symmetry

MDPI

Article

A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective

Hezam Akram Abdulghani *, Niels Alexander Nijdam, Anastasija Collen and Dimitri Konstantas

Geneva School of Economics and Management, University of Geneva, 1211 Geneva, Switzerland; niels.nijdam@unige.ch (N.A.N.); anastasija.collen@unige.ch (A.C.); dimitri.konstantas@unige.ch (D.K.)

* Correspondence: mohammed.akram@unige.ch

Received: 3 May 2019; Accepted: 4 June 2019; Published: 10 June 2019

Abstract: The Internet of Things (IoT) makes our lives much easier, more valuable, and less stressful due to the development of many applications around us including smart cities, smart cars, and smart grids, offering endless services and solutions. Protecting IoT data of such applications at rest either on the objects or in the cloud is an indispensable requirement for achieving a symmetry in the handling and protection of the IoT, as we do with data created by persons and applications. This is because unauthorised access to such data may lead to harmful consequences such as linkage attacks, loss of privacy, and data manipulation. Such undesired implications may jeopardise the existence of IoT applications if protection measures are not taken, and they stem from two main factors. One is that IoT objects have limited capabilities in terms of memory capacity, battery life, and computational power that hamper the direct implementation of conventional Internet security solutions without some modifications (e.g., traditional symmetric algorithms). Another factor is the absence of widely accepted IoT security and privacy guidelines for IoT data at rest and their appropriate countermeasures, which would help IoT stakeholders (e.g., developers, manufacturers) to develop secure IoT systems and therefore enhance IoT security and privacy by design. Toward this end, we first briefly describe the main IoT security goals and identify IoT stakeholders. Moreover, we briefly discuss the most well-known data protection frameworks (e.g., General Data Protection Regulation (GDPR), Health Insurance Portability (HIPAA)). Second, we highlight potential attacks and threats against data at rest and show their violated security goals (e.g., confidentiality and integrity). Third, we review a list of protection measures by which our proposed guidelines can be accomplished. Fourth, we propose a framework of security and privacy guidelines for IoT data at rest that can be utilised to enhance IoT security and privacy by design and establish a symmetry with the protection of user-created data. Our framework also presents the link between the suggested guidelines, mitigation techniques, and attacks. Moreover, we state those IoT stakeholders (e.g., manufacturers, developers) who will benefit most from these guidelines. Finally, we suggest several open issues requiring further investigation in the future, and we also discuss the limitations of our suggested framework.

Keywords: Internet of Things (IoT); security guidelines; privacy guidelines; countermeasures; security goals; attacks; IoT data at rest

1. Introduction

The Internet of Things (IoT) is a network of objects equipped with sensors, actuators, electronics, and connectivity protocols enabling object interaction without human intervention [1]. The IoT is

involved in the creation of a variety of applications and services around us, for example in smart cities, smart cars, smart grids, quality of life applications, and electronic gadgets—all of which make our lives more productive and less stressful. For instance, the authors in [2] proposed an IoT system which can be used to manage students' stress. It is unquestionable that such IoT applications and services provide a huge benefit for human life, yet they may come with a massive cost for individual privacy and security protection. This is because the IoT inherits most of the issues of the Internet associated with location awareness, security, quality of service [3], and most likely amplifies them due to the direct connection with physical objects [4,5].

As IoT applications can store their data locally on objects or remotely in the cloud, based on their storage capabilities, protecting their data at rest is of paramount importance. Several IoT applications may cooperate with each other to accomplish specific tasks or services. If the data integrity of a single IoT application at rest has been compromised, then there is a huge risk of dealing with a cascading effect of the data compromise. For instance, the authors in [6] state that a thermostat deployed in a smart home relies heavily on a smoke detector's data to shut a heating system down in case of danger. However, access of the smoke detector's data by unauthorised objects may put the entire smart home at risk. A countermeasure ensuring the data integrity across multiple Cloud Storage Services (CSSs) was proposed by [7], where reliance on the Third-Part Auditor (TPA) for data verification was eliminated the by use of a decentralised blockchain-based integrity management service. Furthermore, once an Internet of Things (IoT) system stores its data in the cloud, there is no assurance that only authorised objects or users will have access to their data. An example was given by European Union Agency for Network and Information Security (ENISA) (https://www.enisa.europa.eu/), where an employee at the SharpLocks company, attacker, was capable (due to given access rights) to send a malicious update from the company's server to all connected Internet of Things (IoT) objects [8].

However, most security and privacy issues of Internet of Things (IoT) data at rest, such as unauthorised access and weak or absent encryption schemes, arise from two principal reasons. IoT objects have limited capabilities in terms of computational power, memory, and bandwidth [9]. Because of these limitations, a direct implementation of traditional security mechanisms in IoT objects tends to be very difficult without some modifications. This is why a new breed of lightweight IoT security techniques and protocols (e.g., a secure system of uploading and replicating IoT data suggested in [10]) has been developed [11,12]. The second reason, which motivates us to conduct this work, is the lack of widely-accepted security and privacy guidelines for IoT at data at rest, along with their appropriate mitigation techniques. The main objective of such guidelines and countermeasures is to improve IoT security and privacy by design by giving IoT stakeholders (e.g., manufacturers, developers) a chance to embrace such guidelines and countermeasures from the early stages of IoT system development [13]. If IoT stakeholders overlook these guidelines when dealing with IoT data at rest, the appearance of attacks and threats is inevitable.

