A Systematic Literature Review on Secure IoT Data Sharing

Thesis submitted in partial fulfillment of the requirements for the degree of
Master of Theoretical Computer Science
to the The Faculty of Mathematics and Natural Sciences,
at the University of Oslo.

Thanh Thao Thi Tran
Programming & Software Engineering
Department of Informatics, University of Oslo

Supervisors:
Phu NGUYEN
Gencer ERDOGAN
Ketil STØLEN

May 16, 2022

"It has become appallingly obvious that our technology has exceeded our humanity."

Albert Einstein

Abstract

Context: The Internet of Things (IoT) is a popular and rapidly expanding concept. The general contextual motivation is that greater values of the IoT can be realized by enabling IoT data sharing between different stakeholders. However, one of the biggest obstacles is ensuring security and how to enable trust for IoT data sharing. As the IoT gets more involved and integrated into our everyday lives, we focus on how the system handles secure IoT data sharing.

Objectives: In this project, we aim at identifying existing approaches and techniques in the state-of-the-art (SotA) of secure IoT data sharing.

Method: To conduct a systematic literature review, we employ the most recent and widely used guidelines. In addition, we examine the SotA and the state of practice, then we synthesize the collected data, and finally present and discuss our findings.

Results: The extraction of data has led to a number of findings on our topic. In addition to revealing the most addressed domains, our high-level results and statistical numbers emphasize the publication increase and trends as well. We did, however, obtain more in-depth information on the procedures and methods used to preserve security in the data sharing environment. Using blockchain technology and smart contracts, as well as the InterPlanetary File System (IPFS), a decentralized peer-to-peer storage system, are among them. These and other important discoveries do all contribute to an increase in secure IoT data sharing.

Conclusions: There are several points to consider based on the statistical data and discussion of the outcomes, as today's solutions move away from a centralized strategy and towards a more decentralized approach. Based on our findings, we have identified potential research directions for future work in order to establish the most trustworthy environment for secure IoT data sharing. This might involve the combination of sharing and analytics, with the goal of determining whether receiving already processed data or unprocessed raw data makes a difference to stakeholders in the IoT ecosystem. As the statistics show that blockchain technology is widely employed to establish a decentralized solution, it might be useful to research whether there are any significant variations between the blockchain platforms in what they can contribute or if there are any limitations. To summarize, the journey toward secure IoT data sharing has come a long way, and the security of data sharing will improve as research on the topic keeps growing.

Acknowledgements

First, I would like to start to share my gratitude towards my supervisors, Dr. Phu Nguyen, Dr. Gencer Erdogan, and Professor Ketil Stølen. I could not have done this without your guidance throughout my whole master's. All of the knowledge that has been shared, the discussions, and the kind words you have been giving me, when I have been needing a kick of motivation.

Furthermore, I am extremely grateful for all of the support I have gotten from my whole family; their continuous love has been my fuel, especially in the times where I have needed it the most, but also for the nutritious food that they have been providing me when the study hours have been long.

Finally, I am more than thankful for my handful of very good friends at the Department of Informatics; all of our small talks, breaks, and laughs throughout an intense period of time. The support that has been alternated between us, the great feeling of having each other's backs, and the urge of wanting to see each other succeed.

Thanh Thao Thi Tran

Oslo, May 2022

Contents

List of Figures

List of Tables

Acronyms

EC Exclusion Criteria.

GDPR General Data Protection Regulation.

IC Inclusion Criteria.

IDSA International Data Spaces Association.

IoT Internet of Things.

ISO International Organization for Standardization.

OWASP Open Web Application Security Project.

SLR Systematic Literature Review.

SMS Systematic Mapping Study.

SotA state-of-the-art.

Chapter 1

Introduction

This chapter introduces the topic of our study in Section 1.1 by focusing on the significance of the IoT, security and privacy. Furthermore, we go through the project goals for our research on secure IoT data sharing in Section 1.2 before presenting the goal of our study in Section 1.3. Finally, in Section 1.4, we present the structure of the remainder of this thesis.

1.1 Introduction

In recent years, the technology behind the IoT has evolved, making it a far more appealing technology to employ in most systems. The IoT concept has been rapidly adopted and used in smart automobiles, smart houses, smart grids, smart industries and manufacturing. With billions of IoT devices currently connected to the Internet, Cisco expects that 75 billion connected IoT devices will be available in the IoT market by 2025 [1].

IoT refers to all physical devices connected to the Internet for the purpose of collecting and exchanging data all over the world. With these great features in mind, the structure of such systems can, on the other hand, be more complex than what is being expressed. The IoT is a complicated system made up of numerous mechanisms and interconnected computing devices that can send data over a network without requiring any human-to-human or human-to-computer interaction. With great help thanks to wireless technology such as WiFi and Bluetooth, it is now, more than ever, much easier for gadgets to become smarter and more connected.

As the IoT continues to generate massive amounts of data, the technology can assist consumers and businesses. For instance, allowing IoT devices to monitor an individual's blood pressure, smart home lightning based on sensors, and faster electricity recovery time after a power disruption. The possibilities that the IoT can bring to the table with this level of digital intelligence are limitless. However, because IoT data sharing brings such great values, various security concerns may occur as a result of enabling IoT data sharing, in many cases expanding attack surfaces.

Mearian [2] illustrates how data with insecure data management can impact our privacy, by referencing when Nissan Leaf automobiles had a telematic system that leaked all of the historical driving data. Nissan Leaf faced privacy concerns due to the possibility of unauthorized access to a car-owner's sensitive data. In the scenario provided by Mearian [2], a malicious actor might simply gain access to the car owner's routines during the week and know when their residences are left empty.

We are now entering a new phase by expanding the use of smart devices in our surroundings. Because we are welcoming a range of smart devices into our lives, it is more vital than ever to understand the different aspects of these devices and their connectivity. In particular, security and privacy aspects, as well as the potential consequences and drawbacks we might be exposed to. Therefore, we need to gain an understanding of how IoT data is shared nowadays, including how our sensitive and personal data is being retrieved, accessed, stored, and processed, as well as to study the power and influence of data management and governance.

1.1.1 The Importance of the IoT

In recent years, the IoT has experienced significant expansion and adoption. Figure 1.1 illustrates the substantial movement from non-IoT devices to IoT devices over the last decade. Oracle [3] states that the IoT has become one of the most important technologies of the 21st century. The reasons are due to the possibilities of connecting everyday objects, such as cars, kitchen appliances, and baby monitors, to connecting against the internet, allowing for seamless communication between processes, people, and things.

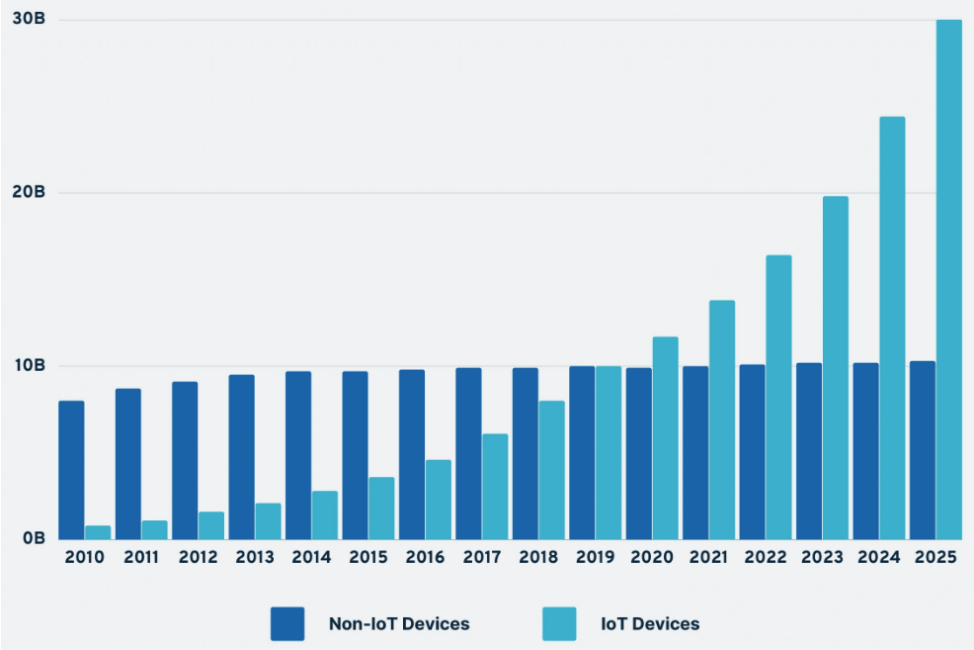

FIGURE 1.1: The growth of the IoT in recent years and the prediction of its growth in upcoming years (retrieved from [4])

With the importance of the IoT and its connectivity capabilities, it is predicted and expected that the trend, growth, and importance of the IoT will continue to increase and expand into different domains and topics in the future [4]. This would thereby imply an increase in people's quality of life as well. The expectation of future increases and expansion of the use of IoT is due to many factors. These factors could be related to the environmental aspects, such as sustainability goals. Amazon has taken the lead in initiating an ask of net-zero carbon emissions by 2040, whereas companies like Mercedes-Benz and Microsoft these days have committed to The Climate Pledge [5]. To achieve such an ambitious goal, companies will need to measure

carbon emissions in coming years. This brings us back to the importance and advantages of the IoT, which can provide measurements as well as effective energy management [6].

The virus COVID-19, which has been a global pandemic since 2019, is another example that has had a big impact in recent years. In addition to the control and statistics of the high case rate, IoT has played a role in appropriately monitoring virus-infected patients [7]. However, with numerous countries experiencing lockdowns, the fear of new lockdowns will only increase and further fuel the importance and expansion of the IoT and its use cases.

1.1.2 The Importance of Security and Privacy for the IoT

Without protection, any connected object can be hacked, demonstrating that security is a critical consideration in the IoT. With billions of connected devices, the attack surface has grown significantly. This was demonstrated in March 2021, when hackers broke into Verkada, a cloud-based video security service [8]. The attackers had access to live footage from a variety of cameras installed in factories, hospitals, jails, and other locations. This attack demonstrates how IoT devices, like network assets, are vulnerable. Because the incident highlighted the importance of security in the IoT, it also raised the issue of privacy. This refers to how surveillance equipment should be used, sensitive data should be maintained, and access to sensitive data should be handled; for example, the privacy of video of patients in hospitals or manufacturing processes in action.

Another incident that demonstrated the significance of IoT security in a very real and significant way was when a Florida water facility was attacked due to a widespread critical infrastructure issue. In February 2021, the threat actor planned to poison the water supply of the Florida city. During the attack, the pointer on a computer screen connected to the water facility began moving on its own, accessing apps that controlled the water levels and supply. The consequences and effects could have been fatal if it had not been for rapid discovery and if the water facility had not responded quickly enough to stabilize the water levels [8].

To prevent these vulnerabilities and attacks from happening, there are a wide range of standards, policies, and guidelines to increase the security and privacy of IoT solutions. Open Web Application Security Project (OWASP) are one of those that lists dangerous risks and threats, which are worth considering when developing web applications. However, they do have a top ten list in regards to IoT security specifically, which is listed in Table 2.1 and elaborated on in Section 2.5 with additional standards, policies, and guidelines relevant to our topic. Although there are many existing standards, policies, and guidelines on what to consider when building these IoT solutions, the elaborated incidents that have occurred in recent years are fundamental factors and reasons to continue research on the topic of IoT and the great value of data sharing, but also to consider its security and privacy aspects as well.

1.2 Motivation

IoT has bloomed in popularity over time as a result of its wide range of use in several fields, including healthcare, education, and industry. The reasons for its rise in

popularity are numerous, ranging from convenience and ease of use, as voice assistants such as Siri and Google Home, to providing efficient alternatives and solutions for Internet connections.

Some of the IoT's greatest value comes from connecting not only "things", but also organizations, customers, suppliers, and any other stakeholders in the IoT's ecosystem, like in smart cities, smart grids, smart industries, and manufacturing. As the IoT evolves and our use of IoT devices grows, it is more critical than ever to guarantee that the devices and systems are secure. Furthermore, data sharing between devices should also ensure, among other things, quality and integrity between stakeholders.

Because the IoT is a continuously evolving topic, it is important to assess the current state-of-the-art addressing the advantages of IoT data sharing, as well as the security considerations that must be taken into account as well. This research can draw the current landscape of approaches for secure IoT data sharing, in addition to what gaps need to be filled, in order to further improve and make the technology of the IoT perform at its optimum in the most secure manner possible.

1.3 Project goals

Because data sharing is a desirable feature of the IoT, a high-level understanding of the components that make up the foundation for secure data sharing is essential. Figure 1.2 illustrates a venn diagram of the Internet of Things, access control, data management, and governance, as well as how they intersect and form a foundation for performing secure IoT data sharing. We conducted a Systematic Literature Review (SLR) in this study, which involved gathering and reviewing all relevant research on secure IoT data sharing. Furthermore, we have extracted a range of data, including what practices and approaches have been used for implementing data sharing, what architecture models are employed, and how the impact of data management and governance is being addressed.

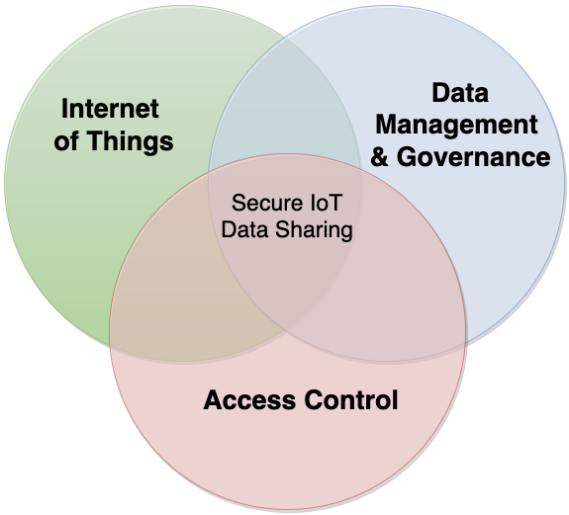

FIGURE 1.2: Venn-diagram of intersection of data sharing, management and governance

The goal of conducting an SLR is to improve our understanding of the topic by identifying the state-of-the-art, as well as the open issues and gaps that need to be

addressed in future studies of secure IoT data sharing. Our review process relies heavily on Research Questions (RQ). These RQs will be utilized and contribute as guidance as we work on specific topics that are crucial and central in the domain of secure IoT data sharing that need to be addressed. The RQs of this thesis are divided into three main research questions. These questions will be used as guidelines during the execution of our SLR. The research questions are defined as follows:

RQ1: What are the solutions for secure IoT data sharing?

This research question provides a global introduction and overview of today's IoT data sharing solutions. The introduction is carried out by addressing the growing interest in the domain, in terms of publications and domain trends, as well to the purpose and benefits from both the general point of view, as well as the domain specific point of view. We also provide a high-level overview of the most utilized data sharing models.

RQ2: What are the security and trust aspects of these IoT data sharing approaches?

After providing a high-level overview on the topic from RQ1, we further continue to a more detailed aspect of IoT data sharing, in regards to the security and trust aspects. This research question is addressing the most common threats and vulnerabilities of IoT data sharing that should be considered. Furthermore, we investigate today's solutions on data sharing and how they preserve security in terms of mechanisms and approaches that are utilized. We also take into account contributing aspects like data management and governance.

RQ3: What are the current limitations of the IoT data sharing and what are the open issues to be further investigated?

From the previous research question, we have identified the many possibilities that data sharing could bring to different solutions and domains. However, by presenting the contributions of different studies, we can reach a common ground of limitations in approaches related to today's IoT data sharing solutions. With respect to these limitations, we investigate the current gaps, open issues, and other areas for further exploration and development, which may lead to the improvement of secure IoT data sharing in general, in addition to increasing the trust aspects as well.

1.4 Thesis Structure

The remainder of this thesis is structured as follows:

Chapter 2 describes background information related to our study, with the elaboration and explanation of key concepts. The purpose of the background information is to make it easy for readers to understand the project, where IoT, security, and relevant standards are in focus.

Chapter 3 covers related work and provides a summary of the papers and the differences that separates our work from existing work. We also elaborate on how, and if, the related papers contribute to our work.

Chapter 4 describes our research methodology used to conduct the systematic literature review and obtain relevant information. In addition, we describe our taxonomy with parameters that have been contributing to the data extraction process.

Chapter 5 summarizes the obtained results from the systematic literature review, and discusses the results to provide answers to our RQs. This chapter includes discussion of our findings, in addition to contributing factors that can be reflected as threats to validity, which illustrates the trustworthiness and reliability of our work.

Chapter 6 provides a summary of this thesis with concluding remarks, which are based on the previous chapters. In addition, we provide potential directions for future work.

Chapter 2

Background

In this section, we elaborate on the most essential technologies and terms to give a better understanding of the topic of the project. We start off by introducing the technology we are going to focus on in Section 2.1, followed by security in Section 2.2, and privacy in Section 2.3. In Section 2.4, we describe the most common methods for conducting literature reviews. Finally, in Section 2.5, we go over today's standards for IoT and data sharing.

2.1 Technologies

The IoT is a broad topic that includes a variety of related subjects. Since there are a lot of aspects to consider with IoT, we will give a brief description of the most relevant ones. Starting with introducing the Internet of Things in Section 2.1.1, followed by one of the biggest values which derive from data sharing, in Section 2.1.2. Furthermore, we will introduce how related subjects, such as data management in Section 2.1.3 and data governance in Section 2.1.4, are of relevance and an important aspect of secure IoT data sharing.

2.1.1 Internet of Things

The IoT aims at connecting things to the Internet for data collection and sharing in our daily lives. The overall idea and goal of IoT is the ability to stay more connected. IoT devices can be everything from your lights to your TV, and almost everything that you come across in day-to-day life. These IoT solutions include a self-reporting system that produces a large stream of real-time data from its surrounding environment, collected by its various sensors and monitors. This feature of IoT has made the technology thrive in recent years, as it brings crucial information to the surface more rapidly, without the need for human intervention.

An important aspect of IoT solutions is its overall design, also referred to as its architecture. In information technology, architecture refers to the design of computer systems, and how the physical and logical interrelationship between the various components of the system shall communicate. We can divide the IoT architecture into three layers: perception, network, and application layer, which are elaborated further in our taxonomy in Section 4.2.2. Based on the IoT device and service, the architecture components may vary.

These smart end-devices tend to be limited in storage and processing capabilities, making it complicated and difficult to handle complex algorithms and tasks [10]–

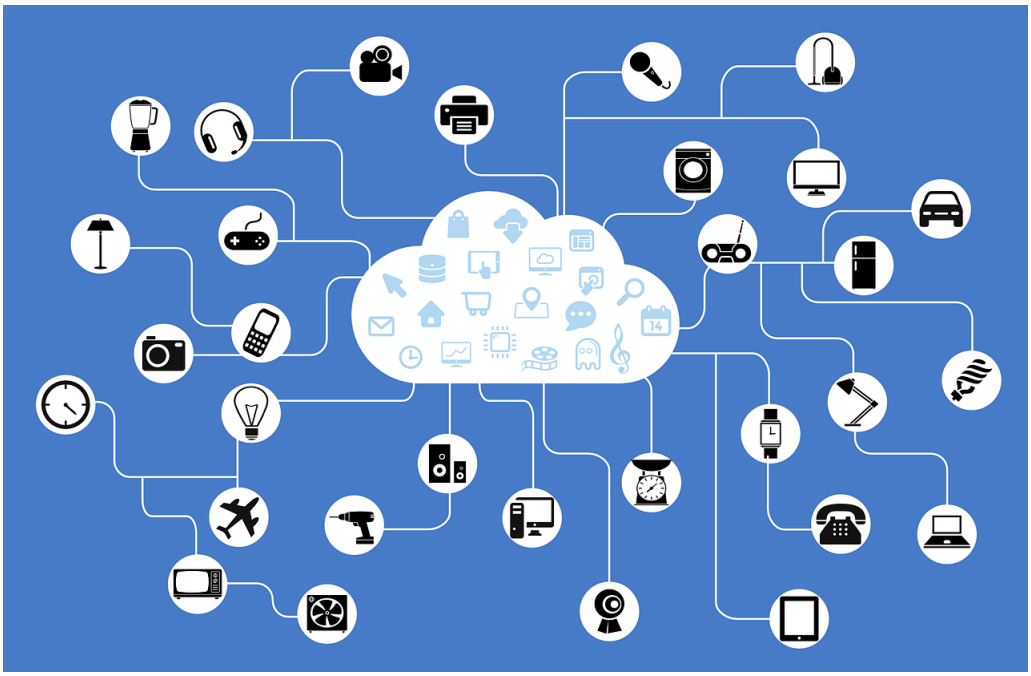

FIGURE 2.1: A map of the many IoT usability areas (retrieved from [9]).

