IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 6, December 2026, pp. 5190~5205
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i6.pp5190-5205

Ethical implications of artificial intelligence in internet of things: a comprehensive review and framework development

Essam S. Hanandeh[1], Belal M. Bataineh[2], Obaida M. Al-Hazaimeh[3], Ashraf A. Abu-Ein[4], Atef A. Obeidat[5]

[1]Department of Cyber Security, Faculty of Computers Science and Information Technology, Jerash University, Jerash, Jordan
[2]Department of Computer Science, Faculty of Information Technology, Jadara University, Irbid, Jordan
[3]Department of Computer Science and Information Technology, Al-Huson University College, Al-Balqa Applied University, Irbid, Jordan
[4]Department of Electrical Engineering, Al-Huson University College, Al-Balqa Applied University, Irbid, Jordan
[5]Department of Information Technology, Al-Huson University College, Al-Balqa Applied University, Irbid, Jordan

Article Info

Article history:

Received Feb 25, 2025
Revised Aug 10, 2026
Accepted Sep 20, 2026

Keywords:

Algorithmic accountability
Artificial intelligence ethics
Data governance
Data privacy
Data rights
Internet of things
Regulatory frameworks

ABSTRACT

An expanding system of networked computing devices that can gather and transmit data autonomously via the internet, the so-called internet of things (IoT) includes sensors and actuators. Ethical concerns are becoming more pervasive in our everyday lives as a result of this expanding technological ecology. Thorough examination is necessary for these new difficulties. This research delves into the many ethical concerns surrounding the IoT, investigating its far-reaching effects on several aspects of human engagement with interconnected technology. Both the technical aspects and the moral considerations of IoT technologies are included in the research. Every participant in the IoT industry, from individual users to large industries, is affected by ethical concerns, and we rigorously examine how these influences cause negative effects. Researchers, practitioners, and legislatures can get practical insights from this study as they navigate the complicated environment of IoT systems coupled with artificial intelligence (AI). The study employs a structured literature review across major academic databases, thematically synthesizes the retrieved findings into a conceptual ethical framework, and illustrates that framework through real-world case studies.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Essam S. Hanandeh
Department of Cyber Security, Faculty of Computers Science and Information Technology, Jerash University
Jerash 26150, Jordan
Email: e.hanandeh@jpu.edu.jo

1. INTRODUCTION

Ashton coined the phrase internet of things (IoT) from improved networking and communication technologies [1]. In particular, internet technology links the online with physical objects, hence the title "internet". Typically, IoT "things" are physical items. In conclusion, IoT refers to items, especially ordinary objects, that are readable, recognized, locatable, addressable, and/or controllable over the internet, whether via radio frequency identification (RFID) or other emerging technologies [2]. The following five point's best describe IoT at this level of the invention process. First, any internet technology may identify and incorporate physical "things" into the online. Second, the integration creates a new technology wander internet "thing". Due to the infinite number of items and relationships, software logic can stimulate advantage trading, which the technology strategy board is exploring. Third, various conflicting human endeavors may drive this technology wander's demand. Individuals may need quick networking to communicate with home gadgets,

while large industry systems like smart cities may need low failure rates and many data exchanges. According to invention history, the fourth and fifth steps interfere. Putting things on "the cloud" is the beauty of leaving other stages to our imagination [3], [4].

IoT items include mobile devices, smart objects, and smart things with virtual identities. Aside from being self-configuring and interoperable, having individual identities, and communicating and exchanging data with other devices and systems, IoT objects should be able to dynamically adapt to changing surroundings and behave accordingly [5]. Therefore, situational awareness and network connectivity are crucial. The IoT needs a solid structure, hence IoT architecture is useful which leads to numerous IoT architectural paradigms. One five-layer IoT architectural paradigm includes perception, network, middleware, application, and business layers [6]. The five-layer concept explains IoT. This paradigm is also the most popular because it forms the basis for early IoT design. The perception layer uses sensors to collect environmental data. The network layer connects smart devices by transferring data to cloud servers for processing. Middleware connects the database and matches services with similar requesters. The application layer models large IoT applications and delivers operation-critical services. The business layer generates business models and manages the system. The layer architecture of the IoT is illustrated in Figure 1 [6], [7].

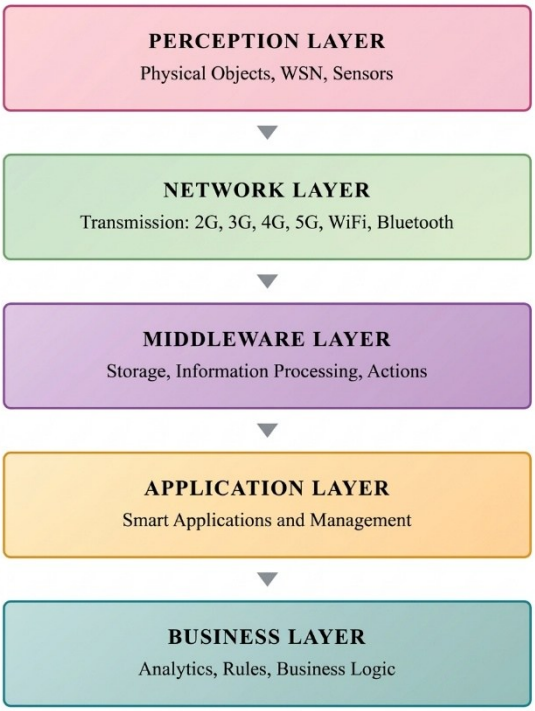

Figure 1. IoT layer architecture

The IoT fog-edge computing (FEC) model adds to the fundamental IoT technical architecture. It includes cloud, edge, fog, and IoT devices. IoT things layer handles detected and recorded data using implanted sensors and actuators. The edge layer, which sits between the end-user and the cloud, provides processing (i.e., routers) and storage (smartphones) to many IoT devices as shown in Figure 2 [7].

Fog layer data can be handled at IoT gateways or micro-data centers like satellites and fog nodes by moving computing below the local area network (LAN) in the fog layer. Big data analytics, industrial-level databases, processing, and data warehousing are cloud layer priorities. Cloud and cloud servers are remote cloud centers that centralize computing. FEC helps plan and build a versatile and scalable IoT platform for frameworks that demand robust detection, analysis, incitation, examination, and control [8].

While current IoT applications have demonstrated significant benefits in various fields, existing systems face several critical limitations that are addressed in this research paper. Traditional IoT frameworks often lack comprehensive ethical oversight mechanisms, particularly as systems evolve to include artificial intelligence (AI) and autonomous decision-making capabilities. Many deployed IoT systems operate with limited transparency, making it difficult for users to understand how their data is processed and decisions are made. Furthermore, the rapid integration of AI technologies into IoT systems has outpaced the development

of appropriate ethical frameworks. Current regulatory approaches often treat IoT and AI ethics separately, failing to address the unique challenges that arise when these technologies converge. Table 1 summarizes the key contributions of this research.

