# Privacy and Trust in IoT Ecosystems with Big Data: A Survey of Perspectives and Challenges

Tuan Minh Nguyen*, and Xuan-Son Vu†‡#

Devr Inc., Florida, USA*‡
Department of Computing Science, Umeå University, Sweden‡
Email: *t.nguyen@devr.com, †s.vu@devr.com, †sonvx@cs.umu.se

***Abstract*—The Internet of Things (IoT) has become a vital part of our daily lives, enabling interconnectedness between various devices and systems. As the amount of data generated by IoT devices and systems continues to increase immensely, privacy and security concerns have emerged as a significant challenge for researchers and enterprises. Although we are aware of how much data IoT devices will generate per day, there is a lack of knowledge of how the collected data will be used. The privacy risks associated with data collection raise individual concerns in the IoT ecosystem. For instance, when sensitive personal information is exposed due to weak security practices, it can result in identity theft, financial fraud, or other types of cybercrime. The misuse of IoT devices also puts someone susceptible to physical risks, such as a compromised medical device leading to health complications. In this paper, we introduce the definition of the next-gen IoT Ecosystem and its relations to Big Data as well as investigate privacy and security risks associated with IoT ecosystems, identify the gaps in current privacy and security practices, and present technical solutions to tackle these problems. We aim to identify challenges and raise awareness about developing secure and privacy-preserving IoT systems in the era of Big Data.**

***Index Terms*—IoT, big data, privacy-enhanced technologies**

## I. Introduction

The rise of IoT has led to the emergence of new applications and services, ranging from smart devices to a network of connected autonomous vehicles, from smart cities to industrial automation. These systems rely heavily on the ability to collect and analyze data from a large number of devices, generating massive amounts of data in the process [27]. The challenge now is to develop systems that can manage, process, and extract meaningful insights from this data while ensuring privacy, security, and compliance with regulations.

A prominent risk associated with the collection and use of data in IoT ecosystems is the potential for privacy violations. The data collected by IoT devices can reveal sensitive information about individuals, including their location, activities, and preferences [16]. This information can be used to build detailed profiles of individuals, which can be exploited for commercial or malicious purposes [20]. In addition, the interconnected nature of IoT systems can create new vulnerabilities and attack surfaces, increasing the risk of cyber-attacks and data breaches [42, 32, 21, 30, 13, 2].

# Corresponding author.

To address these risks, regulations and standards have been developed to govern the collection, use, and sharing of data in IoT ecosystems. For example, the General Data Protection Regulation (GDPR) in Europe requires companies to obtain explicit consent from individuals before collecting and using their data, and to provide them with the right to access, correct, and delete their data [31, 40]. Similar regulations have been implemented in other countries and regions, including the United States (HIPAA, CCPA) and Asia (such as Protection of Personal Data (Decree) or Decree No. 13/2023/ND of Vietnam[1]). Despite these regulations, there are still significant challenges in ensuring privacy and security in IoT ecosystems. For example, Douzis et al. [15] stated that the sheer volume and variety of data generated by IoT devices can make it difficult to identify and manage sensitive information. In addition, according to Koeh et al. [23], the lack of standardization and interoperability among IoT devices and platforms can create fragmentation and complexity, making it harder to enforce regulations and best practices. Besides the privacy regulations, the scientific community has proposed several technological solutions such as edge computing, access control, data anonymization, and privacy-enhancing technologies [44, 9, 35, 39]. However, these solutions have their limitations. Edge computing requires careful data management as these data are raw data generated from users or devices, which could potentially lead to data breaches [17]. Access control may not be effective in a heterogeneous network where devices come from different administrative domains [28]. Data anonymization techniques may not be sufficient to protect sensitive data from de-anonymization attacks [28]. Additionally, privacy-enhancing technologies might not provide sufficient data protection and can cause data distortion [36]. Thus, further research is needed to develop more robust and efficient solutions to address privacy and trust issues in the IoT.

### A. Paper Organization

The remainder of this paper is structured as follows: In Section II, we discuss the history and concept of next-gen IoT ecosystems & Big Data and an overview of their communication methods. Section III and IV discuss the privacy and trust

[1]https://vietnamnews.vn/politics-laws/1521355/government-issues-decree-on-personal-data-protection.html

issues of IoT devices in big data era, efforts to tackle these problems, and the drawbacks of these efforts. In Section V, we present the gaps in existing privacy and security practices. The conclusion and future directions are in Section VI.

## II. Background and Related Works

### A. The next-gen IoT ecosystems

The concept of IoT can be traced back to the early days of the internet, where it was initially used for machine-to-machine (M2M) communication. In the early 2000s, the introduction of wireless sensor networks (WSNs) enabled the development of the first IoT applications, such as smart homes and environmental monitoring systems. However, it was not until the late 2000s when the term "Internet of Things" was coined by Kevin Ashton, and the technology began to gain significant attention [31].

