Advances in Secure IoT Data Sharing

Phu Nguyen, Arda Goknil, Gencer Erdogan, Shukun Tokas, Nicolas Ferry, Thanh Thao Thi Tran

Foundations and Trends® in Privacy and Security

Advances in Secure IoT Data Sharing

Suggested Citation: Phu Nguyen, Arda Goknil, Gencer Erdogan, Shukun Tokas, Nicolas Ferry and Thanh Thao Thi Tran (2024), "Advances in Secure IoT Data Sharing", Foundations and Trends® in Privacy and Security: Vol. 7, No. 1, pp 1–73. DOI: 10.1561/3300000042.

Phu Nguyen
SINTEF
phu.nguyen@sintef.no

Arda Goknil
SINTEF
arda.goknil@sintef.no

Gencer Erdogan
SINTEF
gencer.erdogan@sintef.no

Shukun Tokas
SINTEF
shukun.tokas@sintef.no

Nicolas Ferry
Université Côte d'Azur
Nicolas.FERRY@univ-cotedazur.fr

Thanh Thao Thi Tran
DnB
thaotran98@hotmail.com

now
the essence of knowledge
Boston — Delft

Contents

Advances in Secure IoT Data Sharing

Phu Nguyen[1], Arda Goknil[1], Gencer Erdogan[1], Shukun Tokas[1], Nicolas Ferry[2] and Thanh Thao Thi Tran[3]

[1]*SINTEF, Norway; phu.nguyen@sintef.no, arda.goknil@sintef.no, gencer.erdogan@sintef.no, shukun.tokas@sintef.no*
[2]*I3S/INRIA Kairos, Université Côte d'Azur, France; Nicolas.FERRY@univ-cotedazur.fr*
[3]*DnB, Norway; thaotran98@hotmail.com*

ABSTRACT

The proliferation of IoT devices on the Internet is currently in the billions, and projections anticipate that there will be 50 billion connected IoT devices in the IoT market by 2030. This rapid expansion will result in a substantial increase in data, which includes personal data, generated by these IoT devices. It is estimated that the data volume will reach 73.1 zettabytes by 2025. To fully realize the substantial benefits of the IoT, it is imperative to facilitate the responsible utilization and sharing of this data among various stakeholders. However, it is crucial to establish robust security and trust mechanisms to ensure data integrity and privacy during data sharing. Our objective is to summarize and assess the research efforts that address secure IoT data sharing. We systematically review the state-of-the-art techniques ensuring and preserving security in the IoT data-sharing environment through a systematic literature review (SLR) study. We pose three research questions, define selection

Phu Nguyen, Arda Goknil, Gencer Erdogan, Shukun Tokas, Nicolas Ferry and Thanh Thao Thi Tran (2024), "Advances in Secure IoT Data Sharing", Foundations and Trends® in Privacy and Security: Vol. 7, No. 1, pp 1–73. DOI: 10.1561/3300000042.

and exclusion criteria for primary studies, and extract and synthesize data from these studies to answer our research questions. Our SLR results can help readers to obtain (i) an overview of existing secure IoT data-sharing approaches and related issues, (ii) a deep-dive into Edge-focused secure IoT data sharing solutions, and (iii) research directions that require attention from the research community for follow-up work.

1

Introduction

In recent years, the Internet of Things (IoT) has achieved pervasive ubiquity, driven by its capacity to interconnect commonplace items such as automobiles, household appliances, and infant surveillance devices to the Internet, facilitating seamless communication across processes, individuals, and objects. At present, the global landscape boasts billions of IoT devices in active connection, and it is foreseen that the IoT market will witness the integration of 30 billion connected devices by 2023, as anticipated by Cisco (Grossetete, 2018). IoT technology empowers the creation of intelligent, interoperable entities encompassing both the digital and physical realms, individuals and services, and thereby giving rise to diverse ecosystems primed for secure cross-domain interactions.

Nonetheless, as the IoT ecosystem undergoes continued expansion and diversification, it renders the vast data reservoir vulnerable to various security and privacy risks. The inherently interconnected nature of IoT networks, coupled with the multifaceted spectrum of stakeholders engaged, has precipitated an urgent imperative for establishing resilient data management and governance protocols. The assurance of secure sharing and judicious utilization of data generated within the IoT framework assumes paramount significance in upholding the sanctity of

sensitive information, encompassing aspects of confidentiality, integrity, and accessibility.

The management and governance of data sharing securely within the context of the Internet of Things (IoT) present challenges that are multifaceted. These challenges lie first in the intrinsic complexity and multifaceted nature of IoT systems. On the one hand, IoT systems typically perform distributed sensing, actuating, and processing across multiple layers composed of Thing, Edge, and Cloud resources. Things and Edge devices are operating in the midst of the physical world to sense and collect environmental data, including sensitive data. This creates novel opportunities for bad actors as (i) the devices can be physically accessible and (ii) it is not possible for security experts to anticipate all the possible environmental situations under which the system will operate. On the other hand, these challenges extend beyond the technical facets of data security, encompassing a rich tapestry of regulatory, ethical, and societal dimensions pertinent to data handling. The data generated by IoT systems may traverse organizational demarcations, transcend international borders, and become ensnared in a complex web of legal and compliance prerequisites. Furthermore, IoT ecosystems frequently comprise several stakeholders, ranging from device manufacturers to end-users, each carrying their unique entitlements and obligations about data.

Although several surveys study and classify research on secure IoT data sharing, they do not provide a detailed account and unified analysis of existing solutions (i.e., secure IoT data sharing techniques) for secure IoT data sharing research, the security and trust aspects of these solutions, and their limitations and potential future work (open issues to be further investigated). Few existing studies (Lo *et al.*, 2019; Al-Ruithe *et al.*, 2019; De Prieëlle *et al.*, 2020) have examined related topics of secure IoT data sharing such as data governance and blockchain solutions, but none has done a Systematic Literature Review (SLR) on secure IoT data sharing. We answer three main research questions (also detailed in sub research questions) to address the research on secure IoT data sharing for theoretical and practical implications.

- **RQ1:** *What is the current landscape of solutions for secure IoT data sharing in general?*

- **RQ2:** *What are the specific technical aspects of Edge-focused online IoT data sharing approaches?*
- **RQ3:** *What are the current limitations of the IoT data sharing, and what are the open issues to be further investigated?*

We follow a typical four-step SLR process (Kitchenham and Charters, 2007): (i) the definition of research questions, (ii) a search strategy including the selection of online repositories and search strings, (iii) inclusion and exclusion criteria, and (iv) a data synthesis and extraction procedure. This work is an extension of Tran *et al.* (2023). We conducted an extensive snowballing process (Wohlin, 2014) to enrich and update the list of primary studies. Moreover, with the importance of Edge computing, we deep-dived into the primary studies that have Edge-focused IoT data sharing approaches.

We analyzed the primary studies using our taxonomy of IoT data sharing to provide the answers to our three research questions. Following a top-down approach, we present first a high-level summary of our results. Then, we discuss in more detail the primary studies that have Edge-focused IoT data sharing approaches. Researchers can use this summary and the taxonomy to classify and compare future secure IoT data sharing studies.

The remainder of this monograph is structured as follows. We provide some background concepts in Section 2. Then, Section 3 gives the details of our approach and Section 4 shows our taxonomy for extracting data to answer our RQs. Next, we present the results of our SLR in Section 5. In Section 6, we discuss some possible threats to validity. We compare our study with related work in Section 7 and give our conclusions in Section 8.

2

Background

In this section, we elaborate on the most essential terms to give a better understanding of the topic. First, we elaborate more on the background concept of IoT data sharing in Section 2.1. Then, we give more details on the relevant concepts such as data management Section 2.2, data governance Section 2.3, relevant standardization Section 2.4, and data quality Section 2.5.

2.1 IoT Data Sharing

IoT data sharing is crucial, particularly in inter-business contexts, involving data exchange among various entities and devices. It often employs specialized communication protocols tailored for IoT environments, albeit potentially with reduced security measures. Unlike conventional centralized systems, IoT devices are field-accessible, broadening the attack surface compared to Cloud-based solutions. Furthermore, due to their limited capabilities, security measures on IoT devices must be efficient, ensuring robust protection with minimal footprint. The rise of Edge and Fog computing has further transformed data sharing dynamics, with IoT data now distributed, processed, and stored across the Edge-Cloud continuum, encompassing edge devices like routers and base stations alongside traditional Cloud resources.

Data sharing within IoT systems presents unique challenges, primarily due to the reliance on IoT-specific protocols optimized for constrained environments characterized by limited energy, computing, and bandwidth resources. Consequently, these protocols often compromise security measures to accommodate these limitations. Additionally, IoT systems frequently involve heterogeneous devices from various manufacturers, leading to interoperability issues and potential vulnerabilities arising from inconsistent security implementations across devices. Furthermore, the distributed nature of IoT networks introduces complexities in data management and access control, as data may traverse diverse network nodes and endpoints, increasing the likelihood of unauthorized access and data breaches. Moreover, the dynamic and pervasive nature of IoT deployments introduces challenges in maintaining data integrity and confidentiality, particularly in scenarios where data is generated, processed, and transmitted in real-time across diverse environments. These complexities underscore the need for robust security strategies tailored to the unique characteristics and challenges of IoT data sharing.

For a more structured categorization of the main aspects of IoT data sharing, please see Section 4.

2.2 Data Management

The proliferation of IoT devices is rapidly increasing, leading to a significant surge in data generation. This influx of data necessitates effective solutions for managing large-scale IoT data efficiently. Data management within the IoT ecosystem plays a critical role in ensuring efficient data handling while concurrently maintaining the connectivity and security of smart devices.

Data management in the realm of IoT entails overseeing the storage, retrieval, updating, and maintenance of data records. As stated in the definition of data management by Oracle (2024), data management involves securely, efficiently, and cost-effectively collecting, retaining, and utilizing data. The primary objective of data management is to optimize organizational outcomes by guiding decisions and actions within the framework of policies and regulations.

Data management within the IoT presents several challenges stemming from the unique characteristics of IoT environments. One significant challenge is the sheer volume and velocity of data generated by a vast array of interconnected devices. IoT ecosystems produce massive amounts of real-time data, necessitating efficient storage, processing, and analysis mechanisms. Additionally, the heterogeneity of IoT devices and protocols complicates data interoperability and integration efforts, leading to siloed data and fragmented insights. Security is another critical concern, as IoT deployments are vulnerable to cyber threats due to the distributed nature of devices and limited security capabilities. Data confidentiality, integrity, and availability across diverse IoT networks requires robust encryption, authentication, and access control measures. Furthermore, scalability and reliability are essential considerations in IoT data management, as the expansion of IoT deployments introduces scalability bottlenecks and reliability issues. Addressing these challenges requires comprehensive strategies encompassing data governance, privacy protection, data lifecycle management, and interoperability standards tailored to the unique requirements of IoT ecosystems.

2.3 Data Governance

Data governance encompasses the delineation of roles, accountability structures, and decision-making authority within an organization. In the context of IoT data sharing, it dictates the protocols for data processing, delineates data ownership, and stipulates access permissions under specific conditions (Seiner, 2024). The overarching goal of data governance is to ensure the secure, privacy-compliant, and quality-driven generation and utilization of IoT data. Given the extensive data exchange across diverse ecosystem participants, robust data governance frameworks are indispensable to uphold security, privacy, and data integrity standards.

Data governance in IoT systems encompasses various factors and dimensions that require attention. Data definitions entail specifying which data is to be collected and adhering to established standards. Data production governs the collection and transmission processes. Data usage determines authorized users, sharing permissions, and intended

utilization methods. By establishing rules for these factors and adhering to relevant policies, regulations, and laws, IoT governance can enhance data protection, particularly in terms of privacy and security.

2.4 Standardized Data Sharing

2.4.1 International Data Spaces Association (IDSA)

A relevant association in the context of the data exchange domain is IDSA, with a vision of innovating the future of data exchange in Europe and beyond by creating the important technical standards (IDSA, 2024b). Data spaces are key to the association's vision and should be grounded in European values of trust and self-determination of data usage by the providers of the data. With this facilitation, IDSA guarantees data sovereignty for data owners. The association has developed a broad, open standard for data marketplaces and platforms based on European values. The values are elaborated as follows (IDSA, 2024a):

- Data privacy and security that's the most trusted in the world.
- Equal opportunities through a federated design (so there's a level playing field in data exchange for small and medium-sized enterprises).
- Assurance of data sovereignty for the creator of the data and trust among participants.

2.4.2 GAIA-X

GATA-X is often associated with IDSA. As elaborated in the section above, data spaces are key in IDSA. However, it takes more than a cloud to turn data into something economic. Therefore, there is a need to address the ability to share data in ways that can be controlled by an organization, company, or individual. We therefore introduce you to GAIA-X. GAIA-X is an infrastructure and data ecosystem with guiding principles based on European standards and values. These values can

include openness, transparency, trust, sovereignty, data privacy protection, and usability. GAIA-X has the objective of creating a transparent and open ecosystem where data can be collected, made available, and shared both in a self-determined manner and in a trusted environment (Gaia-X, 2024).

2.5 Data Quality

Ensuring data quality is paramount in IoT data sharing, as the reliability and accuracy of shared data directly impact decision-making processes and the effectiveness of IoT applications. Several key considerations influence data quality within the context of IoT data sharing:

- *Accuracy:* IoT-generated data must accurately reflect the real-world phenomena it represents. Any inaccuracies or errors in data collection, transmission, or processing can lead to flawed insights and decisions.
- *Completeness:* Complete data sets contain all relevant information necessary for analysis and decision-making. Incomplete data may result from sensor failures, communication errors, or missing data points, compromising the integrity of analyses.
- *Consistency:* Consistent data ensures uniformity and coherence across different sources, devices, and time periods. Inconsistent data formats, units of measurement, or naming conventions can hinder data integration and analysis efforts.
- *Timeliness:* Timely access to data is crucial for real-time decision-making and responsiveness in IoT applications. Delays in data transmission or processing may render data obsolete or less actionable.
- *Relevance:* Shared IoT data should be relevant to the intended use case or application. Irrelevant or extraneous data can introduce noise and detract from the effectiveness of analyses and insights.
- *Security and Privacy:* Data shared within IoT ecosystems must be adequately protected against unauthorized access, manipulation,

or disclosure. Robust security measures and privacy-enhancing technologies safeguard sensitive data from malicious actors.

Addressing these aspects of data quality requires comprehensive data governance frameworks, standardized data management practices, and robust quality assurance processes (Goknil *et al.*, 2023). By prioritizing data quality in IoT data-sharing initiatives, organizations can enhance the reliability and trustworthiness of shared data for informed decision-making and operational efficiency.