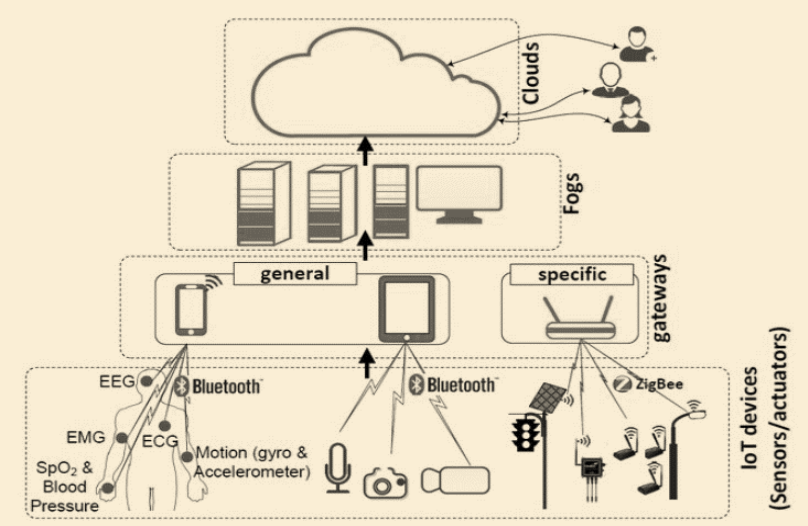

Figure 2. IoT layer architecture – based FEC

Table 1. Research contribution

Description	Contribution	No.
Presenting an all-inclusive review procedure for examining the IoT's ethical dilemmas.	Methodological systematization	1
Examine examples of ethical frameworks in action by analyzing real-world case studies.	Empirical validation	2
Create organized models that connect long-standing issues with the IoT with new guidelines for AI ethics.	Integrated AI ethics framework	3
Examination of the ethical dilemmas that arise in many IoT domains.	Multidisciplinary analysis	4
Practical advice for regulatory and governance methodologies.	Policy guidance	5

The subsequent sections of this work are structured as follows. Section 2 delineates the research technique. Section 3 delineates the ethics of IoT and the integration of AI. Section 4 addresses critical issues related to the IoT, while section 5 provides a discussion on the topic. Section 6 presents ethical challenges in practice and future directions. The conclusion is located in section 7.

2. METHOD

The ethical challenges in IoT systems are thoroughly examined in this paper through the use of a literature review technique and case study analysis. The methodology is based on the standards set by technology ethics research, but we have adjusted it to account for the lightning-fast development of the IoT. Figure 3 illustrates the research methods employed in this research.

To make the review process transparent and reproducible, the literature search was conducted across Scopus, Web of Science, IEEE Xplore, and ACM Digital Library, supplemented by targeted searches of Google Scholar for grey literature such as regulatory texts. The search combined keywords including “IoT ethics”, “AI ethics”, “algorithmic accountability”, “privacy”, and “governance framework”, connected with Boolean operators and restricted primarily to publications from 2020 to 2025 to prioritize recent developments, while a small number of foundational earlier works (e.g., Mason *et al.* [9] that proposed privacy, accuracy, property, and accessibility (PAPA) framework) were retained for conceptual continuity. Records were included if they addressed ethical, legal, or governance dimensions of IoT and/or AI-enabled IoT systems in peer-reviewed venues or official regulatory sources, and were excluded if they focused solely on technical performance without any ethical or governance discussion, were not available in English, or were duplicate records across databases. Screening proceeded in two stages, an initial title / abstract screening followed by full-text review, after which the retained studies were thematically synthesized into the ethical categories and case studies presented in the following sections; while this process draws on

systematic-review conventions such as those promoted by preferred reporting items for systematic reviews and meta-analyses (PRISMA), the study is best characterized as a structured narrative review with a case-study-supported framework, since a formal quantitative meta-analysis was not the aim.

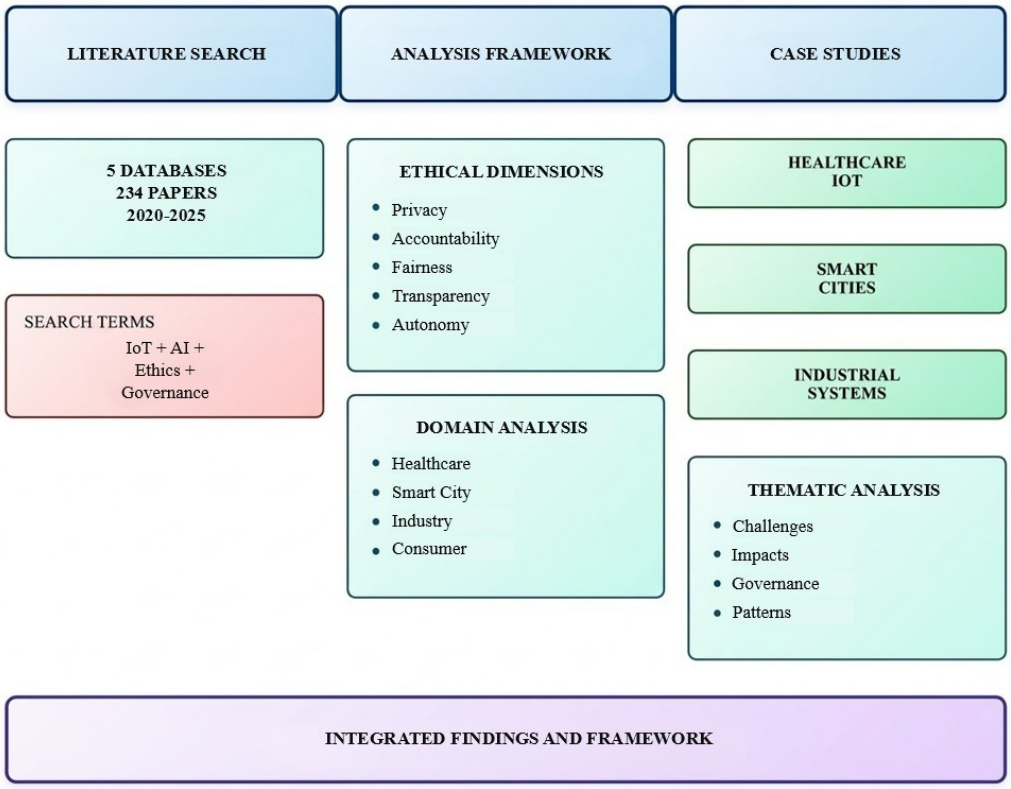

Figure 3. Research methodology

3. ETHICS OF INTERNET OF THINGS AND INTEGRATION OF ARTIFICIAL INTELLIGENCE

Originating from the term "*ethica docens*", Aristotle established ethics as a field of study in the third century before christ. It entails teaching a philosophical perspective on analytical and critical behavior. Furthermore, moral, right or wrong, and just or unjust values serve as the definition and guidelines for human behavior and conduct in society [10]. Ethics in the context of IoT refers to the proper regulation of human behavior toward oneself and others; in other words, they establish what is good or bad and what is right or wrong. Ethics can be thought of as a means of defining what is good and bad, right and wrong, because it deals with establishing the proper regulations for human activities toward both others and oneself in the context of the IoT [11]. The expansion of the IoT may lead to additional ethical quandaries, particularly as the technology continues to surpass the advancement of laws and regulations. The way society functions and plays will be completely transformed by the IoT. In order to guarantee that the IoT is utilized for the benefit of humanity and not the other way around, an ethical framework must be developed [12], [13].

New concepts and ideas should be put forth in order to define the proper regulations and policies for this complex environment because of the IoT system's complexity, heterogeneity, and size. The growth of IoT technologies is the primary source of ethical problems in the IoT [14]. Furthermore, transparency and the ethics of the use and behavior of these systems must be a central focus of the community's ongoing exploration of the risks and opportunities related to IoT-driven systems. Building ethical frameworks is also necessary to help people understand what is good and bad as well as what is appropriate and inappropriate. An ecosystem comprising people, autonomous and self-determining systems, devices, and virtual and physical environments must be relevant to the mechanisms that uphold ethical IoT frameworks [15].

3.1. Ethical challenges in internet of things

Morals and ethics are associated with social behavior standards in the IoT, which is characterized by the presence of billions of devices. The primary subjects of ethical discourse are privacy, integrity,

information access, and property rights [16]. Consequently, it is crucial to consider the following factors when implementing ethics in the context of IoT. Table 2 contains a list of these ethical considerations in the context of IoT.