The IoT has grown rapidly in recent years, paving the way for next-generation ecosystems. These ecosystems are a complex web of smart devices, services, and platforms that use IoT technologies to improve the lives of individuals, organizations, and society.

Next-gen IoT ecosystems are built upon a foundation of advanced technologies, including edge computing, artificial intelligence, machine learning, and big data analytics. These technologies enable the creation of more sophisticated and intelligent systems that can process and analyze vast amounts of data in real-time, providing insights and actionable information to users and stakeholders.

A key feature of next-gen IoT ecosystems is their ability to seamlessly integrate and interoperate with other systems, devices, and platforms, both within and outside of their respective domains. This is achieved through the use of open standards, protocols, and APIs, which facilitate data sharing, collaboration, and interoperability across different sectors.

Another important aspect of next-gen IoT ecosystems is their focus on privacy, security, and trust. With the proliferation of connected devices and the growing threat of cyber attacks and data breaches, it is critical to ensure that IoT systems are designed and implemented in a way that protects the privacy and security of users' data and devices.

To address these challenges, next-gen IoT ecosystems leverage a range of privacy-enhancing technologies (PETs), such as encryption, access control, and secure communication protocols. Additionally, these ecosystems often incorporate distributed ledger technologies, such as blockchain, which can provide a secure and tamper-proof way of storing and managing IoT data and transactions.

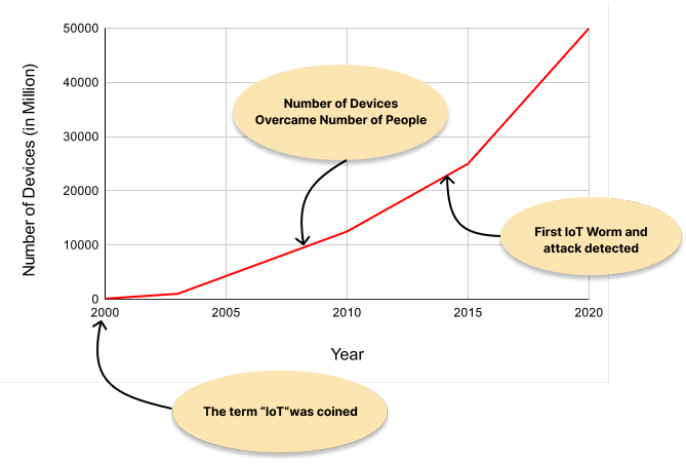


Fig. 1. Timeline of IoTs Evolution [31]

### B. Typical Architecture of IoT Ecosystems

The architecture of an IoT ecosystem refers to the design of the system, including its components, structure, and communication mechanisms. It plays a critical role in the performance and efficiency of the system, especially when it comes to handling large amounts of data generated by IoT devices. The typical components include devices, gateways, cloud platforms, and applications [19] described in Table I and Figure 2.

### C. Relation between next-gen IoT ecosystems and Big Data

The next-generation Internet of Things (IoT) ecosystem is expected to generate massive amounts of data from sensors, mobile devices, and wearables. Big data technologies are needed to process, analyze, and gain insights from IoT data due to its increasing volume, velocity, and variety. Real-time decision-making, predictive analytics, and personalized services can transform businesses, industries, and societies when big data and IoT are combined. [40].

Smart health solutions like remote monitoring and wearable technology are revolutionizing patient care in healthcare thanks to IoT and big data [33]. Smart cities use IoT and big data to improve traffic flow, energy efficiency, and public safety. Smart factories that automate and optimize production processes are being introduced by IoT 4.0, also known as Industry 4.0 [34].

Big data analytics can enable predictive maintenance and real-time monitoring in next-generation IoT ecosystems. Predictive maintenance uses machine learning algorithms to predict equipment failures and avoid costly downtime. Real-time monitoring can alert users to critical events like natural disasters and security breaches.

IoT and big data present many opportunities for innovation and growth, but also pose significant privacy and security risks. IoT devices generate and share massive amounts of personal data, raising concerns about their misuse and exploitation [10].

### D. Related Works

Several works have been proposed in the literature to provide comprehensive reviews of Internet of Things (IoTs) and their privacy & trust related issues. The following related works section highlights the key findings of each journal and their contributions to the field of IoT privacy.