[16]. So how much intelligence can we push to the smart device without compromising the user experience? A traditional and common solution for most of the IoT devices is having the system centralized via a third-party cloud provider, also known as a cloud gateway. A cloud gateway contributes to securely connect the IoT devices to the cloud for sending, processing, and retrieving data [17].

Other common components could, for instance, be stream processing, as the IoT is well known for its production of large data streams. In addition, machine learning could be included as it allows predictive algorithms. As collecting data is of no use if the data is incomprehensible, data transformation is a common component for IoT devices as well. It contributes to data manipulation and translation by, for instance, converting binary data to JSON [17]. With the elaboration of the few components an IoT solution can include, we can draw the conclusion that there are many ways to put together a system that will use IoT.

2.1.2 Data Sharing

One of the biggest values of the IoT is data sharing, which is especially valuable when shared between businesses. Data sharing is the execution and facilitation of sharing an amount of data between multiple people and devices. Following the traditional trend, IoT devices store data in a centralized place, either a cloud or a local data storage. In addition, IoT solutions use this centralized service to further process and analyze the collected data, to extract valuable information.

Today, the IoT is influencing our lifestyle. From our smartphone-controlled air conditioners to smart vehicles providing the shortest route. These gadgets gather and share information about how they are used and the environment in which they are operated in. This type of data is obtained thanks to sensors that are integrated into each device, and that continuously emit data. Figure 2.2 illustrates how various

businesses may take advantage of data sharing. By leveraging data sharing, e.g. between a vehicle and a custom service, it is easier for a mailing service to get real-time vehicle tracking and what packages that are included in the shipment. This makes it easier for the custom service to locate and calculate a package arrival, if a customer, e.g. would like to know the expected delivery date and time.

FIGURE 2.2: Visualisation of how IoT data is shared between different devices in its ecosystem [18].

Another example would be the fire alarm that you got at home. The alarm contains an embedded sensor that continuously transmits data regarding the temperature and smoke level in the room. This data is constantly being analyzed, and if the temperature or smoke level exceeds a specified threshold, the service will alert the fire department. This is just one of a million examples of how smart devices, may make our daily lives easier, by sharing data.

2.1.3 Data Management

The number of IoT devices is expanding at an intense rate. With the expansion of devices being used in everyday life, it implies more data to be handled. With such a large quantity of data, it is therefore necessary and essential to have a proper and efficient solution for handling big IoT data. Data management is an aspect of the IoT ecosystem that manage data in an efficient way, in addition to maintaining the connectivity and security of smart devices.

Data management is the control and processing of data storage, retrieval, updating and records in the IoT. Borrowing the definition from Oracle, data management is the practice of collecting, keeping, and using data securely, efficiently, and cost-effectively [19]. The purpose of data management is to maximise the organisation's benefits through decisions and actions within the boundaries of policy and regulations.

Data management faces a broad range of tasks to be done, in addition to policies, procedures, and practices to follow. Some common activities could be to ensure data security and privacy, data quality [20], maintenance activities and schedule repairs, provide high availability, disaster recovery and archive, while simultaneously

deleting data according to schedules and requirements [21]. As a result, data management is an essential part of the IoT ecosystem.

Other different factors and dimensions worth looking into in regards to data management are presented by DAMA DACH. DAMA consists of recognized leaders in the field of information management with events in the arena of data and information management [22]. DAMA has launched framework papers and is the sponsor of "The DAMA Guide to the Data Management Body of Knowledge" (DAMA-DMBOK Guide), and is now underway with version 2 of this guide (DMBOK2) [1]. When designing a system for secure IoT data sharing, DAMA's input could be quite useful and give great outcomes.

2.1.4 Data Governance

Data governance refers to roles, accountability, and decision rights. In the context of IoT data sharing, data governance establishes how data can and will be processed, who the data owners are, and who can access the data under certain conditions [23]. Data governance aims to ensure that IoT data is generated and used in compliance with security, privacy, quality, and protection, among other things. Appropriate data governance is more crucial than ever when a large volume of data is exchanged across multiple participants in an ecosystem.

FIGURE 2.3: Dimension of data processes for data governance to consider, figure adopted from [23]

The IoT systems' data governance has different factors and dimensions to address. Figure 2.3 illustrates a high-level overview and refers to one of these dimensions, which the data governance need to consider. The dimension includes the data definitions, production and usage. Data definitions can include what data to be collected and should be considered according to standards. The data production regulates how data will be collected and how it will be transferred. Finally, the data usage includes who is permitted to use and share data, as well as how the data is intended to be used. By defining rules for the different factors above, in addition to following policies, regulations, and laws, IoT governance will be able to increase the protection of data in terms of privacy and security.

2.2 Security

The IoT comes in a variety of sizes and shapes, including small, low-cost devices that might bring computing to everyone. Today we have everything from connected healthcare gadgets to home appliances and electrical systems that bring a lot of advantages. With these great advantages, there are also risks that need to be considered as well. With all of this revolutionary IoT technology, the sheer amount of data that is generated is staggering.

By having the IoT track everything, a whole bunch of data is generated and stored that you may or may not be aware of. As smart devices keep getting smarter and

[1] DMBOK2

more connected, so do hackers and cyber criminals. Threat actors have a potentially broader attack surface and various entry points into our data sets and systems, as more gadgets become connected. These points have been discussed in a systematic review of patterns and architectures for IoT security (and privacy) [24]–[26].

Security has various terms and definitions, depending on the domain it is addressed in. However, security, in a general sense, is about protecting the various assets in our system and maintaining the integrity, confidentiality, and availability of data. This can be prevented by blocking and having a defense of assets and digital information against internal and external; both unintentional and malicious, as well as unauthorized access. The defence can include detection, prevention, and response to threats by the use of security policies, software tools and other IT services.

Cybersecurity is a subgroup of general security, which refers to the CIA triad. The CIA triad is a notion that emphasizes the importance of maintaining a balance between data confidentiality, integrity, and availability [27]–[32]. We have elaborated on the CIA triad, as well as the terms authentication and authorization, which are both significant and relevant to our topic.

2.2.1 Confidentiality

One of the fundamental principles of security is confidentiality, which means protecting personal information from being exposed to an unauthorized actor due to threats or data breaches. ISO 27000 defines confidentiality as "the property that information is not made available or disclosed to unauthorized individuals, entities, or processes" [33]. This security term can be connected to the term privacy, since preventing the disclosure of any information usually entails protecting one's privacy. Referring to the example presented by Mearian [2] about the Nissan Leaf data leak, we may draw a connection between how lack of confidentiality can induce vulnerability and hence have an influence on an individual's privacy.

2.2.2 Integrity

The second fundamental principle of security is integrity. Integrity relates to the data's trustworthiness, completeness, and accuracy; in other words, integrity protects and prevents data from being maliciously modified or misused by an unauthorized actor over its entire life cycle. ISO 27000 defines integrity as a "property of accuracy and completeness" [34]. An example that illustrates how fundamental integrity plays into security is when a person with diabetes uses a glucose monitor. The consequences of an unauthorised actor breaking into the system and tampering with this type of sensitive data can, in the worst-case scenario, be fatal for the system's user.

2.2.3 Availability

Finally, the CIA triad's third and final essential concept is availability. An information system has to be available to its authorized users in order to be helpful and valuable. Although availability in the context of security is associated with malicious threats, the most common threats to availability are non-malicious. Unscheduled software downtime, network bandwidth challenges, and hardware breakdowns are examples of these non-malicious threats that could occur [35].

2.2.4 Authentication

The Oxford Dictionaries [36] define the term as "to prove that something is real, true or what somebody claim it is". However, in the context of information security, the term authentication is used to validate one's identity and authority, which is helpful in the context of protecting one's confidentiality. The International Organization for Standardization (ISO) [37] provides a formal description of what is included in the authentication process.

They present two notes for entry. The first is in regards to that "the authentication process involves tests by a verifier of one or more identity attributes provided by an entity to determine, with the required level of assurance, their correctness". The second and last note are that "authentication typically involves the use of a policy to specify a required level of assurance for the result of a successful completion" [37]. However, there are various forms of authentication procedures. Password-based, multi-factor, and certificate-based authentication are the most popular and common in recent years.

2.2.5 Authorization

Although the terms authentication and authorization sound similar, there is a significant difference between the two security processes. Oxford Dictionaries defines authorization as the "official permission or power to do something; the act of giving permission" [38]. While authentication, as we have described previously, confirms one's identity and authority, authorization is the following process, which entails granting the user permission to access a specific resource [39].

2.3 Privacy

The influential study "The Right to Privacy" [40] authored by Louis Brandeis and Samuel Warren in 1890 was a key milestone in the establishment of the current notion of privacy. Brandeis and Warren wrote the study with the purpose of "considering whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual" [41], which lately became one of the most influential essays in the history of American Law.

The terms "security" and "privacy" are related and quite often used interchangeably. Although the terms are difficult to distinguish between, they are in fact different, and the definition of privacy will differ depending on the domain. The Oxford dictionary defines privacy as follows: "a state in which one is not observed or disturbed by other people; the state of being free from public attention". While security is concerned about confidentiality, integrity, availability (CIA), authentication and authorization of information, privacy is concerned with personal information rights.

We elaborate into privacy with respect to information technology in detail. More specifically, IoT data sharing, data protection, and its related countermeasures. To be certain if a solution is preserving privacy, we first need to elaborate on the most relevant terminology, specified by ISO 29100 [42].

2.3.1 Privacy Risk

Risk is most often referred to as the probability, chance, or possible exposure to danger or something happening. When relating risk to privacy of information and communication technology systems, we define it as the chance or probability of personal information loss. To get a more concrete definition, ISO 29100 defines privacy risk as follows:

"Effect of uncertainty on privacy" [42].

2.3.2 Privacy Breach

A breach is often referred to as a violation. When relating breach to privacy of information and communication technology systems, we associate it with when an actor accesses information without the permission, also defined as not having granted authorization. A privacy breach is defined by ISO 29100 as follows:

"Situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements" [42].

2.3.3 Privacy Stakeholder

A stakeholder is an interested or concerned party. When relating stakeholders to IoT systems, they could vary from engineering, end customers, finance, and product management and marketing. When referring to stakeholders in the field of privacy, ISO 29100 elaborates the definition as follows:

"Natural or legal person, public authority, agency or any other body that can affect, be affected by, or perceive themselves to be affected by a decision or activity related to personally identifiable information (PII) processing" [42].

2.4 Review Methods

In Chapter 1, we introduced the topic along with our motivation and goals for this project. Our work consists of identifying and analyzing the state-of-the-art of secure IoT data sharing. As a result, we need to review the most recent stages of the technological development and practice of IoT data sharing, in addition to the influence of data management and governance. Therefore, review is key in our study. Cambridge dictionary define review as follows:

"A process of carefully examining a situation to find out whether changes or improvements need to be made" [43].

An important factor to consider when selecting our review method, is our desire to perform a review in the most transparent and less biased way. Therefore, we want our review method to include a process that distinguishes between bias and non-bias research. The aspect of bias is considered, as it can be seen as a disproportionate weight in favor of something or someone. As a result, bias in this case may lead to a biased presentation of the topic, which we prefer to omit.

To have a better grasp of the field's current state, we must first identify existing review methods, which help to justify why we have chosen systematic literature review as the most appropriate and best practice for our study. We present a brief explanation of the most relevant literature reviews to cover all of the most used

and common ones. We will start by introducing secondary study in Section 2.4.1. Furthermore, we describe the systematic mapping study in Section 2.4.2 and the tertiary study in Section 2.4.3. Finally, in Section 2.4.4, we will introduce the review method we are going to conduct in our project, which is the systematic literature review.

2.4.1 Secondary Study

A secondary study is a strategy that involves using data collected from previous research to answer a specific set of research questions. In other words, secondary study entails collecting and interpreting already existing data, like primary research, that is relevant to our topic. A secondary study, for example, will typically incorporate a number of primary research findings to explain the general findings and overall conclusion. This elaboration might provide a fast summary of the research field to readers. Furthermore, it provides researchers with a quick overview of which fields can possibly be elaborated on in later work. Kitchenham *et al.* [44] defines secondary study as follows:

> *"A study that reviews all the primary studies relating to a specific research question with the aim of integrating/ synthesising evidence related to a specific research question"* [44].

2.4.2 Systematic Mapping Study

A method for mapping and structuring a research domain is Systematic Mapping Study (SMS). In particular, given the situation that the research area we are about to explore is quite broad or contains very little evidence, a SMS may then be suitable. We can plot the domain evidence at a high level by conducting a mapping study. The results from the plot can further be used to identify areas where more primary studies and systematic literature reviews are needed, and can be conducted. Kitchenham *et al.* [44] defines SMS as:

> *"A broad review of primary studies in a specific topic area that aims to identify what evidence is available on the topic"* [44].

2.4.3 Tertiary Study

Tertiary study, also known as tertiary review, is a method that conducts a systematic review of systematic reviews. Specifically, if the domain we are about to investigate has a number of already existing systematic reviews, we can then undertake a tertiary review to answer a wide range of research questions. Kitchenham *et al.* [44] define tertiary study as:

> *"A review of secondary studies related to the same research question"* [44].

2.4.4 Systematic Literature Review

A Systematic Literature Review (SLR) is a review method known for critically identifying, selecting, and evaluating research. As we stated in the introduction of this section, it is important to consider the fairness of the literature's. Therefore, one of SLR's advantage is its well-defined methodology, which contributes to less biased outcomes and results. For instance, an SLR has to be carried out in accordance with a predetermined search strategy. An SLR can be seen as a form of secondary study

(Section 2.4.1), and will be the research method to be applied in our project. Borrowing the definition from Kitchman *et al.* [44], a SLR is defined as follows:

> *"A mean of evaluation and interpreting all available research relevant to a particular research question, topic area, or phenomenon of interest. Systematic reviews aim to present a fair evaluation of a research topic by using a trustworthy, rigorous, and auditable methodology"* [44].

The reason for conducting this type of literature review is because of its process of summarizing existing evidence concerning our topic and identifying gaps in the current research. Furthermore, this review provides an overview of the topic that can be used to find potential new research areas to be further investigated and explored. In other words, as a result of conducting this literature review, we will be able to determine the state-of-the-art in our domain of secure IoT data sharing. To assist us along the way, we will follow the well-known guidelines of Kitchenham *et al.* [44] throughout our project, which will be further explained in Chapter 4.

2.5 Standards

Standards are crucial in our world because they provide a foundation for mutual understanding. Standards can be defined as a way of performing a task that contains specifications and well defined criteria to be constantly used as guidance. In the context of IoT, the standards cover everything from sensor and quality performance such as efficiency, interoperability, and effectiveness, to architecture and security aspects of IoT [45].

To ensure IoT data sharing in the most trusted and secure way feasible, the knowledge of standards, policies, and guidelines are important contributing factors to consider. In this section, we will review and learn from related standards for IoT data sharing, management, and governance. As standards and regulations may vary from country to country and continent to continent, we will be elaborating on the most common ones in regards to our project.

2.5.1 General Data Protection Regulation (GDPR)

One of the most "recent", well-known, and strictest laws in the world is the General Data Protection Regulation (GDPR). The GDPR went into effect in 2016 after being passed by the European Parliament, but it was not until 2018 that all organizations were required to be compliant with the law [46]. The GDPR lays the foundation of guidelines in regards to the collection and processing of personal data from individuals. Any violations of privacy and security requirements will experience penalties with a harsh levy.

Even though the law is applicable to people, operations, and businesses in the EU, requirements and obligations will still be set for other non-European services and operations. To clarify, the law will apply to any operations that are operating in-, or offer service within the European Union (EU) [47]. The IoT technology is appealing due to its data sharing and collecting capabilities of data. The GDPR can be used as a foundation for IoT data sharing solutions in general. However, GDPR can more specifically be used as guidance on what practices should be considered when working with data management and governance.

2.5.2 International Organization for Standardization (ISO)

Introducing a well-known international organization, namely International Organization for Standardization (ISO), which is a non-governmental federation that was founded in 1947. Each country that is a member of the organization has contributed with one standard, resulting in ISO containing standards from over 160 countries.

The purpose of ISO as an organization is to create standards to ensure the safety, quality, and efficiency of services and systems. ISO contributes to the IoT context as it gives an overview of the interoperability of the systems. They also contain guidelines on data exchange and sharing for smart community infrastructure, as IoT is (ISO 37156:2020) [48].

2.5.3 IEEE Standards Association (IEEE SA)

Furthermore, we have the IEEE Standards Association (IEEE SA), which is an organization that facilitates standards related to development and collaboration, with collaborative leaders in more than 160 countries [49]. IEEE SA has a number of existing standards and activities that are related to establishing the necessary environment for IoT technology. Data collection, access, and usage, data administration, and data processing handling are all covered by these standards and activities.

2.5.4 International Data Spaces Association (IDSA)

A relevant association in the context of the data exchange domain is International Data Spaces Association (IDSA), with a vision of innovating the future of data exchange in Europe and beyond by creating the important technical standards [50]. 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 [51]:

- Data privacy and security that's the most rusted 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.

2.5.5 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[52].

2.5.6 Data Quality Assessment

Finally, introducing DNV's White Paper on Data Quality Assessment [53]. As IoT devices tend to generate huge amounts of data, it is important to consider the process of evaluating the data quality. Data quality assessment is a process of validating that the data meets the expectations of the system or users that make use of this data. By including this validation method, it makes risk assessment much easier when obtaining risk boundaries of data usage. Quality assessment, within the risk tolerance thresholds, contributes to the prerequisites for secure, sustainable, and efficient operations.

2.5.7 OWASP Top Ten Internet of Things

The last one we are going to introduce may differ in relation to the other standards, associations, and organizations just presented. The Open Web Application Security Project, also known as OWASP, provides a top ten list [54], where we focus on the list from 2018 related to the IoT. The list was created and meant to capture the most important aspects related to IoT security, more specifically, what to avoid when building, deploying, or managing IoT systems. For the sake of simplicity, the top ten internet of things by OWASP provide a unified guideline for different stakeholders, such as developers, enterprises, and consumers. The top ten list is as follows:

TABLE 2.1: 2018 OWASP Top Ten Internet of Things [55]

No.	Title	Description
I1	Weak, Guessable, or Hard-coded Passwords	Use of easily brute forced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deploys systems.
I2	Insecure Network Services	Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity or availability of information or allow unauthorized remote control.
I3	Insecure Ecosystem Interfaces	Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/ authorization, lacking or weak encryption, and a lack of input and output filtering.
I4	Lack of Secure Update Mechanism	Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

I5	Use of Insecure or Outdated Components	Use of deprecated or insecure software components/ libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain..
I6	Insufficient Privacy Protection	User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.
I7	Insecure Data Transfer and Storage	Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit or during processing.
I8	Lack of Device Management	Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, system monitoring, and response capabilities.
I9	Insecure Default Settings	Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.
I10	Lack of Physical Hardening	Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

Chapter 3

Related Work

This section contains some of the related work to our subject. While the studies may have some similarities to our study, we will be focusing on the extracts that depart from our scope and research. The related studies can be categorized into two types: primary and secondary studies. The former embraces analysis of primary data based on direct observation of a specific research issue, also referred to as an empirical study [44]. The latter is the polar opposite, as the investigations are based on data and research that has previously been acquired in response to a specific research issue.