3

Review Process

This section elaborates on the steps in our review process, which align with established guidelines (Kitchenham and Charters, 2007; Petersen *et al.*, 2015; Wohlin, 2014), encompassing: (a) formulation of Research Questions (RQs), (b) development of a search strategy involving the selection of repositories and formulation of search strings, and (c) the process of study selection based on predefined inclusion and exclusion criteria.

3.1 Research Questions

This SLR answers the three RQs presented in Section 1. We extend them with sub-questions.

RQ1 includes three sub-RQs.

- **RQ1.1 -** *What is the current trend of publications on secure IoT data sharing?* Addressing this question enables us to discern the chronological emergence of secure data sharing as a subject of significance
- **RQ1.2 -** *What are the reported application domains of IoT data sharing?* Responding to this question affords us the opportunity

to pinpoint the specific domains of interest within the ecosystem of IoT data sharing.

- **RQ1.3 -** *What are the purposes and benefits of data sharing considered in the primary studies?* Given our interest in domain identification, we are equally keen on understanding the underlying motivations driving different domains' desires to engage in data sharing, along with the potential benefits that may ensue from such collaborations.

RQ2: What are the specific technical aspects of Edge-focused online IoT data sharing approaches? There are three sub-questions of RQ2.

- **RQ2.1 -** *What are the security aspects covered by the Edge-focused IoT data sharing approaches today in different domains?* Addressing this question would furnish an overview of the prevailing security concerns considered by the existing Edge-focused IoT data sharing approaches. This will help us to understand how the security principles are covered per domain.

- **RQ2.2 -** *What and how are the techniques and approaches used to preserve trust and privacy in Edge-focused IoT data sharing?* Upon identifying the security principles per domain within our defined scope, we proceed to extract insights on how various contributions endeavor to preserve trust and privacy.

- **RQ2.3 -** *In which IoT layers data is being shared, managed and governed, and how do standards support Edge-focused secure data sharing?* In answering this question, we use the IoT World Forum Reference Architecture to locate from which IoT layers data being shared. Since data management and governance play integral roles in facilitating secure IoT data sharing, our analysis investigates the data management and governance frameworks, or standards, used in the primary studies.

RQ3 does not consist of any sub-RQs. However, it helps to express the current issues and suggest possible directions for future research.

3.2 Inclusion and Exclusion Criteria

Given the extensive scope of primary studies yielded by our search strategy, it is imperative to define a set of inclusion and exclusion criteria that all primary papers must adhere to. Our selection process was meticulously executed to ensure transparency and minimize bias, with the requirement that each primary study **must address IoT data sharing in any aspect (directly or indirectly)**. We also filtered out the noises by excluding papers that meet ANY of the exclusion criteria (EC) detailed in Table 3.1.

Table 3.1: Exclusion criteria.

	Exclusion Criteria
EC1	The paper is NOT written in English.
EC3	The paper is NOT detailed enough (less than four-page double-column or six-page single column).
EC4	The paper is published before 2009.
EC5	The paper is NOT peer-reviewed.
EC6	The paper is NOT in a final publication stage.
EC7	The paper is a survey paper.

3.3 Search and Selection Strategy

We have employed two widely-adopted methods for the identification of primary studies: the database search (Kitchenham and Charters, 2007) and manual search through snowballing (Wohlin, 2014).

3.3.1 Database Search

Using online inquiry features of popular publication databases is the most notable approach to scan for primary studies when directing supplemental studies (Kitchenham and Charters, 2007). We used five popular publication databases, i.e., IEEE Xplore[1], ACM Digital Li-

[1] https://ieeexplore.ieee.org

brary[2], ScienceDirect[3], Scopus[4], and Web of Knowledge[5] to search for potential primary studies. These databases contain peer-reviewed articles and provide advanced search capacities.

In alignment with our research questions, we initially identified a set of keywords to formulate our search strings. These keywords were the foundation for retrieving the most pertinent papers from search engines. Subsequently, through a meticulous review of these top-relevant papers, we curated a more refined collection of keywords intricately linked to the overarching themes of data sharing, application domains, security, and governance. This process unfolded iteratively, complemented by evaluating these keywords against search engines to ascertain their effectiveness in retrieving top-relevant papers. The ultimate ensemble of search keywords is presented below, organized according to guidelines from Kitchenham and Charters (2007). The construction of search strings employed Boolean AND and OR operators to assemble these keyword groups. Moreover, we tailored the search query to harmonize with the search engine protocols of each publication database.

(*"data sharing"* **OR** *"sharing"* **OR** *"data exchange"* **OR** *"context sharing"* **OR** *"context aware data sharing"* **OR** *"context-sensitive information sharing"* **OR** *"sharing of data"* **OR** *"sharing data"* **OR** *"ecosystem"* **OR** *"marketplace"* **OR** *"data marketplace"*)

AND (*"Internet of Things"* **OR** *"IoT"* **OR** *"Industry 4.0"* **OR** *"smart cities"* **OR** *"smart city"* **OR** *"smart contract"* **OR** *"manufacturing"* **OR** *"energy"* **OR** *"supply chain"*)

AND (*"access control"* **OR** *"secure"* **OR** *"security"* **OR** *"trust"* **OR** *"trustworthy"* **OR** *"encryption"* **OR** *"data security"* **OR** *"secure communication"* **OR** *"secure data sharing"* **OR** *"context-aware security"* **OR** *"management"* **OR** *"governance"* **OR** *"protocols"* **OR** *"standards"*)

Figure 3.1 gives an overview of the search and selection steps. Our initial filtration was predicated on the evaluation of candidate articles through an analysis of their titles and abstracts. In instances where these summaries did not provide sufficient clarity to make definitive inclusion

[2] https://dlnext.acm.org
[3] https://sciencedirect.com/
[4] https://scopus.com
[5] https://www.webofscience.com/

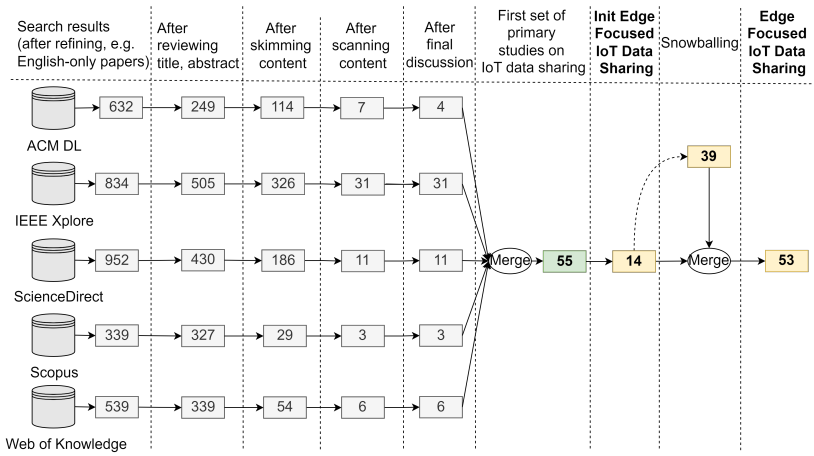

Figure 3.1: Overview of the search and selection steps.

or exclusion determinations, a more comprehensive examination of the article content ensued. If a candidate article was retrieved from multiple databases, we retained it in each corresponding search result during the initial phase. Subsequently, to ensure methodical consistency and eliminate redundancy, the results were harmonized through extensive dialogues among the authors. This collaborative consolidation process culminated in the acquisition of the set of *fifty-five* (55) primary studies (see Table 5.1), ensuring the exclusion of duplicates.

3.3.2 Manual Search for Edge-focused secure IoT data sharing approaches

In the second phase of our study, we specifically targeted Edge-focused secure IoT data sharing approaches. Therefore, we have made more strict selection criteria detailed in Table 3.2. To find the primary studies on Edge-focused secure IoT data sharing approaches, out of the 55 previously found studies (until 2021), we first strictly selected *fourteen* (14) primary studies on Edge-focused IoT data sharing based on the selection criteria detailed in Table 3.2. Then, we conducted a manual search by following the snowballing recommendation by Wohlin (2014). In short, we recursively looked into the references (backward snowballing) and citations (forward snowballing) of the 14 primary studies on Edge-

Table 3.2: Strict inclusion criteria of Edge-focused secure IoT data sharing studies.

	Inclusion Criteria
IC0	The paper addresses IoT data sharing in any aspect (directly or indirectly)
IC1	The paper must explicitly describe IoT data processing or collecting on Edge.
IC2	The paper must have a clear IoT-Edge architecture for data sharing.
IC3	Shared IoT data must be used online.

Table 3.3: Data collection for each research question.

Research Question	Type of Data Extracted
RQ1	Publication trends, domains, purposes, and architectural details for secure IoT data sharing.
RQ2	Edge-focused secure IoT data sharing.
RQ3	Secure IoT data sharing limitations, open issues, and research gaps.

focused secure IoT data sharing. For each of the newly found candidates from snowballing, we also applied a thorough review and selection process based on the title and abstract, skimming and scanning, and cross-checking with discussion among the authors. This supplementary effort yielded an additional *thirty-nine* (39) primary studies (see Figure 3.1). The vast majority of these papers were published more recently (2021-2024). These studies must satisfy ALL the Inclusion Criteria (IC) detailed in Table 3.2. Therefore, in total, we ended up with a set of *fifty-three* (53) primary studies on Edge-focused secure IoT data sharing (see Tables 5.2, 5.3 and 5.4).

Note that there are 14 primary studies on Edge-focused secure IoT data sharing that appear in both the initial set of 55 primary studies on secure IoT data sharing in Table 5.1, as well as the set of 53 primary studies on Edge-focused secure IoT data sharing in Tables 5.2, 5.3 and 5.4.

In summary, our search and selection process culminated with a total of *ninety-four* (94) primary studies eligible for data extraction and subsequent synthesis by the close of 2023 and early 2024. We extracted related information based on our taxonomy (in Section 4) from all these studies according to our RQs (see Table 3.3).

4

A Classification Schema / Taxonomy

The taxonomy is a technique to establish a classification system for all relevant categories that should be extracted in the primary studies. The objective of this taxonomy is to enable extraction and distinguishing data from primary studies that are used to answer our research questions. Data sharing capabilities, IoT architecture, application domain scope, security, trust and data management and governance are all variables that go into the taxonomy. The taxonomy of our research is illustrated in Figure 4.1.

4.1 Capabilities of Data Sharing

- **Type of sharing**: What data is being shared and how is it being shared? This might include everything from personal health information to gadget sensor data.
- **Stakeholders**: After figuring out what data is being shared, we will investigate whom the data is being shared with and between. We will mostly differentiate between:
  - Platform owner: the owner of a platform where both the data owner and the user can take advantage of and trade information.

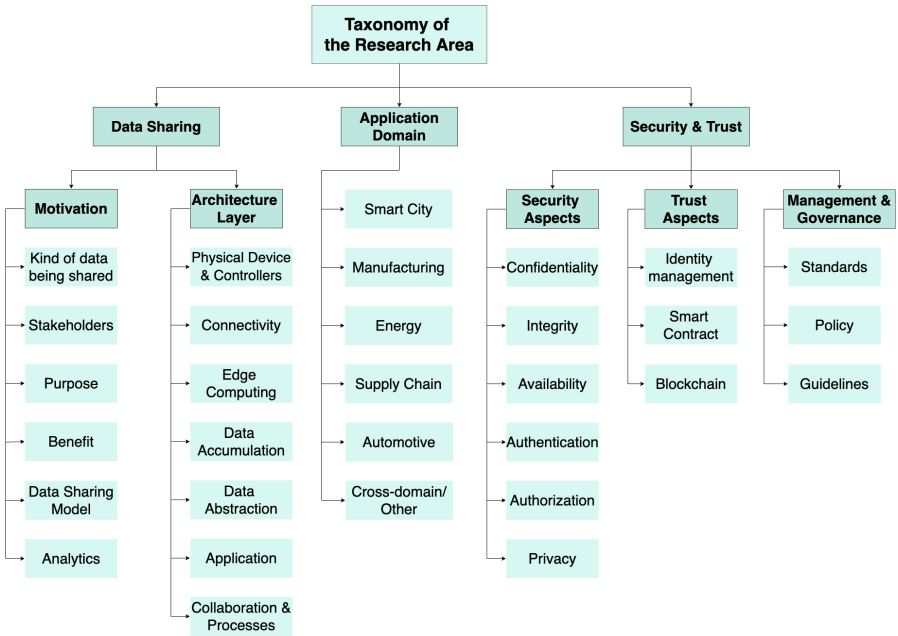

Figure 4.1: Taxonomy of the Research Area

  - Data owner: the ones that share their data.
  - Data user: the ones that take advantage of the data being shared.

- **Purpose**: with the knowledge of what kind of data is being shared and with whom it is being shared, we will be looking into the purpose of the data sharing, implementation reasons, and research.

- **Benefits**: from the purpose, we will see how the data sharing, implementation reasons, and research have contributed in a positive manner in different aspects. For example, by varying from utilizing possible data as a new resource.

- **Data sharing models**: distinguish if the solution is a public or private marketplace, peer-to-peer or a domain-specific sharing.

- **Analytic**: another aspect is data analytic, as data sharing often goes hand in hand with analytic. Therefore, looking into how, or

if, the data is being analyzed in some way could be an interesting extraction.

4.2 IoT Architecture

The seven (7) or five (5) layer architecture is frequently mentioned in regards to the IoT reference model. The IoT World Forum Reference Model (Cisco, 2024) is one of those providing a 7-layer architecture model, where the layers are described as follows:

- **L1 Physical Devices** & **Controllers:** include all the "Things" in IoT, which could be e.g. machines, sensors or devices.
- **L2 Connectivity:** communication and processing units.
- **L3 Edge Computing:** data element analysis and transformation.
- **L4 Data Accumulation:** storage.
- **L5 Data Abstraction:** aggregation and access.
- **L6 Application:** reporting, analytics and control.
- **L7 Collaboration** & **Processes:** involving people and business processes.

IDS Reference Architecture Model (Association, 2024) is one of those that offers a solution based on a model with only five layers: business, functional, process, information, and system. There is, however, a shared understanding of this reference model, which can be broken down into three simple layers. By referring to the different number of levels (L) from Figure 4.2 (Cisco, 2024), the three layers are as follows: perception (L1), network (grouping L2 and L3), and application (grouping L4, L5, L6, L7). In our taxonomy, we will focus on the architecture consisting of only three layers.