In [11], Curzon et al. review PETs, privacy risks and mitigation strategies in smart city. The authors stress the importance of PETs in smart cities to meet regulatory and

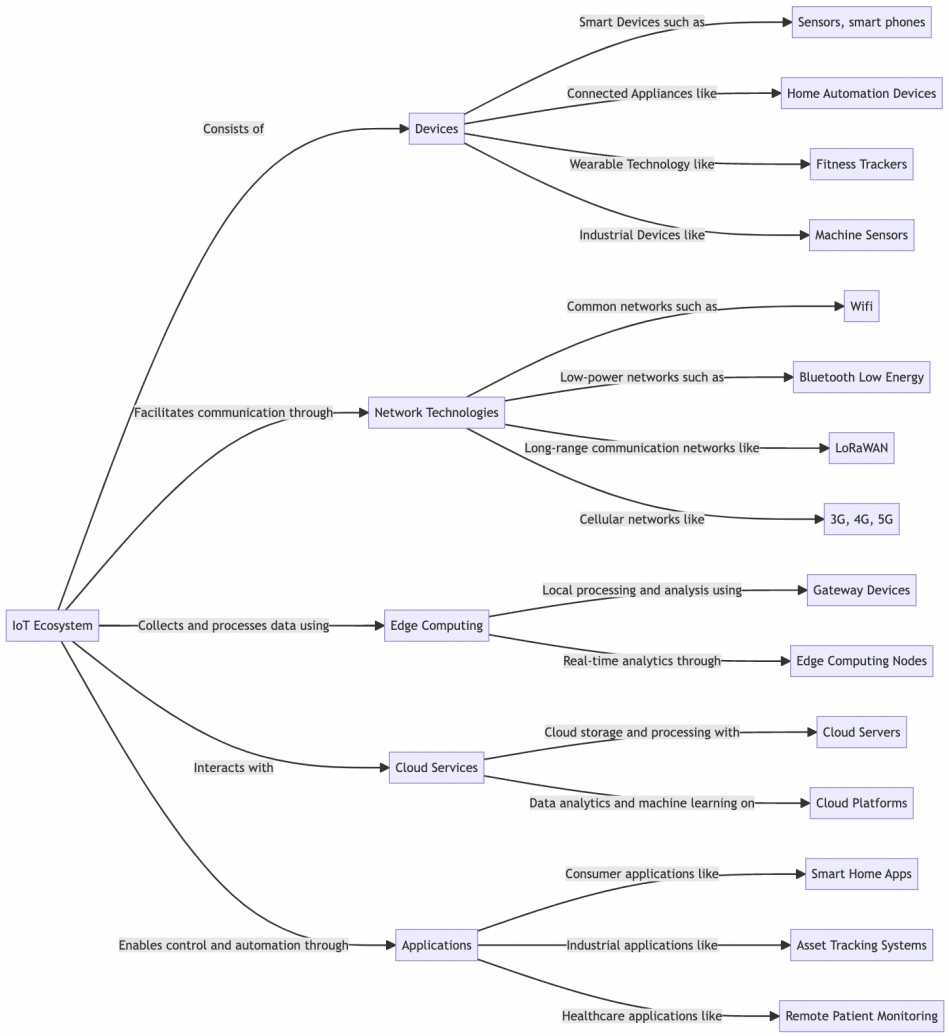


Fig. 2. Illustration of IoT Ecosystem comprises five key elements: (1) Devices, (2) Network Technologies, (3) Edge Computing, (4) Cloud services, and (5) Applications.

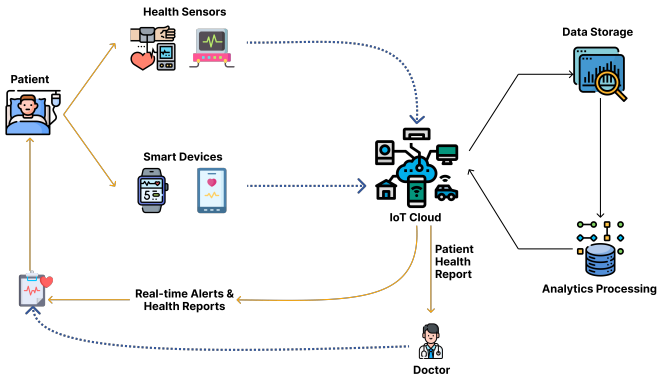


Fig. 3. Example of Smart Health IoT Ecosystem

social expectations. This paper provides a broad overview of privacy-enhancing smart city technologies; however, it lacks sufficient detail on each technology. Furthermore, the authors neglect to assess the effectiveness of each technology.

Cha et al. assess IoT PET development and legal and privacy compliance [8]. The authors categorize 120 primary studies from 2014 to 2017 by privacy protection functions and coverage. They assess PET development in various fields and suggest future research. Since most studies are still in the proof of concept phase, more PET research should focus on holistic privacy preservation.

Li and Palanisamy [25] analyze how legal principles can be supported through a careful implementation of PETs at various layers of a layered IoT architecture model to meet the privacy requirements of individuals interacting with IoT systems. One of the limitations of the work is the lack of broad understanding of the state-of-the-art principles in privacy legislation associated with the design of relevant PETs and how privacy legislation maps to privacy principles which in turn drives the design of necessary PETs to be employed in the IoT architecture stack.