The related works described in this chapter are mainly secondary studies. We have broken down the associated work into three sections since there are a few crucial points we want to emphasize. In Section 3.1, we discuss related research to the topic of IoT data sharing, followed by its core building elements, data management and data governance, in Section 3.2 and 3.3, respectively.

3.1 Secondary Studies on IoT Data Sharing

Two papers that are related to our issue are discussed. Both contain a collection of relevant papers that may be worth reviewing and evaluating further. Furthermore, both studies employ blockchain technology and smart contracts to address data sharing solutions.

The paper by Kuang Lo *et al.* [56] discusses some of the issues that today's data sharing and management solutions face (Section 3.2), as well as how recent research has tackled them. The research touches on several aspects we are curious about. The study invests and focuses on, among other things, how to solve some key issues related to IoT, such as the single-point-of-failure caused by the use of a centralized management server, as well as the challenge of interoperability that arises between IoT platforms, both of which are relevant to our data sharing topic.

Despite the fact that this study discusses the major role of many technologies as a solution to these difficulties, such as a description of blockchain and access control operations, it is more of a high-level overview. However, there are some details we would have liked to get a deeper insight into. For example, which architectural layer is 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 interests. A description of the security strategies utilized, as well as an elaboration of how they contribute to creating the most trustworthy environment for the data sharing process before, during, and after the sharing has occurred, is also of interest. We will therefore complement this research by extracting and expanding on these aspects.

Another interesting study is presented by Alharby *et al.* [57]. From a technological standpoint, they present and focus on a collection of essential studies on smart contracts applied to blockchain. A smart contract is an agreement between untrustworthy parties that is carried out based on some pre-determined rules. They highlight how different blockchain systems have distinct capabilities for developing smart contracts. The goal of their research is to understand the current research areas in smart contracts.Because smart contracts are used in the IoT to ensure trust between two parties, this paper is very relevant to our topic as it creates an assurance of trust in IoT data sharing. However, it is worth noting that there is no specific discussion on data sharing or how smart contracts contribute to a secure environment for the exchange of data.

3.2 Secondary Studies for IoT Data Management

The work presented by Kuang Lo *et al.* [56] was mentioned and cited as a related study in our scope of data sharing in the previous section. However, this research looks at other aspects as well, in regards to IoT data management. They emphasized how the management of data and "things" is complicated, as there is no general established standard for managing the "things" to handle various concerns. For a large number of connected "things", these challenges include data privacy, data security, thing security, and system maintenance.

It is worth noting that this research focuses on "things" management, with a brief mention of data management, though the latter is more relevant to our data sharing scope. Their research, on the other hand, contributes and will be used in our work as it gives an indication of the current state-of-the-art of IoT management and how it remains an issue. Furthermore, it demonstrates the lack of research into the current state of IoT data management. Because our focus is primarily on secure IoT data sharing, we will elaborate on the importance and impact of how data management can help create a more secure and trusted data sharing environment.

3.3 Secondary Studies for IoT Data Governance

For IoT data governance, we found two papers that contribute in their own ways. They both point out the importance of having proper data governance in addition to guidance on further research to be explored.

Al-Ruithe [58] presents an SLR of data governance and cloud governance in their use of data. This paper contributes to our work by providing a structured, methodical, and rigorous approach to understanding the state-of-the-art of data governance and cloud governance. They also 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. They do not, however, elaborate on what impact this might have on IoT data sharing because their primary focus is on data and cloud governance.

The necessity of ecosystem data governance for data platforms is discussed by Prieëlle *et al.* [59]. They highlight the importance of governing access to and use of these platforms, which is crucial for these data platforms' long-term sustainability. Future research directions are mentioned, 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.

This research is relevant to our work by addressing the importance of data governance in the context of the IoT. However, there are significant differences in our work. First and foremost, this study is primarily focused on data governance, whereas we would want to 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. Additionally, their future research direction is something we are very interested in exploring and understanding more about, such as the advantages of data sharing and the importance of data governance access and usage.

Chapter 4

Research Methodology

A research methodology can be defined as a specific procedure to identify, select, and analyze data about a certain topic [60]. In Section 2.4, we introduced the most relevant research methods for our project, and concluded that the SLR would be the most suitable research methodology for our study. In this section, we will elaborate on our research methodology, where the contribution will allow readers and researchers to critically evaluate our study's overall reliability and validity. In order to end up with a well-conducted SLR, we will be following the guidelines of Kitchenham *et al.* [44].

This section are mainly divided into two sub-sections, we elaborate on our review protocol in Section 4.1, before presenting our taxonomy in Section 4.2. However, these two main sub-sections are divided into several atomic parts, which includes in-depth details and descriptions.

4.1 Review Protocol

To differentiate SLR from conventional and traditional literature reviews, SLR consists of different review features that contribute to our research. One of these features is a review protocol. A review protocol contains the process of defining a set of research questions in addition to methods and criteria that will be a part of the review. In other words, our review protocol is used as guidance, which will be carried throughout the review.

To achieve and accomplish the overall aim of this thesis, we will identify and define a set of success criteria. These criteria will be used as a pointer in our research direction, in addition to shaping the way this project will succeed. The following success criteria are defined as follows:

Success Criterion 1
The systematic literature review must find out the existing approaches in the state-of-the-art of secure IoT data sharing, management, and governance. Our SLR should be explained and present a fair evaluation of the topic, in addition to the methods used to generate the results. Our work must be justified and point to the necessity of our research, and it should stand out by not being a duplicate of others' work.

Success Criterion 2
The systematic literature review must explicitly describe the threats and address the validity of solutions related to IoT data sharing. The stakeholders who will benefit from our

research will gain knowledge about today's common threats related to data sharing from our detailed description, as well as be assured of the trustworthiness and validity of our work.

Success Criterion 3
The systematic literature review must assess the topics' current practice and the gap between this and SotA. The stakeholders that will benefit from our research will mainly include researchers. Therefore, our SLR must clearly point to the current practices used and gaps that either have a lack of or no relevant existing research.

We will begin our review methodology by identifying the research questions in Section 4.1.1., based on our success criteria. To obtain answers to the questions, we will have to design a search strategy, as done in Section 4.1.2, to find as many relevant studies as possible on the topic. Moving on, we use our predefined inclusion criteria from Section 4.1.3 and exclusion criteria from Section 4.1.4 on the number of studies found to reduce the likelihood of any bias in our selection phase in Section 4.1.5. Finally, we will create evaluation criteria and a data extraction approach in Section 4.1.6.

4.1.1 Research Questions

In order to conduct our study within the boundaries of the chosen research methodology, the research questions must be defined. The research questions provide the key foundation for the rest of our study and will influence our findings. This is the most important step in the research protocol, as the search process will need to discover studies that address these questions.

RQ1: What are the solutions for secure IoT data sharing?

RQ1.1: What is the current trend of publications on secure IoT data sharing?

RQ1.2: What are the reported application domains of IoT data sharing?

RQ1.3: What are the purpose and benefits of data sharing considered in the primary studies?

RQ1.4: What are the architectures for IoT data sharing in the primary studies?

RQ2: What are the security and trust aspects of these IoT data sharing approaches?

RQ2.1: What are the most common threats and vulnerabilities to IoT data sharing today?

RQ2.2: What and how are the techniques and approaches used to preserve secure IoT data sharing?

RQ2.3: What is the role of data management and governance, and how do their standards, policy and guidelines support trusted and secure data sharing?

RQ3: What are the current limitations of the IoT data sharing and what are the open issues to be further investigated?

4.1.2 Search Strategy

The purpose of our search strategy has been to exhaustively search for as many relevant papers as possible on our topic. As a result, we have implemented a hybrid approach consisting of two different parts: automatic and manual search. In both parts, the inclusion and exclusion criteria (Section 4.1.3 and 4.1.4, respectively) have been applied to select our primary studies based on relevance. This subsection elaborates on how the identification of search strings has been carried out and what electronic databases have been utilized.

Search String Identification: When designing search phrases, it is important to consider that the strings should not be too specific nor too general, so we do not exclude relevant work or result in numerous false positives. In our process of identifying the search string, the research questions have contributed and are utilized as a basis when creating the search keywords. The search keywords have been divided into categories, mainly data sharing, application domain and security. These keywords were later transformed into search strings, which went through several iterations of refinement before reaching the final product shown below. The purpose of having multiple refinement rounds on the search strings is to ensure that the search returns as many relevant publications as possible.

The process of identifying search strings began with the selection of a number of keywords. However, there are many factors to consider when searching for relevant keywords. The topic of IoT data sharing is broad and will continue to grow into different fields. With respect to the search query, we have selected a number of keywords that we believe are relevant to our research. These keywords include terms such as: IoT, Internet of Things, data sharing, data, industry 4.0, data security, data marketplace, context sharing, etc. The keywords can be divided into the following groups:

- Group 1 (data sharing domain): data sharing, sharing, data exchange, context sharing, context-aware data sharing, context-aware information sharing, information sharing, context-sensitive information sharing, sharing of data, sharing data, ecosystems, marketplace, data marketplace
- Group 2 (application domain): Internet of Things, IoT, Industry 4.0, smart cities, smart city, smart contact, manufacturing, energy, supply chain
- Group 3 (security): access control, secure, security, trust, trustworthy, encryption, data security, secure communication, secure data sharing, context-aware security, management, governance, protocols, standards

However, the identification and selection of keywords were not the only factors to consider when building a search string, leading to the next step, the formatting of the query. The process of formatting the query was done using several electronic databases. These databases each have their own unique search engines, with a different number of parameters allowed. As a result, we made every effort to format the query in such a way that we as closely as possible could concatenate Groups 1 AND Group 2 AND Group 3 as follow:

("data sharing" OR "sharing" OR "data exchange" OR "context sharing" OR "context-aware data sharing" OR "context-aware information sharing" OR "information 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")

Automatic Search in Databases: We used five (5) electronic publication databases: IEEE Xplore, ACM Digital Library, ScienceDirect, Web of Knowledge and Scopus to search for possible primary papers. Google Scholar was not selected nor utilized as one of the electronic publication databases, as it returns a number of non-English and non-peer-reviewed papers. The five chosen electronic databases contain peer-reviewed papers. We used the search string identified and elaborated above, which was refined according to the search function provided by the different databases.

Manual Search in Conferences Proceedings and Journals: To ensure the completeness and precision of our study, we conducted a manual search of both conference proceedings and journals. We selected conference papers and journals that were highly ranked with relevance to IoT, security, management, and governance in regards to our scope on secure IoT data sharing such as the paper addressed by Preuveneers *et al* [61] and by Shafagh *et al.*[62].

4.1.3 Inclusion Criteria

Because the search strategy produced a wide range of primary studies with diverse content and outcomes, it was necessary to establish a set of inclusion and exclusion criteria that all primary papers had to meet. Our selection process was conducted in the most transparent and unbiased way possible, with all of the primary studies having to meet all of the following Inclusion Criteria (IC):

IC1 Studies addressing IoT data sharing.

IC2 Studies addressing IoT data sharing architecture models.

IC3 Studies that consider the security and trust aspects of IoT data sharing.

4.1.4 Exclusion Criteria

We have excluded papers according to any of the Exclusion Criteria (EC) listed as follows:

EC1 Non peer-reviewed publications are excluded.

EC2 Papers written in any other language than English will be filtered out and excluded in the search process.

EC3 Papers published before year 2010 will be excluded. According to IBSG [63], it is claimed that the IoT was "born" around year 2008-2009, but did not gain popularity before year 2010, which is a good starting point for us to consider papers from.

EC4 In general, short papers have shown to not include all necessary details. We therefore excluded papers that were less or equal to six pages (single column) and four pages (double column).

These criteria have been utilized to gather all of the relevant information on our topic. To leave no room for misinterpretation, we have specifically clarified two borders. First, original papers have been prioritized to be included rather than reviews and surveys. In general, reviews and surveys have been shown to not always contain sufficient details. However, when we have seen it as relevant, we have discussed the review or/and surveys in the related work section. Secondly, when there has been more than one paper describing the same or quite similar approach, we have looked into all of the papers and considered them as a single approach.

4.1.5 Selection Process

In this section, we will elaborate on how the selection process has been conducted for both the automatic and manual searches, which were briefly introduced in Section 4.1.2. By using the automatic search method, we discovered 55 primary studies related to our topic. From the automatic search results, 7 of these studies were discovered through the manual search. With the combination of both the automatic and manual search, we were left with a final set of 55 primary studies. Figure 4.1 illustrate our search and selection process combined, as well as the number of primary studies we were left with.

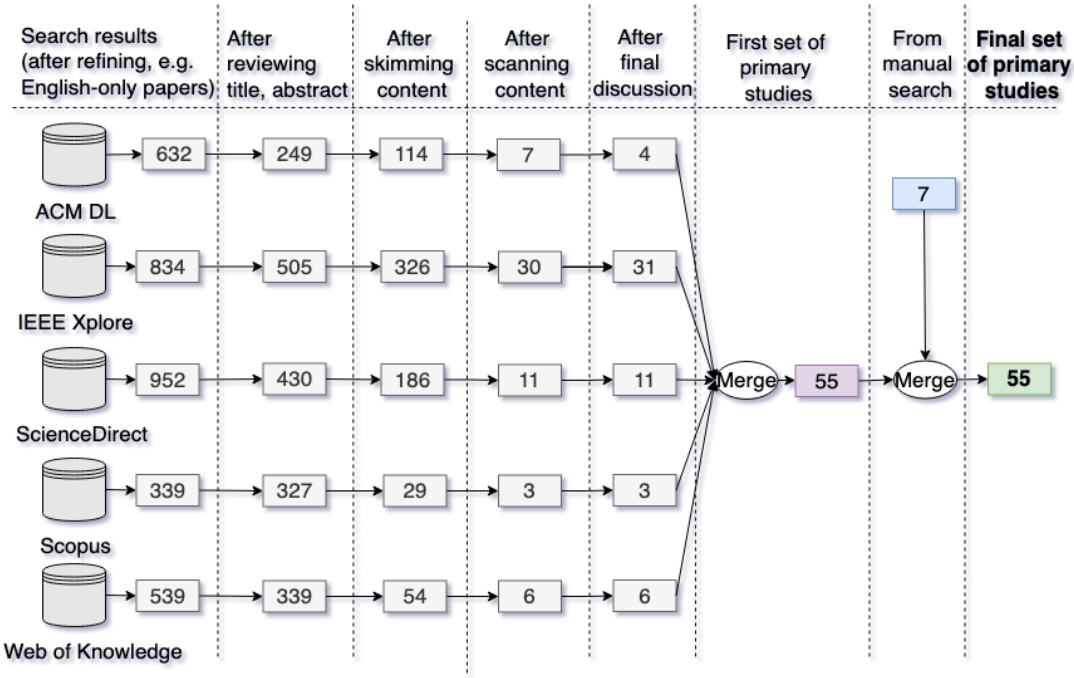

FIGURE 4.1: Overview of the search and selection process

1. *Automatic search:* The first step in our selection process is in regards to all papers found from the automatic search. For each search engine we utilized, we were able to specify which year we would like to see the results from. We would therefore always know that the publication year of every paper was from the year 2010 and later. The procedure of the automatic search started by looking at the titles and abstracts of each paper in the results. If we came across a circumstance where the paper's abstract was inadequate and raised the challenge of either including or excluding it, the paper would often be further examined by reviewing its keywords. If the keywords raised the same issue, the scanning would further continue by roughly looking through the paper's content. We collected and merged all relevant papers found in the repositories, and removed all duplicates in the final quantity of selected papers.
2. *Manual search:* The selection process in regards to the results from the manual search was conducted in a similar way to the selection process of the automatic search. After obtaining the final set of papers for the manual search, we merged the selected papers from the automatic and manual search into one.

4.1.6 Evaluation Criteria and Data extraction strategy

Evaluation criteria are aimed at providing requirements that need to be fulfilled when taking decisions in regards to pointing out the limitations of each selected paper. This assessment makes it easy for researchers and readers to consider different factors when using IoT solutions for developing secure data sharing. The aim of including data extraction was to design forms to accurately document the information we obtained from the various studies.

1. *Security concerns:* The security topic is broad and can include various themes such as authorization, integrity, privacy, and accessibility. We have been categorizing selected studies according to the security challenges they face, and have counted the total number of papers that address each security subject.
2. *Application domain:* IoT data sharing solutions have also been categorized and classified into their related domains as well. Some data sharing solutions have been adopted for a specific IoT domain, whereas for other solutions they have been fit into a broad range of domains. Some examples of application domains could be manufacturing and automotive. The elaboration of the domains we have focused on in this study is specified in our taxonomy in subsection 4.2.3.
3. *Data governance and management approaches:* Data governance and management are linked and have an impact on how IoT data is shared, including everything from data collection to processing and retrieval, as well as the security issues that come with these operations. We have therefore extracted data based on the most common standards related to data governance and management of today's IoT solutions. By collecting the most common standards, policies, and guidelines that are used in today's solutions, it can cause further examination and contribute to mapping the co-relevance to security aspects of data sharing.
4. *Evaluation methods:* We have been reviewing how the solutions have been evaluated, if evaluated, in order to determine the existing constraints of the

solutions. By looking at the sections regarding validation, results, and conclusion of the papers, this data often contains what approaches have been used to evaluate the solutions, in addition to what results the paper has achieved.

One of our research questions is about the current limitations and any open issues to be further investigated (Section 4.1.1). In order to answer this research question, we have, in addition to the aspects above, been reviewing the classification of security concerns, the scope of current IoT data sharing research, and the quality of their results and evaluation.

4.2 Taxonomy of the Research Area

The taxonomy of our research is illustrated in Figure 4.2. This technique establishes a classification system for all relevant categories that should be extracted in the primary studies. The objective of this taxonomy is to enable extracting and distinguishing data from primary studies that may be 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.

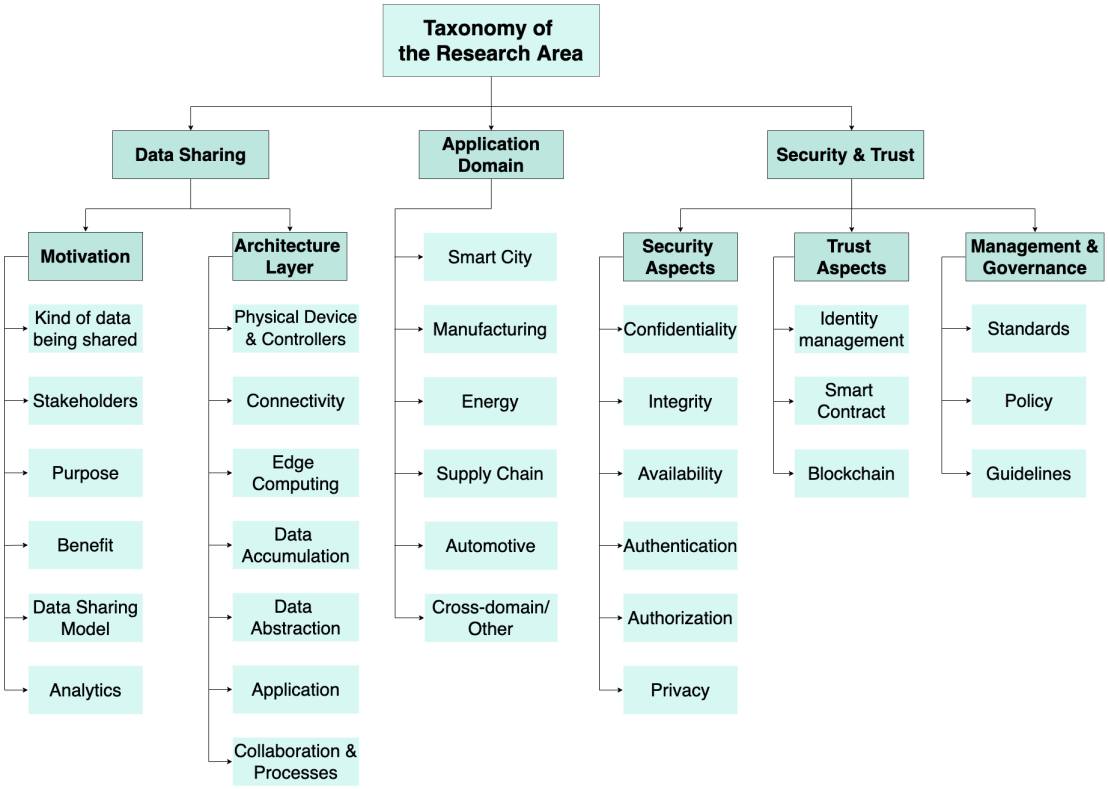

FIGURE 4.2: Taxonomy of the Research Area

4.2.1 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.
  - 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 are a public or private marketplace, peer-to-peer or a domain-specific sharing.
- Analytics: another aspect is data analytics, as data sharing often goes hand in hand with analytics. Therefore, looking into how, or if, the data is being analyzed in some way could be an interesting extraction.