It is clear that the unauthorised access and privacy violations of individuals, associated with data at rest, will appear repeatedly in IoT systems unless the mindset of all IoT stakeholders shifts to properly integrate security and privacy guidelines for IoT data at rest, along with their corresponding countermeasures, at early stages. The first step towards this paradigm shift is the development of a comprehensive set of security and privacy guidelines. However, there is a complete lack of research efforts conducted specifically toward this objective. To the best of our knowledge, there is no paper or document clearly addressing security and privacy guidelines for IoT data at rest along with their mitigation strategies. The existing research proposals [14–21] focus primarily on IoT guidelines in general. They neither provide comprehensive guidelines for IoT data at rest, nor discuss their proper countermeasures. A detailed explanation of such efforts along with a brief comparison between our suggested guidelines for IoT data at rest and theirs is presented in Section 2.

The main contributions of this work are the following:

1. To highlight IoT security goals as well as IoT stakeholders.
2. To summarise the attacks and threats against IoT data at rest.

3. To review a set of implementation techniques by which our suggested guidelines can be implemented and also state those IoT stakeholders who would benefit from these guidelines.
4. To propose a framework of security and privacy guidelines for IoT data at rest that can be utilised to reinforce IoT security and privacy by design.
5. To discuss open issues, limitations, and future work.

The rest of this article is structured as follows. In Section 2, we present the current research studies on IoT guidelines with focus on data at rest, describe the most popular data protection frameworks, and highlight the IoT security goals and distinguish IoT stakeholders. Section 3 discusses threats and attacks on IoT data at rest. We identify the appropriate techniques for mitigating the identified attacks on IoT data at rest in Section 4. A proposed framework on security and privacy guidelines is presented in Section 5. Finally, we discuss open issues for further investigation for future work in Section 6.

2. Related Work

In this section, we outline the current state of the art related to IoT security guidelines, existing frameworks on data protection, and identify the involved stakeholders specific for the IoT environment. We limit our discussion to the guidelines on protecting IoT data at rest as the main topic of this work.

2.1. Research Efforts on IoT Guidelines

In [14], the authors propose a set of security and privacy guidelines for IoT data at rest, such as minimising data storage, minimising data retention, encrypting data storage, and implementing time-period data aggregation. Furthermore, attacks and threats against IoT data at rest are analysed. Having said that, the authors do not provide a comprehensive set of guidelines for IoT data at rest, nor do they state the required implementation techniques to achieve their guidelines.

In [15], the IoT suggests a list of security and privacy guidelines for IoT data at rest like minimising data storage, encrypting data storage, removing sensitive data, and ensuring data availability. However, the IoT does not offer a thorough set of guidelines for IoT data at rest, nor does it identify the countermeasures required to carry out its guidelines. Furthermore, threats and attacks against IoT data at rest remain unchecked.

In [16], the Open Web Application Security (OWASP) suggests different security and privacy guidelines for IoT data at rest, such as minimising data storage, minimising data retention, ensuring authorised access, and preventing physical access. In addition, the OWASP states IoT stakeholders like manufacturers, developers, and customers who may use its guidelines to protect IoT data at rest. Nevertheless, the OWASP neither recognised the required countermeasures to implement its guidelines, nor distinguished possible attacks and threats against IoT data at rest.

In [17], the ENISA proposes several security and privacy guidelines for IoT data at rest, such as minimising data retention, encrypting data storage, defining recovery strategies, informing customers, and ensuring proper data destruction. However, the ENISA does not recognise the IoT stakeholders who may utilise its guidelines, nor does it identify proper solutions to apply its guidelines. Moreover, the ENISA uncovers attacks and threats against IoT data at rest.

In [18], the IoTA suggests a list of security and privacy guidelines for IoT data at rest, including encrypting data storage, informing customers, and removing sensitive data. That said, IoTA neither distinguishes the required implementation techniques to fulfil its guidelines, nor does it point out IoT stakeholders who may use its guidelines. Attacks and threats against IoT data at rest also are left unidentified.

In [19], the IoT Security Foundation (IoTSF) proposes a set of security and privacy guidelines for IoT data at rest, such as the use of distributed data storage, defining recovery strategies, ensuring proper data destruction, and searching on encrypted data. However, the IoTSF neither recognises suitable countermeasures to realise its guidelines, nor distinguishes attacks and threats against IoT data at rest.

In [21], the authors propose a comprehensive set of security and privacy guidelines for the first two levels of CISCO's reference model (i.e., edge nodes and communication). Even though their guidelines are not meant specifically for protecting IoT data at rest, only three of these guidelines (i.e., ensure authorised access, remove or hide sensitive data, and search on encrypted data) can be used to do so. The authors identify all possible threats and attacks against edge nodes and communication, state those IoT stakeholders who may use their guidelines, and recognise suitable implementation techniques to implement them.