In another study, Wright provides a review of current

TABLE I
OVERVIEW OF IOT ECOSYSTEM ARCHITECTURE COMPONENTS

| Components | Description | Pros | Cons | Adoption Level |
|---|---|---|---|---|
| Devices | IoT devices are the physical objects that collect and transmit data, such as sensors, cameras, and wearables | Cost-effective and scalable; Device-specific customization; local processing and real-time data collection | Devices with limited processing power and storage; Needs frequent maintenance and firmware updates; Interoperability issues between device architectures | High |
| Gateway | Gateways refer to intermediaries between IoT devices and the cloud infrastructure, providing additional processing power and connectivity capabilities | Enables efficient data preprocessing and filtering at the edge; Enhances data security and protocol translation; Supports offline operation and local analytics | Adds complexity and cost to the system; Requires careful management of the gateway infrastructure; Potential single point of failure | Moderate |
| Cloud platforms | The cloud infrastructure provides storage, computing, and analytical capabilities and is responsible for processing and analyzing the data generated by IoT devices | Provides scalable data storage and processing infrastructure, centralized management, and advanced analytics; Allows collaboration and integration with other cloud services | Data transmission through networks; Data privacy and security concerns; Real-time latency issues | High |
| Applications | Applications are the software programs that utilize the data generated by IoT devices and provide value to end-users | Application logic and user interface flexibility; Multiple deployment models and seamless integration; Remotely controls IoT devices | Complexity in developing and maintaining the application infrastructure; Potential scalability issues for high-demand apps; Network connectivity dependence | Varied |

progress for privacy support in IoT Blockchains [44]. The author explores the motivations for IoT architectures to incorporate Blockchain capabilities and address privacy concerns. They analyze currently available technological tools for enhancing and measuring privacy and highlight the need for further enhancement for consumer use. However, the paper focuses specifically on privacy in IoT Blockchains and it does not cover other potential privacy enhancing technologies for IoT.

## III. PRIVACY AND TRUST ISSUES IN BIG DATA ERA

The rapid growth of the IoT ecosystem and the massive amounts of data collected have raised significant concerns about privacy and trust. In this section, we summarize recent emerging privacy and security risks associated with the IoT.

### *A. Privacy risks and concerns for users*

The exponential expansion of the IoT ecosystem and the colossal volumes of data being gathered have sparked considerable concerns regarding privacy and trust. IoT devices, such as smart home devices, wearable devices, and health monitoring devices, collect sensitive information about users, such as their location, health information, and daily routines. This data can be used to identify individuals and reveal their habits, preferences, and behaviors.

Moreover, the potential for data breaches and unauthorized access to personal data is a significant concern. IoT devices are often connected to the internet, making them vulnerable to hacking attempts and cyber-attacks. A data breach can have severe consequences, including identity theft, financial loss, and reputational damage.

Another issue related to privacy concerns is the lack of transparency in data collection and usage. Many users are unaware of the type and amount of data collected by IoT devices and how it is being used [7]. This lack of transparency makes it challenging for users to make informed decisions about their privacy and control the use of their data.

### *B. Security risks and threats to data*

The collection and processing of vast amounts of data by IoT devices creates significant security risks. IoT devices are often resource-constrained and have limited computing power, which makes them vulnerable to attacks such as denial-of-service (DoS) attacks [3], malware infections, or VSI-DDoS attacks [41]. Furthermore, IoT devices are often connected to other devices and networks, making them a potential entry point for attackers to gain access to the entire network. A compromised IoT device can lead to significant security breaches and data loss [24].

Another security issue related to IoT is the lack of standardization in security protocols and technologies. The diversity of IoT devices and their communication protocols makes it challenging to establish a unified security framework that can provide adequate protection against attacks [4].

## IV. CURRENT PRIVACY AND SECURITY PRACTICES IN IOT

The rapidly growing IoT ecosystem has led to the emergence of several privacy and security concerns. In response, many governments and organizations have developed policies and regulations aimed at protecting user data privacy and ensuring secure data transmission.

### *A. Data privacy policies and regulations*

To protect personal data from IoT data misuse, data privacy policies and regulations have been created. The Federal Trade Commission (FTC) in the US has guidelines for IoT device manufacturers to ensure reasonable security and consumer data protection. IoT data is subject to the EU's General

Data Protection Regulation (GDPR). Companies must obtain explicit consent from users before collecting or processing their data, allow users to request access to their data, and delete user data upon request under the GDPR [31, 40].

Japan's Act on the Protection of Personal Information and China's Cybersecurity Law are example of IoT data privacy laws in other countries. In addition to legal frameworks, industry standards like ISO 27001 and the NIST Cybersecurity Framework help companies create effective data privacy policies.

Due to IoT development's rapid pace and threats' constant evolution, these policies and regulations may be insufficient. Researchers argue that regulatory bodies have been slow to adapt to these changes and that more proactive measures are needed to address emerging privacy risks in IoT [37].