4.2.2 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 [64] are 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 [65] 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 [64], 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.

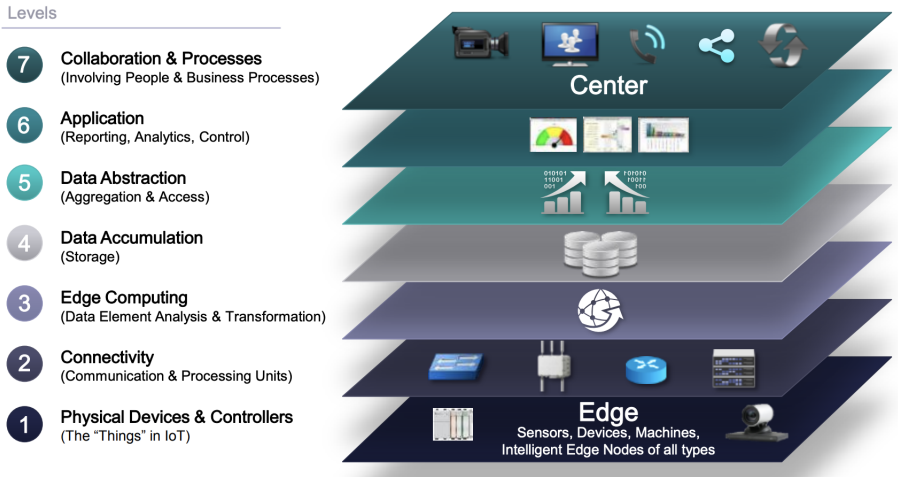

FIGURE 4.3: Overview of the layers in the IoT World Forum Reference Model [64]

4.2.3 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 Space Radar [66] 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 (& 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 / other: includes all the other single domains, but also the ones that do cross each other in the different solutions.

4.2.4 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: protection of personal information from being exposed to an unauthorized actor
- Integrity: the trust and accuracy of the data
- Availability: data being available when needed for authorized users
- Authentication: confirm one's authority
- Authorization: give the users permission to access a resource
- Privacy: protection personal identifiable information

4.2.5 Trust Aspects

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

- Identity management: we look into aspect 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 between each other. This could be evaluated by seeing if the solution includes the following mechanisms:
  - Blockchain: from the definition of [67], 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 [68].

4.2.6 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, for example, obligations regarding deletions of data after two days and not to forward data. 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?

Chapter 5

Results

In this section, we give the key findings and results of our systematic literature review and, based on these, we answer our research questions. We were able to undertake an analysis of the research with the assistance of our pre-defined taxonomy (Section 4.2). We present the high-level statistics in Section 5.1, followed by the low-level specifics of our findings in Section 5.2. Section 5.3 delves deeper into the gaps, followed by a discussion of how the findings answer our research questions in Section 5.4. Finally, we present and discuss the limitation of this study in Section 5.5.

5.1 High-Level Details of IoT Data Sharing

In this section, we present a number of statistical findings. In Section 5.1.1, we introduce the interest and growth in secure IoT data sharing and the statistics of the application domains in Section 5.1.2. Furthermore, we elaborate on the purpose and benefits of data sharing in Section 5.1.3. Finally, in Section 5.1.4, we highlight the statistics of the data sharing models that have been used in the various primary studies.

5.1.1 Interest and Growth

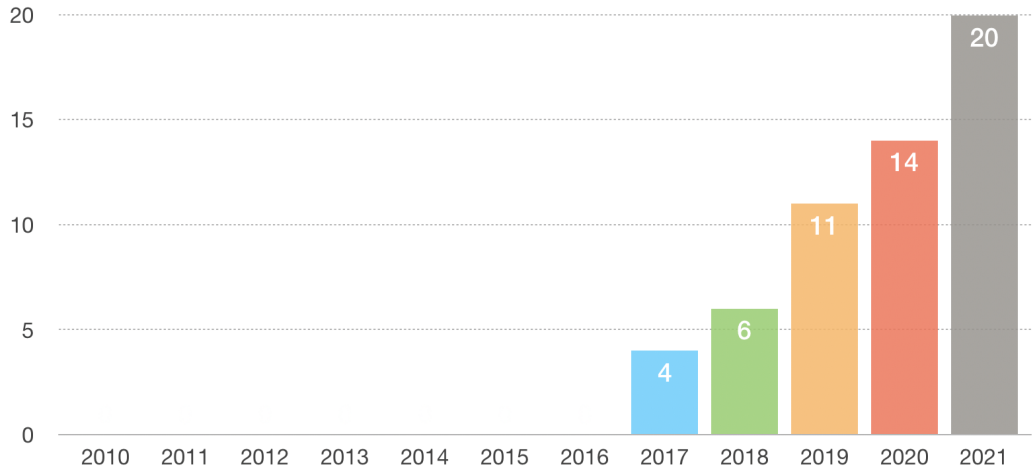

FIGURE 5.1: Overview of the publication year of the primary studies

The representation of publication years of our selection of primary studies from 2010 to 2021 is shown in Figure 5.1. We decided to start the publishing timeline in 2010, due to the "birth" of the Internet of Things, as stated in our exclusion criteria, notably

EC3. Furthermore, because we completed the search process in December 2021, we have decided to end the publication timeline at 2021. The papers published in the last several years, according to the statistical histogram, have been the most relevant to our specific topic of secure IoT data sharing (2020: 14; and 2021: 20 papers).

We hope to see a continuation of the increase of relevant publications in the years to come, as the prediction from Cisco estimates billions of IoT devices already connected to the internet by 2025 [1]. As we completed our search of primary studies in December 2021, we found a total of 55 primary studies. Therefore, we have not included any publications from the year 2022, which may or may not be relevant to our research topic.

In Table 5.1, the primary papers are listen in chronological order by publication year. Each publication has an ID that is represented by a "#" concatenated with a unique number, the year of publication, the title of the study, the citation, and the type of venue. Only conference or journal papers are represented in our selection. The former is represented 21 times out of 55 times, while the latter is represented 34 times out of 55 times.

TABLE 5.1: Overview of our selection of primary studies

#	*Year*	*Title (click to open the corresponding publication)*	*Cite**	v
#1	2017	Towards Blockchain-based Auditable Storage and sharing of IoT data	[62]	C
#2	2017	Secure and Efficient Data Sharing with Atribute-based Proxy Re-encryption Scheme	[69]	J
#3	2017	IoT data privacy via blockchains and IPFS	[70]	J
#4	2017	Big Data Model of Security Sharing Based on Blockchain	[71]	C
#5	2018	A Peer-to-Peer Architecture for Distributed Data Monetization in Fog Computing Scenarios	[72]	J
#6	2018	Continuous Patient Monitoring with a Patient Centric Agent: A Blockchain Architecture	[73]	J
#7	2018	Towards a Decentralized Data Marketplace for Smart Cities	[74]	C
#8	2018	Providing Context Aware Security for IoT Environments Through Context Sharing Feature	[75]	C
#9	2018	A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems	[76]	C
#10	2018	Smart-toy-edge-computing-oriented data exchange based on blockchain	[77]	J
#11	2019	Security and Privacy of Electronic Health Records: Decentralized and Hierarchical Data Sharing using Smart Contracts	[78]	C
#12	2019	Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies	[79]	J
#13	2019	MedChain: Efficient Healthcare Data Sharing via Blockchain	[80]	J
#14	2019	Toward a Decentralized, Trust-Less Marketplace for Brokered IoT Data Trading Using Blockchain	[81]	C
#15	2019	Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks	[82]	C
#16	2019	Towards Multi-party Policy-based Access Control in Federations of Cloud and Edge Microservices	[61]	C

#17	2019	BlendMAS: A Blockchain-Enabled Decentralized Microservices Architecture for Smart Public Safety	[83]	C
#18	2019	BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT	[84]	C
#19	2019	Enabling Industrial Data Space Architecture for Seaport Scenario	[85]	C
#20	2019	Blockchain based Proxy Re-Encryption Scheme for secure IoT Data Sharing	[86]	C
#21	2019	IoT Passport: A Blockchain-Based Trust Framework for Collaborative Internet-of-Things	[87]	J
#22	2020	BEAF: A Blockchain and Edge Assistant Framework with Data Sharing for IoT Networks	[88]	C
#23	2020	A Blockchain-based Medical Data Marketplace with Trustless Fair Exchange and Access Control	[89]	C
#24	2020	Blockchain Smart Contract for Scalable Data Sharing in IoT: A Case Study of Smart Agriculture	[90]	C
#25	2020	Fully Decentralized Multi-Party Consent Management for Secure Sharing of Patient Health Records	[91]	J
#26	2020	Secure data exchange between IoT endpoints for energy balancing using distributed ledger	[92]	J
#27	2020	BDSS-FA: A Blockchain-Based Data Security Sharing Platform With Fine-Grained Access Control	[93]	J
#28	2020	EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange	[94]	J
#29	2020	Decentralized patient-centric data management for sharing IoT data streams	[95]	C
#30	2020	Blockchain-Based Multi-Role Healthcare Data Sharing System	[96]	C
#31	2020	Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices	[97]	J
#32	2020	Subscription-Based Data-Sharing Model Using Blockchain and Data as a Service	[98]	J
#33	2020	Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals	[99]	J
#34	2020	TrustedChain: A Blockchain-based Data Sharing Scheme for Supply Chain	[100]	C
#35	2020	A multi-layered blockchain framework for smart mobility data-markets	[101]	J
#36	2021	Blockchain-Driven Trusted Data Sharing With Privacy Protection in IoT Sensor Network	[102]	J
#37	2021	MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain	[103]	J
#38	2021	Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control	[104]	J
#39	2021	A Cooperative Architecture of Data Offloading and Sharing for Smart Healthcare with Blockchain	[105]	C
#40	2021	ITrade: A Blockchain-based, Self-Sovereign, and Scalable Marketplace for IoT Data Streams	[106]	C
#41	2021	Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain	[107]	J

#42	2021	Medi-Block record: Secure data sharing using block chain technology	[108]	J
#43	2021	PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities	[109]	J
#44	2021	AgriOnBlock: Secured data harvesting for agriculture sector using blockchain technology	[110]	J
#45	2021	BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten	[111]	J
#46	2021	BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications	[112]	J
#47	2021	A conceptual IoT-based early-warning architecture for remote monitoring of COVID-19 patients in wards and at home	[113]	J
#48	2021	A blockchain-based trading system for big data	[114]	J
#49	2021	MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic	[115]	J
#50	2021	SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework	[116]	J
#51	2021	eHealthChain—a blockchain-based personal health information management system	[117]	J
#52	2021	A Threshold Proxy Re-Encryption Scheme for Secure IoT Data Sharing Based on Blockchain	[118]	J
#53	2021	A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection	[119]	J
#54	2021	FAST DATA: A Fair, Secure and Trusted Decentralized IIoT Data Marketplace enabled by Blockchain	[120]	J
#55	2021	Blockchain Assisted Secure Data Sharing Model for Internet of Things Based Smart Industries	[121]	J

[v] Venue type: J = Journal (34), C = Conference (21)

* The papers are also cited in the Bibliography

5.1.2 Domain Specification

As an adaptable technology, IoT is utilized across multiple areas, such as smart cities, manufacturing, energy, supply chain, automotive, and cross-domain/other, as outlined in Section 4.2.3 of our taxonomy. The diverse variety of application domains addressed by the selected primary studies is displayed in Figure 5.2.

The application domain labeled "Cross-domain/other" is the most dominant, represented by 44 out of 55 primary studies. There are four subcategories represented among the papers addressing cross-domain/other, more precisely, the healthcare, surveillance, smart toy, and generic domains. Healthcare had the greatest occupancy, represented by 21 out of 55 primary studies. The generic topic of sensor data comes to share first place with the healthcare domain, being addressed in 21 out of 55 primary studies as well. Whereas for the topic on smart toy and surveillance, they are only addressed in one study each.

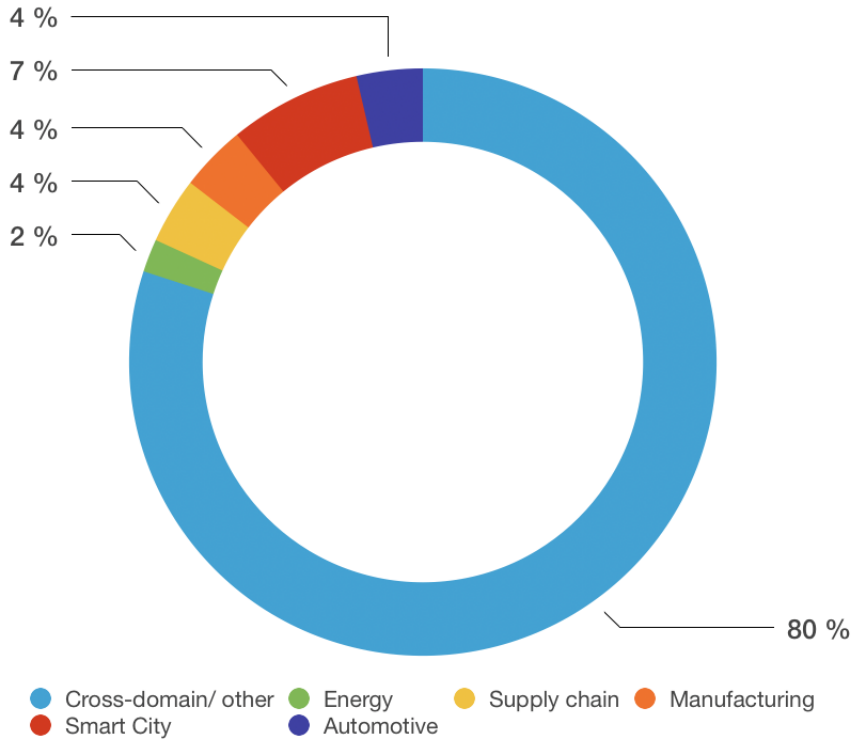

FIGURE 5.2: Overview of the application domain reported in the primary studies

5.1.3 Purpose and Benefits

The primary papers all 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 safely 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 delve further into the purpose and benefits of data sharing applicable specifically to the domain they address. Because our selection of studies covers a wide range of domains, it is evident that there are certain variances in purpose and benefits that are worth mentioning. We elaborate on the findings that have been a recurring theme and stand out the most.

Our findings in Section 5.1.1 clearly show that healthcare is the most prevalent domain in our set of primary studies related to secure IoT data sharing. The findings reveal that the core stakeholders in the healthcare sector are healthcare professionals and patients, and that the benefits of data sharing in the domain provide significant benefits to the stakeholders. The goal of these studies addressing health data sharing is similar to the general purpose and benefit stated above: to develop a reliable and efficient data sharing solution that allows data owners and users to safely exchange their data. However, their purpose and benefits go further.

By leveraging continuous patient monitoring as a tool to supplement traditional medical practice, the health service will be able to provide faster, but most importantly, accurate treatments based on the analysis of the patient's unique health data. As a result, using data sharing in the health sector might contribute to a more stable platform for healthcare professionals to make evaluations and decisions from, while also ensuring that the patient receives the correct treatment at the necessary

time. Therefore, by adapting data sharing, healthcare professionals gain a more effective technique of acquiring data without having to manually monitor patients, potentially transforming the domain from a time-consuming to a more efficient procedure.

Our findings show that the majority of our selection of primary papers with publications addressing the healthcare domain deal with data sharing within the same system. The work by Akkaoui *et al.* [94], 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. This requestor's role and what the data will be used for from the requestor's side are not elaborated on, but the illustrations in the paper, in addition to the division of the stakeholder doctor and requestor, indicate that the requestor may be from a different system.

Data sharing has a significant impact in the manufacturing industry as well. Customers, employees, governments, and organizations are all stakeholders in the manufacturing industry. Our selection of primary studies only includes two studies addressing the manufacturing domain. The research by Bai *et al.* [84] discusses data sharing between equipment nodes and other stakeholders involved. Service providers, smart factories, and third parties such as insurance, scientific research, and finance are particularly identified as the stakeholders.

Bai *et al.* [84] explain how the traditional manufacturing environment is complex, with various manufacturing equipment data often stored in separate systems. Because these systems may belong to multiple service providers, 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 paper. The data on the equipment comprises not just their capacity but also their status data. This data sharing can make research and development technology, manufacturing and distribution audits more effective, which assists production companies in reducing operating and manufacturing costs.

Finally, the studies generally emphasize the significant advantages of utilizing various data resources, as it will advance IoT technology, improve quality of life, and contribute to the global economy, with the goal of achieving more trusted and secure data transfer among various stakeholders, participants, and cross-domain industries.

5.1.4 IoT Data Sharing Architectures

Now that we have underlined the purpose and major benefits that come with data sharing as addressed in the set of the selected studies, we move on to the high-level results of the data sharing architecture models that have been leveraged by the primary studies. The extractions were categorized and filtered based on the data sharing models that were utilized. To be as specific as possible, we aim to extract the essential paradigm, such as determining whether the studies operate as a marketplace and, if so, whether the marketplace is a public or private one. The statistical results illustrated in Figure 5.3 reveal that there are primarily three IoT data sharing models that have been used by the primary studies, namely marketplace, domain-specific sharing, and peer-to-peer.

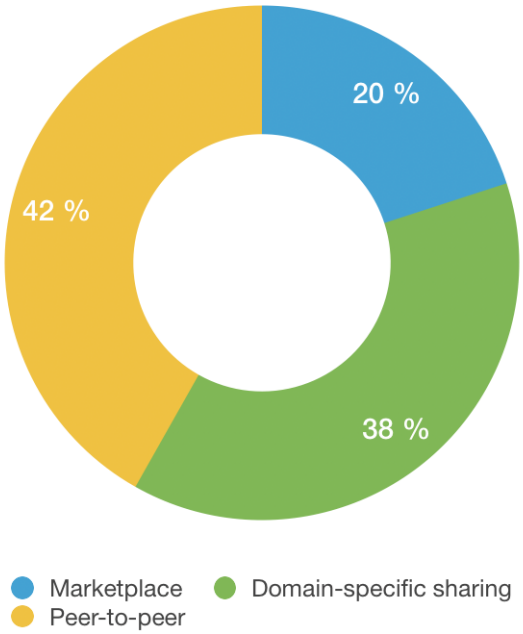

FIGURE 5.3: Statistical overview of the architecture models

The statistical findings, however, reveal that peer-to-peer is the most common model, accounting for 42% of all representation and immersion. Domain-specific sharing is ranked second, with a share of 38%. Finally, the marketplace is only represented by 19% of the set of selected studies. To provide a more exact approximation, the peer-to-peer model is addressed 23 times out of 55, domain-specific sharing 21 times out of 55, and the marketplace are represented 11 times out of the 55 primary studies we have analysed.

To emphasize, the differences between these three data sharing models are in terms of data management and governance perspectives. In domain-specific sharing, only stakeholders and interests from inside the domain are allowed to participate in the process. Peer-to-peer refers to the lack of a middleman; in other words, the absence of a central system in the solution. A marketplace, in contrast to peer-to-peer, implies the presence of a central system, at least to initiate the sharing process.