4.3 Scope of Application Domain

Various instances of business ecosystems can be found across a variety of industries. However, in our taxonomy, we will be using the IDS Data

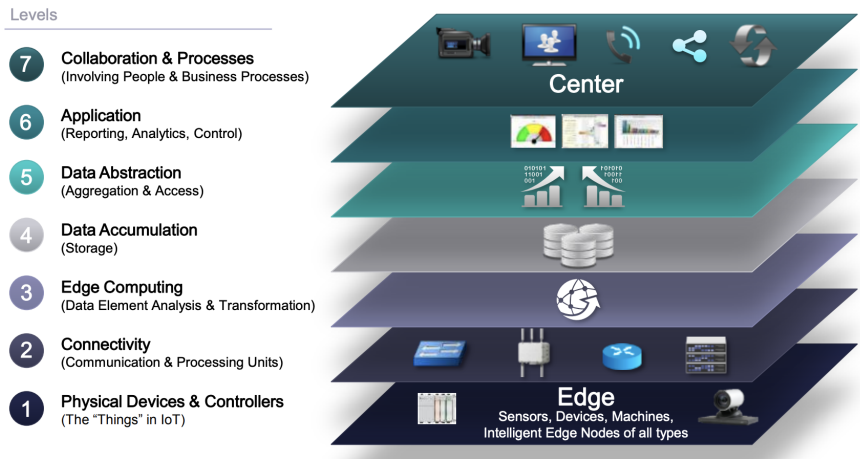

Figure 4.2: Overview of the layers in the IoT World Forum Reference Model (Cisco, 2024)

Space Radar (Matsas, 2024) ecosystems to determine what kind of domain the studies are concerned about:

- **Smart city**: shared use of data for end-to-end consumer services.
- **Manufacturing (and logistics)**: exchange of master and event data along the entire supply chain.
- **Energy**: shared use of process data for predictive asset maintenance.
- **Supply chain**: data sharing between a company and its suppliers to produce and distribute a specific product.
- **Automotive**: all the functions and systems related to a vehicle domain.
- **Cross-domain / Domain-independent**: includes generic solutions that should be applicable for different single domains, or even cross-domain.

4.4 Security Aspects

We also address the security concerns that IoT data sharing has to contend with. Since there are numerous concerns to consider, we will specifically focus on confidentiality, integrity, availability, authentication, authorization, and privacy. In Section 2.2, we defined all of the security concepts. However, the following is a brief definition of each term:

- **Confidentiality**: The protection of personal information from being exposed to an unauthorized actor.
- **Integrity**: The trust and accuracy of the data.
- **Availability**: The property of data being available when needed for authorized users.
- **Authentication**: The property of confirming one's authority.
- **Authorization**: The property of giving the users permission to access a resource.
- **Accountability**: The ability of tracing activities on a system to individuals who may then be held responsible for their actions.[1]
- **Privacy**: The protection of personal identifiable information.

4.5 Trust Aspects

To assess the trustworthiness, security, and data sovereignty support offered by the study solutions, we will be focusing on the following topics:

- **Identity management**: we look into aspects such as if every connected participant has a unique identifier and certificate.
- **Secure communication**: figuring out how the communication between each connected participant in the ecosystem can be assured of confidentiality and authenticity when sharing data

[1] https://csrc.nist.gov/glossary/term/accountability

between each other. This could be evaluated by seeing if the solution includes the following mechanisms:

- **Blockchain**: from the definition by IBM (2024b), a blockchain is a shared and immutable ledger. Blockchain technology is usually used for recording transactions, tracking assets, and building trust.
- **Smart contracts**: are a digital version of contracts that are stored on the blockchain. The benefit of this type of contract is its ability to automatically self-execute when predetermined conditions and terms are met (IBM, 2024a).

4.6 Privacy

The sharing of data across various platforms and ecosystems presents unique challenges to privacy. The essence of privacy in IoT data sharing involves safeguarding personally identifiable information (PII) against unauthorized access and misuse. In the context of this work, privacy concerns in IoT encompass a wide range of issues from data collection to storage of data to its sharing and processing thereof. In addition, privacy involves obligations and prohibitions from regulatory instruments, such as the GDPR or AI act. For example, GDPR requires the handling of personal data as per core privacy principles and other articles clarifying sensitivity of the data, need for impact assessments in data processing scenarios, and the use of appropriate state of the art controls to protect the personal data. When evaluating the primary studies, we will assess whether such provisions and obligations, such as purpose limitation, data minimization, privacy by design, data subject access rights, compliance, accountability, etc., are covered.

4.7 Management and Governance

We will identify the obligations that the primary papers highlight in terms of data management and governance. These obligations can include duties in terms of data ownership, data consumption and usage control. An example of such obligations includes the deletion of data

after two days. We will focus on the following areas in particular to precisely identify the obligations highlighted in the papers:

- **Standards**: what kind of specification or other precise design criteria has been considered?
- **Policy**: what kind of *mandatory* guidance, advice, and support have been considered?
- **Guidelines**: what kinds of *voluntary* general guidance, advice, and support have been considered?

In addition, we will be looking into other aspects of the solutions regarding whether any identity management has been adopted, or how secure communications are handled. The use of blockchain technology and smart contracts can be used as examples of how to secure communication. An influencing topic for both security and trust is the assessment of data management and governance. We will identify if there are any specific standards, guidelines or policies that have been taken into consideration.

5

Results

Tables 5.1-5.4 altogether present the 94 selected primary studies. We extracted data according to our taxonomy and then conducted analyses of these studies to answer the research questions as follows.

5.1 High-Level Details (RQ1)

Answering RQ1.1-What is the current trend of publications on secure IoT data sharing: We visualize the publication trend of the first set of 55 secure IoT data sharing primary studies in Table 5.1 to answer RQ1.1. As depicted in Figure 5.1 all of our primary studies in Table 5.1 were published after 2016. Figure 5.1 illustrates the 55 primary studies that have been published since 2017, which according to the histogram, have been the most relevant to our specific topic of secure IoT data sharing (2020: 14; and 2021: 20 papers). We can observe an increasing growth of interest in the topic of secure IoT data sharing with 14 primary studies published in 2020 and 20 published in 2021.

Table 5.1: The initial set of the 55 primary studies of secure IoT data sharing.

#	Year	PV	Title (click to open the corresponding publication)
#1	2017	C	Towards Blockchain-based Auditable Storage and sharing of IoT data
#2	2017	J	Secure and Efficient Data Sharing with Atribute-based Proxy Re-encryption Scheme
#3	2017	J	IoT data privacy via blockchains and IPFS
#4	2017	C	Big Data Model of Security Sharing Based on Blockchain
#5	2018	J	A Peer-to-Peer Architecture for Distributed Data Monetization in Fog Computing Scenarios
#6	2018	J	Continuous Patient Monitoring with a Patient Centric Agent: A Blockchain Architecture
#7	2018	C	Towards a Decentralized Data Marketplace for Smart Cities
#8	2018	C	Providing Context Aware Security for IoT Environments Through Context Sharing Feature
#9	2018	C	A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems
#10	2018	J	Smart-toy-edge-computing-oriented data exchange based on blockchain
#11	2019	C	Security and Privacy of Electronic Health Records: Decentralized and Hierarchical Data Sharing using Smart Contracts
#12	2019	J	Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies
#13	2019	J	MedChain: Efficient Healthcare Data Sharing via Blockchain
#14	2019	C	Toward a Decentralized, Trust-Less Marketplace for Brokered IoT Data Trading Using Blockchain
#15	2019	C	Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks
#16	2019	C	Towards Multi-party Policy-based Access Control in Federations of Cloud and Edge Microservices
#17	2019	C	BlendMAS: A Blockchain-Enabled Decentralized Microservices Architecture for Smart Public Safety
#18	2019	C	BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT
#19	2019	C	Enabling Industrial Data Space Architecture for Seaport Scenario
#20	2019	C	Blockchain based Proxy Re-Encryption Scheme for secure IoT Data Sharing
#21	2019	J	IoT Passport: A Blockchain-Based Trust Framework for Collaborative Internet-of-Things
#22	2020	C	BEAF: A Blockchain and Edge Assistant Framework with Data Sharing for IoT Networks
#23	2020	C	A Blockchain-based Medical Data Marketplace with Trustless Fair Exchange and Access Control
#24	2020	C	Blockchain Smart Contract for Scalable Data Sharing in IoT: A Case Study of Smart Agriculture
#25	2020	J	Fully Decentralized Multi-Party Consent Management for Secure Sharing of Patient Health Records
#26	2020	J	Secure data exchange between IoT endpoints for energy balancing using distributed ledger
#27	2020	J	BDSS-FA: A Blockchain-Based Data Security Sharing Platform With Fine-Grained Access Control
#28	2020	J	EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange
#29	2020	C	Decentralized patient-centric data management for sharing IoT data streams

Table 5.1: Continued.

#	Year	PV	Title (click to open the corresponding publication)
#30	2020	C	Blockchain-Based Multi-Role Healthcare Data Sharing System
#31	2020	J	Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices
#32	2020	J	Subscription-Based Data-Sharing Model Using Blockchain and Data as a Service
#33	2020	J	Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals
#34	2020	C	TrustedChain: A Blockchain-based Data Sharing Scheme for Supply Chain
#35	2020	J	A multi-layered blockchain framework for smart mobility data-markets
#36	2021	J	Blockchain-Driven Trusted Data Sharing With Privacy Protection in IoT Sensor Network
#37	2021	J	MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain
#38	2021	J	Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control
#39	2021	C	A Cooperative Architecture of Data Offloading and Sharing for Smart Healthcare with Blockchain
#40	2021	C	ITrade: A Blockchain-based, Self-Sovereign, and Scalable Marketplace for IoT Data Streams
#41	2021	J	Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain
#42	2021	J	Medi-Block record: Secure data sharing using block chain technology
#43	2021	J	PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities
#44	2021	J	AgriOnBlock: Secured data harvesting for agriculture sector using blockchain technology
#45	2021	J	BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten
#46	2021	J	BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications
#47	2021	J	A conceptual IoT-based early-warning architecture for remote monitoring of COVID-19 patients in wards and at home
#48	2021	J	A blockchain-based trading system for big data
#49	2021	J	MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic
#50	2021	J	SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework
#51	2021	J	eHealthChain—a blockchain-based personal health information management system
#52	2021	J	A Threshold Proxy Re-Encryption Scheme for Secure IoT Data Sharing Based on Blockchain
#53	2021	J	A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection
#54	2021	J	FAST DATA: A Fair, Secure and Trusted Decentralized IIoT Data Marketplace enabled by Blockchain
#55	2021	J	Blockchain Assisted Secure Data Sharing Model for Internet of Things Based Smart Industries

PV: Publication venue; J: Journal; C: Conference.

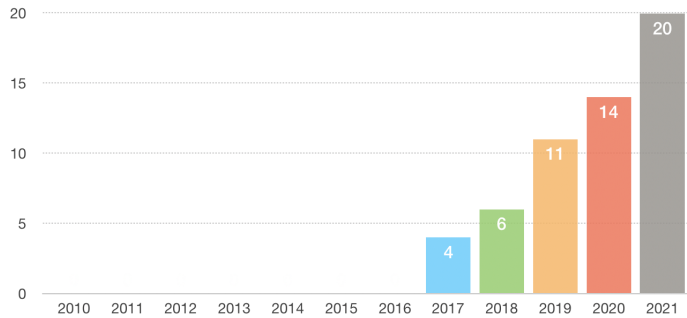

Figure 5.1: The publication years of the first set of 55 primary studies

In the second phase of our study that was strictly for Edge-focused approaches, we only conducted snowballing on 14 primary studies but already got 39 new primary studies that were published in recent years (2021-2024). This big increase shows the continual trend of growth of interest in the topic of IoT data sharing.

Answering RQ1.2-What are the reported application domains of IoT data sharing: As an adaptable technology, IoT is utilized across multiple areas. We divided the application domain according to IDS Data Space Radar[1] as follows: smart cities, manufacturing, energy, supply chain, automotive, and cross-domain/other. The application domain labeled "Cross-domain/domain-independent" is the most dominant, represented by 44 out of 94 primary studies. The papers addressing cross-domain/other are divided into four subcategories: healthcare, surveillance, smart toys, and generic domains. Healthcare and the generic topic have a shared first place, being represented by 21 out of 94 primary studies. This is in contrast with the topics of smart toys and surveillance, which are each addressed in a single study. For the other domains, energy is represented by one paper, while as for supply chain, manufacturing, and automotive, they are presented in two papers each, and smart city in four.

Tables 5.2-5.4 show the application domains that the Edge-focused primary studies address. For each study, we can also see for what purpose

[1] https://internationaldataspaces.org/adopt/data-space-radar/

that IoT data are shared. Figure 5.2 shows the main application domains addressed in the 53 primary studies of Edge-focused IoT data sharing. Nearly half of the studies (40.5%) are not domain-specific. Healthcare is an important application domain that needs data sharing with security and privacy, which addressed by more than one-third of the primary studies (35.7%). Smart City and Transport/Mobility are also very visible application domains.

Table 5.2: The 53 primary studies of Edge-focused secure IoT data sharing (Part 1/3).

#	PV	Application domain	Data sharing purpose
Yu *et al.*, 2024	J	Domain-independent	Leverage edge computing for proximity-based data processing and blockchain technology for immutable and tamper-proof data recording, enhancing the trust, security, and efficiency of IoT data sharing.
Sharma *et al.*, 2024	J	Healthcare	The purpose is to establish a secure, transparent, and efficient system for remote patient monitoring.
Li *et al.*, 2024	J	Domain-independent	To address confidentiality concerns in IoT systems by enabling secure, end-to-end encrypted message distribution from IoT devices to authorized subscribers. This is achieved while allowing for efficient revocation of access rights, ensuring data confidentiality even if the message broker is fully compromised.
Wang *et al.*, 2023	J	Domain-independent	To achieve effective data supervision and secure data sharing in IIoT by introducing a blockchain-enabled data-sharing scheme based on proxy re-encryption, which ensures secure storage and access authentication, efficient data storage, and improved data sharing efficiency.
Li *et al.*, 2023	J	Healthcare	To overcome obstacles in medical data sharing due to insufficient collaboration among medical institutions and concerns regarding security and privacy in traditional cloud-based platforms. By integrating blockchain and edge computing, MSNET aims to provide a secure, efficient, and scalable method for medical data sharing, fostering collaboration and innovation in the healthcare industry.
Banavathu and Meruva, 2023	J	Domain-independent	To provide efficient and secure data storage for IoT-related smart computing systems. By utilizing AI and blockchain technology, it aims to securely capture user authentication, prevent user-related attacks like distributed denial-of-service (DDOS), and ensure data integrity and security.

Table 5.2: Continued.