### *B. Technological Solutions*

As the IoT continues to grow and evolve, various technological solutions have been proposed to address the privacy and security challenges that arise with the collection and use of large amounts of personal data. This section will discuss some of the key technological solutions that are being developed to address these issues. Table II introduces the discussion, methodology, and key findings of notable IoTs and PETs (Privacy-enhancing Technologies) studies.

*1) Data Anonymization:* Data anonymization protects privacy by modifying or removing personally identifiable information (PII). It involves transforming data so it can no longer be linked to a specific person [12]. Masking, perturbation, and generalization are common data anonymization methods. Masking removes or replaces data identifiers like names, social security numbers, and phone numbers. A pseudonym or random number can replace a name, for instance. Perturbation adds noise or changes data values to make it harder to identify individuals. Generalization reduces data granularity, such as grouping zip codes into regions or ages into age ranges.

*2) Access Control:* IoT security requires access control. It prevents security breaches and ensures system resources and services comply with security policies. Edge computing devices over heterogeneous networks cannot directly apply cloud access control policies. Smart things are expected to share their resources, computational power, and administrative domains. Thus, an access control policy should limit network connection, resource access, and service consumption.

Implementing a role-based access control (RBAC) model can improve access control. User roles with specific privileges and restrictions can be assigned to users or devices based on their needs and functions using this model [12]. IoT devices can be restricted to feeding data collectors only the data needed for a specific service or application, while data collectors can authenticate users and devices as legitimate data owners. An RBAC model makes it easier to enforce access control policies across administrative domains and keep the system secure.

*3) Blockchain:* Blockchain can solve IoT data transparency and user control issues. Blockchain-based decentralized platforms allow users to control data access and use. Blockchain lets users view and track their data usage, increasing transparency and accountability [1].

Blockchain technology can also address data aggregation and sharing privacy concerns. Smart contracts, self-executing contracts with the terms of the agreement between multiple stakeholders written directly into code, can govern data-sharing agreements. Smart contracts can ensure that data is shared only according to pre-agreed terms, can enforce data minimization and pseudonymization, as well as pre-agreed data sharing terms [14].

Decentralized identity solutions are another way Blockchain can improve user control and transparency. Blockchain-based decentralized identity systems give users more control over their personal data and who can access it. This can prevent the unauthorized collection and use of personal data and provide users with greater transparency over who has access to their data and for what purposes [14].

*4) Privacy-enhancing Technologies:* Privacy-enhancing technologies (PETs) ensure fundamental data protection principles are met in a system [8]. These technologies empower individuals, reduce personal data usage, and secure data. Privacy-by-design incorporates a set of principles into system development to address privacy concerns and comply with data protection laws. Federated Learning, Differential Privacy, and Pseudonymization are popular IoT PETs.

- **Federated Learning**: Federated learning allows multiple parties to collaboratively train a machine learning model without sharing data. Send the model to each party and have them train it locally on their data. The parties then send their updated models to a central server, where they are combined to create a more accurate model [43]. The formula for federated learning can be expressed as follows:

$$w^* = \text{argmin}_w \frac{1}{n} \sum_{i=1}^{n} E_{x_i, y_i \sim P_i} \left[ L\left(w, x_i, y_i\right) \right] \quad (1)$$

  Here, $w$ is the model parameters, $n$ is the number of parties, $P_i$ is the probability distribution of the data at party $i$, $L$ is the loss function, and $E$ denotes the expected value. The goal of federated learning is to find the optimal model parameters $w^*$ that minimize the average loss over all parties [26].
- **Differential Privacy**: Differential privacy is a technique that allows data to be analyzed while preserving the privacy of individuals in the dataset. Before processing by algorithms, random noise is added to the data to make it difficult to infer the presence or absence of any particular individual [29]. The formula for differential privacy can be expressed as follows:

$$\Pr\left[M\left(D_1\right) \in S\right] \leq e^{\epsilon} \Pr\left[M\left(D_2\right) \in S\right] + \delta \quad (2)$$

  Here, $M$ is the analysis function, $D_1$ and $D_2$ are two datasets that differ by at most one individual, $S$ is the output space, $\epsilon$ is the privacy budget, and $\delta$ is the probability of the output deviating from the true value