5.2 Low-Level Security Details

This section delves into the deeper details of our findings. Section 5.2.1 begins by introducing the threats and vulnerabilities. Furthermore, we elaborate on the techniques and approaches used to secure the solutions in Section 5.2.2, before diving into the details of data management and governance in Section 5.2.3.

5.2.1 Threats and vulnerabilities

Vulnerability refers to the quality or state of being exposed to the possibility of being attacked or harmed [122]. Solutions built and implemented by humans will always consist of human errors, which implies that vulnerabilities are inevitable. With vulnerabilities in existing solutions, the possibility for a threat to exploit a vulnerability increases.

However, by adhering to the OWASP top ten outlined in Section 2.5.7, solutions can prevent, or at the very least mitigate, the vulnerabilities. As a reminder, the OWASP top ten identifies the most serious risks and vulnerabilities that could affect IoT security. Table 5.2 illustrates what the primary studies handle, in terms of what kind of risks they address according to the OWASP list. The parameter "paper number" in the table is used as a reference to the primary studies presented in Table 5.1.

TABLE 5.2: List of issues compared to the OWASP top ten 2018

*Paper number**	**OWASP top ten**									
	I1	**I2**	**I3**	**I4**	**I5**	**I6**	**I7**	**I8**	**I9**	**I10**
#1						✓	✓			
#2					✓		✓			
#3		✓					✓			
#4							✓			
#5							✓			
#6						✓	✓			
#7						✓	✓			
#8							✓			
#9						✓	✓			
#10		✓					✓			
#11						✓	✓			
#12							✓			
#13						✓	✓			
#14						✓	✓			
#15		✓				✓	✓			
#16			✓				✓			
#17		✓					✓			
#18						✓	✓			
#19					✓					
#20		✓			✓		✓			
#21							✓			
#22		✓					✓			
#23		✓					✓			
#24							✓			
#25		✓					✓			
#26		✓					✓			
#27							✓			
#28		✓					✓			
#29						✓	✓			
#30							✓			
#31							✓			
#32					✓	✓	✓			

#33							✓			
#34		✓				✓				
#35		✓				✓	✓			
#36		✓								
#37							✓			
#38		✓				✓	✓			
#39			✓			✓	✓			
#40				✓		✓				
#41					✓		✓			
#42							✓			
#43						✓				
#44							✓			
#45						✓				
#46						✓				
#47						✓				
#48							✓			
#49							✓			
#50						✓				
#51						✓	✓			
#52							✓			
#53					✓	✓	✓			
#54		✓				✓	✓			
#55							✓			
Total papers that handle the issue (✓):	0	15	2	1	6	24	46	0	0	0

* The Paper number is referenced from Table 5.1

I1-I10 is referred from OWASP top 10 list in Table 2.1

✓ = handles the issue, **X** = lack of description about how it is handled, = not mentioned

The statistical findings show that the OWASP Top Ten list contains three outstanding vulnerabilities, primarily in the areas of insecure network services (I2), insufficient privacy protection (I6), and insecure data transfer and storage (I7), with the latter being the most well-represented by the primary studies. However, it is worth mentioning that these are not the only vulnerabilities covered; there are a few others, with one or two papers addressing insecure ecosystem interfaces (I3), a lack of secure update mechanism (I4), the use of insecure or obsolete components (I5), and a lack of device management (I8). There are no studies addressing weak, guessable, or hardcoded passwords (I1), insecure default settings (I9), or lack of physical hardening (I10).

5.2.2 Preserving Security - Techniques and approaches

The techniques and approaches used to preserve secure data sharing are wide. Since this subsection is broad and addresses many aspects, we are dividing the findings into two points. The first one, being the diverse use of techniques and approaches to preserve secure data sharing, and the second, being the statistical results related to security and its sub-groups of specifications. The security specification is in regards to the number of papers addressing different security aspects such as confidentiality, integrity, availability, authentication, authorization, and privacy.

The main contributions of the studies show that many of the recent solutions with respect to trusted IoT data sharing leverage the possibilities of blockchain technology, as illustrated in figure 5.4. The figure shows how 51 out of 55 primary studies utilize blockchain technology; 32 studies out of 55 primary studies utilize smart contracts; 10 papers address access control; and one paper utilizes the IDSA architecture [85]. Even though some papers utilize blockchain alone, most of the papers combine the blockchain technique with either smart contracts, access control, or identity management, or a combination of several.

The utilization of smart contracts varied from the studies. For example, the paper by Akkaoui *et al.* [94] elaborates how they use smart contracts to ensure automated regulation of rules and policies that govern access to the shared health data in a non-deniable way, where as the paper by Xu *et al.* [93] uses the smart contract in two ways, the first one being for validation, while the other contract is for decryption purposes. Just like how smart contracts solutions and use cases differ from study to study, so does access control management. Bai *et al.*[84] utilize a verification node, which is responsible for access management, with the access control policies written on the blockchain. In the paper by Alsharif *et al.* [89], they allow sellers of data to enforce their own access control policy on their encrypted records.

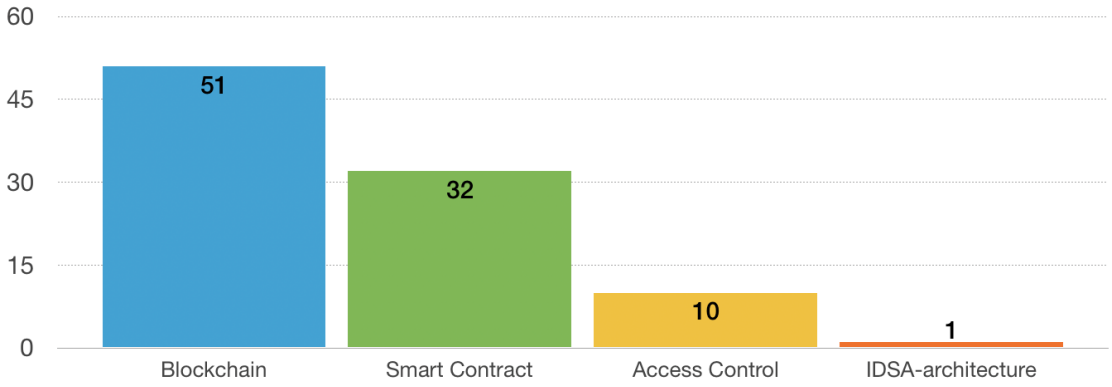

FIGURE 5.4: Statistics over trust aspects included by the primary studies

While 51 papers utilize the blockchain technology, 17 of these papers address what kind of blockchain type they deploy. From the selection of primary studies, there are 9 studies that are taking advantage of the Hyperledger Fabric, while 8 studies are addressing Ethereum. Figure 5.5 show the different representation of Hyperledger Fabric and Ethereum of the different domains. Domains that do not appear in this figure do not specify any specific blockchain type leveraged or do not include blockchain technology in their solution.

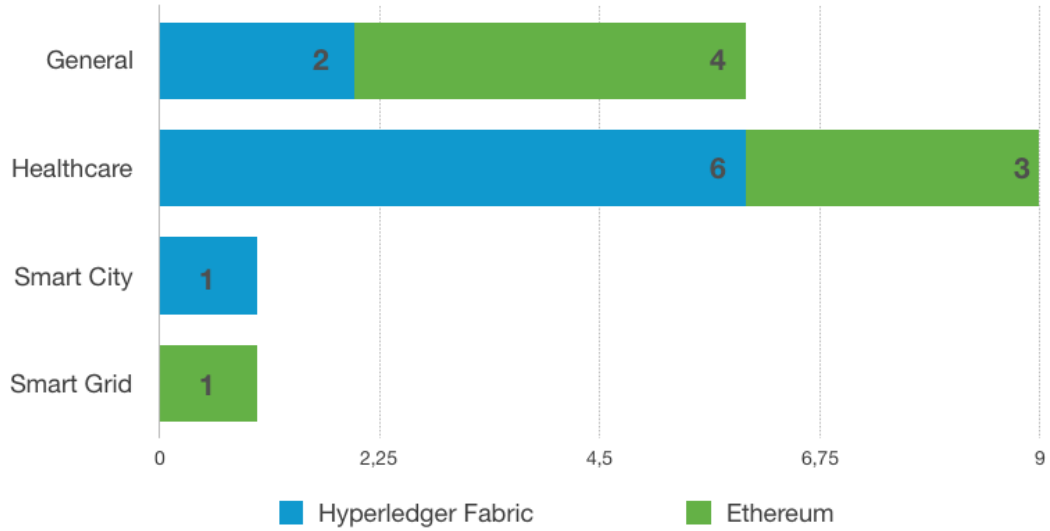

FIGURE 5.5: Blockchain types represented by the different domains

Hyperledger Fabric is mentioned in two [88] [120], and Ethereum in four [81] [86] [106] [114] of the studies with solutions addressing the general domain. In the healthcare domain, six studies [99] [111] [115] [116] [117] [119] leverage Hyperledger Fabric while three studies [91] [94] [103] use Ethereum. There is one paper [109] within the smart city domain that uses Hyperledger Fabric and one other paper [92] in the domain of the smart grid that uses Ethereum. There are many possibilities with each one of the different blockchain types. However, without any permission and the total transparency of Ethereum, the cost may affect the performance of scalability and privacy. Whereas for the Hyperledger, the consensus and access control have to be well defined. As the healthcare sector is the most addressed domain and tends to be associated with sensitivity and personal information, it is worth looking into why some studies, specifically three, have been utilizing the public Ethereum platform in this domain, as the Ethereum platform consists of total transparency.

The first paper by Akkaoui *et al.* [94] on EdgeMediChain points out that the Ethereum blockchain consists of a large, global development community, in addition to being completely open source and supporting a variety of use cases such as smart contracts and decentralized applications. As a result of these beneficial characteristics, the contribution has been to implement a prototype on the Ethereum blockchain to validate and evaluate the feasibility as well as the performance. As their contribution leverages the Ethereum blockchain in combination with smart contracts, they have included a permission mechanism. In their solution, all functions executed in the contract are logged in the ledger. Therefore, they exude an energetic and positive view of Ethereum's transparency. Since all transactions are going to be recorded, the blockchain is considered hacker-resistant, which will lead to it being more difficult to commit fraud within the system. Since everyone can join the Ethereum network, the solution assumes that the health data being shared is encrypted and anonymized to protect the privacy and real identity of patients.

As for the two others regarding MedShare by Minguyne *et al.* [103] and multi-party consent management by Madine *et al.* [91], they do combine the public Ethereum blockchain in combination with smart contracts as well. For the first one, a lot of

the focus is related to the implementation of the prototype and, thereafter, the performance evaluation. As for the latter one, they do address that even though their contribution keeps all patient data secure using public-key infrastructure (PKI) cryptography, certain sensitive files cannot be shared on the public Ethereum network due to privacy issues. However, they do address one possible solution to this problem, which is to use forks of Ethereum that are permissioned and private, such as Quorum and Hyperledger Besu.

Not only do the trust aspects and mechanisms presented in Figure 5.4, in addition to the different blockchain types, have an effect on data sharing. It is also the contribution, impact, and most importantly, the layers at which the data sharing is being done. The elaboration of the different architectural layers is done in our taxonomy, which can be found in Section 4.2.2. To summarize, the original seven layers have been divided into only three layers, namely perception, network, and application. A short description of what the three layers are covering is as follows:

- Perception: all the "Things" in IoT, e.g. machines, sensors or devices
- Network: communication and processing units, data element analysis and transformation
- Application: storage, aggregation and access, reporting, analytics and control, involving people and business processes

Based on the findings, the statistical results presented in Figure 5.6 give an overview of which architecture layer the data is being shared on. There is a noticeable layer that stands out from the crowd, namely the network layer, which is the most leveraged layer to share data on from our findings across the selection of our primary studies. The network layer is presented 35 times, followed by the application layer being represented 17 times, and finally the perception layer being represented 3 times.

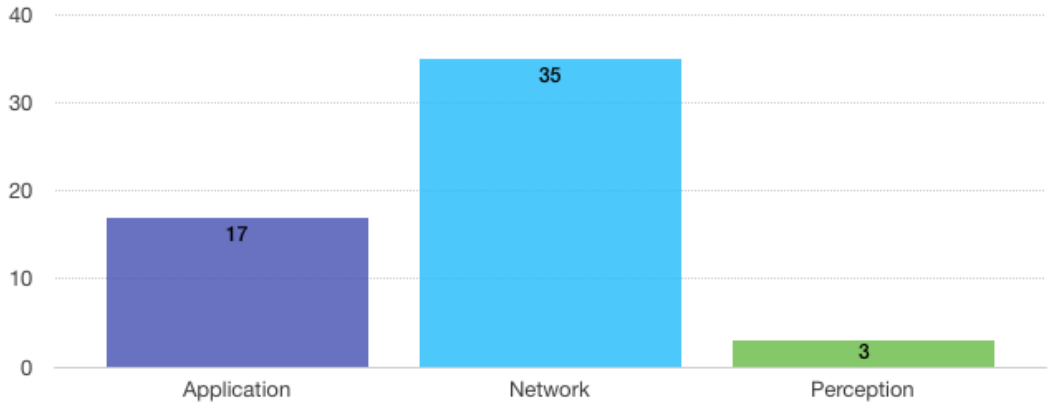

FIGURE 5.6: Overview of which architecture layer the data sharing are being done at

To leverage the great benefits of data sharing, the technical aspects of how the data is stored need to be considered as well. Today's solutions are trying to remove themselves from a traditional centralized solution and move to a more decentralized solution. With this in mind, the primary studies we have collected are introducing a distributed protocol for sharing and storing called the Interplanetary File System (IPFS). Compared with cloud storage, IPFS, as the peer-to-peer storage network it is[123], prevents the problem of a single point of failure.

However, with the introduction of the peer-to-peer protocol for sharing and storing, there are still some papers that utilize the cloud storage solution to save and retrieve encrypted data. More specifically, there are 13 studies [70] [72] [74] [76] [90] [91] [93] [94] [96] [100] [105] [116] [118], utilizing the peer-to-peer IPFS data storage protocol, while there are seven studies [69] [86] [98] [104] [105] [107] [119] that still utilize the traditional centralized cloud storage. The use of a third-party cloud service have been incorporated in some way or another, either as a primarily storage of data, or just a back-up storage.

When storing the data, studies have pointed out the huge difference between storing raw data versus encrypted data directly in their storage system. The findings show that a great number of selected primary studies have addressed this difference. There are 17 papers that utilize encryption. There are, however, only 11 papers addressing what type of encryption they utilize. From this number, there are six studies [69] [86] [91] [120] [114] [118] in total that utilize proxy re-encryption, while five other studies [76] [78] [93] [103] [89] practice attribute-based encryption (ABE) in their solution.

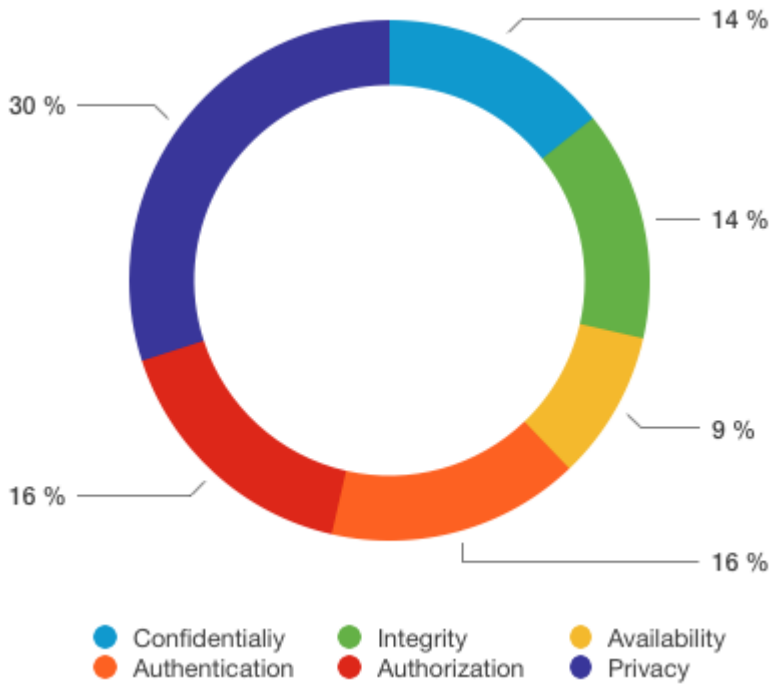

FIGURE 5.7: Security and its sub-groups of specification

The techniques and approaches that have been elaborated and presented have been the most regularly addressed and highlighted through a number of the primary studies. These techniques are also the protection mechanisms used to preserve security amongst the assets, which in this case are related to data. Moving forward from the techniques and approaches, we will measure from the statistical results what the most concerning security, in addition to privacy, topics are today.

As illustrated in Figure 5.7, the most concerning topic related to IoT data sharing is in regards to privacy, with an occupancy of 30%, followed by authentication with 16% and authorization of 16%. The statistical results show that availability is the least presented security topic with only 10%, when it comes to IoT data sharing.

However, to give a more precise presentation, Table 5.3 presents the selection of primary studies and the security qualities that they address. There are 20 studies about confidentiality, 20 studies about integrity, and 13 research studies about availability. Authentication, on the other hand, is represented 22 times, whereas authorization is represented 23 times. Privacy is the most frequently mentioned security quality, appearing in 42 of the 55 primary studies. According to the extraction, only five papers are concerned with the CIA triad. Three of the papers concerned with the CIA triad are in the healthcare domain [78] [90] [91] , while one study deals with smart cities [74] and the another with the generic domain [88].

5.2.3 Role of Data Management and Governance

The data governance establish the policies and procedures, which the data management implements. A few studies look at the necessity for access control from the standpoint of the data owner. A few ideas, in particular, would allow data owners control over their own data. A few other papers address GDPR [74] [109] and the California Consumer Privacy Act [74]. However, most of the primary articles do not go into as much detail or emphasis on the importance of data management and governance as we would like to see. In general, the primary studies have revealed relatively little information about the role and impact of data management and governance.

Because the value of data sharing is derived from the data itself, it is important to assess the data's quality for the purposes of reuse and valid analysis. DNV are experts in assurance and risk management, and are using their expertise to improve safety and performance while also setting industry benchmarks [124]. They have released a framework for data quality assessment [53], which explains how to assess data quality and was elaborated on in Section 2.5.6. The framework emphasizes the importance of data quality assessment and the need for continual monitoring of the quality. ISO 8000 [125] is another organization that provides approaches for managing, measuring, and improving the quality of data and information. However, none of the selected primary studies included inputs from DNV or ISO 8000, or other relevant data quality frameworks, demonstrating a lack of data quality management in the context of IoT data sharing.