Table 2. Ethical issues in IoT

References	Moral factors	Description
[17]	Owner identification challenge	Recognizing numerous things is essential for engaging with the IoT. Accurately identifying the owner of a certain thing is tough due to the extensive data associated with numerous objects. Given the gravity of the issue, the IoT system must autonomously manage the acquisition of this data without the user's consent.
[18]	Public-private boundary	As both categories of data are collected by the sensors together, the IoT system may struggle to differentiate between public and private data due to the absence of clear boundaries between them.
[19]	Attacks on people's lives	Security breaches in computer-only systems can damage data or systems. The IoT connects homes, cars, smart meters, and more, so a breach might impact lives. Assailants could hijack a home's energy, causing serious injury. Hackers or viruses can damage regular computers or erase data. IoT assaults will continue to hurt lives. Attackers might access a traditional IoT medical application and change a single data point to give the wrong medication, which could endanger the patient.
[20]	Ambiguity	As technology improvements blur the barrier between natural and artificial entities, it becomes increasingly difficult to delineate and define system boundaries with the proliferation of IoT devices.
[21]	Unpredictable behavior	Interconnected devices, gadgets, and artifacts in the IoT ecosystem may unintentionally disrupt people's day-to-day activities and change the trajectory of events.
[22]	Difficult control	Centralized control and governance will end as a result of the ever-increasing quantity of devices, hubs, switches, and data. Data transfers will get faster and cheaper in response to demand as the volume of data grows, but this will leave little room for oversight, leaving systems open to new vulnerabilities.

3.2. The integration of artificial intelligence ethics in internet of things systems

The integration of AI into IoT systems introduces new ethical dimensions that go beyond traditional concerns about privacy and security. As IoT devices become more autonomous and capable of making independent decisions, issues of algorithmic accountability, bias, and transparency become central to the ethical deployment of the IoT. Table 3 provides a summary of important AI ethics frameworks that are applicable to the IoT.

Table 3. Key IoT - AI ethics frameworks

References	Framework / concept	Principal areas of emphasis	IoT significance
[23]	European Union (EU) AI Act (2024)	Risk-based categories, transparency, human oversight, risk management	Provides the regulatory foundation for the ethical use of the IoT in healthcare, transportation, and critical infrastructure.
[24]	IEEE ethically aligned design (EAD)	Data agency, human rights, transparency, and accountability	Guides the ethical design of AI-powered IoT, ensuring responsible autonomous decisions that impact human well-being.
[25]	Distributed IoT algorithmic accountability	Accountability for multi-agent decisions, emergent behavior, responsibility sharing between humans and AI, responsibility between organizations	Draws attention to novel issues with responsibility in distributed IoT networks with numerous autonomous nodes.
[26]	UNESCO AI ethics recommendation	Proportionality, precaution, protection of human rights	Includes topics such as the handling of personal data by IoT systems and decisions that have an impact on persons and communities.
[27]	OECD AI principles	Sustainable development, human-centered principles, and inclusive growth	Makes sure that the IoT puts people's happiness ahead of efficiency.

4. THE CRITICAL INTERNET OF THINGS ISSUES - ENHANCED ANALYSIS

IoT systems have a number of fundamental and essential difficulties that contribute to their failure. This section will define and discuss a number of these essential concerns. These concerns are organized around Mason's PAPA framework, namely PAPA, together with interoperability as an additional dimension. A structured framework that groups these challenges into technical, social, and governance dimensions is then presented at the end of the section.

4.1. Internet of things privacy threats

As mentioned in section 3, the IoT applications include billions of devices, sensors and actuators connecting to the internet. Accordingly, a large amount of information are generated, which increase the difficulty of privacy tasks [28]. Washington [29] defines the privacy as "The claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others". Privacy is not just devoted to information, it also devoted for communications, body and territory. The various forms of personal data that an organization collects and manages, such as financial and medical data, are referred to as information privacy. Protecting the sensed data that is transferred between two communicating nodes is a communication privacy concern. Concerns about body privacy include external harm as well as people's physical safety. The boundaries of physical spaces, such as homes, workplaces, and public areas, are the focus of territorial privacy [30]. Since the data gathered and sensed is passive, less intrusive, and ubiquitous, privacy is more important and harder to achieve from an IoT standpoint. This is because users lose control of their personal information and aren't aware that they are being tracked. In addition, as shown in Table 4, several privacy issues arise from the characteristics of the IoT, which in turn lead to violations of user privacy.

Table 4. Several privacy issues

References	Privacy issues	Description
[31]	Threat of an identifier	The IoT allows devices to sense and gather a wealth of data about people and their interactions with their environments since it is pervasive. In most cases, third-party service providers handle the processing of such data. Identity theft occurs when personal details, such as a person's name or whereabouts, are linked to an identifier. Emerging technology and the integration of disparate approaches raise the identification hazard in the IoT. Use of surveillance cameras in non-security contexts to study consumer behavior for advertising and data analysis is one example of such a method.
[32]	The threat of localization and tracking	Localization and tracking involve the hazards of tracing an individual's whereabouts across time and place using global positioning system (GPS) data, internet traffic, or cell phone location. Geographic data and spatial information analysis are becoming popular due to the availability of large spatial and spatiotemporal data. As IoT develops, location-aware applications and their accuracy, data collection technologies, and user interaction with IoT devices that record identity, location, and activity appear to increase localization threats.
[33]	Profiling	Profiling involves tracking and categorizing an individual's actions throughout time. Data is often collected without users' consent and mixed with other personal information to provide a more complete picture. Today, e-commerce, targeted advertising, and credit scoring use profiling. Profilers risk leaking your private information to anyone who views your targeted ad on the same computer or browser. Many find it annoying to be followed and monitored. As the IoT has grown, data collection has increased due to more data sources and devices. Wearables and household devices will provide previously inaccessible qualitative data.
[34]	Life-cycle Transitions	Any change in ownership of a customer product over its lifetime poses a risk to the customer's privacy. Since most people keep the same computers, cellphones, and cameras throughout their lives, this problem seldom arises. There will be a greater risk of privacy disclosure due to ownership transitions when products that are more commonplace are connected and store personal information.
[34]	Inventory Attack	Inventory attacks involve stealing data about objects' locations and properties. IoT fingerprints like communication speed, reaction time, etc. can be utilized for inventory attacks. If IoT succeeds, all smart objects will be internet-addressable. Unauthorized parties could use this to catalog a target's belongings. Inventory attacks can profile people since distinctive objects expose personal information.
[31]	Linkage	Merging diverse data sources and integrating disparate systems creates a "linkage threat". Integrating several types of person information reveals unexpected facts to the owner. An invasion of privacy occurs when data is disclosed. Integrating enterprises will enhance the linkage danger by generating a more distributed and heterogeneous system, which will increase system complexity and limit data gathering transparency in the IoT.

4.2. Information accuracy

The second issue with Mason's framework is accuracy, pertaining to the truthfulness, precision, and authenticity of data. It also addresses accountability for mistakes and adverse events. Besides mistake avoidance, accuracy concerns include both system and information precision. As technology, systems get increasingly complex, so too do inquiries regarding accountability presently, the integrity of the entire socio-technical system is at risk, rather than merely the precision of the data. Such inquiries have recently been regularly discussed within the context of accountability [35]. The widespread and autonomous nature of the IoT, characterized as a "system of systems" has sparked significant discussion regarding accountability. It is unsurprising that numerous scholars have examined the legal dimensions of IoT and accountability, as accountability is often predicated on legal statutes. Although the law delineates permissible and impermissible actions, ethical issues are often overlooked. A prevalent understanding of accountability

encompasses concerns related to safety and security, privacy and monitoring, as well as governance and responsibility. Consequently, it intersects with Mason's additional categories. Argued that the primary concern regarding IoT accountability is determining who bears responsibility for ensuring the technology operates and is employed as intended.