TABLE II
DISCUSSION OF NOTABLE IOTS & PETS RESEARCH

| Research | Year | Methodology | Key Findings |
|---|---|---|---|
| "Securing the Internet of Things: A Standardization Perspective" [23] | 2014 | In-depth review of IoT communication security solutions, focusing on standard CoAP security protocols and standardization efforts to adapt and enhance DTLS for IoT applications | Identifying issues like device boot-strapping, key management, authorization, privacy, and message fragmentation, emphasizing the need for standardized solutions to enable secure and interoperable IoT deployments |
| "Modular and generic IoT management on the cloud" [15] | 2018 | A Future Internet cloud service with a flexible API for managing devices, users, and permissions and on-the-fly data collection from IoT devices | IoT devices generate massive amounts of data, making it difficult to identify and manage sensitive information |
| "Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems" [38] | 2018 | Proposing new protocols for fully homomorphic encryption (FHE) and secure multiparty computation (secure MPC) in wireless mesh Smart Grid Advanced Metering Infrastructure (AMI) networks | The proposed protocols encrypted (FHE) or computed shares on a randomly generated polynomial (secure MPC) smart meter reading data and performed hierarchical aggregation without revealing the actual readings |
| "Multi-Agent Visualization for Explaining Federated Learning" [43] | 2019 | The proposed multi-agent visualization system visualizes Federated Learning's coordination and mechanism | The multi-agent visualization system simplifies Federated Learning by explaining input and output processes |
| "Blockchain and Federated Learning for 5G Beyond" [26] | 2020 | A deep reinforcement learning algorithm optimizes resource sharing in a privacy-preserving scheme for beyond 5G networks by integrating Blockchain with federated learning | Blockchain-federated learning enhances the security and privacy of trained parameters, protecting user data |

by more than a certain amount. The goal of differential privacy is to ensure that the output of the analysis function is indistinguishable whether a particular individual is present in the dataset or not.

- **Pseudonymization**: Pseudonymization is a technique that replaces identifying information with pseudonyms, or fake names, to protect the privacy of individuals in a dataset [6]. The formula for pseudonymization can be expressed as follows:

$$P_i = f(D_i) \tag{3}$$

Here, $D_i$ is the data of individual $i$, $f$ is a pseudonymization function, and $P_i$ is the pseudonymized data. The goal of pseudonymization is to make it difficult to identify individuals in the dataset, while still allowing the data to be analyzed.

## V. GAPS IN EXISTING PRIVACY AND SECURITY PRACTICES

### A. Lack of standardization in IoT security

IoT security standardization is one of the biggest gaps in privacy and security. With so many devices, applications, and communication protocols, it's hard to set security standards for all IoT systems. The lack of standardization in the IoT ecosystem makes it easier for malicious actors to exploit security vulnerabilities.

To address this issue, many organizations have developed their own security guidelines and best practices, such as the IoT Security Foundation, the Industrial Internet Consortium, and the Open Connectivity Foundation [22, 5, 18]. However, these guidelines are not universally adopted, and there is still a need for a more comprehensive and standardized approach to IoT security. Regulators and policymakers who must ensure IoT devices and systems comply with privacy and security regulations also struggle with standardization. Developing effective regulatory frameworks that can keep up with the rapidly changing IoT landscape is difficult without clear and consistent standards [37].

### B. Privacy issues in data sharing and aggregation

Data sharing and aggregation is another IoT privacy and security problem. IoT devices capture massive volumes of user data, raising concerns regarding data sharing and access [7]. Especially when data is transferred between businesses or third-party service providers.

Data aggregation, which combines and analyzes data from many sources, can also compromise privacy. Data points can show an individual's behavior, preferences, and routines even if they are not recognizable [38].

Stronger IoT data collecting, sharing, and use regulations are needed to address these concerns. This includes explicit criteria for organization-to-organization data sharing agreements and technical means to anonymize or de-identify data before sharing or aggregating.

### C. The need for user control over data

The lack of user data control in IoT privacy and security practices is a major issue. Many IoT devices and systems collect data without telling users what it is, how it is used, and who has access to it. User trust is eroded and privacy risks are increased by this lack of transparency [7]. To fix this, IoT data must be more transparent and user-controlled. This includes clear and concise privacy policies, consent management tools, and the ability to delete or modify data.

IoT device and system supply chains must also be more transparent and accountable. This includes clear information about the security and data protection measures in place to protect IoT devices and systems from cyber threats and user privacy.

## VI. CONCLUSION & FUTURE DIRECTIONS

In conclusion, this paper has discussed the emerging privacy and trust issues in the context of IoTs and demonstrated the negative impact that these issues can have on users' privacy and trust. The paper has highlighted the importance

of addressing these issues through technical measures such as privacy-enhancing technologies, access control, and data anonymization. However, the paper also acknowledges that there are gaps in existing privacy and security practices, and that there is a lack of standardization in IoT security. To address these challenges, it is recommended that more research be focused on developing secure and privacy-preserving mechanisms while developing IoT systems and communications. This is particularly important in the context of the big data era, where vast amounts of data are being collected and analyzed. By developing robust privacy and security practices, the IoT industry can increase public acceptance and confidence in using these technologies, leading to the growth and innovation of the IoT ecosystem.

## REFERENCES


[1] Ahmed Alkhateeb et al. "Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review". In: *Sensors* 22.4 (2022). ISSN: 1424-8220. DOI: 10.3390/s22041304.

[2] Raja Waseem Anwar et al. "Security Threats and Challenges to IoT and its Applications: A Review". In: *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*. 2020, pp. 301–305. DOI: 10.1109/FMEC49853.2020.9144832.