2.2. Data Protection Frameworks

The lack of efficient standards, regulation, and weak governance is a cause of IoT security and privacy issues. However, some initiatives at a national level have been proposed, which we briefly present in the following:

General Data Protection Regulation (GDPR): In December of 2016, the European Union (EU) voted to use the GDPR as a replacement for the outdated Data Protection Directive (DPD) proposed in 1996. The main goal of the DPD was to preserve individuals' personal information within the EU from being misused and to allow individuals in the EU to have better control over their personal data. The GDPR is intended to substitute the DPD as a regulation, and it will cover the whole EU as unified law. The GDPR has included six major changes (e.g., in terms of the definition of personal data, individual rights, data controllers and processors, and global impact) compared to the DPD. The detailed explanation of each of these, for interested readers, can be found in [22]. To preserve personal data, the GDPR imposes six fundamental principles, the details of which can be found in [23]. Not all IoT applications deal with personal information—for instance, Industrial Internet of Things (IIoT) applications. However, this may be the case in the majority of IoT systems (e.g., healthcare). It is obvious that the market of IoT solutions is increasing worldwide, including Europe, and it is a relevant topic requiring thorough management. One example is a digital transformation of healthcare due to the fast growth of wearable and interconnected medical objects which provide remote health monitoring. Therefore, healthcare data is highly sensitive, and it attracts the attention of attackers. Addressing this, authors in [24] identified different attacks associated with the IoT multi-cloud e-Healthcare environment, such as side-channel attacks and malicious insider attacks. Healthcare data must thus be covered under the scope of the GDPR. Other important IoT applications which deal with personal data like smart metering and smart home applications must also be covered under the scope of the GDPR.

Health Insurance Portability and Accountability Act (HIPAA): The main goal of the HIPAA is to protect individuals from losing their health insurance if they have pre-existing health problems or if they change their jobs. However, over time, the HIPAA has been extended to minimise the administrative and cost burdens of healthcare processes. Most recently, the HIPAA has concentrated on developing standards as well as requirements to ensure the security and privacy of Personal Health information (PHI) which can be created, stored, or transferred in several formats (e.g., written documents and verbal conversations). PHI may include anything in patient health records, such as images, names, email addresses, and other information. As patients demand their data to be secure, HIPAA's security and privacy rules, discussed in detail in [25], require that healthcare organisations embrace a set of processes and procedures to assure the highest level of patient confidentiality. Under HIPAA, a covered organisation may not utilise or reveal PHI unless it has received explicit consent from a patient to do so. It is unquestionable that the IoT will change the healthcare experience. Several examples are available on the market to illustrate how the IoT has simplified the process of care management. For instance, collecting information in users' homes will assist healthcare providers in comprehending users' health in a comprehensive way, in choosing suitable treatment plans, altering the plans as time progresses, and most importantly anticipating future health actions. It is clear that the IoT can be utilised by healthcare organisations to reduce costs and simultaneously enhance health outcomes in patients. Hence, healthcare IoT solutions must be covered under the scope of HIPAA.

Industrial Internet Consortium (ICC): The ICC is an organisation developed in 2014 to improve the growth of interconnected objects. The primary goal of tnis organisation is to build an alliance of companies, academia, and governments to cooperate on the development of test beds for real-world systems. Furthermore, it has been actively involved in supporting the necessities of standards in the IoT industry. Toward this end, in 2016 the ICC proposed a security framework developed specifically for the IoT. The main purpose of this security framework is to establish global industry acceptance on how to develop secure IoT systems [26].

IoT Security Foundation (IoTSF): The IoTSF is a non-profit company that has been reinforcing the IoT industry since 2015. This reinforcement includes developing security and privacy guidelines, courses, and training. The IoTSF also has addressed the issues in the industry, and more importantly it has struggled to cover the gap via a cooperative initiative with many companies dealing with the IoT. This kind of cooperation attempts to share expertise, knowledge, and enhance best practices. To contribute to such objectives, the IoTSF in [19], for example, proposed an IoT framework as a checklist which can be used by IoT manufacturers to simplify their compliance to the IoTSF framework.

2.3. IoT Security Goals and Stakeholders

In this section, we first discuss security goals specific to the IoT environment. In the literature, traditional security goals are broken down into three primary sets: (i) confidentiality, (ii) integrity, and (iii) availability, referred to as the Confidentiality, Integrity and Availability triad (CIA-triad). Confidentiality assures that only authorised objects or users can get access to sensitive data. As several IoT objects might deal with sensitive data such as medical records and credit cards, the confidentiality of such data must be preserved. The impact of unauthorised access to medical objects, which may reveal personal data or lead to life-threatening situations, has been illustrated in [27]. In the IoT context, integrity is also crucial, since it ensures IoT data has not been tampered with. If the integrity of IoT data has been compromised, undesired consequences may take place, for instance compromising a patient's privacy as a result of revealing their insulin pump [28]. IoT availability is essential, as it guarantees that IoT data is available and accessible to its users. Even though the CIA-triad is popular, it fails to address new threats which appear in a cooperative environment, according to [29]. To tackle this issue, the authors in [29] propose a complete list of security goals known as the Information, Assurance, and Security (IAS) octave, by studying a huge amount of information in the state-of-the-art of security. Table 1 summarises the security goals suggested by the Information, Assurance, and Security (IAS) octave, along with their definitions and abbreviations associated with the IoT environment.