#	PV	Application domain	Data sharing purpose
Samuel *et al.*, 2023	J	Healthcare	To ensure the security, privacy, and anonymity of COVID-19 patient information sharing.
Alshehri *et al.*, 2023	J	Healthcare	Ensuring the security of the remote patient monitoring (RPM).
Cheikhrouhou *et al.*, 2023	J	Healthcare	Ensuring the security of the remote patient monitoring (RPM).
Umran *et al.*, 2023	J	Petroleum industry	To provide a decentralized, low-power consumption, fast, scalable, secure, privacy-preserving, and trusting architecture for data sharing within the petroleum industry in Iraq. The architecture aims to improve blockchain performance, security, authentication, privacy preservation, and address blockchain storage limitations.
Isaja *et al.*, 2023	J	Manufacturing	To empower zero-waste value chain strategies with meaningful, reliable, and trustful data by providing a solution for end-to-end industrial data traceability, trust, and security. It aims at the secure and effective sharing of quality-related information within the supply chain business ecosystem to drive quality optimization actions towards zero-defect manufacturing.
Patel and Shrimali, 2023	J	Agriculture	To address the issues mentioned in the agriculture sector by connecting various stakeholders through the usage of IoT devices and smart contracts in Ethereum. The issues are: transparency, timeliness, traceability, security, and immutability resulting in financial loss, crop contamination, and spoilage.
Sengupta *et al.*, 2023	J	Domain-independent	To propose a fair, accountable, and secure data sharing scheme named FairShare for IIoT, which prevents fraudulent activities, achieves fairness, ensures accountability of services provided by the parties, and secures data privacy through cryptographic techniques.
Guan *et al.*, 2023	J	Smart Hotels	Secure hotel data while enhancing customer service. IDS and blockchain to share data for these services.
Hao *et al.*, 2023	J	Domain-independent	Data-sharing among various domains.
Manoj *et al.*, 2023	J	Agriculture	This work proposes an AgriSSIOracle framework for trusted agricultural IoT data sharing and decentralized oracle-based data access for production risk management.

PV: Publication venue; J: Journal; C: Conference.

Table 5.3: The 53 primary studies of Edge-focused secure IoT data sharing (Part 2/3).

#	PV	Application domain	Data sharing purpose
Shang *et al.*, 2022	J	Energy	To address the challenges of large computing overhead and low data sharing security in microgrid data processing. It leverages blockchain technology within a cloud-edge-terminal architecture to enhance the security and efficiency of key management and data sharing among microgrid components.
Jeoung *et al.*, 2022	J	Smart City	The purpose is to to register occupants and the personalized thermal sensation vote (TSV) prediction model for training, and control indoor temperatures while ensuring the security of occupant and building data.
Wei *et al.*, 2022	J	Domain-independent	To provide a trustable cross-system data sharing service for IoT by adopting blockchain to construct a multicenter data management framework, thereby establishing a credible environment for data sharing and addressing security concerns with attribute-based encryption (ABE).
Daidone *et al.*, 2022	J	Healthcare	To empower data owners by allowing them to define how their data can be used and to verify the compliance with their privacy preferences without relying on a centralized authority.
Nguyen *et al.*, 2022	C	Domain-independent	A novel dynamic context-based policy enforcement framework to support IoT data sharing (on-Edge) based on dynamic contracts.
Firouzi *et al.*, 2022	J	Healthcare	Discussed aspects of health data monetization covering business models, challenges and potential solutions. Reference architecture proposed balancing data monetization with compliance to security and privacy regulations.
Zuo and Qi, 2022	J	Oil and gas industry	To create a decentralized, immutable, and transparent environment for the automatic monitoring and control of industrial operations in the oil and gas industry, aiming to increase operation and asset efficiency, safety, and to ensure real-time monitoring and control remotely.
Zaabar *et al.*, 2021	J	Healthcare	Contribute to the healthcare management systems' robustness and to avoid recorded security limitations in commonly used systems for smart healthcare.
Abbas *et al.*, 2021	J	Transportation	Using private blockchain to design a decentralized platform to address data security and transparency issues in smart cities' transportation systems.
Zhang *et al.*, 2021	J	Domain-independent	A secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing.
Singh *et al.*, 2021	J	Manufacturing	Data-sharing among various domains working in collaboration in the IIoT environment.

Table 5.3: Continued.

#	PV	Application domain	Data sharing purpose
Mayer *et al.*, 2021	J	Healthcare	To create a secure and efficient architecture for managing PHRs by integrating Blockchain, Fog Computing, and the IoT. This aims to address challenges related to the security, privacy, and real-time processing of sensitive medical data, enhancing the capabilities of healthcare services and supporting precision medicine.
Nguyen *et al.*, 2021 (#39)	C	Healthcare	To facilitate healthcare by efficiently offloading and sharing health data with improved Quality of Service (QoS), enhanced data privacy and security, and low smart contract costs. It aims to overcome challenges in data offloading and sharing due to centralized healthcare architectures, such as low QoS, data privacy, system security, and to provide a trustworthy access control mechanism using smart contracts for secure EHR sharing.
Egala *et al.*, 2021 (#38)	J	Healthcare	Provided a platform for different stakeholders in the healthcare industry to make digital agreements.
Ma *et al.*, 2021 (#36)	J	Transport/ITS (Internet of Vehicles)	secure sharing of IoV data scheme based on blockchain (called IoVChain) divides data into public data that can be shared in plain text and private data that must be kept strictly confidential, combines current privacy protection technology.

PV: Publication venue; J: Journal; C: Conference.

Table 5.4: The 53 primary studies of Edge-focused IoT secure data sharing (Part 3/3).

#	PV	Application domain	Data sharing purpose
Nawaz *et al.*, 2020	J	Domain-independent	The purpose of EdgeBoT is to enable secure peer-to-peer (P2P) data transactions within the IoT, leveraging edge computing and Ethereum blockchain. It aims to shift data processing closer to the data source (edge of the network) and ensure data ownership and privacy through blockchain technology.
Hang *et al.*, 2020	J	Smart farming and Aquaculture	To provide fish farmers with secure storage for preserving large amounts of agriculture data that cannot be tampered with. The platform aims to automate agriculture data processing, including outlier filtering before generating records into the ledger, to improve agriculture data integrity.

Table 5.4: Continued.

#	PV	Application domain	Data sharing purpose
Zichichi *et al.*, 2020	J	Transport	Provide access and share data from vehicules using Blockchain and DFS.
Gimenez *et al.*, 2020	C	Seaport/ Transport	An open cross-layer framework and an associated methodology and tools to achieve interoperability among heterogeneous IoT platforms.
Akkaoui *et al.*, 2020 (#28)	J	Healthcare	Enabling healthcare information exchange (HIE) between health authorities to facilitate the process of sharing health data (i.e.,EMRs and PHD).
Al-Zahrani, 2020 (#32)	J	Domain independent	Ease of administration, collaboration, global accessibility and compatibility among different platforms.
Ur Rahman *et al.*, 2020 (#24)	C	Smart city	A large number of resource owners can share their agriculture data sharing in an secure manner and update, create or delete policies.
Makhdoom *et al.*, 2020 (#43)	J	Smart city	A blockchain-based innovative framework for integrity and privacy-preserving IoT data sharing in a smart city environment.
Dwivedi *et al.*, 2019	J	Healthcare	The use of a blockchain to provide secure management and analysis of healthcare big data.
Sarabia-Jácome *et al.*, 2019 (#19)	C	Seaport/ Transport	Adopting the Industrial Data Space (IDS) reference architecture, a seaport data space based on IDS architecture to share information in a secure and interoperable manner.
Pham *et al.*, 2019	C	Domain independent	Adopting smart contracts to enable a trustless data sharing mechanism without need of the third-party.
Zheng *et al.*, 2019 (#12)	J	Healthcare	Provide a way to store and share the health information in more secured and effective manner.
Bai *et al.*, 2019 (#18)	J	Manufacturing	Manufacturing equipment data sharing and maintenance service sharing from smart manufacturing.
Xu *et al.*, 2019 (#17)	C	Smart City	Data provider grants the access and offers service to the requester in an secure manner.

Table 5.4: Continued.

#	PV	Application domain	Data sharing purpose
Kang *et al.*, 2019 (#15)	J	Automotive	Accurate reputation management for high-quality data sharing among vehicles.
Preuveneers and Joosen, 2019 (#16)	C	Domain independent	Leveraging microservice technologies, give a flexible, scalable and adhere to security needs.
Tang *et al.*, 2019 (#21)	C	Domain independent	Enable a decentralized cross-platform collaboration.
Fu *et al.*, 2018	J	Domain independent	The main objective is to address challenges in data processing, secure data storage, efficient data retrieval, and dynamic data collection within the Industrial Internet of Things (IIoT) by leveraging a framework that integrates fog computing and cloud computing.
Özyilmaz *et al.*, 2018	C	Domain independent	To create a blockchain-based decentralized and trustless data marketplace facilitating transparent and democratic access to consented IoT data.
Griggs *et al.*, 2018	J	Healthcare	Use of blockchain for its decentralisation, tracability and security properties. Use smart contracts to facilitate automatic analysis of health data collected based on custom threshold values for each patient, which can trigger alerts for unusual activity.
Mollah *et al.*, 2017	J	Domain independent	To share and search data securely by IoT smart devices at the edge of cloud-assisted IoT.
Dorri *et al.*, 2017	C	Smart homes/Smart City	To provide a lightweight, scalable, and distributed security and privacy safeguard for IoT devices within a smart home context for secure and private data sharing and access control, without significant energy, delay, or computational overhead.

PV: Publication venue; J: Journal; C: Conference.

Answering RQ1.3-What are the purposes and benefits of data sharing considered in the primary studies: All the primary papers share a common purpose and goal in their studies and work: To develop a reliable and efficient data sharing solution that allows data owners and users to securely exchange their data while making data sources more accessible to authorized actors. There are some studies that only offer a broad overview of the purpose and benefits, while others

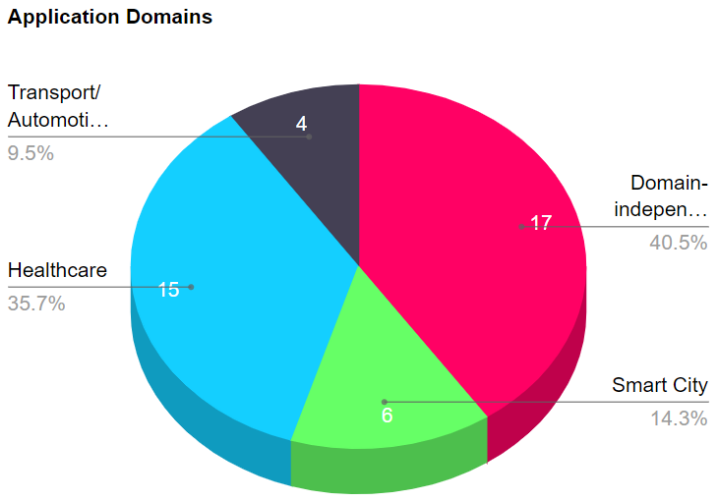

Figure 5.2: Application Domains of the Edge-focused IoT Data Sharing Approaches

delve further into the purpose and benefits of data sharing applicable specifically to the domain they address, such as papers #18 and #28 (see Table 5.1).

Our findings show that the majority of primary papers with publications addressing the healthcare domain deal with data sharing within the same system. The work by paper #28, on the other hand, may be categorized as addressing data exchange in cross-healthcare systems. Doctors are one of the stakeholders, as they give healthcare to patients, which implies data sharing within the same system. However, there is another stakeholder referred to as the "requestor" of data. As the division of stakeholders is represented by doctor, patient, and requestor, it indicates that the "requestor" may be from a different system.

Data sharing also has a significant impact in the manufacturing industry, which involves many different stakeholders, e.g., customers, employees, and supply-chain organizations. Paper #18 explains how the traditional manufacturing environment is complex, with various manufacturing data, e.g., equipment data, which is often stored in separate systems. Because these systems may belong to multiple service providers, and manufacturing organizations may not have direct control over this type of data and may be unable to comprehend the true and

full value of the massive amount of data generated. As a result, the aim and benefits of sharing equipment data are explored in depth in this monograph. The data on the equipment comprises not just their capacity, but also their status data. Data sharing can empower R&D, making manufacturing and distribution audits more effective, which assists production companies in reducing operating and manufacturing costs. For Edge-focused approaches, the purposes are detailed in Tables 5.2-5.4.

5.2 Low-Level Details of Edge-focused Data Sharing Solutions (RQ2)

To answer RQ2, we have deep-dived into the 53 primary studies of Edge-focused IoT data sharing as shown in Tables 5.2-5.4.

5.2.1 Answering RQ2.1-What are the security aspects covered by Edge-focused IoT Data Sharing approaches today in different domains?

The security aspects addressed by the various solutions and approaches in the identified primary studies may be grouped into the following four main categories.

- Fundamental security principles, which includes confidentiality, integrity, and availability. This is typically referred to as the CIA triad.
- Extended security principles, which includes authentication, authorization, and accountability.
- Additional security properties, which includes anonymity, traceability, and immutability.
- Security mechanisms and controls, which includes access control, encryption, and authenticity.

Most of the primary studies address more than one security category mentioned above. Thus, the numbers shown in this sub-section reflects

the number of papers addressing the specific security aspect. Figures 5.3-5.6 illustrate the security categories addressed by the primary studies with respect to their application domains. Note that in this section, we have merged the domains identified in our answer to RQ1.2 that are closely related to industry and smart city. The domain independent and healthcare domain remain the same as in our answer to RQ1.2.

- The merged domains related to industry include: automotive, manufacturing, oil and gas industry, smart farming, agriculture, aquaculture, and energy.
- The merged domains related to smart city include: smart city in general, transport, seaport, smart homes, and smart hotels.

With respect to fundamental security principles, most of the approaches address integrity (23), followed by confidentiality (18) and availability (14). Viewing it from the specific domains, we observe from Figure 5.3 that domain independent and smart city approaches consider fundamental security principles more or less evenly, while healthcare and industry approaches mainly consider integrity. Although confidentiality and integrity is also important for the healthcare and industrial approaches, integrity is considered more important for these domains, which indicates that the correctness and quality of data is important in critical infrastructures.

With respect to extended security principles, most approaches are concerned with authentication principles (18), followed by authorization (13) and accountability (3). Viewing it from the specific domains, we observe from Figure 5.4 that all domains consider authentication principles evenly, while the domain independent and smart city approaches also prioritize authorization, in comparison to the healthcare and industry domains. Accountability, however, seems to be neglected by all domains.