The IoT must be harmonized with initiatives that educate individuals regarding their personal data usage and enhance transparency in data flow and utilization, given its potential application as surveillance apparatus. Due to the potential for failures that may cause physical injury, it is imperative to prioritize safety and security [6]. Consequently, accountability concerning IoT pertains to the entity responsible for the system's correct functioning and the prevention of harm. This is especially vital when autonomous systems may perform physical manipulation. The challenges of physical manipulation in robotics have been extensively examined by Kernaghan [36]. In a small or medium-sized enterprise with constrained resources and restricted delegation of power, a single employee or a small group may assume the predominant responsibility; they must be cognizant of the associated hazards. The reliability and accuracy of the acquired information is a separate concern. Inaccurate information regarding an employee's conduct may be retained, processed, and disseminated, jeopardizing the individual's reputation both personally and professionally. An IoT solution equipped with sensors might track an employee's location while utilizing a business vehicle [19]. The employer may form incorrect conclusions and generate unjustified trust difficulties if the location sensor in this case yields faulty data, indicating that the employee has remained stationary or has deviated from the designated route.

The collected IoT data is often susceptible to modification, presenting an additional opportunity for exploitation. Conclusions derived from data must be approached with caution, as it cannot be presumed that the information provided by IoT systems is consistently reliable. These remarks indicate that to utilize the output of the IoT solution judiciously and derive valid conclusions, it is imperative to acknowledge the potential for erroneous or misleading information. Finally, minimizing personal discrimination resulting from mismanaged or misinterpreted data significantly relies on data accuracy. Employees must be informed about and given authority over the collection and dissemination of data, while simultaneously being protected against discrimination resulting from erroneous or unethical data acquisition. Nonetheless, discrimination may manifest in several forms. Key risk factors to consider include the tendency of IoT solutions to facilitate the collection and amalgamation of data irrelevant to one's profession, while also enabling observers to engage in profiling and form subjective assessments of individuals being observed. When its veracity cannot be fully verified, it is inadvisable to utilize any data that may be perceived as blurring the distinction between personal and professional in decision-making [12].

4.2.1. Factors defining internet of things data accuracy

The original PAPA model has been expanded to incorporate new digital-age technologies and environments as necessary. For example, new ethical concerns have been identified that are specifically related to big data, such as governance, interpretation, and behavioral surveillance. Additional enhancements are required for AI and other emergent technologies.

i) Accuracy of data collection: given the dependability and logic of data-driven decision-making, the accuracy of the data collected is critical. When employees' performance is evaluated and decisions about career development, hiring, or firing are made, using incorrect data has a negative impact on both the firm and the people. According to the company, inaccurate data might be utilized intentionally or unintentionally. The deliberate use of inaccurate data creates moral quandaries that can adversely harm the company's brand and internal relationships. However, mistakenly employing incorrect data would likely reduce or eliminate the intended benefits of data-driven decision-making. The quality of the IoT solutions employed is critical when considering the aspects that influence the accuracy of the data collected. The quality and cost of the solutions vary. Multipurpose IoT devices provide businesses an economical method to access a variety of beneficial functions, but quality tradeoffs are usually unavoidable. Various optimization criteria, such as the demand for compact devices or low energy consumption, as well as the need for cost-efficiency, may have a negative impact on data quality. Furthermore, utilizing the same elements in many sensor models complicates cross-validation and increases the chance of systematic errors, even when comparing and verifying different sensor models. Problems with real measurement accuracy, timeliness, completeness, relevance (i.e., utility), volume, or data source concordance are some examples of data quality difficulties.
ii) Selection of data: businesses must choose data gathering kind, source, and time ethically. The optimal data gathering choices raise the possibility of accurate and valuable employee performance data and reduce the danger of injury from improper data collection and/or misleading analysis. Whether the variables were chosen to facilitate accurate and logical analysis is crucial in this case. Are variables accurately measuring real-world phenomena? Are the granularity measurements accurate? Can we trust

every chosen and measured attribute? When used together, are measurements comparable? When multiple data types are employed, accuracy is crucial because a single distorted attribute can invalidate the study. Even with perfect analysis, bad data selection might skew future analysis. If the critical components are miscalibrated, monitoring daily averages instead of per-second measurements can destroy any relevant data. By monitoring the wrong qualities, decision-makers may get a false impression of accuracy since data collection, management, and analysis are operational, but the measurements may not precisely reflect the reality.

iii) Accuracy of analysis: even with properly acquired and selected data, inaccurate analysis might invalidate results. Again, intentional or accidental activities may cause issues. Despite literature on data analysis best practices, organizations may not have the skills and knowledge to conduct ethical and practical analyses. Carefully selected data can reduce the likelihood of complex analysis yielding false conclusions, but it may miss critical characteristics. For instance, ignoring the lack of material for processing and only examining industrial machinery usage during a given time period to assess employee performance is likely to yield inaccurate results. Additionally, optimizing machinery usage time may not be the best strategy and that optimizing other metrics like finished goods production, product quality, or employee coordination would yield higher profits. In addition to IoT data, trustworthy analysis often requires supporting data and effective control methods. Note that AI-based data analysis is getting more prevalent. Although this may reduce human mistake, AI cannot be trusted as a solution to human behavior problems.

iv) Accuracy of governance: as indicated earlier, data is not static, and the accuracy of data-driven decisions is affected by a myriad of human factors. From more basic data governance to more complex organizational (or intero-organizational) governance, there are several ways in which governance practices can affect the accuracy of data. Data governance encompasses a wide range of information processes targeted at ensuring the high quality of managed data. Data corruption, physical loss, communication failures, accidental modifications, migration mistakes, and malicious deletion or manipulation are all possibilities due to poor data governance, which in turn increases the likelihood of data inaccuracies. Data quality management frameworks like Wang's [37] total data quality management are suitable for controlling IoT data, even if there aren't yet any that are tailored to IoT data specifically. In addition, corporate governance has a substantial effect on the outcomes of data-centric decision-making. It makes no difference how faithfully the underlying data reflects reality; if the decision-making process is flawed due to governance concerns, the results may be incorrect or unpleasant. Ethical considerations around data use should be considered by governance since data use may affect the individuals whose data is collected. In order to ensure that judgments are based on accurate information and not erroneous information, it is necessary to control all levels of accuracy.

4.3. Property of information

Property or ownership-related problems constitute the third category of ethical dilemmas in Mason's PAPA framework [35]. Mason [9] in 1986 employed inquiries such as “Who possesses the information?” to clarify the issues within this category. What constitutes fair and just exchange rates? Who governs the information transmission routes, and what is the appropriate method for distributing access? The matters of data ownership and collection must be considered, as data has increased in value and IoT technology can generate and collect it more efficiently. Nevertheless, as information and data do not possess the same characteristics as physical property, the complexities of their status as property are quite intricate. Mason asserts that knowledge possesses diverse values or attributes, and although its acquisition may be costly, its reproduction and transmission are straightforward. Information is challenging to safeguard as it can be replicated without eliminating the original. The IoT raises numerous ethical concerns due to its capacity for rapid and extensive data collection, notwithstanding the existence of various organizations and regulations aimed at safeguarding data and information, including intellectual property rights and recent initiatives to protect individuals' rights to their personal information.

IoT systems can store data on servers for various purposes, including post-processing and trend analysis of value. Understanding data ownership, retention duration, and disposal responsibility is essential from the employee's viewpoint. The employee must be cognizant of their rights to retain, handle, and utilize the data, as well as their capacity to limit such actions by external entities. Keeping the employee informed about property-related issues is likely to aid in preventing and preparing for any ethical dilemmas. Efforts have been made to redefine the concept of information ownership, a very ambiguous issue. Instead of ownership, for example, Mason *et al.* [9] suggested the concept of mastery over data (Datenherrschaft). Their idea posits that individuals should have control over the utilization of their data and the entities with whom they choose to share it. Subsequently, the authors [38]–[41] illustrated that mastery of data constitutes an ethically permissible method of data ownership from four ethical viewpoints (Locke, Kant, Heidegger, and Rawls). The concept can be utilized in numerous contexts, despite its original design for patient information.