Table 1. IoT security goals [4].

Security Requirements	Definition	Abbreviations
Confidentiality	Only authorised objects or users can get access to the data	CONF
Integrity	Data completeness and accuracy is preserved	INTG
Non-repudiation	The IoT system can validate the occurrence of any event	NREP
Availability	Ensuring the accessibility of an IoT system and its services	AVAL
Privacy	The presence of privacy rules or policies	PRIV
Auditability	Monitoring of the IoT object activity	AUDI
Accountability	End users can take charge of their actions	ACNT
Trustworthiness	Reliability on IoT object identity	TRST

In order to build a framework of security and privacy guidelines that is suitable for all aspects of the IoT environment life cycle, we first propose a classification of identified IoT stakeholders into four groups, depicted in Table 2. It relates the main stakeholders with their associated role, in order to dictate the degree of guideline adaptation and stakeholder impact.

Table 2. IoT stakeholders [21].

Stakeholders	Roles	Abbreviations
Manufacturer	Building IoT hardware products	MAN
Developer	Developing IoT software solutions or services	DEV
Provider	Providing services for IoT products to customers	PRV
Consumer	Using IoT objects in different aspects of their daily lives	CNS

3. Attacks on IoT Data at Rest

In this section, we describe attacks and threats applicable for IoT data at rest and correlate them with the IoT security goals identified in Table 1. More specifically, we annotate with "⚠" when the security goal in question is violated by the described attack.

(AT1) **Misuse of data remnants**: This type of attack takes place when IoT objects are taken in possession by other end users either by voluntary life cycle transitions (second-hand, recycling) or due to loss, theft, malfunctioning, and other involuntarily causes. Even though there is the possibility that the data of such objects may be deleted before they are sold, this is not always the case for all sold objects. Those objects which store valuable information during their entire life cycle (e.g., personal photos and passwords) could be a primary target for many attackers, since they are not discarded properly during their end-of-life period or their data are not purged completely during attempted data cleanup [30]. This attack directly violates all security goals (see Table 3), as the attacker has full control and access to the physical storage.

Table 3. The violated security goals by AT1.

CONF	INTG	NREP	AVAL	PRIV	AUDI	ACNT	TRST
⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠

(AT2) **Linkage attack**: The probability of unauthorised access, as well as leaks of sensitive information, grows significantly with the data sources of linked IoT systems, where each additional link creates exponential exposure. When intercepting and cross-referencing between multiple data sources leads to partial data identification, it is called a linkage attack [31]. This attack violates confidentiality (CONF), integrity (INTG), and privacy (PRIV) security goals (see Table 4), as the attacker is manipulating the intercepted data without directly interfering with the actual IoT object(s). Therefore, other security goals are not applicable.

Table 4. The violated security goals by AT2.

CONF	INTG	NREP	AVAL	PRIV	AUDI	ACNT	TRST
⚠	⚠			⚠			

(AT3) **Data manipulation**: The illegitimate modification of data at rest can be accomplished by two methods: (i) exploiting several vulnerabilities in the application program interface such as SQL injection and cross-site scripting, and (ii) taking advantage of weak security mechanisms like small or weak passwords [32,33]. Similar to the "misuse of data remnants" attack, all security goals are violated (see Table 5), as the attacker operates directly on the IoT object.

Table 5. The violated security goals by AT3.

CONF	INTG	NREP	AVAL	PRIV	AUDI	ACNT	TRST
⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠

(AT4) **Side-channel attacks**: This attack is based on the discovery of information by analysing exposed side properties of the algorithmic implementation, such as processing timing, power consumption, or even associated sounds. This type of attack may take place due to the absence of secure methods of processing and storing IoT data, for instance storing unencrypted data either in the cloud or on IoT objects. The authors in [34] discuss several data leakage attacks on CSSs, such as the confirmation of a file and learning the content of files. In the case of file confirmation, an adversary who already knows the plain text content of a file can examine if a duplicate of the file has been stored elsewhere in the CSS. In the case of learning the contents of the file, the adversary can reveal highly sensitive data, since the attacker already recognises most the of file and attempts to guess or identify the unknown segments of file by examining whether the output of the encryption meets the observed cipher text. Similarly to the "linkage attack", the CONF, INTG, and PRIV security goals are violated (see Table 6) as the attacker is indirectly revealing the private data, already generated and processed by the IoT object.

Table 6. The violated security goals by AT4.

CONF	INTG	NREP	AVAL	PRIV	AUDI	ACNT	TRST
⚠	⚠			⚠			

(AT5) **Denial of Service (DoS)**: DoS attacks in cloud computing prevent CSSs from offering their normal services or solutions for a period of time. The authors in [35] stated that DoS attacks which compromise the availability of such CSSs stem from many contributing factors, the most notable of which are resource exhaustion, process disruption, physical disruption, and data corruption. For instance, the authors in [31] state that an attacker could flood a CSS with fake data at high frequency, which in turn makes this storage service spend most of its time validating the authenticity of this data and therefore unable to reply to any valid requests in a timely fashion. The inability of timely response may cause a delay which is not preferable for most IoT applications, specifically real-time applications like air traffic systems and Near-Field Communication (NFC) payment. For interested readers, a recently published survey of DoS attacks in the cloud can be found in [35]. First of all, the availability (AVAL) is affected by this attack, as implied by the definition of the attack. Accountability (ACNT) is also no longer guaranteed due to the slow response times of the system. For INTG, the guaranteed transmission and/or storage can be compromised, especially for real-time applications. Auditability (AUDI) is also violated, since the system cannot perform continuous monitoring of the object's activity. Table 7 represents the violated security goals by this attack.