TABLE 5.3: Application domains and security & privacy concerns from the primary studies

*Primary study #**	*Domain*	Security					Privacy
		C	I	Av	AuthN	AuthZ	
#1 [62]	Generic				X	X	
#2 [69]	Healthcare	X					X
#3 [70]	Generic				X	X	
#4 [71]	Generic	X					X
#5 [72]	Generic		X				
#6 [73]	Healthcare			X	X		
#7 [74]	Smart City	X	X	X		X	X
#8 [75]	Generic				X	X	X
#9 [76]	Supply Chain			X			X
#10 [77]	Smart Toy	X	X				
#11 [78]	Healthcare	X	X	X			X
#12 [79]	Healthcare						X

#13 [80]	Healthcare						X
#14 [81]	Generic						X
#15 [82]	Automotive				X	X	X
#16 [61]	Generic					X	
#17 [83]	Smart City				X	X	
#18 [84]	Manufacturing				X	X	X
#19 [85]	Generic		X				X
#20 [86]	Generic	X					
#21 [87]	Generic				X	X	X
#22 [88]	Generic	X	X	X			X
#23 [89]	Healthcare						X
#24 [90]	Healthcare	X	X	X			X
#25 [91]	Healthcare	X	X	X	X	X	X
#26 [92]	Smart Grid				X	X	
#27 [93]	Generic					X	
#28 [94]	Healthcare	X	X				X
#29 [95]	Healthcare			X			X
#30 [96]	Healthcare		X				X
#31 [97]	Generic	X			X	X	X
#32 [98]	Generic				X	X	X
#33 [99]	Healthcare		X				X
#34 [100]	Supply Chain		X	X			X
#35 [101]	Generic					X	X
#36 [102]	Automotive			X	X		X
#37 [103]	Healthcare	X					X
#38 [104]	Healthcare	X		X	X	X	X
#39 [105]	Healthcare				X		X
#40 [106]	Generic				X	X	X
#41 [107]	Generic	X	X		X		
#42 [108]	Healthcare				X	X	
#43 [109]	Smart City		X			X	X
#44 [110]	Generic	X	X		X		X
#45 [111]	Healthcare						X
#46 [112]	Healthcare	X		X	X		X
#47 [113]	Healthcare						X
#48 [114]	Generic	X	X			X	X
#49 [115]	Healthcare	X	X		X		X
#50 [116]	Healthcare	X	X			X	X
#51 [117]	Healthcare					X	X
#52 [118]	Generic	X					
#53 [119]	Healthcare		X	X			X
#54 [120]	Generic						X
#55 [121]	Manufacturing		X		X	X	X
Number of primary papers that address the corresponding quality characteristic		20	20	13	22	23	42

* The paper number is referenced from Table 5.1

C: Confidentiality, **I**: Integrity, **Av**: Availability, **AuthN**: Authentication, **AuthZ**: Authorization, **P**: Privacy

5.3 Gaps and Limitations

In this section, we present the gaps and limitations on IoT data sharing, including security and other open issues in this context. Section 5.3.1 addresses the main open limitations, before proceeding to the open issues in Section 5.3.2. Finally, in Section 5.3.3 we give a security evaluation of the selected primary studies against the OWASP top ten.

5.3.1 IoT Data Sharing Limitations

Throughout this study, we have identified some limitations, illustrated in Table 5.4. The limitations we are highlighting in this section are in regards to data sharing and its architecture. There were very few studies that directly addressed and discussed the limitations of their own solutions, but we still managed to find a couple that did. More precisely, there were nine research publications that discussed some type of limitation in regards to their contribution.

TABLE 5.4: List of limitations

ID	Limitation
Limitation1	Stress testing
Limitation2	Complexity
Limitation3	Scalability
Limitation4	Throughput/ Performance

A limitation that has been seen through a number of studies and findings is the lack of stress testing (*limitation1*). However, there are only four studies that explicitly address this limitation with their contribution, namely the contributing paper by Ali *et al.* [70], Zaghloul *et al.* [78], Sarabia-Jacome *et al.* [85] and Jamil *et al.* [99]. Stress testing means testing against different use cases and seeing the results of utilizing a larger scale network. In addition, a variety of the studies operate on one blockchain platform, but do mention the wish to test their solution on other blockchain platforms to see if the results could have significant meaning. As the IoT technology is widely used and connects a variety of devices within different domains and areas, it would be useful to see results on the performance when putting the solution under stress.

Furthermore, another limitation of IoT data sharing and its architecture is the concern about the heterogeneity nature of IoT (*limitation2*). As IoT technology makes human life more connected than ever over 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 [126]. 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.

Another limitation that is addressed is scalability (*limitation3*). The definition of scalability, when related to the domain of computer science, is the measure of a system's ability to increase or decrease in performance and cost in response to changes in

application and system processing demands [127]. When the studies mention scalability as a limitation, they refer to the growth in the number of participants and transactions. As a side note, as the complexity of a system increases, it will have an effect on the scalability of the same system. A hand-full of solutions find it difficult to handle moving parts and components, in addition to the foundational scalability of a decentralized marketplace. To summarize, as the primary studies are concerned about the complexity of their solution, there will also be an indirect concern about scalability as well.

Last, we have the limitation, which resolves around the throughput and performance of the solutions (*limitation4*). One of the papers elaborates on their blockchain architecture, which is hardly supported by high throughput performance. More specifically, the study related to smart toy edge computing data exchange [77] revealed that the maximum throughput was estimated to be a maximum of 50.000 requests per second. In general, as the IoT is often connected to critical infrastructure domains such as healthcare, the performance would have significant meaning, where the outcome of the effects could be critical.

FIGURE 5.8: The Internet of things and its wide range of connectivity (retrieved from [9])

5.3.2 Open Issues

Throughout our extraction, there were five papers [69] [74] [76] [95] [104] that mention more-or-less the open issues regarding their contributions in their papers. The other papers did not explicitly mention open issues, but we still extracted some form of open issues. The main findings related to the open issues have been divided into four topics, namely GDPR, access policy, cost, and storage. Table 5.5 reveals the issue with an ID, issue name and the phase in which the issue occurs in (before, during or after data sharing; or if its just a general issue that does not belong to any specific phase).

The paper by Lucking *et al* [95] discusses permission-less data management that empowers patients to securely and selectively share their own personal data. This paper discusses data management but mentions their lack of focus on how to address the compliance of GDPR; for instance, the erase of personal data (*issue1*). The open

issues were stated by the authors and are specific to their paper. On the other hand, this is an overall issue that applies to IoT data sharing or IoT security in general.

TABLE 5.5: List of open issues accumulated

ID	Issue	Phase
issue1	GDPR	General
issue2	Access Policy	Implementation
issue3	Cost	Implementation
issue4	Storage	Implementation

The paper presented by Wang *et al.* [76] discuss the data storage and sharing scheme in their contribution. They elaborate that their solution is safe only if the Ethereum blockchain network and the attribute-based encryption scheme are safe. They do mention that their contribution does not include an access policy update (*issue2*).

The paper from Ramachandran *et al.* [74] on decentralized data marketplace for smart cities do address the concern of cost (*issue3*). The concern about cost is associated with the transactions and the contracts used, which must be minimized to reduce the cost involved in using a decentralized data marketplace. They do, however, propose a solution that is worth investigating: a special short data format for storing metadata in the blockchain.

A common topic which turns out to be a recurring point in many, if not all of the studies, is the security issues regarding data storage (*issue4*). Some of today's solutions still utilize the cloud server. For instance, in eHealth, the contributions store a patient's health data and use medical records with the help of a centralized third-party solution. Even though the storage phase is done in combination with encryption, the solution utilizing a third-party solution still suffers from a single-point-of-failure. The paper by Al-Zahrani [98] is one of six that utilizes this type of storage system. The other papers that utilize a third party cloud provider are presented by Chen *et al.* [119], Manzoor *et al.* [107], Nguyen *et al.* [105], Manzoor *et al.* [86] and Sepehri *et al.* [69].

5.3.3 Security Evaluation

Section 5.2.1 includes a map of how well the primary studies were handling the common issues of OWASP's top ten threats and vulnerabilities. Table 5.2 represents the evaluation of the selection of primary studies against the OWASP top ten issues of IoT. To summarize, the contributions of the studies are evaluated and, if handled, a mark of ✓is included, or a blank (" ") if they do not handle or discuss the issue. There might be some check marks on contributions that may not handle the issue to a full extent due to the difference in scope. However, we have chosen to mark them as resolved as long as they handle the issue in some way, rather than if they do not cover it at all.

I1 is about weak, guessable, or hardcoded passwords. This can include the use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grant unauthorized access to deployed systems. As illustrated in Table 5.2, there are no primary studies handling I1. The

statistical results indicate that passwords as an authentication mechanism are not as widely used as the prime method when it comes to the topic of IoT data sharing.

I2 describes insecure network services, which resolves the unneeded or insecure network services running on the device itself. More specifically, those exposed to the internet that compromise the confidentiality, integrity, authenticity, or availability of information or allow unauthorized remote control. From the selection of primary studies, there are 14 studies that address L2. Most of the papers handle this issue by proposing an IoT network architecture with a decentralized access control.

I3 is about insecure ecosystem interfaces. The interfaces can vary from web, back-end API, cloud, and mobile interfaces. There are two primary papers that are concerned with I3, namely the paper by Preuveneers *et al.* [61] on multi-party policy-based access control and the study by Nguyen *et al.* [105] on cooperative architecture of data offloading and sharing for smart healthcare. The former handles the issue by having a configuration that creates more concurrent network connections from different clients to the cloud. The contribution to the latter was a decentralized IPFS storage system that was integrated with Amazon cloud and its network setup.

I4 resolves around the lack of a secure update mechanism, which can include the lack of firmware validation on the device, lack of secure delivery (un-encrypted in transit) and lack of notifications of security changes due to updates. Only one primary study, namely the paper presented by Niya *et al.* [106], addresses I4. To address the lack of secure delivery, the contribution of this paper is to have a privacy-aware data offloading scheme where data offloading is done to the edge server under system constraints.

I5 highlight the use of insecure or outdated components that would expose the device to being compromised. This includes the use of third-party software or hardware components. There are 7 out of 52 studies that include a third party solution, which is regarded as an insecure component when storing IoT data. The rest of the selection of primary studies have addressed the single-point-of-failure which occurs with the utilization of third party components. Therefore, the rest of the selection handles the issue by finding other ways to go from a traditional centralized third party solution to a more decentralized one.

I6 is addressing insufficient privacy protection, which means that a user's personal information is stored on the device or in the ecosystem that is used insecurely, improperly, or without permission. There are 24 primary papers discussing I6. The selection of primary studies has not generally addressed privacy protection from a device level, but rather from an ecosystem perspective. The papers that are handling the issue are making the data owners in control of their own data. With this measure, the data owner's privacy is regulated by themselves to a certain extent. In the combination of data owners' own control, there is strict access control with smart contracts, in addition to the removal of the traditional centralized storage solution to a more decentralized one.

I7 is concerned with insecure data transfer and storage. This could occur with a lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit or during processing. There are 43 primary papers

that are concerned with I7. All of the primary papers are concerned with storing raw data. First, they elaborate on the security concerns with storing raw data before introducing encryption as a solution. Many of the studies utilize encryption, whether it is of the type of attribute-based encryption or proxy re-encryption type, varies. When utilizing encryption, the contributions have utilized cryptographic keys, which are often saved within the smart contract. Most solutions include encryption in combination with strict access control, which was briefly mentioned in I6. They handle the access control in such a manner that the data owner is in control of what conditions and authentication should be fulfilled before granting access to the assets.

I8 is about a lack of device management. This includes a lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring and response capabilities. These issues are more related to the device than the ecosystem in which data is shared. Therefore, there are no primary studies in our selection of primary studies that address I8.

I9 resolves around insecure default settings. This is in regards to devices or systems shipped with insecure default settings or lacking the ability to make the system more secure by restricting operators from modifying configurations. There are zero studies in our selection of primary studies that address I9.

I10 discussed the lack of physical hardening, which can include everything from measures that allow potential attackers to gain sensitive information that could help in a future remote attack or take local control of the device. As mentioned in I8, this issue is also too specific related to the device level of data sharing. As a result, there are no studies in our selection of primary studies that address I10.

5.4 Discussion

This study provides a detailed analysis of the state-of-the-art in terms of secure data sharing and architecture for the IoT. We have elaborated on the process for the search and selection of the primary papers, in addition to the extraction of data, and presented the findings of our analysis. This section discusses our findings presented in Section 5.1–5.3 with the objective of answering our research questions.

5.4.1 What are the solutions for secure IoT data sharing? (RQ1)

In Section 5.1, we displayed a variety of statistical numbers and results, related to the solutions on secure IoT data sharing. As the results illustrate, studies that do address our topic and are relevant have been published in most recent years. From the findings, we elaborated on the high-level details such as interest and growth, domain specifications, purpose and benefits of data sharing, and the architecture models utilized for IoT data sharing.

We stated in Section 3.1 how the study introduced by Kuang Lo *et al.* [56] lacked some aspects. This was especially true in regards to the absence of information about who the stakeholders are in specific domains and why data sharing could be beneficial and of interest. Prielle *et al.* [59] also emphasized the lack of research on the

many types of benefits that data sharing could bring to the table. However, we were able to complement the work of both Kuang Lo *et al.* [56] and Prielle *et al.* [59] in regards to purpose and benefits of data sharing, as well as address some of the stakeholders involved. For example, we elaborated based on our primary studies that the stakeholders in the domain of manufacturing could be service providers, smart factories, and third parties. We were able to extract not only the domain's stakeholders, but also the purpose and benefits of why data sharing, for example equipment data sharing, could be beneficial.

According to our research, the healthcare industry has been the most popular and in the wind domain in recent years. However, the fact that healthcare is the most discussed topic in our research also gives us an indication that other domains need to be given greater attention when it comes to the use of IoT data sharing. Based on our findings, we can clearly claim that research in domains such as energy and manufacturing, which are relevant to our topic, is lacking. By shedding light on these topics as well, it will reveal not just the opportunities that may be further explored but also the security risks that come with exchanging data in the energy and manufacturing domains, as well as other domains.

Our taxonomy, as defined in Section 4.2, has served as a guide for extracting relevant data to answer the research questions. We can conclude that it has been challenging to fully answer RQ1 in terms of today's solution in the aspects of analytics. This is due to a lack of information as many studies do not cover or address the topic of data sharing in combination with analytic aspects, at least not in-depth. However, this could be related to the fact that most studies probably want to assure a secure manner of sharing data before they include other factors, such as data analytics. On the other hand, it is important to note that data analysis has benefits, such as reducing the amount of analysis that other stakeholders must perform. With this in mind, one can debate whether data analysis before sharing data to a stakeholder is restricting, in the sense that the stakeholder could have an interest in raw data for their own analysis tools and goals.

In conclusion, we anticipate an increase in papers addressing the research topic of secure IoT data sharing due to the widespread recognition of the importance and impact of IoT in our daily lives, as well as the recent growth in interest, and the prediction of future growth due to factors such as sustainability goals elaborated in Section 1.1.1.

5.4.2 What are the security and trust aspects of these IoT data sharing approaches? (RQ2)

In Section 5.2, we addressed some of the more in-depth details and aspects of the primary studies. We are aware, however, of the enormous diversity of strategies and approaches available in regards to our topic, making it difficult and not feasible to cover all of them in this study. Several detailed facts were discovered during the extraction process. However, the technical details of the trust and security mechanisms and approaches used, as well as the security benefits and drawbacks associated with their use, are the most important findings.

From the related work addressed in Chapter 3, Kuang Lo *et al.* [56] did not have a description of what architectural layer(s) that were used for the execution of data sharing. Our work complements this aspect by dividing the IoT World Forum Reference Model [64] into three layers, where our findings show that data sharing on

the network layer has been the most preferable. However, one could debate why the network layer is the most preferable in comparison to the application or perception layer, in addition to the question of whether the movement from a centralized to a more decentralized solution has been a factor. Additionally, the study looked at how blockchain and access control procedures could help with the key issue of a centralized solution's single-point-of-failure. This was, however, elaborated upon with a high-level perspective.

Our findings are in agreement with the related work by Kuang Lo *et al.* [56], as several of our selected primary studies would move towards a decentralized solution, based on blockchain technology and access control management, which brings the possibility of preventing single-point-of-failure. We were able to conduct further extractions on the blockchain technology. For example, we extracted the differences between public and private blockchains, where 17 studies highlight the difference between Hyperledger Fabric and Ethereum.

However, our data shows that blockchain and access control were not the only strategies and approaches used to prevent the critical single-point-of-failure problem. Because data sharing is frequently a procedure that often requires an agreement between two or several parties, where smart contracts are often employed, the data must be kept safe until the agreement is fulfilled. As a result, the use of IPFS, a decentralized peer-to-peer storage system, has become very widespread.

FIGURE 5.9: How a peer-to-peer network on the left are illustrating the connectivity of the real world on the right (retrieved from [9])

The work by Prieelle *et al.* [59] highlighted the importance of governance in access and usage for future research directions. This was, however, in relation to data platforms. Kuang Lo *et al.* [56] also addressed a topic related to governance, namely data management and its lack in research. Our work has struggled to supplement the aspects of both data management and governance to the related work, as the primary studies do not mention specific policies, standards, or guidelines that have been taken into account in their contributions.

The statistical data from our extraction, in terms of security, are the results of the contribution's use of a variety of methodologies and approaches. As shown, there is an average and equal distribution of concerns about various security topics. On the other hand, the topic of privacy stands out because it is discussed nearly twice as much compared to any security term. There are only six contributions that cover the CIA principles. Even if other studies might cover the aspects of the CIA triad, contributions that lack elaboration and explanation could not be included. Because

the CIA triad forms the core foundation for developing secure information systems, a lack of awareness could lead to threats and vulnerabilities when applying the various solutions to everyday life.

We discussed how the taxonomy helps as a guide in determining what data would be extracted to address and answer the research questions in the previous subsection. As a result, we can conclude that we have some shortcomings in the findings that contribute to our inability to fully answer RQ2. In particular, RQ2.3, in terms of the impact and role of data management and governance. This is because the majority of the primary studies we looked at did not include any specific standards, policies, or procedures that might have contributed to their solution for secure IoT data sharing. Even though GDPR was mentioned a few times, there was no in-depth explanation of how it was used as a contributing factor to secure the data sharing process. An additional lack of research is in regards to the aspect of identity management. Some papers may have briefly mentioned identities and certificates related to connected participants. However, because this has not been thoroughly elaborated on, it cannot be included in our statistical findings.

5.4.3 What are the current limitations of the IoT data sharing and what are the open issues to be further investigated? (RQ3)

The limits and unresolved issues were presented and elaborated in Section 5.3, based on the findings of the selection of primary studies. By revealing these limitations and issues, it contributes to a clear understanding of what the studies lack in terms of research, awareness of rules, guidelines, and standards, and other potential limits of their contribution. However, it is worth noting that the limitations are specific to a specific contribution, which can be resolved. Whereas for the open issues, it might be of a greater-scale of difficulty, but should not be impossible to handle. Another advantage of illustrating the limitations and open issues is the possibility of other research directions worth exploring and the introduction of a more in-depth analysis of issues that are not that obvious.

The list of open issues and limitations, in addition to comparing the studies against the OWASP list, was carried out to provide a scope of gaps in the primary studies. The studies illustrate gaps in current research within the fields of IoT data sharing and general IoT security. Even though we used the OWASP list from 2018, it is still relevant, especially since these issues may still be found in today's solutions. Our elaboration in Section 1.1.2 could be evidence that these problems have still arisen in recent years.

The obtained findings by evaluating the primary studies against the OWASP list were not surprising in the sense that insecure network services (I2), insufficient privacy protection (I6), and insecure data storage and transfer (I7) were the most addressed OWASP issues in regards to our scope of secure IoT data sharing. Our statistical findings, however, reveal that the ten OWASP security concerns are not equally represented. The majority of studies are focused on the three security threats outlined, whereas two studies deal with I3, one with I4, and six with I5. Furthermore, I1, I8, I9, and I10 have not been represented in any way. We may conclude that I2, I6, and I7 are the most important factors to consider while using IoT data sharing. Nevertheless, the statistical evidence gives us an overview that several OWASP threats and vulnerabilities have been neglected and overlooked. It is worth mentioning

that a lack of understanding and awareness of the other OWASP threats and vulnerabilities could pose a risk while incorporating their contributions into everyday life. Therefore, a comparison of today's solution against OWASP or other standards should be further investigated to see if there is a continuation in studies neglecting fundamental practices and standards.

According to the findings, privacy is highly represented in the primary studies. On the other hand, the lack of basic security aspects is also shown by the statistics, which is supported by the fact that just a few of the selected studies address the CIA triad. Therefore, an aspect to be further investigated is the evaluation of security and privacy concerns that are being addressed in today's solution on our scope of secure IoT data sharing.

From our findings, there is a lack of research and attention in the context of data management and governance. This was clearly demonstrated in the study by Lucking *et al.* [95], which stated that their contribution lacked a focus on how to manage GDPR compliance. The influence of data management and governance has varied depending on what has been addressed, and no precise findings have been made regarding what standards, policies, and guidelines have been taken into account in the various contributions and implementations.

