and Internet of Things Models in Healthcare Domain. *Computational and Mathematical Methods in Medicine*, 2021:6834800, 2021.

17. Wangze Ni, Han Wu, Peng Cheng, Lei Chen, Xuemin Lin, Lei Chen, Xin Lai, and Xiao Zhang. CoinMagic: A Differential Privacy Framework for Ring Signature Schemes, 2020.
18. Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to Leak a Secret. pages 552–565, 2001.
19. Monero: secure, private, untraceable cryptocurrency. Website, Accessed March 21, 2023.
20. Tomislav Car, Ljubica Pilepić Stifanich, and Mislav Šimunić. INTERNET OF THINGS (IOT) IN TOURISM AND HOSPITALITY: OPPORTUNITIES AND CHALLENGES. *ToSEE – Tourism in Southern and Eastern Europe*, 5:163–175, 2019.
21. José-Antonio Cervantes, Luis-Felipe Rodríguez, Sonia López, and Félix Ramos. A biologically inspired computational model of moral decision making for autonomous agents. In *2013 IEEE 12th International Conference on Cognitive Informatics and Cognitive Computing*, pages 111–117, 2013.
22. S. Bringsjord, K. Arkoudas, and P. Bello. Toward a general logicist methodology for engineering ethically correct robots. *IEEE Intelligent Systems*, 21(4):38–44, 2006.
23. Sahil Sholla, Roohie Naaz Mir, and Mohammad Ahsan Chishti. Towards the design of ethics aware systems for the Internet of Things. *China Communications*, 16:209 – 221, 2019.
24. Noah Goodall. *Machine Ethics and Automated Vehicles*, pages 93–102. 06 2014.