Table 7. The violated security goals by AT5.

CONF	INTG	NREP	AVAL	PRIV	AUDI	ACNT	TRST
	⚠		⚠		⚠	⚠	

(AT6) **Insider attack**: An insider threat takes place when either a former or a current user who has authorised access to an object's data or CSSs misuses these access rights to compromise the IoT security goals, such as confidentiality, integrity, and availability. Malicious insiders can be considered as a considerable threat to many organisations. They can adversely influence a company's mission and reputation, and therefore they can pose a major impact to any business. The cyber-security intelligence index [36] in 2016 stated that 60% of all attacks are derived by insiders. From this percentage, it can be said that malicious insiders make a great contribution, since the majority of such attacks (44.5%) were caused by them. In its recently published survey [37], EY identified several types of insider threats such as fraud, infrastructure sabotage, and unauthorised trading. In the IoT context, the whole IoT ecosystem—starting from objects located in different environments and their data and applications in the cloud—may be vulnerable to insider threats. Toward this end, the authors in [24] illustrate

the applicability of malicious insider attacks in all the layers of IoT multi-cloud-based e-healthcare architecture composed of four layers. In layer 1 (physical), where several sensors are deployed to collect the health data of different patients, an insider attacker (in this case) could alter the settings to send incorrect data to the healthcare companies. The attacker could also obtain and reveal patient information. Likewise, in layer 2 (network) where many connectivity protocols (e.g., Bluetooth Low Energy) are utilised to transfer the patient data to the next layer, a malicious insider could carry out many unwanted activities, such as redirecting the packets to a vicious network and compromising the availability of health data by initiating a DoS attack on the network. In layer 3 (cloud), malicious insiders could perform a set of malicious activities like gaining unauthorised access to patient data, altering e-health applications, modifying data stored in the storage, and executing collision attacks. Layer 4 (application) is also susceptible to malicious insider attacks. This is because any authorised entity from lower to upper levels could uncover or alter patient heath data, which would certainly impact the level of trust among patients, doctors, and health organisations [24]. Similar to the "misuse of data remnants" attack, all security goals are violated (see Table 8) as the attacker operates directly on the IoT object.

Table 8. The violated security goals by AT6.

CONF	INTG	NREP	AVAL	PRIV	AUDI	ACNT	TRST
⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠

(AT7) **Homogeneity attack**: Several anonymisation-based solutions have been proposed (e.g., *k*-anonymity and t-closeness techniques), but some of them lack a method in which the diversity of their sensitive attributes is not supported, making such techniques like *k*-anonymity vulnerable to homogeneity attacks. This attack is applicable to cases where there are identical records within data sets. Similarly to the "linkage attack", the CONF, INTG, and PRIV security goals are violated (see Table 9), as the attacker is indirectly capable of attributing the private data to specific identities.

Table 9. The violated security goals by AT7.

CONF	INTG	NREP	AVAL	PRIV	AUDI	ACNT	TRST
⚠	⚠			⚠			

(AT8) **Unauthorised access**: IoT data are vulnerable to different attacks because of their storage either in IoT objects or remotely in the cloud with no supervision of their holders. It is also expected that the number of threats and attacks will be intensified, since attackers can gain access to such data once they are not properly protected due to the absence of strong encryption techniques. Furthermore, data might be placed in several data centres located in different countries, and such countries may have a high power to access these data without the permission of their holders [38,39]. Another example of unauthorised access can be found in [40]. The authors state that an adversary may gain access to IoT data illegitimately during the migration procedure of a virtual machine to an untrusted host, which might reveal its sensitive data. Similar to the "misuse of data remnants" attack, all security goals are violated (see Table 10), as the attacker has direct access to the data on the IoT object or in the CSS.

Table 10. The violated security goals by AT8.

CONF	INTG	NREP	AVAL	PRIV	AUDI	ACNT	TRST
⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠

(AT9) **Identification**: An identification attack can be considered as one of the most common threats against IoT data in which an attacker can link some identifier attributes (e.g., name, address) with some

individuals. Similar to the "linkage attack", the CONF, INTG, and PRIV security goals are violated (see Table 11) as the attacker is indirectly capable of attributing the private data to specific identities.

Table 11. The violated security goals by AT9.

CONF	INTG	NREP	AVAL	PRIV	AUDI	ACNT	TRST
⚠	⚠			⚠			

(AT10) **Hash collision**: The key goal of the collision attack is to reveal two input strings of a hash function that give the same hash value. Because a hash function has variable input lengths and a short fixed-length output, there is the possibility that two different inputs generate the same output, and this case is known as a collision [41,42]. As a consequence, an attacker can compromise the encryption key and therefore intercept or have access to the IoT object's data. Similarly to the "linkage attack", the CONF, INTG, and PRIV security goals are violated (see Table 12), as the attacker is indirectly revealing the private data already generated and processed by the IoT object.