To summarize, there should be further research on the security and privacy aspects of today's data sharing solutions, including the methods and strategies used to ensure secure IoT data sharing. By looking into the relationship between various trust and security mechanisms and methodologies as well as the security and privacy evaluation of studies, one may be able to uncover underlying reasons why, for instance, the CIA triad is not being addressed as much as desired. Additional future research should also be the elaboration of the significance and influence of data management and governance. For example, detailed evaluations of the standards, policies, and guidelines currently in use should be provided, as should explanations of how each standard or policy contributes to the security of one or several aspects of data sharing.

5.5 Threats to Validity

In this section, we discuss the different concerns, limitations, and threats to the validity of our systematic literature review. The elaboration on validity will be conducted by combining our experience from the work with the knowledge gained from the guidelines introduced by Kitchenham *et al.* [44].

5.5.1 Search Process

There are a number of pitfalls when performing a systematic literature review. One of them is related to how the search process have been conducted. Section 4.1.2 regarding our search strategy includes the keywords and queries, which were adjusted based on the database search engine and thereafter applied to the different electronic databases. The grouping of different domains, such as data sharing, application and security domains, including the keywords, which were then separated into the domain groups, can therefore be used as proof of the validity and limitations of the study, as there are an infinite number of other keywords that could be included in the search query.

However, to defend the selection of our search query, we performed a test case to have a handful of quality test set papers that we believe are relevant and should be included in our research. These test papers are used to estimate the quality of our search query results. If the search results in the electronic database X includes all of the test set papers that are published by X, we know that the relevance of the other papers in the result is somehow relevant. If not, we may believe there is a lot of noise in our search.

Secondly, since the number of hits as a result of our search on the IEEE Xplore database gave a number greater than 2000, we had to filter the result to only include papers related to "Internet of Things". This is a threat to our study due to the limitations resulting from the filtering, since there may be papers in the original IEEE Xplore result that might be of our interest but unfortunately have not been included in our research.

5.5.2 Selection of Primary Studies

The studies that have been included in our selection of primary studies from our SLR, by passing our inclusion and exclusion criteria, in addition to being relevant based on our predefined taxonomy, can still be doubtful. There might be relevant studies we have overlooked or publications we have missed out on during our search phase, specifically when searching, skimming, and selecting the relevant papers from the results of our search query. It is also worth mentioning that the process of selecting primary studies was completed in December 2021, which means that we have missed out on the latest publications from early 2022 that may be of interest.

5.5.3 Data Extraction

We briefly mentioned in Section 5.4 that we have chosen to not include papers in some statistical results if they do not elaborate or discuss their methods and security mechanisms to a certain extent. However, this line between including or not including papers in some statistical results may vary based on the researchers and their knowledge of the research field. With this in mind, there may be inconsistencies in our statistical model and data, implying that we may have some marginal differences that prevent us from offering 100 percent accuracy.

5.5.4 The Snowballing Process

The snowballing process is usually a part of the search process and is often performed after the automatic and manual search. The snowballing strategy is often executed to ensure that the final set of primary papers is complete. The technique includes searching the reference list, papers that cite a current primary paper, and personal home page publication lists of current primary studies for possible additional primary papers.

However, we did not perform this process and can therefore not categorize our systematic literature review as a fully exhaustive in-depth study. With the non-existent execution of the snowballing process, we may have missed some primary studies relevant to our scope on secure IoT data sharing. Therefore, as we have not carried out the snowballing process, this may be regarded as a limitation to our study.

Chapter 6

Conclusions and Future Work

The amount of already existing work related to IoT data sharing is enormous. On the other hand, few solutions, focus on data sharing in combination with taking into account certain guidelines and policies, which can be critical in the whole IoT data sharing ecosystem. In Section 6.1, we conclude our SLR and highlight the remarks. Finally, in Section 6.2, we make recommendations for future work.

6.1 Conclusions

Traditionally, centralized cloud-based solutions have dominated in the IoT data sharing domain. This implies that the solution relies on a single trusted third-party. However, there is a growing interest in utilizing blockchain's decentralized qualities. From our findings, the objectives behind the use of blockchain are the following: the removal of the centralized third party, immutability, improved data sharing, enhanced security, and reduced overhead costs in distributed applications.

This study contains background information on data sharing in the context of the IoT as well as its related subjects, such as data management and governance. In addition, we have elaborated on the most relevant security terminology to distinguish between trusted and non-trusted data sharing. We have analyzed some related work, before elaborating on our research methodology. Finally, we presented our findings and discussed them in regards to how they answer our research questions.

In our introduction, we discussed various concerns, particularly those related to security and privacy, that might contribute to secure data sharing. With the assistance of our methodology, we have been able to analyze the current state-of-the-art of IoT data sharing. According to our findings, there are some weaknesses in the number of existing IoT data sharing solutions. More specifically, in regards to the absence of addressing some aspects related to data sharing, such as security, testing, and the necessity of data management and governance, all of which lead to a lack of trust and the secure aspect of IoT data sharing. We had three success criterias used as foundation for conducting this study, in addition to our research questions elaborated in Section 4.1. of our review protocol:

- The systematic literature review must find out the existing approaches in the state-of-the-art of secure IoT data sharing, management, and governance.
- The systematic literature review must explicitly describe the threats and address the validity of solutions to IoT data sharing.

- The systematic literature review must assess the topics' current practice and the gap between this and the state-of-the-art.

We have now managed to:

- Discover the most widely used approaches in the current state-of-the-art of secure IoT data sharing, management, and governance.
- Elaborated on the threats and most concerning vulnerabilities, in addition to comparing the solutions against the OWASP top ten, in an attempt to emphasize the validity of the different contributions.
- Brought up the current practices used and the gaps that exist, especially regarding the necessity of data management and governance contributions, and their important influence on the domain.

With our study, we hope to see a continuation of the increase in relevant publications in the years to come. There are some gaps in the SotA to be addressed regarding security, as we discussed in Section 5.4, especially in addition to privacy and data management and governance. With more research, tools, studies, secure solutions, specific guidelines, policies, and standards on data sharing, we can increase the connectivity with safety and trustworthiness increasing as well.

6.2 Future Work

Researchers have in recent years discovered the importance of addressing secure IoT data sharing among the stakeholders, as illustrated by Figure 5.1. Even though research on the topic has increased in recent years, there is still a need for further research in the field since IoT is becoming an increasingly important part of our everyday lives.

There have been remarks on our findings, which have been recurring in a number of studies. We elaborate on these discoveries by first looking at the decentralized approach in Section 6.2.1, before examining the possibilities that collaboration across domains could bring to the table in Section 6.2.2. In Section 6.2.3, we discuss the benefits of data sharing and analytics combined, before moving on to data management and governance in Section 6.2.4. Furthermore, we elaborate on an extension of our SLR in Section 6.2.5, before finally addressing the importance of data quality in Section 6.2.6.

6.2.1 The Decentralized Approach

We have begun to move in the direction of leaving the traditional centralized cloud-based approach, heavily relying on a single trusted third party. However, with the increasing discovery of blockchain as an emerging technique to provide an approach for managing data in a decentralized manner, there are still many aspects of this approach and its related components to consider, in addition to doing further research on. These aspects can be considered the gap between public versus private blockchain, and which is the most preferable blockchain technology type that should be utilized in specific IoT domains and the reasoning behind it. In addition, as a result of the choice of blockchain type, what ripple effects may occur.

6.2.2 Collaboration Across Domains

Cooperation and collaboration by sharing IoT resources among different stakeholders in a specific domain has been shown to give an advantage in increasing the quality of day-to-day life. However, exchanging data beyond the specific domain and across domains has not been explored to its fullest yet. This was particularly evident in our findings, especially in the healthcare domain, where we discovered that they were mostly concerned about data sharing within the same system. Therefore, the combination of different data sources with data sharing across domains can enable IoT technology to reach even further and discover even more possibilities in the future, as well as increase the quality of life in parallel.

6.2.3 The Effects of Combining Sharing and Analytics

From our extraction, we have found that there is a lack of material about the combination of data analytics and sharing. However, in the search and selection process, there are numerous papers addressing the issue which can occur when the data owner analyses the raw data and shares this analysed data instead of the raw data. More specifically, the discussion of whether receiving already analyzed and processed data or unprocessed data makes a difference to stakeholders in the IoT ecosystem. Further research on combining data sharing and analytics can lead to increased knowledge of trade-offs and what data type is preferred in the market.

6.2.4 Data management and governance

There are 46 out of 55 primary papers that are concerned about I7 from the OWASP Top Ten, illustrated in Table 5.3. To give a brief reminder of what I7 from the OWASP top ten is addressing, it is related to insecure data transfer and storage. This security threat is addressed in the primary studies through access control in the IoT data sharing environment. The fundamental principle is that data owners should have the right to decide whether, with whom, and when to share their data. Based on our findings, this is an interesting topic which is in the spotlight, and it would be great to have further research on how to make access control the most secure and applicable in diverse solutions. However, our findings show there is a lack of research on the topic of data management and governance. Therefore, future research should highlight both the need and importance of data management and governance, in addition to address specific standards, policies and guidelines that should be or are considered as well.

6.2.5 An extension of our SLR

We discussed some of the threats to our work in Section 5.5, where one was in regards to the snowballing process elaborated in Section 5.5.4. A proposal for future research on our scope and study is to perform the snowballing method on the list of the selected primary studies to both enrich and update the list of primary studies. This, in turn, can contribute to an enrichment, reinforcement, and update on already existing analyses while also uncovering new analyses that have yet to be identified.

6.2.6 Data Quality

The great value of data sharing often derives from the data itself. Therefore, it is important that the data being sent and received is of quality to ensure that analyses

and the use of data are valid. However, our findings show a lack of addressing the importance of data quality, in addition to the assessment of data quality. We elaborated that DNV have published a data quality assessment framework [53], in addition to quality assessment methods by ISO 8000 [125]. Future research should have a focus on data quality in regards to the scope of IoT data sharing, where the consideration of DNV and ISO 8000's contributions could be of interest.

Bibliography

[1] L. Horwitz, *The future of iot miniguide: The burgeoning iot market continues*, Accessed: 06.05.2021. [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/future-of-iot.html.

[2] L. Mearian, *Hackers can access the nissan leaf via insecure apis*, Accessed: 19.02.2021. [Online]. Available: https://www.computerworld.com/article/3036964/hackers-can-access-the-nissan-leaf-via-insecure-apis.html.

[3] Oracle, *What is iot?* Accessed: 12.05.22. [Online]. Available: https://www.oracle.com/internet-of-things/what-is-iot/.

[4] e. t. Josh Howarth, *80+ amazing iot statistics (2022-2030)*, Accessed: 12.05.22. [Online]. Available: https://explodingtopics.com/blog/iot-stats.

[5] A. Staff, *Mercedes-benz joins the climae pledge*, Accessed: 12.05.22. [Online]. Available: https://www.fierceelectronics.com/electronics/role-iot-sensors-covid-19.

[6] P. Wegner, *Global iot market size grew 22% in 2021 — these 16 factors affect the growth trajectory to 2027*, Accessed: 12.05.22. [Online]. Available: https://iot-analytics.com/iot-market-size/#:~:text=In%20short,plays%20in%20reaching%20sustainability%20goals..

[7] F. E. Ehtesham Peerzade, *The role of iot sensors in the covid-19 fight*, Accessed: 12.05.22. [Online]. Available: https://www.fierceelectronics.com/electronics/role-iot-sensors-covid-19.

[8] Technative, *Cyber attacks from 2021 we need to talk about*, Accessed: 12.05.22. [Online]. Available: https://technative.io/cyber-attacks-from-2021-which-we-need-to-talk-about/#:~:text=The%20Verkada%20breach%3A%20The%20dark,cloud%2Dbased%20video%20security%20service..

[9] pixabay, *Internet of things*, Accessed: 10.05.22. [Online]. Available: https://pixabay.com/.

[10] N. Ferry, J. Dominiak, A. Gallon, E. González, E. Iturbe, S. Lavirotte, S. Martinez, A. Metzger, V. Muntés-Mulero, P. H. Nguyen, A. Palm, A. Rego, E. Rios, D. Riviera, A. Solberg, H. Song, J.-Y. Tigli, and T. Winter, "Development and operation of trustworthy smart iot systems: The enact framework," in *Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment*, J.-M. Bruel, M. Mazzara, and B. Meyer, Eds., Cham: Springer International Publishing, 2020, pp. 121–138, ISBN: 978-3-030-39306-9.

[11] N. Ferry, H. Song, R. Dautov, P. Nguyen, F. Chauvel, *et al.*, "Model-based continuous deployment of sis," *DevOps for Trustworthy Smart IoT Systems*, p. 59, 2021.

[12] N. Ferry, P. H. Nguyen, H. Song, E. Rios, E. Iturbe, S. Martinez, A. Rego, *et al.*, "Continuous deployment of trustworthy smart iot systems.," *The Journal of Object Technology*, 2020.

[13] N. Ferry and P. H. Nguyen, "Towards model-based continuous deployment of secure iot systems," in *2019 ACM/IEEE 22nd International Conference on*

Model Driven Engineering Languages and Systems Companion (MODELS-C), 2019, pp. 613–618. DOI: 10.1109/MODELS-C.2019.00093.

[14] N. Ferry, P. Nguyen, H. Song, P.-E. Novac, S. Lavirotte, J.-Y. Tigli, and A. Solberg, "Genesis: Continuous orchestration and deployment of smart iot systems," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1, 2019, pp. 870–875. DOI: 10.1109/COMPSAC.2019.00127.

[15] P. Nguyen, N. Ferry, G. Erdogan, H. Song, S. Lavirotte, J.-Y. Tigli, and A. Solberg, "Advances in deployment and orchestration approaches for iot - a systematic review," in *2019 IEEE International Congress on Internet of Things (ICIOT)*, 2019, pp. 53–60. DOI: 10.1109/ICIOT.2019.00021.

[16] P. H. Nguyen, N. Ferry, H. S. Gencer Erdogan, S. Lavirotte, J.-Y. Tigli, and A. Solberg, "A systematic mapping study of deployment and orchestration approaches for iot," 2019.

[17] Microsoft, *Azure iot reference architecture - azure reference architectures*, Accessed: 04.03.2021. [Online]. Available: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/iot.

[18] Quartic.ai, *Smart manufacturing*, Accessed: 04.05.2021. [Online]. Available: https://www.quartic.ai/smart-manufacturing/.

[19] Oracle, *What is data management?* Accessed: 01.03.2021. [Online]. Available: https://www.oracle.com/database/what-is-data-management/.

[20] P. H. Nguyen, S. Sen, N. Jourdan, B. Cassoli, P. Myrseth, M. Armendia, and O. Myklebust, "Software engineering and ai for data quality in cyber- physical systems - sea4dq'21 workshop report," *SIGSOFT Softw. Eng. Notes*, vol. 47, no. 1, 26–29, 2022, ISSN: 0163-5948. DOI: 10.1145/3502771.3502781. [Online]. Available: https://doi.org/10.1145/3502771.3502781.

[21] M. H. Mervat Abu-Elkheir and N. A. Ali, *Data management for the internet of things: Design primitives and solution*, Accessed: 02.05.2022. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3871070/.

[22] damadach, *Who we are. our mission*, Accessed: 13.05.22. [Online]. Available: https://damadach.org/.

[23] R. S. Seiner, *Data governance and the internet of things*, Accessed: 04.05.2021. [Online]. Available: https://www.slideshare.net/Dataversity/data-governance-and-the-internet-of-things.

[24] T. Rajmohan, P. H. Nguyen, and N. Ferry, "A decade of research on patterns and architectures for iot security," *Cybersecurity*, vol. 5, no. 1, pp. 1–29, 2022.

[25] T. Rajmohan, P. H. Nguyen, and N. Ferry, "Research landscape of patterns and architectures for iot security: A systematic review," in *2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, 2020, pp. 463–470. DOI: 10.1109/SEAA51224.2020.00079.

[26] T. Rajmohan, P. H. Nguyen, and N. Ferry, "A systematic mapping of patterns and architectures for iot security.," 2020.

[27] B. Bernard, *What is cia (in cybersecurity)?* Accessed: 03.05.2022. [Online]. Available: https://www.deepwatch.com/blog/cia-in-cybersecurity/#:~:text=In%20cybersecurity%2C%20CIA%20refers%20to,of%20your%20information%20security%20program..

[28] P. H. Nguyen, S. Ali, and T. Yue, "Model-based security engineering for cyber-physical systems: A systematic mapping study," *Information and Software Technology*, vol. 83, pp. 116–135, 2017, ISSN: 0950-5849. DOI: https://doi.org/10.1016/j.infsof.2016.11.004. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950584916303214.

[29] P. H. Nguyen, M. Kramer, J. Klein, and Y. L. Traon, "An extensive systematic review on the model-driven development of secure systems," *Information and Software Technology*, vol. 68, pp. 62–81, 2015, ISSN: 0950-5849. DOI: https://doi.org/10.1016/j.infsof.2015.08.006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950584915001482.

[30] L. Lúcio, Q. Zhang, P. H. Nguyen, M. Amrani, J. Klein, H. Vangheluwe, and Y. L. Traon, "Chapter 3 - advances in model-driven security," in *Advances in Computers*, ser. Advances in Computers, A. Memon, Ed., vol. 93, Elsevier, 2014, pp. 103–152. DOI: https://doi.org/10.1016/B978-0-12-800162-2.00003-8. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128001622000038.

[31] P. H. Nguyen, J. Klein, Y. Le Traon, and M. E. Kramer, "A systematic review of model-driven security," in *2013 20th Asia-Pacific Software Engineering Conference (APSEC)*, vol. 1, 2013, pp. 432–441. DOI: 10.1109/APSEC.2013.64.

[32] P. H. Nguyen, K. Yskout, T. Heyman, J. Klein, R. Scandariato, and Y. Le Traon, "Sospa: A system of security design patterns for systematically engineering secure systems," in *2015 ACM/IEEE 18th International Conference on Model Driven Engineering Languages and Systems (MODELS)*, 2015, pp. 246–255. DOI: 10.1109/MODELS.2015.7338255.

[33] I. 27000, *Information technology — security techniques — information security management systems — overview and vocabulary*, Accessed: 16.05.2022. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en.

[34] ——, *Information technology — security techniques — information security management systems — overview and vocabulary*, Accessed: 16.05.2022. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en.

[35] Certmike, *Confidentiality, integrity and availability - the cia triad*, Accessed: 09.05.22, 2016. [Online]. Available: https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/.

[36] O. L. Dictionaries, *Authenticate*, Accessed: 10.05.22. [Online]. Available: https://www.oxfordlearnersdictionaries.com/definition/english/authenticate.

[37] ISO, *It security and privacy - a framework for identify management - part 1: Terminology and concepts*, Accessed: 10.05.22. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en.

[38] O. L. Dictionaries, *Authorization*, Accessed: 10.05.22. [Online]. Available: https://www.oxfordlearnersdictionaries.com/definition/english/authorization.

[39] P. H. Nguyen, P. H. Phung, and H.-L. Truong, "A security policy enforcement framework for controlling iot tenant applications in the edge," in *Proceedings of the 8th International Conference on the Internet of Things*, ser. IOT '18, Santa Barbara, California, USA: Association for Computing Machinery, 2018, ISBN: 9781450365642. DOI: 10.1145/3277593.3277602. [Online]. Available: https://doi.org/10.1145/3277593.3277602.

[40] L. D. B. Samuel D. Warren, *The right to privacy*, Accessed: 04.10.2021. [Online]. Available: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.

[41] ——, *The right to privacy*, Accessed: 04.10.2021. [Online]. Available: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

[42] ISO, *Iso/iec 29100:2011(en) information technology — security techniques — privacy framework*, Accessed: 18.10.2021. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en.

[43] C. Dictionary, *Review*, Accessed: 03.05.2022. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/review.