[3] Vidal Attias, Luigi Vigneri, and Vassil Dimitrov. "Preventing Denial of Service Attacks in IoT Networks through Verifiable Delay Functions". In: *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*. 2020, pp. 1–6. DOI: 10.1109/GLOBECOM42002.2020.9322260.

[4] Debasis Bandyopadhyay and Jaydip Sen. "Internet of Things: Applications and Challenges in Technology and Standardization". In: *Wireless Personal Communications* 58.1 (May 2011), pp. 49–69. ISSN: 1572-834X. DOI: 10.1007/s11277-011-0288-5.

[5] J. Blackstock. "Standardising a Moving Target: The Development and Evolution of IoT Security Standards". English. In: *IET Conference Proceedings* (Jan. 2018), 24 (9 pp.)–24 (9 pp.)(1).

[6] Luca Bolognini and Camilla Bistolfi. "Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation". In: *Computer Law & Security Review* 33.2 (2017), pp. 171–181. ISSN: 0267-3649. DOI: https://doi.org/10.1016/j.clsr.2016.11.002.

[7] Claude Castelluccia et al. "Enhancing Transparency and Consent in the IoT". In: *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 2018, pp. 116–119. DOI: 10.1109/EuroSPW.2018.00023.

[8] Shi-Cho Cha et al. "Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges". In: *IEEE Internet of Things Journal* PP (Oct. 2018), pp. 1–1. DOI: 10.1109/JIOT.2018.2878658.

[9] Pietro Colombo and Elena Ferrari. "Privacy Aware Access Control for Big Data: A Research Roadmap". In: *Elsevier Big Data Research* 2 (Dec. 2015), pp. 145–154. DOI: 10.1016/j.bdr.2015.08.001.

[10] David De Cremer, Bang Nguyen, and Lyndon Simkin. "The integrity challenge of the Internet-of-Things (IoT): on understanding its dark side". In: *Journal of Marketing Management* 33.1-2 (2017), pp. 145–158. DOI: 10.1080/0267257X.2016.1247517.

[11] James Curzon, Abdulaziz Almehmadi, and Khalil El-Khatib. "A survey of privacy enhancing technologies for smart cities". In: *Pervasive and Mobile Computing* 55 (2019), pp. 76–95. ISSN: 1574-1192. DOI: https://doi.org/10.1016/j.pmcj.2019.03.001.

[12] Giuseppe D'Acquisto et al. "Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics". In: (Dec. 2015). DOI: 10.2824/641480.

[13] Mehiar Dabbagh and Ammar Rayes. "Internet of Things Security and Privacy". In: Oct. 2017, pp. 195–223. ISBN: 978-3-319-44858-9. DOI: 10.1007/978-3-319-44860-2_8.

[14] SINIŠA DOMAZET. "PROTECTION OF PERSONAL DATA ON THE EXAMPLE OF SMART CONTRACTS". In: *The Twelfth International Conference on Business Information Security*, p. 37.

[15] Konstantinos Douzis et al. "Modular and generic IoT management on the cloud". In: *Future Generation Computer Systems* 78 (2018), pp. 369–378. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2016.05.041.

[16] European Commission. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[17] Elahe Fazeldehkordi and Tor-Morten Grønli. "A Survey of Security Architectures for Edge Computing-Based IoT". In: *IoT* 3.3 (2022), pp. 332–365. ISSN: 2624-831X. DOI: 10.3390/iot3030019.

[18] Teklay Gebremichael et al. "Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges". In: *IEEE Access* 8 (2020), pp. 152351–152366. DOI: 10.1109/ACCESS.2020.3016937.

[19] Dimitrios Georgakopoulos et al. "Discovery-Driven Service Oriented IoT Architecture". In: Oct. 2015, pp. 142–149. DOI: 10.1109/CIC.2015.34.

[20] Henrik Twetman, Gundars Bergmanis-Korats. *Data brokers and securities*. 2020. URL: https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf.

[21] Shuodi Hui et al. “Systematically Quantifying IoT Privacy Leakage in Mobile Networks”. In: *IEEE Internet of Things Journal* PP (Nov. 2020), pp. 1–1. DOI: 10.1109/JIOT.2020.3038639.

[22] Vinay M. Igure, Sean A. Laughter, and Ronald D. Williams. “Security issues in SCADA networks”. In: *Computers & Security* 25.7 (2006), pp. 498–506. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2006.03.001.

[23] Sye Loong Keoh, Sandeep Kumar, and Hannes Tschofenig. “Securing the Internet of Things: A Standardization Perspective”. In: *Internet of Things Journal, IEEE* 1 (June 2014), pp. 265–275. DOI: 10.1109/JIOT.2014.2323395.