Control over data can be superseded in certain situations, therefore it is crucial to acknowledge that this concept is not definitive. Nonetheless, the concept of mastery over data facilitates the clarification of issues related to data or information ownership. Who possesses authority over or ownership of IoT data? Information can be stored on either external or internal servers. The involvement of an external actor or organization complicates the distribution of ownership and control. In the initial circumstance, it is likely quite straightforward to oversee and understand. This multi-organizational environment presents several property-related concerns, particularly around data usage and permissible objectives. What data can be collected and retained, and how can small and medium enterprises (SMEs) utilizing IoT solutions ascertain the data that will be gathered? Clarifying approval-related concerns is equally vital when considering employee viewpoints. Specifically, how to secure the agreement of monitored staff while considering ethical risk concerns. Explicit criteria must be established for the data, specifying if it is collected for commercial purposes and if so, by whom and at what expense.

4.4. Accessibility

Accessibility is the fourth category of ethical issues that Mason [9] in 1986 addresses [35]. This category focuses on what information, under what circumstances, and with what safeguards an individual or organization has the right or privilege to obtain. Since literacy has been the primary means of obtaining information, Mason [9] in 1986 connected it to access to information. He did point out, though, that in order to actually have access to information, one must possess the resources and know-how to do so. Accessibility, then, involves both granting and restricting access. The issues of how, when, and to whom access is granted give rise to the ethical considerations. However, accessibility issues become more complicated because information may be viewed as an organization's valuable property or as something that needs to be protected because of privacy concerns [42].

The degree to which accessibility has been managed depends in part on privacy, which is perhaps the focus area with the strongest connection to the other three focus areas. Employees who are entitled to access their personal information should therefore be reminded of its purpose. Potential conflicts are more likely to be avoided the more thoroughly information sharing is communicated. The degree of safety measures, which guarantee that only the designated individuals can access the data, is an equally significant factor. Even seemingly, insignificant problems can grow into major ones, particularly when they involve personal data leaks. Can it be argued that management is responsible for managing data security and access rights? If the management lacks the necessary resources or expertise to guarantee careful evaluation of the aforementioned factors, it should speak with a service provider or another outside party that is able to take the necessary steps. This category contains a wide range of potential hazards, including those related to network security, application security, communication security, and general device security. To prevent any predictable problems, the person responsible for ensuring safety should be chosen with care and consideration. The general idea here is that moral obligations and values do matter, regardless of whether they can be fulfilled on their own.

4.5. Interoperability

The capacity of many systems to enable the transfer and utilization of data amongst themselves is known as interoperability. This ensures that all components will be in perfect harmony. Companies in the private sector place a high importance on interoperability since it seeks to solve common problems including information duplication, fragmentation, and the use of several, incompatible information systems. Organizational control and efficiency collapse under these conditions. Public organizations must prioritize interoperability in order to facilitate optimal collaboration, development, integration, and service delivery, just as private enterprises do it. In particular, it makes it easier for various apps to work together to create new services, which in turn helps public policy come to fruition. As a result, the information society and e-governance can progress. One must be familiar with the two tiers of interoperability, namely semantic and technological, in order to gain a better grasp. When two or more systems are able to interpret each other's data, it is called semantic interoperability. At this tier, the data must be substantial and practical. When two or more software components are technically compatible, they can work together despite differences in programming language and user interface. One major reason interoperability is crucial is the ease with which all of your data can be managed together in a structured manner. As a result, it boosts productivity, ensures data cohesiveness, and maximizes adaptability.

4.6. Structured framework for internet of things ethical challenges

A multi-dimensional framework was presented that classified the ethical issues found in IoT systems into three categories: technology, society, and government. Figure 4 presents the proposed

framework for the ethical challenges of the IoT. For IoT systems connected with AI, we present (1) as a risk assessment approach, that examines ethical implications across various dimensions.

$$Ethical\ Risk = \frac{Impact\ Severity \times Probability \times Stakeholder\ Vulnerability}{Mitigation\ Effectiveness \times Oversight\ Capability} \quad (1)$$

Based on this score, people can be classified into one of four risk categories, which determines the management approach: Risk might be low (1-3), intermediate (4-6), high (7-8), or critical (9-10).



Figure 4. Ethical challenges framework

5. DISCUSSION

The discussion part examines the ethical dilemmas related to the IoT by evaluating its consequences for individuals, organizations, and society. The IoT has significant prospects for innovation and convenience, while it simultaneously poses issues with privacy, security, and accountability. These difficulties underscore the conflict between technical advancement and ethical accountability. Comprehending these challenges is essential for formulating policies and procedures that encourage responsible IoT use.

5.1. Internet of things private threats

IoT devices typically lack strong security mechanisms and clear data management policies, which leads to the intense collecting, storing, and sharing of personal data, which in turn causes the privacy issues listed in Table 5. As Table 5 shows, each privacy threat discussed in section 4.1 is linked to one or more of the ethical issues identified in Table 2, with difficult identification appearing in all six threats. This indicates that improving the identification of owners and objects, together with clearer boundaries between public and private data, would mitigate several privacy threats simultaneously.

5.2. Accuracy of information

Poor decision-making, brought on by an absence of explicit data management regulations and robust accuracy information mechanisms in most IoT devices, results in the privacy difficulties outlined in Table 6.

Table 6 maps each of the four accuracy factors described in section 4.2.1 to the ethical issues of Table 2 that they affect. The borderline between public and private data and the risk of attacks on people's lives recur across all four factors, which shows that inaccurate information can have consequences beyond poor decisions.

Table 5. The causes of privacy threat issues

No.	Privacy threats	Impacts
1	Identification	– Difficult identification
		– Unpredictable behavior
		– Borderline between public and private
2	Localization and tracking	– Difficult identification
		– Ambiguity
		– Borderline between public and private
		– Difficult control
3	Profiling	– Difficult identification
		– Ambiguity
		– Life theater
4	Life cycle transition	– Difficult identification
		– Life attack
		– Difficult control
5	Inventory attack	– Difficult identification
		– Borderline between public and private
		– Life attack
		– Ambiguity
		– Unpredictable behavior
		– Difficult control
6	Linkage	– Difficult identification
		– Borderline between public and private
		– Ambiguity
		– Difficult control

Table 6. The causes of accuracy information

No.	Accuracy of information	Impacts
1	Accuracy of data collection	– Difficult identification
		– Borderline between public and private
		– Life attack
2	Selection of data	– Borderline between public and private
		– Life attack
		– Ambiguity
3	Accuracy of analytics	– Difficult identification
		– Borderline between public and private
		– Life attack
4	Accuracy of governance	– Borderline between public and private
		– Life attack

5.3. Property of information

The identification of information properties is a complex and ongoing issue, as previously mentioned. This ethical dilemma can be better understood by drawing parallels to problems with the IoT. Accurate identification will simplify this ethical dilemma with regard to the owner of the information. In addition, the complexity can be reduced by reducing ambiguity and drawing a clear boundary between the public and private sectors. The avoidance of both attackers and unexpected actions is also important.

5.4. Accessibility

Accessibility is performed by improving identification and control, in addition to mitigating life attack, unpredictable behavior and ambiguity. Furthermore, accurate determine the borderline between public and private in IoT is important to improve accessibility. In this way, accessibility depends on the same safeguards discussed in section 4.4, since only designated individuals should be able to access personal data under clearly communicated conditions.

5.5. Interoperability

Interoperability is achieved by reducing the difficulty of identification and by increasing the amount of control that one has over the IoT. This is important because unresolved identification problems and weak control mechanisms are two of the recurring ethical issues identified earlier in Tables 4 and 5, so any gain in interoperability directly reduces their severity. Consequently, treating interoperability as an ethical safeguard,

rather than as a purely technical convenience, helps ensure that improvements in data exchange do not come at the expense of accountability or user oversight.