Table 12. The violated security goals by AT10.

CONF	INTG	NREP	AVAL	PRIV	AUDI	ACNT	TRST
⚠	⚠			⚠			

4. Mitigation Techniques for Protecting Data at Rest

In this section, we analyse existing methods of IoT data protection and attribute these mitigation techniques for the attack vectors, identified in Section 3.

(MT1) **Deduplication schemes**: Attributed to attacks *AT4* and *AT8*. Data deduplication is a method in which only a unique copy of redundant IoT data is stored, and links (not actual data) to the copies are provided. This is why this technique can be used as a backup strategy. Therefore, the development of secure deduplication schemes capable of detecting identical data copies and storing them once is a need and challenge at the same time. To this end, several data deduplication techniques have been proposed in the literature which can be classified broadly into two categories (i.e., server-side and client-side) based on the location at which data deduplication is accomplished [31].

Note that despite the benefits of deduplication schemes in saving disk space, minimising network bandwidth, and preventing unauthorised access, these techniques are susceptible to side-channel attacks. For instance, the authors in [34] state that implementing deduplication techniques in cloud storage may cause side-channel attacks like identifying files, learning the contents of files, and a covert channel. The authors also illustrate several practical solutions, such as encryption and proof of ownership, to mitigate such attacks. Toward this point, a few secure deduplication techniques have been proposed, described below.

In [43], the authors propose a novel deduplication algorithm in which a given file is broken into multiple segments. Each segment is encrypted by a user, and the encryption process involves both a secure hash function and a block encryption technique. These segments have an index tree, which is composed of the hash values of these segments. The index tree is generated and encrypted by the user using an asymmetric algorithm. The authors claim that, if it is implemented, their approach will prevent storage providers from getting access to users' data or their decryption keys. In [44], the authors propose a new deduplication technique based on Attribute-Based Encryption (ABE) to encrypt data stored in the cloud and simultaneously provide secure access to this data. According to the authors' evaluation, this technique is suitable for practical deployment due to its effectiveness, scalability, and efficiency. Other research proposals associated with this topic can be found in [45,46]

For interested readers, a recently published survey regarding this topic can be found in [47].

(MT2) **Secure storage schemes**: Attributed to attacks *AT3*, *AT4*, *AT8*, and *AT10*. Secure storage techniques can be used to prevent IoT data breaches. Several research proposals have

been introduced, classified broadly into two categories: (i) cryptographic-based schemes and (ii) non-cryptographic-based schemes. An example cryptographic-based scheme can be found in [48]. The authors propose a secure IoT storage technique in which aggregated IoT data can be stored securely on an object based on Shamir's secret sharing method. To protect IoT data on such a system, Shamir's secret sharing algorithm was used, along with internal padding. Data in this approach, prior to being stored, are divided into many segments and each segment is stored in different storage objects. Another example cryptographic-based scheme is presented in [49]. The authors propose a new technique based on an elliptic curve algorithm, which allows different users to access and store their data securely from the cloud. Moreover, it assures that neither the cloud storage provider nor unauthorised users can gain access to the data. This approach is also capable of protecting individuals' data, even when the cloud provider is compromised due to its data encryption.

In [50], the authors propose a novel architecture in which individuals and companies can securely upload and store their data in the cloud. This architecture is composed of things, gateway, network infrastructure, and cloud. To collect data in this architecture, IoT objects or things are deployed in the physical environment. The need for gateways in this architecture, which uses as an intermediate layer between objects and the cloud, stems from the fact that not all IoT objects are equipped with connectivity protocols (e.g., Wi-Fi) that allow them to connect to the Internet and transmit their data. The administrator in this system plays a key role in defining responsibilities according to the job functionality described in the organisation. For the interested readers, other research efforts associated with this topic can be found [51–54].

An example of a non-cryptographic-based scheme can be found in [55]. The authors propose a new storage schema called POTSHARDS which offers long-term security for IoT data without involving any encryption techniques. The security of this scheme is derived from dividing data into so many segments (each segment has its own pointers) and scattering them into different storage. If an attacker wants to get data of one segment, he needs to get all its pointers, which are distributed in several storage objects.

(MT3) **Access control**: Attributed to attacks *AT6* and *AT8*. Attributed to attack *AT3*. Many research efforts have been proposed to control access to stored IoT data by customers or companies. Such efforts can be divided broadly into four categories: (i) Mandatory Access Control (MAC), (ii) Discretionary Access Control model (DAC), (iii) Role Based Access Control model (RBAC), and (iv) ABE. Having integrated MAC into an IoT system, the system administrator will have privileges to manage the customers' roles and rights. In MAC, it is also possible for the system administrator to manipulate access policies, resulting in the prevention of customers from accessing the system. This type of access method can be added to sensitive systems like military and research centres [56]. If DAC is integrated into an IoT system, the customers will have the right to manipulate the access rules for any object. This approach is extremely dangerous if an attacker gains access rights to a customer account. Thus, it is not wise to give one customer full rights to the IoT system.