With respect to additional security properties, most approaches are focusing on implementing traceability (12), while few approaches address anonymity (5) and immutability (8) explicitly. Viewing it from the specific domains, we observe from Figure 5.5 that the healthcare domain is the only domain that considers all additional security properties, which shows that the healthcare domain is extra careful in protecting

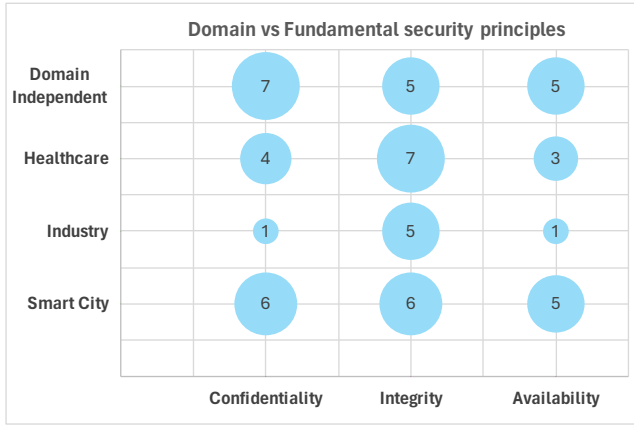

Figure 5.3: Fundamental security principles considered in each domain

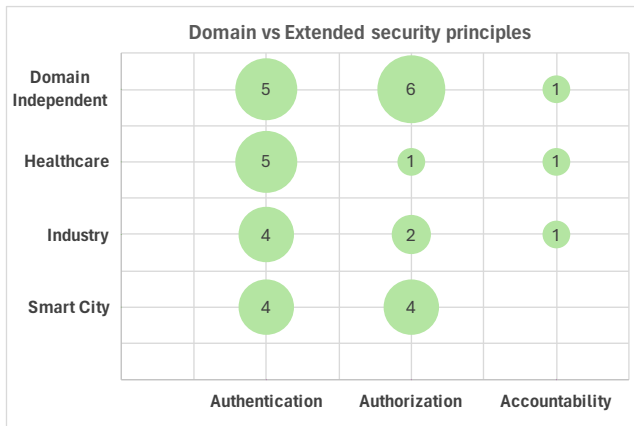

Figure 5.4: Extended security principles considered in each domain

patient-sensitive data. The industry and smart city domains implement traceability and immutability to some extent, while the domain independent approaches barely address any of the additional security properties.

Finally, with respect to security mechanisms and controls, the approaches are mainly focusing on access control (15) and encryption (13) mechanisms to protect the data from unauthorized users, while some approaches use mechanisms to ensure the authenticity (5) of data,

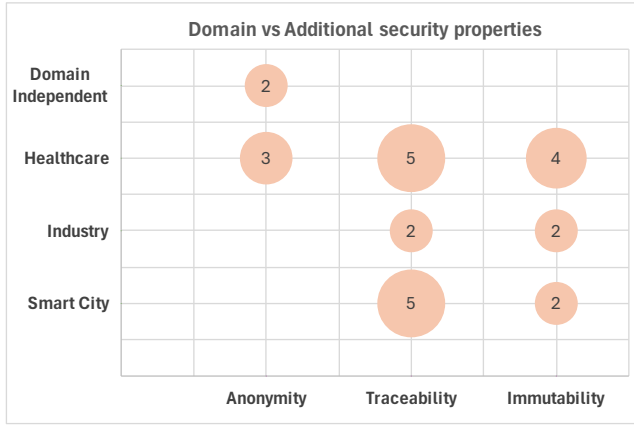

Figure 5.5: Additional security properties considered in each domain

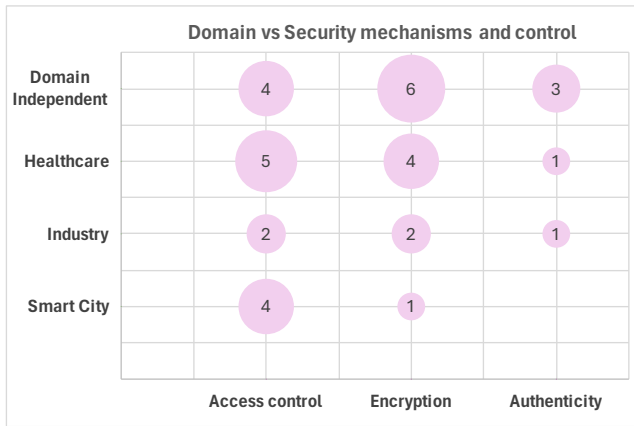

Figure 5.6: Security mechanisms and controls considered in each domain

especially for non-repudiation purposes. Viewing it from the specific domains, we observe from Figure 5.6 that most approaches implementing access control and encryption mechanisms belong to the domain independent and healthcare approaches.

Blockchain technology is applied in 42 out of the 52 primary studies that address Edge-focused data sharing solutions (see Section 5.2). Blockchain is used in the 42 approaches as an enabling technology to mainly implement and ensure data integrity (e.g., Firouzi *et al.*,

2022, Daidone *et al.*, 2022, Singh *et al.*, 2021), traceability (e.g., Guan *et al.*, 2023, Li *et al.*, 2023, Zichichi *et al.*, 2020), immutability (e.g., Sharma *et al.*, 2024, Zuo and Qi, 2022, Zaabar *et al.*, 2021), and secure transactions (e.g., Yu *et al.*, 2024, Umran *et al.*, 2023, Wei *et al.*, 2022).

5.2.2 Answering RQ2.2 - What and how are the techniques and approaches used to preserve trust and privacy in Edge-focused IoT data sharing?

Trust

Our systematic review identified several trust mechanisms and aspects within the domain of secure IoT data sharing, with a particular focus on edge computing solutions. The predominant trust mechanisms addressed across the reviewed literature are: (i) *blockchain technology*, (ii) *encryption and cryptographic techniques*, (iii) *trusted execution environments and trust models*, and (iv) *other trust mechanisms*. Table 5.5 lists the primary studies and the trust mechanisms they support.

Table 5.5: Trust mechanisms and primary studies with a focus on edge computing solutions.

Trust Mechanism	Primary Studies
Blockchain technology	Tang *et al.* (2019), Kang *et al.* (2019), Xu *et al.* (2019), Bai *et al.* (2019), Zheng *et al.* (2019), Ur Rahman *et al.* (2020), Al-Zahrani (2020), Makhdoom *et al.* (2020), Zichichi *et al.* (2020), Ma *et al.* (2021), Guan *et al.* (2023), Griggs *et al.* (2018), Zaabar *et al.* (2021), Abbas *et al.* (2021), Daidone *et al.* (2022), Sharma *et al.* (2024), Wei *et al.* (2022), Sengupta *et al.* (2023), Özyilmaz *et al.* (2018), Zuo and Qi (2022), Isaja *et al.* (2023), Dorri *et al.* (2017), Umran *et al.* (2023), Wang *et al.* (2023), Hang *et al.* (2020), Manoj *et al.* (2023), Jeoung *et al.* (2022), Cheikhrouhou *et al.* (2023), Samuel *et al.* (2023), Egala *et al.* (2021), Nawaz *et al.* (2020), Yu *et al.* (2024), Banavathu and Meruva (2023), Akkaoui *et al.* (2020), Mayer *et al.* (2021), Li *et al.* (2023), Nguyen *et al.* (2021), and Patel and Shrimali (2023)
Encryption and cryptographic techniques	Ma *et al.* (2021), Wei *et al.* (2022), Özyilmaz *et al.* (2018), Banavathu and Meruva (2023), Wang *et al.* (2023), Li *et al.* (2024), Zhang *et al.* (2021), Fu *et al.* (2018), and Nawaz *et al.* (2020)
Trusted execution environments and trust models	Mollah *et al.* (2017)
Other trust mechanisms	Preuveneers and Joosen (2019), Pham *et al.* (2019), Nguyen *et al.* (2022), Dwivedi *et al.* (2019), and Shang *et al.* (2022)

Blockchain technology has emerged as a pivotal force in enhancing the trustworthiness and security of data sharing within IoT environments. The analysis of 38 papers in this category reveals several core applications and benefits of blockchain across various IoT domains:

- *Decentralized Trust and Security.* Blockchain's intrinsic nature of decentralization eliminates the need for central authorities, reducing potential points of failure and increasing system resilience against attacks. For instance, Tang *et al.* (2019) and Kang *et al.* (2019) highlight how blockchain facilitates secure peer-to-peer interactions and transactions without intermediaries, thereby enhancing data integrity and trust among IoT devices.

- *Smart Contracts for Automated Enforcement.* Smart contracts automate various processes, including compliance, data sharing agreements, and access controls, directly within the blockchain. This automation reduces administrative overhead and speeds up operations while ensuring compliance with pre-defined rules. For instance, Griggs *et al.* (2018) showcases how smart contracts can manage data access and patient monitoring tasks securely and efficiently.

- *Privacy and Data Integrity.* Blockchain enhances privacy and data integrity through its cryptographic foundation, ensuring that data once entered into the blockchain cannot be altered undetected. For instance, Makhdoom *et al.* (2020) and Daidone *et al.* (2022) emphasize the role of blockchain in enabling secure, traceable exchanges that protect user data against unauthorized access and modifications.

- *Sector-Specific Applications.* The versatility of blockchain is evident in its applications across various sectors within IoT: *Healthcare* (e.g., Samuel *et al.*, 2023, and Zaabar *et al.*, 2021, discuss blockchain's role in ensuring the security and confidentiality of sensitive health data), *Industrial IoT* (e.g., Sengupta *et al.*, 2023, and Cheikhrouhou *et al.*, 2023, explore how blockchain solutions tailor security features for industrial settings and critical infrastructures), and Smart Cities and Agriculture (e.g., Manoj *et al.*,

2023, Patel and Shrimali, 2023, and Hang *et al.*, 2020, illustrate the use of blockchain in managing and securing data in smart city environments and agricultural operations).

While blockchain offers significant advantages, the papers also discuss challenges such as scalability, energy consumption, and integration complexities with existing technologies. Future research directions suggested include developing more energy-efficient blockchain solutions and hybrid architectures that integrate blockchain with other emerging technologies like fog computing and AI to enhance scalability and efficiency in IoT.

Encryption and cryptographic techniques are paramount in securing IoT data exchanges and storage, addressing the concerns of data privacy, integrity, and authenticity. A significant subset of the reviewed literature emphasizes the role of encryption and cryptographic techniques in fostering trust in IoT data sharing environments. These methods are vital for ensuring data integrity, confidentiality, and access control, which are crucial for the adoption of IoT solutions in sensitive or critical applications:

- *Blockchain-Integrated Encryption Methods.* These works integrate the blockchain technology with encryption to ensure trust with robust data security and privacy in IoT environments. Ma *et al.* (2021) utilize homomorphic encryption within a blockchain framework to allow computations on encrypted data, ensuring privacy without exposing actual data values. Wei *et al.* (2022) combine blockchain with traditional cryptographic techniques for secure data access management. Özyilmaz *et al.* (2018) feature cryptographic voting protocols in a blockchain-based, trustless environment, enhancing security and transparency in IoT data marketplaces. Banavathu and Meruva (2023) discuss novel blockchain and cryptographic methods that enhance secure data storage within IoT networks.

- *Proxy-based and Identity-based Encryption Techniques.* These papers discuss cryptographic solutions to ensure trust while facilitating secure, flexible data access and sharing. Wang *et al.* (2023)

establish trust via proxy re-encryption, allowing secure decentralized control over data. Li *et al.* (2024) introduce a proxy-aided identity-based encryption scheme that supports secure data exchange and dynamic access revocation.

- *Secure Data Storage and Integrity.* These works emphasize securing data integrity and safe storage mechanisms, ensuring that data remains protected both at rest and during transactions. Zhang *et al.* (2021) employ data proxy signatures to maintain data integrity and ensure authenticated access in a scalable manner. Fu *et al.* (2018) focus on secure data processing methods to safeguard sensitive information from unauthorized access. Nawaz *et al.* (2020) use blockchain to authenticate data ownership and secure data sharing in edge computing setups.

These papers collectively highlight the evolving landscape of cryptographic techniques in IoT environments. Each method contributes uniquely to enhancing trust, addressing needs ranging from privacy preservation and secure access to robust data integrity and ownership verification.

Trusted execution environments and trust models: Mollah *et al.* (2017) highlight the utilization of Trusted Execution Environments (TEEs) in edge computing scenarios to establish secure data sharing and searching mechanisms. The paper's trust model is predicated on the assumption that edge servers are semi-trusted. By leveraging TEEs, it aims to enhance security in edge computing by ensuring that data operations, even on semi-trusted servers, are performed in a secure manner that isolates them from other processes and potential threats. The trust model articulated in this study offers a robust framework for IoT environments, where the integrity and confidentiality of data must be managed with utmost diligence due to the semi-trusted nature of peripheral computing resources. This model effectively mitigates potential vulnerabilities inherent in edge computing architectures, providing a dependable and secure mechanism for data handling.

Other trust mechanisms go beyond the conventional use of blockchain, encryption, and trusted execution environments. These mecha-

nisms offer approaches to ensuring data integrity, privacy, and secure access in various application domains:

- *Identity and Access Management.* Preuveneers and Joosen (2019) implement identity management strategies to strengthen trust among interacting entities by ensuring that only authorized users can access certain data based on predefined policies.
- *Transparency and Traceability.* Pham *et al.* (2019) introduce transparency and traceability mechanisms that are critical for maintaining public trust and verifying the integrity of shared data.
- *Dynamic and Decentralized Control Systems.* These systems describe adaptive and decentralized frameworks that respond to changing conditions and requirements, ensuring secure and efficient data management. Nguyen *et al.* (2022) implement dynamic contracts that adapt to situational changes for tailored data sharing. Shang *et al.* (2022) establish trust through the implementation of a decentralized infrastructure that supports secure and reliable data sharing in microgrid applications. Dwivedi *et al.* (2019) ensure trust through decentralized control and proof of authority. They employ proof of authority and public key infrastructure to ensure only authorized devices and users can access and participate in the network, maintaining trust among participants.

We note that in practice, Edge servers can be powerful.[2] Edge-focused IoT data sharing leverages Edge computing power, which is nowadays powerful enough to employ different cryptography algorithms as well as other trust mechanisms. Our systematic survey has revealed a rich tapestry of trust mechanisms enhancing security and data integrity across various IoT applications. We categorized the trust mechanisms into four main areas: blockchain technology, encryption and cryptographic techniques, trusted execution environments, and other innovative trust mechanisms. Blockchain technology is predominantly

[2] https://www.ibm.com/docs/en/cloud-private/3.2.0?topic=servers-preparing-install-edge-computing

utilized to provide immutable records and decentralized control, enhancing transparency and accountability. Encryption and cryptographic techniques, including homomorphic encryption and proxy re-encryption, are critical in securing data confidentiality and integrity. Trusted execution environments focus on secure data operations on semi-trusted platforms, ensuring data processing is isolated from potential threats. Lastly, other trust mechanisms, such as policy-based access control and dynamic policy enforcement, play vital roles in managing access, ensuring data integrity, and adapting security measures to context-specific needs. Collectively, these mechanisms address diverse challenges in IoT environments, providing robust frameworks to foster trust among stakeholders and facilitate secure data exchanges.