5.6. Enhanced analysis: property of information in artificial intelligence-internet of things ecosystems

In AI-enabled IoT contexts, where data is not only gathered but also converted, analyzed, and used to provide insights and predictions, the question of information ownership becomes even more complicated. The complex nature of the process of creating data value in smart IoT systems is not well addressed by conventional models of property. Ownership questions therefore extend from the raw data collected by devices to the insights and predictions produced by AI models, and concepts such as mastery over data (Datenherrschaft), discussed in section 4.3, offer a more suitable basis for clarifying who controls each stage of this process.

5.7. Enhanced analysis: accessibility in the artificial intelligence-internet of things era

Access issues in IoT systems are compounded by the incorporation of AI, resulting in new kinds of digital divide and exclusion. As IoT systems become more sophisticated and autonomous, ensuring fair access becomes increasingly critical and challenging. Users who lack the resources or know-how to obtain and control their information, as noted in section 4.4, are at greater risk of being excluded from the benefits of AI-enabled IoT services.

5.8. Enhanced analysis: interoperability as ethical infrastructure

Integrating social and ethical considerations into operational compatibility in IoT systems is just as important as ensuring technological compatibility. Interoperability across IoT systems affects equity in the market, user agency, and energy allocation. When systems cannot exchange and interpret each other's data, users become locked into single providers and lose control over their information, which weakens the accountability discussed in section 5.5.

5.9. Positioning relative to existing ethical frameworks

The proposed ethical framework does not replace current frameworks, but rather builds upon these and its role is best understood in terms of: OECD AI principles, UNESCO recommendation on the ethics of AI, the EU AI Act, and IEEE ethically aligned design. The primary orientation of each instrument is compared to the AI integration gap addressed by the present framework, in this case, a jointly managed AI and IoT system as a whole, in Table 7. It is important to acknowledge that the framework outlined herein is a conceptual synthesis that has not undergone empirical evaluation by experts or Delphi consultation, nor has it been implemented in real-world settings consequently, the effects and results described are hypotheses and may lack validity in practical scenarios.

Table 7. Positioning of the proposed framework relative to existing ethical instruments

Instrument	Primary orientation	Gap addressed by the proposed framework
OECD AI principles	General, technology-neutral principles for trustworthy AI policy.	Ignores device level IoT issues with identification, localization and inventory attacks.
UNESCO AI ethics recommendation	Human-rights-centered values for AI, aimed at member states.	Provides no advice or how-to information on distributed sensor networks and / or sensor issues of accuracy and accessibility that are specific to IoT.
EU AI Act	Legally binding, risk-tiered regulation of AI systems within the EU.	Controls use of AI, without declaring the risk of the actual physical and sensor-based qualities of IoT devices.
IEEE ethically aligned design	Engineering-oriented guidance for autonomous and intelligent systems design.	Rather than on the ethical considerations of IoT multi-stakeholder ecosystems in which the AI system operates, it focuses on the design of the AI system.

6. REAL-WORLD ETHICAL CHALLENGES AND FUTURE DIRECTIONS

Three instances involving real-world ethical challenges are discussed in this section. Figure 5 shows the three main areas of the IoT. This includes ethics in healthcare-remote patient monitoring, smart city surveillance-balancing privacy and security, and industrial IoT-monitoring and autonomous workers.

While this study has made great strides in addressing the ethical challenges of the IoT, many urgent problems remain that require solutions from different fields. Research on the future ethical challenges brought forth by the IoT and AI is depicted in Figure 6. These directions are grouped into priority research areas, emerging research questions, methodological innovations, and implementation challenges, all of which require interdisciplinary collaboration.