If RBAC is integrated into an IoT system, customers can gain access to resources based on their roles and responsibilities in the system. Several research proposals have been conducted in relation to this topic [57–59]. For instance, the authors in [59] suggest new five principles known as ASSAA for the next-generation RBAC. They claim that these principles are applied to access control in general despite the fact that they are developed specifically for RBAC. ABE provides adaptable one-to-many encryption without prior information of who will be accessing this information. It also draws attention to fine-grained access techniques over outsourced data. The identification of a customer in ABE is accomplished by a set of attributes which can be used to define the access policy of the customer [60]. Recently, several research proposals have attempted to implement ABE in fog computing [61–63]

(MT4) **Recovery strategy**: Attributed to attacks *AT3* and *AT5*. Despite the importance of providing high availability and disaster recovery for IoT storage, a few state-of-the-art research proposals have been found. In [10], authors investigated the problem of uploading IoT data from a set of several sensors and creating different replicas of these data on distributed storage in the cloud. The applicability of this

approach depends on the existence of several distributed data centres known as mini-clouds. In [64], authors propose a new replication approach to minimise power consumption, delay, and the cost of uploading a huge amount of data sent by several IoT applications. Each application is composed of too many small objects. To reduce time latency, the authors deployed local cloud computing resources. Other research proposals related to this topic can be found in [65–67].

(MT5) **Anonymisation schemes**: Attributed to attacks *AT2*, *AT7*, *AT8* and *AT9*. Such solutions can fall broadly into three categories: (i) *K*-anonymity, (ii) *l*-diversity, and (iii) *t*-closeness. *K*-anonymity is a technique in which the privacy of data holders is preserved when they issue their data, preventing threats associated with subject identification. This technique assures that the information of each person cannot be identified from a set of at least $k(-1)$ individuals . The concept of *k*-anonymity represents data as a table composed of a set of rows and columns. Each row indicates the insertion of new information related to a specific entity and it should not be unique [11], whereas each column represents an attribute for the entity. Two techniques have been used to achieve *k*-anonymity. The first is suppression, in which the values of some attributes are substituted by an asterisk $*$. The second is generalisation, in which the personal values of attributes are changed by values in a wider range. For instance, if the attribute *age* is used, the value 35 can be substituted by the term <40.

In the IoT, *k*-anonymity can be used for the localisation of smart objects to enhance location privacy. This can solve security issues related to the need for a third entity for managing different *k*-anonymity sets for several queries, the inapplicability of using universal GPS indoors, and obfuscation. In [68], the authors propose a tree-based location privacy technique against multi-precision attacks using a new location query technique in which multi-precision queries are fully supported. In [69], the authors propose another *k*-anonymity technique in which data can be released based on concrete generalisation.

L-diversity is suggested to mitigate the weakness of *k*-anonymity, which is its inability to prevent homogeneity and background attacks. In [70], the authors propose a new and powerful privacy technique known as *l*-diversity which can be used to prevent several attacks (e.g., homogeneity attack). Moreover, they perform an experimental evaluation to show that the proposed technique is practical, and that it can be implemented effectively.

T-closeness was first coined in [71] to overcome the shortcomings of *k*-anonymity and *l*-diversity associated with attribute inspiration. The authors in [71] propose that a distribution of sensitive information in any set must be close or connected to their scattering in the whole database. To summarise the value of this work, the authors used different real examples and experiments. In [72], the authors suggest a decomposition technique with $(n-1)$ closeness, the main purpose of which is to preserve privacy in the case of several sensitive attributes by reducing the amount of sensitive information which can be elicited from the published data in the *t*-closeness situation.

(MT6) **Transient data storage**: Attributed to attacks *AT1* and *AT4*. The existing research proposals have focused on managing the persistent data in IoT systems. In this case, data may be stored even after such systems have finished their executions. Nevertheless, a handful of research works have concentrated on managing transient IoT data generated during systems executions. The importance of transient data stems from processing data during system execution to generate new versions of data which may be stored in storage for users' needs or may be purged, and therefore it can reduce threats associated with such data. In [73], the authors propose a new system of managing transient IoT data in which this data can be processed, placed, and managed. This system is composed of several components, including a resource estimator, transient data characteriser, and data manager. Other research proposals related to this topic can be found in [74–76].

(MT7) **Searchable Encryption (SE)**: Attributed to attacks *AT5* and *AT6*. Another way to protect data in IoT storage is to perform information retrieval on encrypted data, which is known as SE—an approach that boomed in 2000. The main idea behind this technique can be summarised as follows: An object indexes and encrypts its data, and then it sends its encrypted data along with an index to a server. In order to search for given data, the object needs to generate a trapdoor through which the server can execute search operations directly on encrypted data, and the output will also be encrypted.

This field is known as homomorphic encryption. In this regard, Fully Homomorphic Encryption (FHE) was proposed in 2009 by Gentry [77]. That being said, the key distribution and user revocation in a multi-user search setting is a need and a challenge at the same time. Toward this end, some traditional technologies, like broadcast encryption proposed in [78] and secret sharing suggested in [79], can be used to cope with the key distribution issue. User revocation can be solved using either a trusted third party, proposed in [80], or a semi-trusted third party, suggested in [81].