Privacy

A review of literature demonstrates a strong focus on the use of encryption, anonymisation, and secure blockchain technology to address privacy concerns in various contexts. The key methodologies and technologies employed to enhance privacy, as extracted from recent literature is the following:

Anonymization, encryption and access control: Griggs *et al.* (2018) utilizes a traditional privacy technique, anonymisation, to anonymous addresses before sharing the data to protect patient identity. Özyilmaz *et al.* (2018) anonymize and encrypt the data before sharing, while Fu *et al.* (2018) emphasize encryption at edge servers and before outsourcing to the cloud server, to preserve privacy before it is stored on the cloud, ensure protection against unauthorized access and "honest-but-curious" cloud servers. Approaches by Xu *et al.* (2019), Zhang *et al.* (2021), and Shang *et al.* (2022) delve into advanced and sophisticated encryption algorithms like Hierarchical Attribute-Based Encryption (HABE), homomorphic encryption, and elliptic curve cryptography (ECC), emphasizing the confidentiality of shared data. Jeoung *et al.* (2022) mention attribute-based encryption and the ABAC model for maintaining privacy by ensuring that only users with specific attributes can access certain data, reflecting the GDPR's data minimization and access control provisions.

Distributed ledger: Several studies (e.g., Dorri *et al.*, 2017; Sarabia-Jácome *et al.*, 2019; Mayer *et al.*, 2021) introduce blockchain technology to enhance privacy through decentralized control, secure communications, and strict access controls via smart contracts, ensuring compliance with GDPR principles. Dwivedi *et al.* (2019) and Makhdoom *et al.* (2020) propose ring signatures and the division of the blockchain network into channels for enhancing user anonymity and segregating data types for privacy. Nguyen *et al.* (2021) and Li *et al.* (2023) highlight the role of DLT and edge computing in preserving privacy by keeping data close to the source and processing data locally to maintain confidentiality. Isaja *et al.* (2023) argues that permissioned DLT significantly boosts privacy through cryptographic methods and ensure stakeholders' pseudonymity by dissociating their sensitive information from their Process/Product/Data (PPD) hallmarks on the ledger.

Zero-Knowledge Proofs (ZKP): Zichichi *et al.* (2020) focus on distributed key management systems and ZKPs to guarantee privacy without disclosing data or access policies, adhering to GDPR's requirements for confidentiality and transparency. The permissioned DLT in Isaja *et al.* (2023) also supports zero-knowledge proofs to confirm the accuracy of PPD hallmarks without disclosing underlying data, enabling privacy-preserving protocols.

Privacy-enhancing technologies (PETs): The studies by Egala *et al.* (2021), Nguyen *et al.* (2021), and Firouzi *et al.* (2022) incorporate privacy-preserving machine learning, anonymous patient records algorithms, and multi-party computations (MPC), considering the balance between regulatory compliance and current market practices. Daidone *et al.* (2022) and Yu *et al.* (2024) showcase the implementation of explicit privacy preferences and off-chain data storage strategies to manage and enforce privacy according to the data owner's stipulations, in line with GDPR's accountability and privacy by design principles.

While the aforementioned privacy-preserving and privacy-enhancing techniques in the literature show promise for enhancing privacy in IoT ecosystems, their implementation in resource-constrained IoT devices presents significant challenges. IoT devices often operate with limited computational power, memory, and energy resources, making it difficult to support complex and computationally intensive advanced encryption

algorithms and maintain large distributed ledgers in real world IoT environments. For instance, implementing advanced encryption algorithms (such as homomorphic encryption or MPC) or zero-knowledge proofs often requires heavy computational resources, which may not be available on low-end IoT sensors or actuators. In addition, network limitations, such as limited bandwidth and intermittent connectivity, can further impede the efficient implementation of PETs and real-time privacy-preserving data processing. Furthermore, in IoT networks where real-time data processing is crucial, the latency introduced by PETs can be detrimental to both performance and real-time privacy protections. The heterogeneity of IoT devices across large-scale deployments also complicates the standardization of privacy-preserving techniques across diverse IoT ecosystems, challenging the maintenance of efficient and consistent privacy measures. Collectively, these constraints underscore the need for lightweight, efficient privacy-preserving techniques tailored specifically for IoT, balancing robust data protection with the practical limitations of IoT hardware as well as heterogeneity of IoT environments.

5.2.3 Answering RQ2.3 - In which IoT layers data is being shared, managed, and governed, and how do standards support Edge-focused secure data sharing?

Layers in which data is being shared

As discussed before, IoT data sharing solutions are often composed of multiple nodes possibly deployed across the whole computing continuum. Regarding the infrastructure layers in which the data is shared, we found that most of them are located at the Cloud and Edge layers, and often as a combination of these two layers (e.g., Kang *et al.*, 2019, Sarabia-Jácome *et al.*, 2019, Tang *et al.*, 2019). Not only does the data circulate between these two layers, but these are also privileged for data storage (e.g., Sharma *et al.*, 2024). In most cases, Cloud is used to store historical data in decentralized storage solutions with the objective to facilitate the creation of cloud-based applications. When only Cloud infrastructure is used to store the data, the Edge and Things layers typically have the same role of gathering and forwarding the data to the Cloud (e.g., Nguyen *et al.*, 2021).

Several approaches also use the Edge layer to store data in a decentralized manner, for instance using blockchains (e.g., Tang *et al.*, 2019, Isaja *et al.*, 2023, Sengupta *et al.*, 2023, Guan *et al.*, 2023). When both the Edge and Cloud layers are used to store data, we noticed two main approaches : (i) the same data storage mechanism (e.g., blockchain) is used across the layers or (ii) different mechanisms and data are stored in the layers, for instance, in Sharma *et al.* (2024), the data is stored at the Edge and Cloud layers with different purpose (data is shared at multiple layers, including a blockchain layer for recording transactions and an off-chain database for storing sensitive patient data such as EHRs and sensor information). We also noticed that for most of the approaches, the Thing layer is only used to collect and publish data to the other two layers. Finally, in some limited cases, the Edge layer is not exploited and data is directly transmitted from Things to the Cloud.

Regarding the location of the mechanisms for secure data sharing, considering the IoT world Forum, most of them are located at the network and application layers as depicted in Figure 5.7. This is probably due to the limited computing resources available at the perception layer (i.e., typically the things). Nevertheless, some approaches also provide solutions at the Perception layer, such as end-to-end encryption (Li *et al.*, 2024).

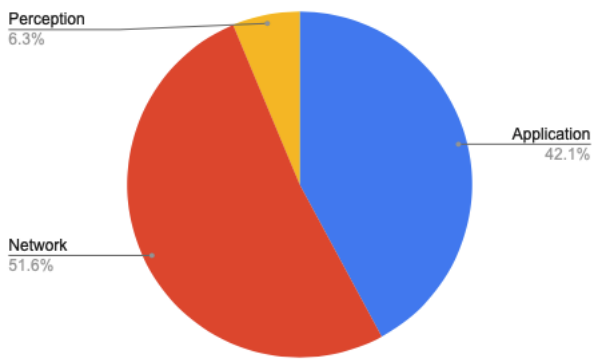

Figure 5.7: Location of the solutions for secure data sharing according to the IoT World Forum layers

- **Data Management and Governance:**

  The literature reviewed illustrates a trend toward data management and governance frameworks that prioritize security, user control, and compliance with regulatory requirements.

  Proactive data management and governance tools: Solutions such as Distributed Identity Management (DIM) by Firouzi *et al.* (2022), decentralized oracles for smart contracts by Manoj *et al.* (2023), and the use of decentralized autonomous organizations (DAOs) by Li *et al.* (2023) represent innovative data management governance technologies that empower users while ensuring secure and transparent data handling. The EdgeMediChain model presented by Akkaoui *et al.* (2020) and the BI-FERH framework by Guan *et al.* (2023), showcase specialized architectures that address the unique requirements of data governance in health data management and IoT devices, respectively.

  Decentralized data management: Research by Sarabia-Jácome *et al.* (2019), Dwivedi *et al.* (2019), and Shang *et al.* (2022) focus on decentralization of data management, advocating for structures that allow data to be governed at the source. This methodology supports efficient and collaborative governance across various platforms, as seen in the architecture proposed by Akkaoui *et al.* (2020). In addition, decentralized storage systems are proposed in Egala *et al.* (2021) and Cheikhrouhou *et al.* (2023), which enhances data management by distributing data across secure networks, which mitigates the risk of centralized data breaches.

  Multi-layered governance: Fog Computing layer leverages local data processing and storage, thus keeping sensitive information closer to the edge and minimizing exposure to centralized vulnerabilities. Research by Mayer *et al.* (2021) and Nguyen *et al.* (2021) employs multi-layered governance approaches, utilizing cloud computing, fog computing, and edge computing to keep data secure, localized, and in compliance with governance policies.

  Blockchain and smart contract based data management and governance: Several studies, such as Dorri *et al.* (2017), Özyilmaz

et al. (2018), and Mayer *et al.* (2021), leverage blockchain and smart contracts. These technologies provide decentralized, transparent, and secure frameworks for data management, emphasizing the enforceability of governance policies and user-defined access controls.

- **Standardization:**

  To our surprise, very few primary studies have made use of standardization efforts such as IDSA's reference architecture. While none of the selected primary studies mention GAIA-X, there are only two primary studies (Gimenez *et al.*, 2020; Sarabia-Jácome *et al.*, 2019) that present the IoT data sharing approaches using IDSA's architecture in the seaport sector. Gimenez *et al.* (2020) show how their INTER-IoT solution facilitates secure and robust data exchange among diverse stakeholders within the port community, presenting INTER-IoT as an economical and user-friendly solution suitable for both stakeholders and systems integrators. Sarabia-Jácome *et al.* (2019) present a seaport dataspace to enable data sharing between different stakeholders in a secure and interoperable manner. Implementing IDS Connectors in combination with the FIWARE IoT platform, data is not shared as it, but processing (data cleaning, filtering, aggregation) can be carried out on the edge before sharing.

  ISO 8000[3] is a standard that provides approaches for managing, measuring, and improving the quality of data and information. However, none of the selected primary studies included inputs from ISO 8000, or other relevant data quality frameworks, demonstrating a lack of data quality management in the context of IoT data sharing.

5.3 Gaps and Limitations (RQ3)

This section discusses our findings to answer RQ3. Throughout this study, we have identified some limitations and gaps that are worth mentioning.

[3] https://www.iso.org/obp/ui/#iso:std:iso:8000:-61:ed-1:v1:en

IoT data sharing challenges often come with the heterogeneity nature of IoT. As IoT technology makes every digital asset more connected than ever over to the Internet, it also implies the existence of a wide range of links from devices to multiple points such as endpoint devices, applications and cloud platforms (Medium, 2024). More specifically, the studies show that the limitation occurs when the incidence of combinations and adding of different technologies could lead to the growth of complexity.

Regarding the location of the secure data sharing mechanisms, we observed first that several approaches are still not fully exploiting the potential of the Cloud-Edge continuum. In these approaches, data is collected by sensors at the Things layer and directly sent to the Cloud. Whilst not exploiting all of the benefits offered by Edge computing, the adoption of such architecture might be driven by the reduced maintenance effort they require. We also noticed that for most of the approaches, the Thing layer is only used to collect and publish data to the other two layers. More effort should be put on securing this layer as it is essentially composed of devices deployed on the field, which can be potentially physically accessible to malicious behaviors.

Viewing the security aspects in a broad perspective, one clear limitation we see is that the industry and smart city domains are lagging behind the healthcare and the general approaches when it comes to considering and implementing security aspects. However, one could argue that the domain independent approaches could also enhance the security in the industrial and smart city applications, but this is not an assumption that can be taken given the reviewed literature.

It is of course promising that the approaches for the healthcare domain are addressing all of the security aspects described in previous sections, considering that this is a critical societal infrastructure and that sensitive personal data is processed. In the worst case, life may be at stake if security is not properly addressed. However, in practice, the healthcare domain is actually struggling to implement security by design, ensure secure connections and assess the security during operations; especially in the context of connected medical devices.[4]

[4] https://ceur-ws.org/Vol-3674/RP-paper6.pdf

The exploration of trust mechanisms in IoT data sharing reveals a multifaceted approach to addressing security concerns across different layers and domains of IoT infrastructure. The diversity in trust mechanisms—from blockchain and cryptographic solutions to trusted execution environments —underscores the complexity and necessity of adopting multi-layered security strategies in IoT ecosystems. While blockchain offers a robust platform for transparency and decentralized control, cryptographic techniques ensure the confidentiality and integrity of data. On the other hand, trusted execution environments provide secure processing capabilities in semi-trusted or potentially hostile environments, enhancing the security perimeter around sensitive data operations. The emerging trends in utilizing smart contracts and dynamic policies indicate a shift towards more autonomous and adaptive security frameworks that can respond in real time to threats and changing environmental conditions. These findings suggest that integrating these diverse trust mechanisms can lead to more resilient IoT systems. However, the challenge remains in seamlessly integrating these technologies to balance security, efficiency, and usability without compromising the performance of IoT systems. As IoT networks expand and become more ingrained in critical infrastructure, the need for comprehensive and interoperable security solutions becomes increasingly paramount.

While existing literature demonstrates a growing awareness of privacy concerns in IoT data sharing as well as emerging PETs to fulfil regulatory requirements (such as GDPR), there remains a lack of empirical evidence in terms of scalability and efficiency, particularly in real-world IoT settings where resources are constrained.

The reviewed literature indicates a promising trend towards integrating privacy-by-design principles into IoT data sharing architectures, as evidenced by the increasing use of PETs such as encryption, anonymization, and blockchain technology. However, the challenge of ensuring ongoing compliance with evolving regulatory framework (such as GDPR, Digital Service Act, EU AI act) requires continued research and adaptation of these technologies to balance the data utility and individual's privacy.

Last but not least, another significant gap in the existing IoT data sharing approaches that we identified and analyzed is the insufficient utilization of standardization efforts such as IDSA's reference architecture, or ISO 8000 regarding data quality. Even though IDSA only released a stable version of the Dataspace Protocol recently, the IDS reference architecture model has been available for many years and going to become version 5, which is aligned with the latest developments in the Dataspace protocol. On the other hand, data quality is a crucial yet often overlooked aspect of IoT. However, enhancing data quality in these systems remains challenging and warrants special attention. Prior to sharing data, it is essential to detect and manage potential quality issues such as erroneous values, missing data, noise, and data drift, which can occur at various stages of data collection and processing. Additionally, maintaining data continuity across the edge-cloud continuum is vital. ISO 8000, the global standard for Data Quality and Enterprise Master Data, should be used in many data sharing solutions where data quality is crucial. To make the IoT data sharing approaches more practical and usable by industry, it is key to leverage such standards as part of the foundation for future research work in this topic.