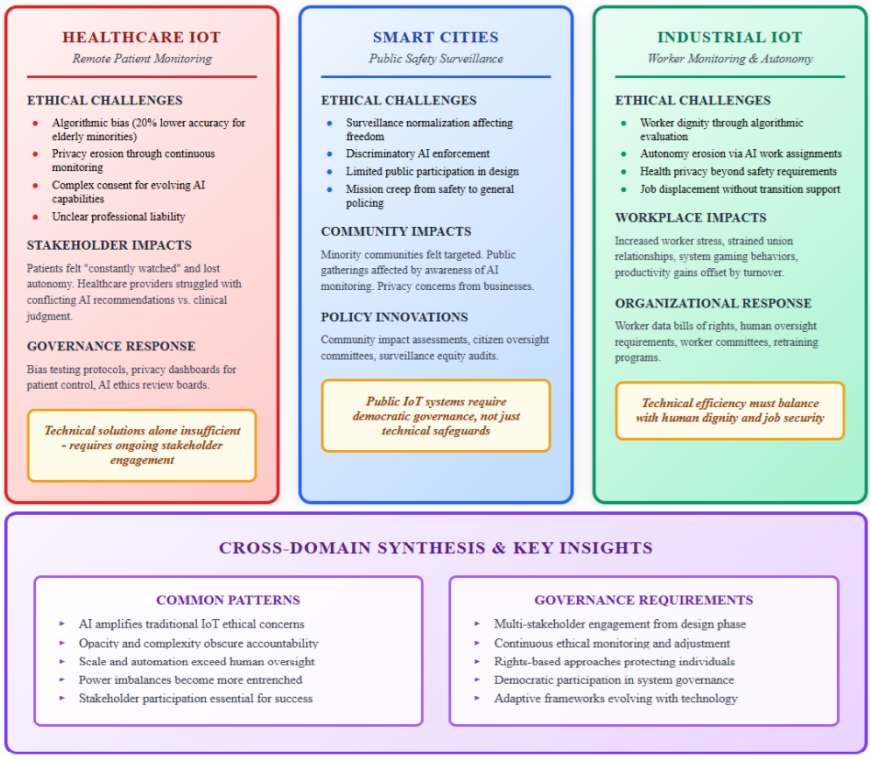

Figure 5. Three case studies: real-world ethical challenges

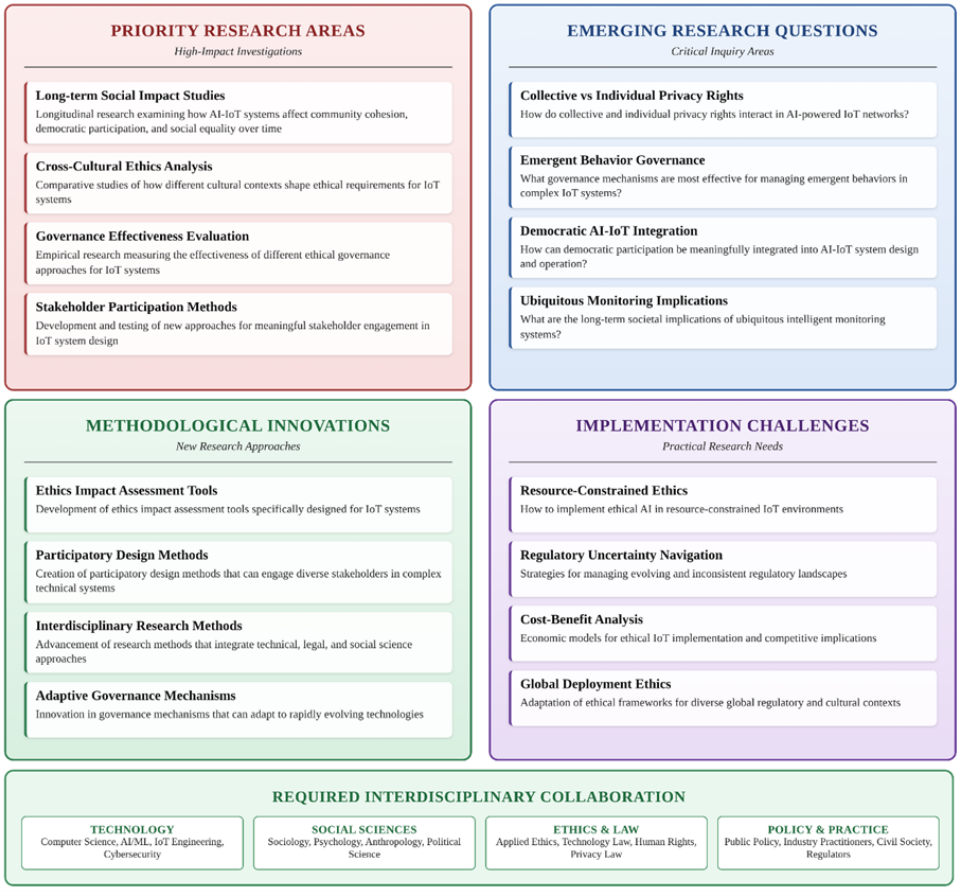

Figure 6. Future research directions in IoT ethics

7. CONCLUSION

This paper discusses the ethical considerations highlighted to assess their impact on IoT applications. This article provides a comprehensive overview of ethical and IoT issues, analyzing the impact of ethical considerations on the IoT domain from the standpoint of IoT challenges. A comprehensive analysis of IoT challenges and ethical considerations is also presented. This review provides a comprehensive analysis of the harmful impact of ethical issues on the IoT area. This research advances the nascent domain of AI ethics by demonstrating that ethical dilemmas in IoT systems necessitate comprehensive strategies that encompass both conventional information ethics and novel algorithmic accountability concerns. The comprehensive paradigm establishes a foundation for future theoretical advancements in the ethics of distributed systems and the design of human-AI interaction, although, as a conceptual synthesis, it still requires empirical and expert validation before its practical effectiveness can be considered demonstrated. Finally, the discourse and suggestions for guiding future research directions are presented to enhance ethical considerations.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Essam S. Hanandeh	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Belal M. Bataineh		✓		✓		✓	✓			✓				
Obaida M. Al-Hazaimeh	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	
Ashraf A. Abu-Ein	✓		✓	✓	✓		✓			✓	✓		✓	
Atef A. Obeidat		✓		✓		✓	✓			✓				

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors confirm that they have no ties or participation in any organization or institution with a financial or non-financial stake in the subject matter or material covered in this manuscript.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] N. Rawindaran, "Legal considerations and ethical challenges of artificial intelligence on internet of things and smart cities," in *Data Protection in a Post-Pandemic Society*, Cham, Switzerland: Springer, 2023, pp. 217–239, doi: 10.1007/978-3-031-34006-2_8.

[2] N. K. Agarwal, G. S. Batra, D. M. Patel, and E. G. AbdAllah, "Impacts of internet of things (IoT) leveraging radio frequency identification (RFID) and internet protocol (IP) on business continuity (BC) and disaster recovery (DR)," in *2024 IEEE Cyber Science and Technology Congress (CyberSciTech)*, Nov. 2024, pp. 512–517, doi: 10.1109/CyberSciTech64112.2024.00091.

[3] H. Bangui, B. Buhnova, and M. Ge, "Social internet of things: ethical AI principles in trust management," *Procedia Computer Science*, vol. 220, pp. 553–560, 2023, doi: 10.1016/j.procs.2023.03.070.

[4] A. Botta, W. D. Donato, V. Persico, and A. Pescapè, "Integration of cloud computing and internet of things: a survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, Mar. 2016, doi: 10.1016/j.future.2015.09.021.

[5] L. Kumar and M. Varshney, "Designing of RFID-based IoT model for automated parking system with mobile communication," *Journal of Computational Analysis and Applications*, vol. 33, no. 5, pp. 1025–1036, 2024.

[6] M. J. Bawaneh, O. M. Al-Hazaimeh, M. M. Al-Nawashi, M. H. Al-Bsool, and E. Hanandah, "Enhanced IoT cybersecurity through machine learning - based penetration testing," *Applied Computer Science*, vol. 21, no. 2, pp. 96–110, 2025, doi: 10.35784/acs_7397.

[7] H. Kuchuk and E. Malokhvii, "Integration of IoT with cloud, fog, and edge computing: a review," *Advanced Information Systems*, vol. 8, no. 2, pp. 65–78, Jun. 2024, doi: 10.20998/2522-9052.2024.2.08.

[8] M. Burhan *et al.*, "A comprehensive survey on the cooperation of fog computing paradigm-based IoT applications: layered architecture, real-time security issues, and solutions," *IEEE Access*, vol. 11, pp. 73303–73329, 2023, doi: 10.1109/ACCESS.2023.3294479.

[9] R. O. Mason, C. P. Collins, and E. L. Cox, "Four ethical issues of the information age," *MIS Quarterly*, vol. 10, no. 1, pp. 5–12, Mar. 1986, doi: 10.2307/248873.