[24] Kenneth Kimani, Vitalice Oduol, and Kibet Langat. “Cyber security challenges for IoT-based smart grid networks”. In: *International Journal of Critical Infrastructure Protection* 25 (2019), pp. 36–49. ISSN: 1874-5482. DOI: https://doi.org/10.1016/j.ijcip.2019.01.001.

[25] Chao Li and Balaji Palanisamy. “Privacy in Internet of Things: From Principles to Technologies”. In: *IEEE Internet of Things Journal* 6.1 (2019), pp. 488–505. DOI: 10.1109/JIOT.2018.2864168.

[26] Yunlong Lu et al. “Blockchain and Federated Learning for 5G Beyond”. In: *IEEE Network* 35.1 (2021), pp. 219–225. DOI: 10.1109/MNET.011.1900598.

[27] Mehdi Mohammadi et al. “Deep Learning for IoT Big Data and Streaming Analytics: A Survey”. In: *IEEE Communications Surveys & Tutorials* 20.4 (2018), pp. 2923–2960. DOI: 10.1109/COMST.2018.2844341.

[28] R. Narmadha. “Heterogeneous network security management”. In: *International Journal of Intelligent Enterprise* 6 (Jan. 2019), p. 32. DOI: 10.1504/IJIE.2019.10021616.

[29] Thai-Hung Nguyen et al. “Emerging Privacy and Trust Issues for Autonomous Vehicle Systems”. In: Jan. 2022, pp. 52–57. DOI: 10.1109/ICOIN53446.2022.9687196.

[30] Mookyu Park, Haengrok Oh, and Kyungho Lee. “Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective”. In: *Sensors* 19 (May 2019), p. 2148. DOI: 10.3390/s19092148.

[31] Francesco Restuccia, Salvatore D’Oro, and Tommaso Melodia. “Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking”. In: *IEEE Internet of Things Journal* 5.6 (2018), pp. 4829–4842. DOI: 10.1109/JIOT.2018.2846040.

[32] Muhammad Shafiq et al. “The Rise of “Internet of Things” Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks”. In: *Wireless Communications and Mobile Computing* 2022 (Aug. 2022), p. 12. DOI: 10.1155/2022/8669348.

[33] Yasmeen Shaikh, V. K. Parvati, and S. R. Biradar. “Survey of Smart Healthcare Systems using Internet of Things (IoT) : (Invited Paper)”. In: *2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)*. 2018, pp. 508–513. DOI: 10.1109/IC3IoT.2018.8668128.

[34] F. Shrouf, J. Ordieres, and G. Miragliotta. “Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm”. In: *2014 IEEE International Conference on Industrial Engineering and Engineering Management*. 2014, pp. 697–701. DOI: 10.1109/IEEM.2014.7058728.

[35] Baobao Song et al. *Digital Privacy Under Attack: Challenges and Enablers*. 2023. arXiv: 2302.09258.

[36] William Stadler. “Risks of Privacy-Enhancing Technologies: Complexity and Implications of Differential Privacy in the Context of Cybercrime”. In: *Security and Privacy From a Legal, Ethical, and Technical Perspective*. Ed. by Christos Kalloniatis and Carlos Travieso-Gonzalez. Rijeka: IntechOpen, 2020. Chap. 7. DOI: 10.5772/intechopen.92752.

[37] Hui Suo et al. “Security in the Internet of Things: A Review”. In: *2012 International Conference on Computer Science and Electronics Engineering*. Vol. 3. 2012, pp. 648–651. DOI: 10.1109/ICCSEE.2012.373.

[38] Samet Tonyali et al. “Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems”. In: *Future Generation Computer Systems* 78 (2018), pp. 547–557. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2017.04.031.

[39] Nguyen Truong et al. “Privacy Preservation in Federated Learning: An insightful survey from the GDPR Perspective”. In: *Computers & Security* 110 (July 2021), p. 102402. DOI: 10.1016/j.cose.2021.102402.

[40] Xuan-Son Vu. “Privacy-guardian: the vital need in machine learning with big data”. PhD thesis. Umeå University, 2020.

[41] Xuan-Son Vu, Maode Ma, and Monowar Bhuyan. “MetaVSID: A Robust Meta-Reinforced Learning Approach for VSI-DDoS Detection on the Edge”. In: *IEEE Transactions on Network and Service Management* (2022).

[42] Rolf Weber. “Internet of Things – New security and privacy challenges”. In: *Computer Law & Security Review* 26 (Jan. 2010), pp. 23–30. DOI: 10.1016/j.clsr.2009.11.008.

[43] Xiguang Wei et al. “Multi-Agent Visualization for Explaining Federated Learning”. In: *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence, IJCAI-19*. July 2019, pp. 6572–6574.

[44] Steven A. Wright. “Privacy in IoT Blockchains: with Big Data comes Big Responsibility”. In: *2019 IEEE International Conference on Big Data (Big Data)*. 2019, pp. 5282–5291. DOI: 10.1109/BigData47090.2019.9006341.