6

Threats to Validity

Our systematic literature review spans various approaches and domains. The review process incorporates both automated (e.g., search queries) and manual (e.g., data extraction) components. Consequently, it is conceivable that some pertinent studies and information may have eluded our review. In this section, we outline several measures adopted to address this potential limitation.

6.1 Internal Validity

Search Queries. One potential challenge in conducting an SLR pertains to the precision of the search process, specifically concerning the choice of keywords and queries. The query used is a crucial aspect that substantiates the study's validity and outlines its limitations since an extensive array of possible keywords exist for inclusion in the search query. To justify our selection of the search query, we performed a test case to identify a selection of high-quality test papers deemed pertinent to our research objectives. These test papers served as benchmarks to assess the effectiveness of our search query results. When the results from the electronic database X encompass all the test papers published by X, it signifies that the other papers within the results possess rele-

vance. In contrast, an absence of these test papers may indicate a higher degree of extraneous data (commonly known as "noise") in our search results.

Study Inclusion and Exclusion. An additional concern in our study pertains to the selection of primary studies. Even though the studies included, having met our predefined criteria and aligning with our predefined taxonomy, are considered relevant, a degree of uncertainty may persist. It is plausible that some studies eluded our notice, or we inadvertently omitted publications during our search phase. For example, "edge/fog computing" could be some keywords to be included in our search string, even though IoT and "Internet of Things" are already part of the search string and normally cover the papers that mention edge/fog computing. To mitigate this risk, we executed cross-validation procedures involving a minimum of two authors and subsequently engaged in group discussions to identify and eliminate papers that did not meet the stipulated scientific contribution criteria in accordance with our selection standards.

Data Extraction. The risk in data extraction lies in the possibility of errors, inconsistencies, or missing information during the process, which can undermine the quality and reliability of the study's findings. To mitigate this risk effectively, we ensured clear data extraction guidelines (what data points should be collected, the format for recording them, and instructions for handling different types of data), utilized multiple reviewers, and conducted inter-reviewer checks (reviewers compared their findings and resolved any disparities or uncertainties through discussion and reference to the extraction guidelines).

6.2 External Validity

The online repositories we use in an SLR can restrict our review results in several ways, such as size and depth (smaller repositories may have limited coverage, potentially missing out on critical studies), domain specificity (some online repositories are specialized and may primarily contain literature from specific domains), and search features (some online repositories may have limited search functionalities). To mitigate this risk, we selected repositories that are renowned for hosting studies

featured in prominent academic publications and have a history of being extensively utilized in prior survey papers.

6.3 Reliability Validity

Replicating our SLR study is feasible by strictly adhering to the documented procedures we have outlined in our review process. These steps include the systematic selection of primary studies, data extraction, and data synthesis. However, it is essential to acknowledge that despite following the same protocol, there may still be variations in the results obtained by different researchers. This divergence is primarily attributed to the manual aspects of the review process, where human judgment and interpretation come into play. Specifically, data extraction and synthesis often involve subjective decisions made by researchers. Different individuals may interpret and summarize information from primary studies slightly differently, leading to variations in the synthesized findings. As a result, while replication is attainable, there is the possibility of encountering inconsistencies in the outcomes. To mitigate this risk, we maintained transparency in the review process, employed clear data extraction guidelines, and documented our decisions.

7

Related Work

Several surveys in the literature explored existing security threats in the IoT landscape. One of the most prominent studies is the survey conducted in Alaba *et al.* (2017), which provides valuable details on existing security threats in the IoT (at multiple layers). It also describes possible scenarios in which possible attacks are analysed. Open research issues in IoT security in general are described as well. This survey complements our review very well as we more specifically focus on the secure IoT data sharing aspect.

Song *et al.* (2023) provide a survey of blockchain-based data sharing and exchange platforms, highlighting the enhancement of data privacy, security, and trust through decentralized architectures. The use of blockchain is highlighted as a solution for decentralized data storage, exchange access control, identity authentication, and copyright protection, ensuring data integrity and preventing unauthorized access or tampering. While the survey discusses the integration of IoT within the context of blockchain-based data sharing and exchange, it does not specifically address IoT data sharing like in this survey. Thus, our survey complements Song *et al.* (2023) by specifically addressing data sharing within IoT. Similarly, the survey by Sengupta *et al.* (2020),

classifies existing security attacks and focuses on blockchains and how exploiting it in IoT applications can be beneficial. Nevertheless, it does not focus on the specific topic of secure IoT data sharing.

Although Byabazaire *et al.* (2020) does not report a systematic literature review, they discuss challenges in maintaining data quality across different IoT applications and suggest integrating trust-based techniques with blockchain technology for secure, end-to-end data quality assurance. They highlight the role of trust in enhancing data quality for IoT shared data, proposing trust as a novel metric for data quality assessment. The authors emphasize the need for secure data sharing mechanisms to ensure data remains of high quality throughout its life cycle.

Wan *et al.* (2020) report a systematic literature review on blockchain-enabled information sharing within a supply chain. Their study focuses specifically on the impact of blockchain technology on supply chain information sharing, identifying that blockchain ensures verifiability and enhances collaboration among supply chain members. The authors highlight blockchain's potential in various industries, including healthcare and construction, and discuss barriers to blockchain adoption, such as conflict of interest and lack of understanding. The authors suggest that future developments should focus on balancing information sharing and hiding, and emphasize the need for further research on blockchain's practical application and performance evaluation in supply chains.

Dubovitskaya *et al.* (2020) provide a systematic literature review on the application of blockchain technology in oncology for data-sharing. The authors highlight the blockchain's ability to provide transparency, traceability, and immutability, within the domains of primary care, medical research and pharmaceutical supply chain. The authors also note that blockchain alone cannot ensure data privacy and security, and highlight the need for combining blockchain with cryptographic techniques. Their study suggests designing privacy-preserving hybrid data storage and developing interoperable infrastructures compliant with international laws, as future research directions.

While the topic of secure IoT data sharing is becoming more important, it may still be only the end of the beginning. A few existing studies like Lo *et al.* (2019), Al-Ruithe *et al.* (2019), and De Prieëlle

et al. (2020) are relevant to secure IoT data sharing, but none have the scope of our study, nor answer our questions.

Lo *et al.* (2019) elaborate on the issues that data management solutions face, as well as the key issue of single-point-of-failure caused by the use of centralized management servers. Our study and Lo *et al.* (2019) complement each other by pointing out technologies as a solution to the single-point-of-failure, such as blockchain as smart contracts. However, our work further extracted on the architectural layers Rajmohan *et al.* (2022) used for the execution of data sharing, who the stakeholders in different domains are, and why data sharing is of interest to adapt for these stakeholders and domains.

Al-Ruithe *et al.* (2019) present an SLR of data governance and cloud governance in their use of data. They highlight the need for more advanced research in data governance, in addition to suggesting areas for further research within data governance, which can be taken into account when conducting our research. However, they do not go into detail on the implications for IoT data sharing because their main focus is on data and cloud governance.

The necessity of ecosystem data governance for data platforms is discussed by De Prieëlle *et al.* (2020). Future research directions are elaborated, such as the importance of data platform governance in access and usage as a primary concern. They also emphasize that there is a lack of research on the many types of benefits that data sharing generates, which is an important future research direction as well. However, we focus on data sharing as the primary topic, with data governance and its impact on data sharing as a subtopic. Furthermore, they do not address various standards, policies, and guidelines that have been considered.

8

Conclusions

This work disseminates the outcomes of our SLR focus on research pertaining to secure IoT data sharing. The act of securely sharing IoT-generated data assumes a pivotal role in fostering collaborative, well-informed decision-making, driving innovation, and elevating operational efficiencies across a spectrum of industries. The employment of secure IoT data-sharing methodologies empowers organizations to not only safeguard sensitive information but also streamline the exchange of data, thereby harnessing invaluable insights to steer data-driven strategies and applications. The SLR was executed in alignment with established protocols, encompassing the formulation of research questions, development of a comprehensive search strategy, definition of inclusion and exclusion criteria, and the adoption of rigorous data synthesis and extraction techniques.

Our systematic search and selection procedure yielded a total of 94 primary studies published between 2017 and early 2024. The noteworthy increase in the number of studies in recent years underscores a growing interest in secure IoT data sharing research. Our primary objective revolved around the comprehensive analysis of the treatment of secure data sharing within the realm of IoT applications. This entailed

evaluating the efficacy of the proposed secure data sharing techniques in facilitating these applications. Our investigation encompassed an exploration of the reported application domains for IoT data sharing, an examination of the underlying purposes and benefits of data sharing, an assessment of the prevalent threats and vulnerabilities associated with IoT data sharing, a scrutiny of secure IoT data sharing techniques, and an evaluation of the role of data management and governance. To address these facets and respond to three overarching research questions, along with seven sub-questions, we systematically acquired and synthesized data from the selected primary studies. Our SLR leads us to the following conclusions:

1. Secure IoT data sharing is getting more and more attention in the research community. Making IoT data sharing secure is of critical importance in most of the IoT application domains for different purposes.

2. Integrity, confidentiality, and availability are the three most addressed security principles in the Edge-focused primary studies. Integrity and confidentiality are required in domains dealing with sensitive data such as healthcare and industry-related. Especially, integrity is key in primary studies involving critical infrastructures.

3. While existing literature demonstrates a growing awareness of privacy concerns in IoT data sharing as well as emerging PETs to fulfil regulatory requirements (such as GDPR), there remains a lack of empirical evidence in terms of scalability and efficiency, particularly in real-world IoT settings where resources are constrained.

4. The predominant trust mechanisms addressed across the reviewed literature are: (i) *blockchain technology*, (ii) *encryption and cryptography techniques*, (iii) *trusted execution environments and trust models*. Edge-focused IoT data sharing leverages Edge computing power, which is nowadays powerful enough to employ different cryptography algorithms as well as other trust mechanisms.

5. The existing literature has an insufficient utilization of standardization efforts such as IDSA's reference architecture, or ISO 8000 regarding data quality. To make the IoT data sharing approaches more practical and usable by industry, it is key to leverage such standards as part of the foundation for future research work in this topic.

Acknowledgements

The research leading to this publication has partially received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreements 101070455 (DYNABIC) and 101095634 (ENTRUST), the SINTEF's SEP project IDS4Edge, and 338909 (Privacy@Edge) part of the IKTPLUSS program funded by the Research Council of Norway.

References

Abbas, K., L. Tawalbeh, A. Rafiq, A. Muthanna, I. Elgendy, and A. Abd El-Latif. (2021). "Convergence of Blockchain and IoT for secure transportation systems in smart cities. Secur. Commun. Netw. 2021, 1–13 (2021)".

Akkaoui, R., X. Hei, and W. Cheng. (2020). "EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange". *IEEE Access*. 8: 113467–113486. DOI: 10.1109/ACCESS.2020.3003575.

Alaba, F. A., M. Othman, I. A. T. Hashem, and F. Alotaibi. (2017). "Internet of Things security: A survey". *Journal of Network and Computer Applications*. 88: 10–28.

Alshehri, S., O. Bamasaq, D. Alghazzawi, and A. Jamjoom. (2023). "Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IoT Environment". *IEEE Internet of Things Journal*. 10(5): 4239–4256. DOI: 10.1109/JIOT.2022.3217087.

Association, I. D. S. (2024). "Reference Architecture Model". URL: https://internationaldataspaces.org/wp-content/uploads/IDS-RAM-3.0-2019.pdf.

Bai, L., M. Hu, M. Liu, and J. Wang. (2019). "BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT". *IEEE Access*. 7: 58381–58393. DOI: 10.1109/ACCESS.2019.2914223.

Banavathu, R. and S. Meruva. (2023). "Efficient secure data storage based on novel blockchain model over IoT-based smart computing systems". *Measurement: Sensors*. 27: 100741. DOI: https://doi.org/10.1016/j.measen.2023.100741.

Byabazaire, J., G. O'Hare, and D. Delaney. (2020). "Data Quality and Trust: Review of Challenges and Opportunities for Data Sharing in IoT". *Electronics*. 9(12). DOI: 10.3390/electronics9122083.

Cheikhrouhou, O., K. Mershad, F. Jamil, R. Mahmud, A. Koubaa, and S. R. Moosavi. (2023). "A lightweight blockchain and fog-enabled secure remote patient monitoring system". *Internet of Things*. 22: 100691. DOI: https://doi.org/10.1016/j.iot.2023.100691.

Cisco. (2024). "Fast Innovation require Fast IT". URL: https://www.cisco.com/c/dam/global/en_ph/assets/ciscoconnect/pdf/bigdata/jim_green_cisco_connect.pdf.

Daidone, F., B. Carminati, and E. Ferrari. (2022). "Blockchain-Based Privacy Enforcement in the IoT Domain". *IEEE Transactions on Dependable and Secure Computing*. 19(6): 3887–3898. DOI: 10.1109/TDSC.2021.3110181.

De Prieëlle, F., M. De Reuver, and J. Rezaei. (2020). "The Role of Ecosystem Data Governance in Adoption of Data Platforms by Internet-of-Things Data Providers: Case of Dutch Horticulture Industry". *IEEE Transactions on Engineering Management*: 1–11.

Dorri, A., S. S. Kanhere, R. Jurdak, and P. Gauravaram. (2017). "Blockchain for IoT security and privacy: The case study of a smart home". In: *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. 618–623. DOI: 10.1109/PERCOMW.2017.7917634.

Dubovitskaya, A., P. Novotny, Z. Xu, and F. Wang. (2020). "Applications of blockchain technology for data-sharing in oncology: Results from a systematic literature review". *Oncology*. 98(6): 403–411. DOI: 10.1159/000504325.

Dwivedi, A. D., G. Srivastava, S. Dhar, and R. Singh. (2019). "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT". *Sensors*. 19(2). DOI: 10.3390/s19020326.

Egala, B. S., A. K. Pradhan, V. Badarla, and S. P. Mohanty. (2021). "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control". *IEEE Internet of Things Journal*. 8(14): 11717–11731. DOI: 10.1109/JIOT.2021.3058946.

Firouzi, F., B. Farahani, M. Barzegari, and M. Daneshmand. (2022). "AI-Driven Data Monetization: The Other Face of Data in IoT-Based Smart and Connected Health". *IEEE Internet of Things Journal*. 9(8): 5581–5599. DOI: 10.1109/JIOT.2020.3027971.

Fu, J.-S., Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang. (2018). "Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing". *IEEE Transactions on Industrial Informatics*. 14(10): 4519–4528. DOI: 10.1109/TII.2018.2793350.