[44] B. Kitchenham and S Charters, *Guidelines for performing systematic literature reviews in software engineering*, 2007. [Online]. Available: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf.

[45] ISO, *Consumers and standards: Partnership for a better world*, Accessed: 03.05.2022. [Online]. Available: https://www.iso.org/sites/ConsumersStandards/1_standards.html#:~:text=Standards%20ensure%20consistency%20of%20essential,an%20invaluable%20source%20of%20knowledge..

[46] G. EU, *What is gdpr, the eu's new data protection law*, Accessed: 03.05.2022. [Online]. Available: https://gdpr.eu/what-is-gdpr/#:~:text=The%20GDPR%20entered%20into%20force,were%20required%20to%20be%20compliant..

[47] ——, *What is gdpr, the eu's new data protection law?* Accessed: 03.04.2021. [Online]. Available: https://gdpr.eu/what-is-gdpr/.

[48] ISO, *Iso 37156:2020(en)smart community infrastructures — guidelines on data exchange and sharing for smart community infrastructures*, Accessed: 19.02.2021. [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso:37156:ed-1:v1:en.

[49] I. A. T. for Humanity, *Ieee data access and use policy*, Accessed: 19.02.2021. [Online]. Available: https://www.ieee.org/ieee-data-access-and-use-policy.html.

[50] IDSA, *Innovating the future of daa exchange in europe and beyond*, Accessed: 03.05.2022. [Online]. Available: https://internationaldataspaces.org/we/.

[51] ——, *Idsa is at the forefront of europe's digital future*, Accessed: 03.05.2022. [Online]. Available: https://internationaldataspaces.org/we/ids-in-europe/.

[52] Gaia-X, *Gaia-x: A federated data infrastructure for europe*, Accessed: 19.02.2021. [Online]. Available: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

[53] DNV, *Data quality assessment framework*, Accessed: 14.05.22. [Online]. Available: https://rules.dnv.com/docs/pdf/DNV/RP/2017-01/DNVGL-RP-0497.pdf.

[54] T. O. Foundation, *Owasp top 10 provacy risks*, Accessed: 04.10.2021. [Online]. Available: https://owasp.org/www-project-top-10-privacy-risks/.

[55] OWASP, *Owasp top 10 internet of things*, Accessed: 15.03.2022. [Online]. Available: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf.

[56] S. K. Lo, Y. Liu, S. Y. Chia, X. Xu, Q. Lu, L. Zhu, and H. Ning, "Analysis of blockchain solutions for iot: A systematic literature review," *IEEE Access*, vol. 7, pp. 58 822–58 835, 2019. DOI: 10.1109/ACCESS.2019.2914675.

[57] M. Alharby, A. Aldweesh, and A. v. Moorsel, "Blockchain-based smart contracts: A systematic mapping study of academic research (2018)," in *2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB)*, 2018, pp. 1–6. DOI: 10.1109/ICCBB.2018.8756390.

[58] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "A systematic literature review of data governance and cloud data governance," *Personal and Ubiquitous Computing*, vol. 23, Nov. 2019. DOI: 10.1007/s00779-017-1104-3.

[59] F. De Prieëlle, M. De Reuver, and J. Rezaei, "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*, pp. 1–11, 2020. DOI: 10.1109/TEM.2020.2966024.

[60] U. of the Witwatersrand, *Resarch support: Research methodology*, Accessed: 04.05.2022. [Online]. Available: https://libguides.wits.ac.za/c.php?g=693518&p=4914913#:~:text=Research%20methodology%20is%20the%20specific,study's%20overall%20validity%20and%20reliability..

[61] D. Preuveneers and W. Joosen, "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)*, 2019, pp. 29–38. DOI: 10.1109/EuroSPW.2019.00010.

[62] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of iot data," in *Proceedings of the 2017 on Cloud Computing Security Workshop*, ser. CCSW '17, Dallas, Texas, USA: Association for Computing Machinery, 2017, 45–50, ISBN: 9781450352048. DOI: 10.1145/3140649.3140656. [Online]. Available: https://doi.org/10.1145/3140649.3140656.

[63] Postscapes, *Internet of things (iot) history*, Accessed: 12.10.2021. [Online]. Available: https://www.postscapes.com/iot-history/.

[64] Cisco, *Fast innovation require fast it*, Accessed: 30.08.2021. [Online]. Available: https://www.cisco.com/c/dam/global/en_ph/assets/ciscoconnect/pdf/bigdata/jim_green_cisco_connect.pdf.

[65] I. D. S. Association, *Reference architecture model*, Accessed: 19.02.2021. [Online]. Available: https://internationaldataspaces.org/wp-content/uploads/IDS-RAM-3.0-2019.pdf.

[66] M. Matsas, *Data space radar*, Accessed: 26.08.2021. [Online]. Available: https://internationaldataspaces.org/adopt/data-space-radar/.

[67] IBM, *What is blockchain technology?* Accessed: 23.02.2022. [Online]. Available: https://www.ibm.com/topics/what-is-blockchain.

[68] ——, *What are smart contracts on blockchain?* Accessed: 23.02.2022. [Online]. Available: https://www.ibm.com/topics/smart-contracts.

[69] M. Sepehri and A. Trombetta, "Secure and efficient data sharing with atribute-based proxy re-encryption scheme," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ser. ARES '17, Reggio Calabria, Italy: Association for Computing Machinery, 2017, ISBN: 9781450352574. DOI: 10.1145/3098954.3104049. [Online]. Available: https://doi.org/10.1145/3098954.3104049.

[70] M. S. Ali, K. Dolui, and F. Antonelli, "Iot data privacy via blockchains and ipfs," in *Proceedings of the Seventh International Conference on the Internet of Things*, ser. IoT '17, Linz, Austria: Association for Computing Machinery, 2017, ISBN: 9781450353182. DOI: 10.1145/3131542.3131563. [Online]. Available: https://doi.org/10.1145/3131542.3131563.

[71] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," in *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, 2017, pp. 117–121. DOI: 10.1109/BIGCOM.2017.31.

[72] F. de la Vega, J. Soriano, M. Jimenez, and D. Lizcano, "A peer-to-peer architecture for distributed data monetization in fog computing scenarios," *WIRELESS COMMUNICATIONS & MOBILE COMPUTING*, 2018, ISSN: 1530-8669. DOI: 10.1155/2018/5758741.

[73] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with a patient centric agent: A block architecture," *IEEE Access*, vol. 6, pp. 32 700–32 726, 2018. DOI: 10.1109/ACCESS.2018.2846779.

[74] G. S. Ramachandran, R. Radhakrishnan, and B. Krishnamachari, "Towards a decentralized data marketplace for smart cities," in *2018 IEEE International Smart Cities Conference (ISC2)*, 2018, pp. 1–8. DOI: 10.1109/ISC2.2018.8656952.

[75] E. de Matos, R. T. Tiburski, L. A. Amaral, and F. Hessel, "Providing context-aware security for iot environments through context sharing feature," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 1711–1715. DOI: 10.1109/TrustCom/BigDataSE.2018.00257.

[76] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38 437–38 450, 2018. DOI: 10.1109/ACCESS.2018.2851611.

[77] J. Yang, Z. Lu, and J. Wu, "Smart-toy-edge-computing-oriented data exchange based on blockchain," *Journal of Systems Architecture*, vol. 87, pp. 36–48, 2018, ISSN: 1383-7621. DOI: https://doi.org/10.1016/j.sysarc.2018.05.001. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1383762118300638.

[78] E. Zaghloul, T. Li, and J. Ren, "Security and privacy of electronic health records: Decentralized and hierarchical data sharing using smart contracts," in *2019 International Conference on Computing, Networking and Communications (ICNC)*, 2019, pp. 375–379. DOI: 10.1109/ICCNC.2019.8685552.

[79] X. Zheng, S. Sun, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies," *JOURNAL OF MEDICAL INTERNET RESEARCH*, vol. 21, no. 6, 2019, ISSN: 1438-8871. DOI: 10.2196/13583.

[80] B. Shen, J. Guo, and Y. Yang, "Medchain: Efficient healthcare data sharing via blockchain," *APPLIED SCIENCES-BASEL*, vol. 9, no. 6, 2019. DOI: 10.3390/app9061207.

[81] S. Bajoudah, C. Dong, and P. Missier, "Toward a decentralized, trust-less marketplace for brokered iot data trading using blockchain," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 339–346. DOI: 10.1109/Blockchain.2019.00053.

[82] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, 2019. DOI: 10.1109/JIOT.2018.2875542.

[83] R. Xu, S. Y. Nikouei, Y. Chen, E. Blasch, and A. Aved, "Blendmas: A blockchain-enabled decentralized microservices architecture for smart public safety," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 564–571. DOI: 10.1109/Blockchain.2019.00082.

[84] L. Bai, M. Hu, M. Liu, and J. Wang, "Bpiiot: A light-weighted blockchain-based platform for industrial iot," *IEEE Access*, vol. 7, pp. 58 381–58 393, 2019. DOI: 10.1109/ACCESS.2019.2914223.

[85] D. Sarabia-Jácome, I. Lacalle, C. E. Palau, and M. Esteve, "Enabling industrial data space architecture for seaport scenario," in *2019 IEEE 5th World Forum*

on Internet of Things (WF-IoT), 2019, pp. 101–106. DOI: 10.1109/WF-IoT.2019.8767216.

[86] A. Manzoor, M. Liyanage, A. Braeke, S. S. Kanhere, and M. Ylianttila, "Blockchain based proxy re-encryption scheme for secure iot data sharing," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2019, pp. 99–103. DOI: 10.1109/BLOC.2019.8751336.

[87] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, "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*, ser. SACMAT '19, Toronto ON, Canada: Association for Computing Machinery, 2019, 83–92, ISBN: 9781450367530. DOI: 10.1145/3322431.3326327. [Online]. Available: https://doi.org/10.1145/3322431.3326327.

[88] C. Huang and Y. Hu, "Beaf: A blockchain and edge assistant framework with data sharing for iot networks," in *2020 IEEE/ACM Symposium on Edge Computing (SEC)*, 2020, pp. 370–375. DOI: 10.1109/SEC50012.2020.00054.

[89] A. Alsharif and M. Nabil, "A blockchain-based medical data marketplace with trustless fair exchange and access control," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 2020, pp. 1–6. DOI: 10.1109/GLOBECOM42002.2020.9348192.

[90] M. Ur Rahman, F. Baiardi, and L. Ricci, "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)*, 2020, pp. 1–7. DOI: 10.1109/GCAIoT51063.2020.9345874.

[91] M. M. Madine, K. Salah, R. Jayaraman, I. Yaqoob, Y. Al-Hammadi, S. Ellahham, and P. Calyam, "Fully decentralized multi-party consent management for secure sharing of patient health records," *IEEE Access*, vol. 8, pp. 225 777–225 791, 2020. DOI: 10.1109/ACCESS.2020.3045048.

[92] J. Bartol, A. Souvent, N. Suljanović, and M. Zajc, "Secure data exchange between iot endpoints for energy balancing using distributed ledger," in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, 2020, pp. 56–60. DOI: 10.1109/ISGT-Europe47291.2020.9248899.

[93] H. Xu, Q. He, X. Li, B. Jiang, and K. Qin, "Bdss-fa: A blockchain-based data security sharing platform with fine-grained access control," *IEEE Access*, vol. 8, pp. 87 552–87 561, 2020. DOI: 10.1109/ACCESS.2020.2992649.

[94] R. Akkaoui, X. Hei, and W. Cheng, "Edgemedichain: A hybrid edge blockchain-based framework for health data exchange," *IEEE Access*, vol. 8, pp. 113 467–113 486, 2020. DOI: 10.1109/ACCESS.2020.3003575.

[95] M. Lücking, R. Manke, M. Schinle, L. Kohout, S. Nickel, and W. Stork, "Decentralized patient-centric data management for sharing iot data streams," in *2020 International Conference on Omni-layer Intelligent Systems (COINS)*, 2020, pp. 1–6. DOI: 10.1109/COINS49042.2020.9191653.

[96] Y. Yu, Q. Li, Q. Zhang, W. Hu, and S. Liu, "Blockchain-based multi-role healthcare data sharing system," in *2020 IEEE International Conference on E-health Networking, Application Services (HEALTHCOM)*, 2021, pp. 1–6. DOI: 10.1109/HEALTHCOM49281.2021.9399028.

[97] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, "Data sharing system integrating access control mechanism using blockchain-based smart contracts for iot devices," *APPLIED SCIENCES-BASEL*, vol. 10, no. 2, 2020. DOI: 10.3390/app10020488.

[98] F. A. Al-Zahrani, "Subscription-based data-sharing model using blockchain and data as a service," *IEEE Access*, vol. 8, pp. 115 966–115 981, 2020. DOI: 10.1109/ACCESS.2020.3002823.

[99] F. Jamil, S. Ahmad, N. Iqbal, and D. Kim, "Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals," English, *Sensors (Switzerland)*, vol. 20, no. 8, 2020, Cited By :79. DOI: 10.3390/s20082195.

[100] G. Le, Q. Gu, Q. Jiang, and W. Lin, "Trustedchain: A blockchain-based data sharing scheme for supply chain," in *2020 International Conference on Data Mining Workshops (ICDMW)*, 2020, pp. 895–901. DOI: 10.1109/ICDMW51313.2020.00128.

[101] D. López and B. Farooq, "A multi-layered blockchain framework for smart mobility data-markets," *Transportation Research Part C: Emerging Technologies*, vol. 111, pp. 588–615, 2020, ISSN: 0968-090X. DOI: https://doi.org/10.1016/j.trc.2020.01.002. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0968090X19300361.

[102] Z. Ma, L. Wang, and W. Zhao, "Blockchain-driven trusted data sharing with privacy protection in iot sensor network," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25 472–25 479, 2021. DOI: 10.1109/JSEN.2020.3046752.

[103] M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang, and X. Jia, "Medshare: A privacy-preserving medical data sharing system by using blockchain," *IEEE Transactions on Services Computing*, pp. 1–1, 2021. DOI: 10.1109/TSC.2021.3114719.

[104] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11 717–11 731, 2021. DOI: 10.1109/JIOT.2021.3058946.

[105] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "A cooperative architecture of data offloading and sharing for smart healthcare with blockchain," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2021, pp. 1–8. DOI: 10.1109/ICBC51069.2021.9461063.

[106] S. R. Niya, D. Dordevic, and B. Stiller, "Itrade: A blockchain-based, self-sovereign, and scalable marketplace for iot data streams," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2021, pp. 530–536.

[107] A. Manzoor, A. Braeken, S. S. Kanhere, M. Ylianttila, and M. Liyanage, "Proxy re-encryption enabled secure and anonymous iot data sharing platform based on blockchain," *Journal of Network and Computer Applications*, vol. 176, p. 102 917, 2021, ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2020.102917. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804520303763.

[108] C. Singh, D. Chauhan, S. A. Deshmukh, S. S. Vishnu, and R. Walia, "Mediblock record: Secure data sharing using block chain technology," *Informatics in Medicine Unlocked*, vol. 24, p. 100 624, 2021, ISSN: 2352-9148. DOI: https://doi.org/10.1016/j.imu.2021.100624. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352914821001143.

[109] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "Privysharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," *Computers Security*, vol. 88, p. 101 653, 2020, ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2019.101653. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016740481930197X.

[110] H. Patel and B. Shrimali, "Agrionblock: Secured data harvesting for agriculture sector using blockchain technology," *ICT Express*, 2021, ISSN: 2405-9595. DOI: https://doi.org/10.1016/j.icte.2021.07.003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959521000862.

[111] E. Balistri, F. Casellato, C. Giannelli, and C. Stefanelli, "Blockhealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten," *ICT Express*, vol. 7, no. 3, pp. 308–315, 2021, ISSN: 2405-9595. DOI: https://doi.org/10.1016/j.icte.2021.08.006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959521000953.

[112] K. Mohammad Hossein, M. E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, "Bchealth: A novel blockchain-based privacy-preserving architecture for iot healthcare applications," *Computer Communications*, vol. 180, pp. 31–47, 2021, ISSN: 0140-3664. DOI: https://doi.org/10.1016/j.comcom.2021.08.011. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366421003054.

[113] A. I. Paganelli, P. E. Velmovitsky, P. Miranda, A. Branco, P. Alencar, D. Cowan, M. Endler, and P. P. Morita, "A conceptual iot-based early-warning architecture for remote monitoring of covid-19 patients in wards and at home," *Internet of Things*, vol. 18, p. 100 399, 2022, ISSN: 2542-6605. DOI: https://doi.org/10.1016/j.iot.2021.100399. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660521000433.

[114] D. Hu, Y. Li, L. Pan, M. Li, and S. Zheng, "A blockchain-based trading system for big data," *Computer Networks*, vol. 191, p. 107 994, 2021, ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2021.107994. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S138912862100116X.

[115] M. Kumar and S. Chand, "Medhypchain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in covid-19 pandemic," *Journal of Network and Computer Applications*, vol. 179, p. 102 975, 2021, ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2021.102975. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804521000023.

[116] D. E. Majdoubi, H. E. Bakkali, and S. Sadki, "Smartmedchain: A blockchain-based privacy-preserving smart healthcare framework," English, *Journal of Healthcare Engineering*, vol. 2021, 2021, Cited By :1. DOI: 10.1155/2021/4145512.

[117] P. Pawar, N. Parolia, S. Shinde, T. O. Edoh, and M. Singh, "Ehealthchain—a blockchain-based personal health information management system," English, *Annales des Telecommunications/Annals of Telecommunications*, vol. 77, no. 1-2, pp. 33–45, 2022. DOI: 10.1007/s12243-021-00868-6.

[118] Y. Chen, B. Hu, H. Yu, Z. Duan, and J. Huang, "A threshold proxy re-encryption scheme for secure iot data sharing based on blockchain," *ELECTRONICS*, vol. 10, no. 19, 2021. DOI: 10.3390/electronics10192359.

[119] Y. Chen, L. Meng, H. Zhou, and G. Xue, "A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection," *WIRELESS COMMUNICATIONS & MOBILE COMPUTING*, vol. 2021, 2021, ISSN: 1530-8669. DOI: 10.1155/2021/6685762.

[120] A. Dixit, A. Singh, Y. Rahulamathavan, and M. Rajarajan, "Fast data: A fair, secure and trusted decentralized iiot data marketplace enabled by blockchain,"

IEEE Internet of Things Journal, pp. 1–1, 2021. DOI: 10.1109/JIOT.2021.3120640.

[121] G. Manogaran, M. Alazab, P. M. Shakeel, and C.-H. Hsu, "Blockchain assisted secure data sharing model for internet of things based smart industries," *IEEE Transactions on Reliability*, vol. 71, no. 1, pp. 348–358, 2022. DOI: 10.1109/TR.2020.3047833.

[122] Lexico, *Vulnerability*, Accessed: 24.10.2021. [Online]. Available: https://www.lexico.com/en/definition/vulnerability.

[123] IPFS, *How ipfs works*, Accessed: 19.04.2022. [Online]. Available: https://docs.ipfs.io/concepts/how-ipfs-works/.

[124] DNV, *About dnb*, Accessed: 14.05.22. [Online]. Available: https://www.dnv.com/about/index.html.

[125] ISO, *Iso 8000-61:2016(en) data quality — part 61: Data quality management: Process reference model*, Accessed: 14.05.22. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:8000:-61:ed-1:v1:en.

[126] medium, *Manageing complexity of iot sensors, endpoints, gateways, and network bottlenecks*, Accessed: 25.04.2022. [Online]. Available: https://medium.com/technology-hits/managing-complexity-of-iot-sensors-endpoints-gateways-and-network-bottlenecks-5207775150d0#:~:text=IoT%20ecosystems%20are%20complex.,mobile%20applications%20and%20cloud%20platforms..

[127] Gartner, *Scalability*, Accessed: 20.04.2022. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/scalability#:~:text=Scalability%20is%20the%20measure%20of,application%20and%20system%20processing%20demands..