[10] Z. R. Abdulqader, D. M. Abdulqader, O. M. Ahmed, H. R. Ismael, H. S. Ahmed, and L. Haji, "Responsible AI development for sustainable enterprises a review of integrating ethical AI with IoT and enterprise systems," *Journal of Information Technology and Informatics*, vol. 3, no. 2, pp. 129–156, 2024.
[11] P. Onu *et al.*, "Integration of AI and IoT in smart manufacturing: exploring technological, ethical, and legal frontiers," *Procedia Computer Science*, vol. 253, pp. 654–660, 2025, doi: 10.1016/j.procs.2025.01.127.
[12] Prerna and S. Sharma, "From data to decisions: cloud, IoT, and AI integration," in *Integration of Cloud Computing and IoT*, Boca Raton, Florida: Chapman and Hall/CRC, 2024, pp. 461–479, doi: 10.1201/9781032656694-26.
[13] S. G. Tzafestas, "Ethics and law in the internet of things world," *Smart Cities*, vol. 1, no. 1, pp. 98–120, Oct. 2018, doi: 10.3390/smartcities1010006.
[14] E. Nehme, R. E. Sibai, J. B. Abdo, A. R. Taylor, and J. Demerjian, "Converged AI, IoT, and blockchain technologies: a conceptual ethics framework," *AI and Ethics*, vol. 2, no. 1, pp. 129–143, Feb. 2022, doi: 10.1007/s43681-021-00079-8.
[15] N. Y. Fares and M. Jammal, "AI-driven IoT systems and corresponding ethical issues," in *AI and Society*, Boca Raton, Florida: Chapman and Hall/CRC, 2022, pp. 233–248, doi: 10.1201/9781003261247-17.
[16] A. Wakili and S. Bakkali, "Ethical considerations in the integration of internet of things (IoT) technologies within digital health: a comprehensive framework for evaluation," in *International Conference on Advanced Intelligent Systems for Sustainable Development*, 2024, pp. 219–231, doi: 10.1007/978-3-031-52385-4_21.
[17] W. Fei, H. Ohno, and S. Sampalli, "A systematic review of IoT security: research potential, challenges, and future directions," *ACM Computing Surveys*, vol. 56, no. 5, pp. 1–40, May 2024, doi: 10.1145/3625094.
[18] K. A. Vågen, "Internet of things—public-private partnerships for innovation and digitalization in smart municipalities," M.S. Thesis, Norwegian University of Science and Technology, Trondheim, Norwegia, 2020. [Online]. Available: https://hdl.handle.net/11250/2777022
[19] A.-S. Rahman, M. S. T. Anubhove, M. Zeyad, S. M. M. Ahmed, and M. A. A. Walid, "Study of city crimes with smart solutions integrating into smart cities, internet of things (IoT), and cybersecurity systems," in *2024 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC)*, 2024, pp. 1–6, doi: 10.1109/ASSIC60049.2024.10508004.
[20] M. Franceschetti, D. M. Buchegger, R. Seiger, and B. Weber, "Toward IoT-based process analytics: extending event knowledge graphs with ambiguity," in *Enterprise, Business-Process and Information Systems Modeling*, Cham, Switzerland: Springer, 2025, pp. 176–192, doi: 10.1007/978-3-031-95397-2_11.
[21] F. Allhoff and A. Henschke, "The internet of things: foundational ethical issues," *Internet of Things*, vol. 1–2, pp. 55–66, Sep. 2018, doi: 10.1016/j.iot.2018.08.005.
[22] D. Popescul and M. Georgescu, "Internet of things – some ethical issues," *The USV Annals of Economics and Public Administration*, vol. 13, no. 2(18), pp. 210–216, 2013.
[23] European Union, "Regulation (EU) 2024/1689 of the European parliament and of the council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending regulations (EC)," *wipo.int*, 2024. Accessed: Oct. 13, 2026. [Online]. Available: https://www.wipo.int/wipolex/en/legislation/details/24023
[24] K. Shahriari and M. Shahriari, "Ethically aligned design: a vision for prioritizing human wellbeing with artificial intelligence and autonomous systems," in *2017 IEEE Canada International Humanitarian Technology Conference (IHTC)*, Jul. 2017, pp. 197–201, doi: 10.1109/IHTC.2017.8058187.
[25] J. Borenstein and A. Howard, "Emerging challenges in AI and the need for AI ethics education," *AI and Ethics*, vol. 1, no. 1, pp. 61–65, Feb. 2021, doi: 10.1007/s43681-020-00002-7.
[26] UNESCO, *Recommendation on the ethics of artificial intelligence*. Paris, France: United Nations Educational, Scientific and Cultural Organization, 2022.
[27] OECD, *Recommendation of the council on artificial intelligence*. Paris, France: OECD Legal Instruments, 2019.
[28] K. Khadka, "Privacy challenges in IoT and cyber-physical systems: trends, threats, and mitigation strategies," in *Mobile Web and Intelligent Information Systems*, Cham, Switzerland: Springer, 2026, pp. 159–172, doi: 10.1007/978-3-032-02060-4_11.
[29] A. F. Westin, "Privacy and freedom," *Washington and Lee Law Review*, vol. 25, no. 1, 1968.
[30] Y. W. Cheng and A. Bilal, "Regulatory data privacy concerns in proliferating IoT era of telecommunication data monetisation: a systematic literature review," *Computing*, vol. 107, no. 9, Sep. 2025, doi: 10.1007/s00607-025-01542-8.
[31] S. Rizvi, R. Pipetti, N. McIntyre, J. Todd, and I. Williams, "Threat model for securing internet of things (IoT) network at device-level," *Internet of Things*, vol. 11, Sep. 2020, doi: 10.1016/j.iot.2020.100240.
[32] G. Pettorru, V. Pilloni, and M. Martalò, "Trustworthy localization in IoT networks: a survey of localization techniques, threats, and mitigation," *Sensors*, vol. 24, no. 7, Mar. 2024, doi: 10.3390/s24072214.
[33] M. Safi, S. Dadkhah, F. Shoeleh, H. Mahdikhani, H. Molyneaux, and A. A. Ghorbani, "A survey on IoT profiling, fingerprinting, and identification," *ACM Transactions on Internet of Things*, vol. 3, no. 4, pp. 1–39, Nov. 2022, doi: 10.1145/3539736.
[34] D. Vakalis, R. T. Hellwig, M. Schweiker, and S. Gauthier, "Challenges and opportunities of internet-of-things in occupant-centric building operations: towards a life cycle assessment framework," *Current Opinion in Environmental Sustainability*, vol. 65, Dec. 2023, doi: 10.1016/j.cosust.2023.101383.
[35] R. O. Mason, "Applying ethics to information technology issues," *Communications of the ACM*, vol. 38, no. 12, pp. 55–57, Dec. 1995, doi: 10.1145/219663.219681.
[36] K. Kernaghan, "The rights and wrongs of robotics: ethics and robots in public organizations," *Canadian Public Administration*, vol. 57, no. 4, pp. 485–506, Dec. 2014, doi: 10.1111/capa.12093.
[37] R. Y. Wang, "A product perspective on total data quality management," Communications of the ACM, vol. 41, no. 2, pp. 58–65, Feb. 1998, doi: 10.1145/269012.269022.
[38] J. S. S. Koskinen, "The concept of Datenherrschaft of patient information from a Heideggerian perspective," *Journal of Information, Communication and Ethics in Society*, vol. 17, no. 3, pp. 336–353, Aug. 2019, doi: 10.1108/JICES-04-2018-0031.
[39] J. Koskinen, "Lectio praecursoria, Datenherrschaft – an ethically justified solution to the problem of ownership of patient information," *Finnish Journal of eHealth and eWelfare*, vol. 8, no. 2–3, pp. 139–142, 2016.
[40] J. Koskinen, "Datenherrschaft – an ethically justified solution to the problem of ownership of patient information," Ph.D. dissertation, University of Turku, Turku, Finland, 2016.
[41] J. S. S. Koskinen, V. M. A. Kainu, and K. K. Kimppa, "The concept of Datenherrschaft of patient information from a Lockean perspective," *Journal of Information, Communication and Ethics in Society*, vol. 14, no. 1, pp. 70–86, 2016, doi: 10.1108/JICES-06-2014-0029.
[42] R. H. Weber, "Internet of things – new security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, Jan. 2010, doi: 10.1016/j.clsr.2009.11.008.

BIOGRAPHIES OF AUTHORS



Dr. Essam S. Hanandeh received the degree of a Ph.D. in Computer Information Systems in 2008. He joined Zarqa University, Jordan in 2008 up to 2024 then join to Jerash University in 2025. He is an associate professor in the Department of Cybersecurity within the Faculty of Computer Science and Information Technology at Jerash University, Jordan. He has been worked for 15 years as programmer and system analyst. He published over 30 research paper in international journals and conferences. He can be contacted at email: e.hanandeh@jpu.edu.jo.



Dr. Belal M. Bataineh received the B.S. in Computer Science and Information System from Philadelphia University, Amman, Jordan in 1998; M.S. degrees from Red Sea University, Al-Khartoum, Sudan in 2002; and Ph.D. degree in Computer Information System / Artificial intelligence from Arab Academy for Banking and Financial Sciences, Amman, Jordan in 2008. He is an assistant professor at the Department of Computer Science, Faculty of Information Technology, Jadara University, Irbid, Jordan. His current research interests include AI, machine learning, security, image processing, and NLP. He can be contacted at email: b.bataineh@jadara.edu.jo.



Dr. Obaida M. Al-Hazaimeh earned a B.Sc. in Computer Science from Jordan's Applied Science University in 2004 and an M.Sc. in Computer Science from Malaysia's Universiti Sains Malaysia in 2006. In 2010, he earned a Ph.D. in Network Security (Cryptography) from Malaysia. He is a full professor at Department of Computer Science and Information Technology, Al-Balqa Applied University. Cryptology, image processing, machine learning, and chaos theory are among his primary research interests. He has published around 61 papers in international refereed publications as an author or co-author. He can be contacted at email: dr_obaida@bau.edu.jo.



Dr. Ashraf A. Abu-Ein is a full professor in the Department of Electrical Engineering, Al-Balqa Applied University. He has completed his Ph.D. at National Technical University of Ukraine, Computer Engineering “computers, computing systems, and networks”, 2007. Now, he is a full professor at Al-Balqa Applied University, Al-Huson University College, Jordan. Network and wireless network are among his primary research interests. He has published around 31 papers in international refereed publications as an author or co-author. He can be contacted at email: ashraf.abuain@bau.edu.jo.



Atef A. Obeidat received the B.Sc. degree in Computer Science from Yarmouk University, Irbid, Jordan, in 1991; the M.Sc. degree in Computer Science from the University of Jordan, Amman, Jordan, in 2001; and the Ph.D. degree in Computer Science from Novosibirsk State Technical University, Novosibirsk, Russia, in 2009. He has been an associate professor of Computer Science at Al-Balqa Applied University since 2018. He is currently a member of the Department of Information Technology, Al-Huson University College, Al-Balqa Applied University, Al-Salt, Jordan. He has authored or coauthored more than 40 refereed journal and conference papers. His research interests include the applications of AI and the security of computers and networks. He can be contacted at email: Dr.atefob@bau.edu.jo.