Gaia-X. (2024). "Gaia-X: A Federated Data Infrastructure for Europe". URL: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

Gimenez, P., M. Llop, E. Olivares, C. Palau, M. Montesinos, and M. Llorente. (2020). "Interoperability of IoT platforms in the port sector". *Proceedings of 8th Transport Research Arena TRA*: 27–30.

Goknil, A., P. Nguyen, S. Sen, D. Politaki, H. Niavis, K. J. Pedersen, A. Suyuthi, A. Anand, and A. Ziegenbein. (2023). "A Systematic Review of Data Quality in CPS and IoT for Industry 4.0". *ACM Computing Surveys*.

Griggs, K. N., O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh. (2018). "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring". *Journal of medical systems*. 42: 1–7.

Grossetete, P. (2018). "IoT and the Network: What is the future?" Cisco. URL: https://blogs.cisco.com/networking/iot-and-the-network-what-is-the-future.

Guan, Q., J. Lei, C. Wang, G. Geng, Y. Zhong, L. Fang, X. Huang, and W. Luo. (2023). "BI-FERH: Blockchain-IoT based framework for securing smart hotel". *Computer Science and Information Systems*. 20(4): 1541–1568.

Hang, L., I. Ullah, and D.-H. Kim. (2020). "A secure fish farm platform based on blockchain for agriculture data integrity". *Computers and Electronics in Agriculture*. 170: 105251. DOI: https://doi.org/10.1016/j.compag.2020.105251.

Hao, X., W. Ren, Y. Fei, T. Zhu, and K.-K. R. Choo. (2023). "A Blockchain-Based Cross-Domain and Autonomous Access Control Scheme for Internet of Things". *IEEE Transactions on Services Computing*. 16(2): 773–786. DOI: 10.1109/TSC.2022.3179727.

IBM. (2024a). "What are smart contracts on blockchain?" URL: https://www.ibm.com/topics/smart-contracts.

IBM. (2024b). "What is blockchain technology?" URL: https://www.ibm.com/topics/what-is-blockchain.

IDSA. (2024a). "IDSA is at the forefront of Europe's digital future". URL: https://internationaldataspaces.org/we/ids-in-europe/.

IDSA. (2024b). "Innovating the future of daa exchange in Europe and beyond". URL: https://internationaldataspaces.org/we/.

Isaja, M., P. Nguyen, A. Goknil, S. Sen, E. J. Husom, S. Tverdal, A. Anand, Y. Jiang, K. J. Pedersen, P. Myrseth, J. Stang, H. Niavis, S. Pfeifhofer, and P. Lamplmair. (2023). "A blockchain-based framework for trusted quality data sharing towards zero-defect manufacturing". *Computers in Industry*. 146: 103853. DOI: https://doi.org/10.1016/j.compind.2023.103853.

Jeoung, J., S. Jung, T. Hong, and J.-K. Choi. (2022). "Blockchain-based IoT system for personalized indoor temperature control". *Automation in Construction*. 140: 104339. DOI: https://doi.org/10.1016/j.autcon.2022.104339.

Kang, J., R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang. (2019). "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks". *IEEE Internet of Things Journal*. 6(3): 4660–4670. DOI: 10.1109/JIOT.2018.2875542.

Kitchenham, B. A. and S. Charters. (2007). "Guidelines for performing Systematic Literature Reviews in Software Engineering". *Tech. rep.* No. EBSE 2007-001. Software Engineering Group. URL: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf.

Li, C., R. Chen, Y. Wang, Q. Xing, and B. Wang. (2024). "REEDS: An Efficient Revocable End-to-End Encrypted Message Distribution System for IoT". *IEEE Transactions on Dependable and Secure Computing*: 1–18. DOI: 10.1109/TDSC.2024.3353811.

Li, Z., J. Zhang, J. Zhang, Y. Zheng, and X. Zong. (2023). "Integrated Edge Computing and Blockchain: A General Medical Data Sharing Framework". *IEEE Transactions on Emerging Topics in Computing*: 1–14. DOI: 10.1109/TETC.2023.3344655.

Lo, S. K., Y. Liu, S. Y. Chia, X. Xu, Q. Lu, L. Zhu, and H. Ning. (2019). "Analysis of Blockchain Solutions for IoT: A Systematic Literature Review". *IEEE Access*: 58822–58835.

Ma, Z., L. Wang, and W. Zhao. (2021). "Blockchain-Driven Trusted Data Sharing With Privacy Protection in IoT Sensor Network". *IEEE Sensors Journal*. 21(22): 25472–25479. DOI: 10.1109/JSEN.2020.3046752.

Makhdoom, I., I. Zhou, M. Abolhasan, J. Lipman, and W. Ni. (2020). "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities". *Computers & Security*. 88: 101653. DOI: https://doi.org/10.1016/j.cose.2019.101653.

Manoj, T., K. Makkithaya, and N. V.G. (2023). "A trusted IoT data sharing and secure oracle based access for agricultural production risk management". *Computers and Electronics in Agriculture*. 204: 107544. DOI: https://doi.org/10.1016/j.compag.2022.107544.

Matsas, M. (2024). "Data Space Radar". URL: https://internationaldataspaces.org/adopt/data-space-radar/.

Mayer, A. H., V. F. Rodrigues, C. A. d. Costa, R. d. R. Righi, A. Roehrs, and R. S. Antunes. (2021). "FogChain: A Fog Computing Architecture Integrating Blockchain and Internet of Things for Personal Health Records". *IEEE Access*. 9: 122723–122737. DOI: 10.1109/ACCESS.2021.3109822.

Medium. (2024). "Manageing Complexity Of IoT Sensors, Endpoints, Gateways, And Network Bottlenecks". Medium.

Mollah, M. B., M. A. K. Azad, and A. Vasilakos. (2017). "Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things". *IEEE Cloud Computing*. 4(1): 34–42. DOI: 10.1109/MCC.2017.9.

Nawaz, A., J. Peña Queralta, J. Guan, M. Awais, T. N. Gia, A. K. Bashir, H. Kan, and T. Westerlund. (2020). "Edge Computing to Secure IoT Data Ownership and Trade with the Ethereum Blockchain". *Sensors*. 20(14). DOI: 10.3390/s20143965.

Nguyen, D. C., P. N. Pathirana, M. Ding, and A. Seneviratne. (2021). "A Cooperative Architecture of Data Offloading and Sharing for Smart Healthcare with Blockchain". In: *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 1–8. DOI: 10.1109/ICBC51069.2021.9461063.

Nguyen, H.-H., P. H. Phung, P. H. Nguyen, and H.-L. Truong. (2022). "Context-driven Policies Enforcement for Edge-based IoT Data Sharing-as-a-Service". In: *2022 IEEE International Conference on Services Computing (SCC)*. 221–230. DOI: 10.1109/SCC55611.2022.00041.

Oracle. (2024). "What Is Data Management?" URL: https://www.oracle.com/database/what-is-data-management/.

Özyilmaz, K. R., M. Doğan, and A. Yurdakul. (2018). "IDMoB: IoT Data Marketplace on Blockchain". In: *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. 11–19. DOI: 10.1109/CVCBT.2018.00007.

Patel, H. and B. Shrimali. (2023). "AgriOnBlock: Secured data harvesting for agriculture sector using blockchain technology". *ICT Express*. 9(2): 150–159. DOI: https://doi.org/10.1016/j.icte.2021.07.003.

Petersen, K., S. Vakkalanka, and L. Kuzniarz. (2015). "Guidelines for conducting systematic mapping studies in software engineering: An update". *Information and Software Technology*. 64: 1–18.

Pham, H.-A., T.-K. Le, T.-N.-M. Pham, H.-Q.-T. Nguyen, and T.-V. Le. (2019). "Enhanced Security of IoT Data Sharing Management by Smart Contracts and Blockchain". In: *2019 19th International Symposium on Communications and Information Technologies (ISCIT)*. 398–403. DOI: 10.1109/ISCIT.2019.8905219.

Preuveneers, D. and W. Joosen. (2019). "Towards Multi-party Policy-based Access Control in Federations of Cloud and Edge Microservices". In: *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 29–38. DOI: 10.1109/EuroSPW.2019.00010.

Rajmohan, T., P. H. Nguyen, and N. Ferry. (2022). "A decade of research on patterns and architectures for IoT security". *Cybersecurity*. 5(1): 1–29.

Al-Ruithe, M., E. Benkhelifa, and K. Hameed. (2019). "A systematic literature review of data governance and cloud data governance". *Personal and Ubiquitous Computing*.

Samuel, O., A. B. Omojo, S. M. Mohsin, P. Tiwari, D. Gupta, and S. S. Band. (2023). "An Anonymous IoT-Based E-Health Monitoring System Using Blockchain Technology". *IEEE Systems Journal*. 17(2): 2422–2433. DOI: 10.1109/JSYST.2022.3170406.

Sarabia-Jácome, D., I. Lacalle, C. E. Palau, and M. Esteve. (2019). "Enabling Industrial Data Space Architecture for Seaport Scenario". In: *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. 101–106. DOI: 10.1109/WF-IoT.2019.8767216.

Seiner, R. S. (2024). "Data Governance and the Internet of Things". URL: https://www.slideshare.net/Dataversity/data-governance-and-the-internet-of-things.

Sengupta, J., S. Ruj, and S. D. Bit. (2020). "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT". *Journal of network and computer applications*. 149: 102481.

Sengupta, J., S. Ruj, and S. Das Bit. (2023). "FairShare: Blockchain Enabled Fair, Accountable and Secure Data Sharing for Industrial IoT". *IEEE Transactions on Network and Service Management*. 20(3): 2929–2941. DOI: 10.1109/TNSM.2023.3239832.

Shang, J., R. Guan, Y. Tong, *et al.* (2022). "Microgrid data security sharing method based on blockchain under Internet of Things architecture". *Wireless Communications and Mobile Computing*. 2022.

Sharma, A., S. Kaur, and M. Singh. (2024). "A secure blockchain framework for the internet of medical things". *Transactions on Emerging Telecommunications Technologies*. 35(1): e4917. DOI: https://doi.org/10.1002/ett.4917.

Singh, P., M. Masud, M. S. Hossain, and A. Kaur. (2021). "Cross-domain secure data sharing using blockchain for industrial IoT". *Journal of Parallel and Distributed Computing*. 156: 176–184. DOI: https://doi.org/10.1016/j.jpdc.2021.05.007.

Song, R., B. Xiao, Y. Song, S. Guo, and Y. Yang. (2023). "A Survey of Blockchain-Based Schemes for Data Sharing and Exchange". *IEEE Transactions on Big Data*. 9(6): 1477–1495. DOI: 10.1109/TBDATA.2023.3293279.

Tang, B., H. Kang, J. Fan, Q. Li, and R. Sandhu. (2019). "IoT Passport: A Blockchain-Based Trust Framework for Collaborative Internet-of-Things". In: *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies. SACMAT '19*. Toronto ON, Canada: Association for Computing Machinery. 83–92. DOI: 10.1145/3322431.3326327.

Tran, T., P. Nguyen., and G. Erdogan. (2023). "A Systematic Review of Secure IoT Data Sharing". In: *Proceedings of the 9th International Conference on Information Systems Security and Privacy - ICISSP*. INSTICC. SciTePress. 95–105. DOI: 10.5220/0011674200003405.

Umran, S. M., S. Lu, Z. A. Abduljabbar, and V. O. Nyangaresi. (2023). "Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry". *Internet of Things*. 24: 100969. DOI: https://doi.org/10.1016/j.iot.2023.100969.

Ur Rahman, M., F. Baiardi, and L. Ricci. (2020). "Blockchain Smart Contract for Scalable Data Sharing in IoT: A Case Study of Smart Agriculture". In: *2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)*. 1–7. DOI: 10.1109/GCAIoT51063.2020.9345874.

Wan, P. K., L. Huang, and H. Holtskog. (2020). "Blockchain-Enabled Information Sharing Within a Supply Chain: A Systematic Literature Review". *IEEE Access*. 8: 49645–49656. DOI: 10.1109/ACCESS.2020.2980142.

Wang, F., J. Cui, Q. Zhang, D. He, C. Gu, and H. Zhong. (2023). "Lightweight and Secure Data Sharing Based On Proxy Re-Encryption for Blockchain-Enabled Industrial Internet of Things". *IEEE Internet of Things Journal*: 1–1. DOI: 10.1109/JIOT.2023.3340567.

Wei, X., Y. Yan, S. Guo, X. Qiu, and F. Qi. (2022). "Secure Data Sharing: Blockchain-Enabled Data Access Control Framework for IoT". *IEEE Internet of Things Journal*. 9(11): 8143–8153. DOI: 10.1109/JIOT.2021.3111012.

Wohlin, C. (2014). "Guidelines for snowballing in systematic literature studies and a replication in software engineering". In: *EASE'14*. 38.

Xu, R., S. Y. Nikouei, Y. Chen, E. Blasch, and A. Aved. (2019). "BlendMAS: A Blockchain-Enabled Decentralized Microservices Architecture for Smart Public Safety". In: *2019 IEEE International Conference on Blockchain (Blockchain)*. 564–571. DOI: 10.1109/Blockchain.2019.00082.

Yu, J., B. Yan, H. Qi, S. Wang, and W. Cheng. (2024). "An Efficient and Secure Data Sharing Scheme for Edge-Enabled IoT". *IEEE Transactions on Computers*. 73(1): 178–191. DOI: 10.1109/TC.2023.3325668.

Zaabar, B., O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid. (2021). "HealthBlock: A secure blockchain-based healthcare data management system". *Computer Networks*. 200: 108500. DOI: https://doi.org/10.1016/j.comnet.2021.108500.

Al-Zahrani, F. A. (2020). "Subscription-Based Data-Sharing Model Using Blockchain and Data as a Service". *IEEE Access*. 8: 115966–115981. DOI: 10.1109/ACCESS.2020.3002823.

Zhang, L., M. Peng, W. Wang, Z. Jin, Y. Su, and H. Chen. (2021). "Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing". *Transactions on Emerging Telecommunications Technologies*. 32(10): e4315. DOI: https://doi.org/10.1002/ett.4315.

Zheng, X., S. Sun, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Meré. (2019). "Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies". *J Med Internet Res.* 21(6): e13583. DOI: 10.2196/13583.

Zichichi, M., S. Ferretti, and G. D'angelo. (2020). "A Framework Based on Distributed Ledger Technologies for Data Management and Services in Intelligent Transportation Systems". *IEEE Access.* 8: 100384–100402. DOI: 10.1109/ACCESS.2020.2998012.

Zuo, Y. and Z. Qi. (2022). "A Blockchain-Based IoT Framework for Oil Field Remote Monitoring and Control". *IEEE Access.* 10: 2497–2514. DOI: 10.1109/ACCESS.2021.3139582.