It is worth mentioning that the ABE proposed in [82] was used by Sun et al. to develop the Attribute-Based Keyword Search (ABKS) scheme to offer fine-grained search authorisation in the cloud, proposed in [83,84].

(MT8) **Distributed data repositories**: Attributed to attack *AT5*. Several research studies have been proposed related to this topic. In [85], authors propose a new secure storage scheme for sharing data in public storage (in the cloud) known as a shield. Both authentication and access control in this approach are granted by a proxy server. A new version of Merkle hash tree was introduced to achieve integrity check and file content update. Moreover, both key management and effective permission revocation can be accomplished using a hierarchical key organisation. Another example of integrating access control into secure storage can be found in [86]. The authors propose a new secure storage repository called Cryptonite for sharing a huge amount of scientific data in the cloud. This approach provides an easy way for its users to securely store and share their data in the cloud without revealing their sensitive data, not only to unauthorised users or attackers, but also to the cloud storage provider and system itself.

It is also worth mentioning that a secure version of Hadoop Distributed File System (HDFS) can be used to achieve this objective, and research proposals associated with this topic are described below.

In [87], the authors propose a secure version of HDFS in which two security countermeasures are involved to prevent hackers from getting data in the cloud. The first countermeasure is a trust mechanism established between the name node used to manage data nodes and the end user. This type of trust mechanism requires that the end user be authenticated in order to access name node. To achieve this objective, the end user first sends a hash function, and then the name node compares hash functions, which are Secure Hash Algorithm 2 (SHA-2), generated by both the end user and the name node. The end use is only authorised to access the system if the compare result is correct. For the other countermeasure, random encryption methods like Rivest–Shamir–Adleman (RSA), Advanced Encryption Standard (AES) and Rivest Cipher 6 (RC6) are used on data to prevent an adversary from gaining access to the data. The encryption and decryption processes are accomplished by MapReduce, which allows data aggregation and the parallel processing of a huge amount of data.

Another example of secure HDFS which is equipped with three countermeasures can be found in [88].

(MT9) **Introspection**: Attributed to attacks *AT5* and *AT6*. Another technique which can be used to conserve users' sensitive information is introspection, by checking all the activities on a virtual machines (VMs) in which IoT data are stored. The main idea behind this technique is to inspect the state of the Central Processing Unit (CPU) for each VM, detect the malicious software on the VM, and check Input & Output (IO) for records or files. Nevertheless, users' privacy may be compromised as a consequence of losing one object's integrity by malicious software.

(MT10) **Blockchain**: Attributed to attacks *AT2*, *AT6*, and *AT8*. The use of blockchain technology in the IoT has several advantages—the most dominant of which are decentralisation, trust, and non-repudiation. It is clear that the previously mentioned countermeasures can be used to solve different security and privacy issues (e.g., unauthorised access and data leakage) associated with IoT data at rest. However, there is a need for blockchain technology to address other important issues, such as untrusted Third-Party Auditors (TPAs) and data integrity across different cloud storage. A handful of research proposals have been put forward to contribute to these objectives, the most recently published of which can be found in [7,89–91]. In [7], the authors propose a blockchain-based solution to provide a decentralised process in which data integrity for IoT data stored in semi-trusted

clouds is verified and checked. Furthermore, the authors illustrate the feasibility of their approach by applying a proof of concept on a personal (private) blockchain system. In [89], the authors first propose three different requirements to allow IoT systems to share and store their data in an untrustworthy environment such as untrusted TPAs. Such requirements are divided into three categories: (i) trusted trading, (ii) trusted privacy, and (iii) trusted data access. Moreover, they propose a decentralised architecture based on blockchain technology to accomplish the above-mentioned requirements. The authors also demonstrate the feasibility of this technique by implementing a proof of concept on an Ethereum blockchain. In [90], the authors suggest a data-centric approach based on blockchain technology which concentrates on sharing, resilience, and the auditable preservation of data. However, the authors only present the initial design of their approach, which is a blockchain-based end-to-end encrypted data storage system. Secure and permanent data management is achieved as a result of using blockchain as an auditable access control level to a distributed storage level. In [91], the authors propose a blockchain-based storage system called Sapphire. This system is designed specifically for data analytics in IoT. In this system IoT data coming from different IoT applications like smart home, smart grid, and smart city are classified into two categories, namely, text data and media data. This classification is accomplished by a data classifier. The collected data in both formats (i.e., text or media) are stored in large-scale blockchain-based storage via a customer process. Each IoT object in Sapphire is represented as an Object-based Storage Device (OSD). Sapphire links the system interface model through the Put/Get application program interface. The main building block of Sapphire is a large-scale storage system which uses the hash-based mapping approach to divide the key address space into OSDs. The OSDs are used as a technique to enhance load balancing and more importantly to simplify the cooperative caching. The number of OSDs may be scaled up or down in size based on the number of physical objects which may join or depart the system. To investigate the issue of fault tolerance caused by storage node failure, several data replicas are used.

(MT11) **Physical security**: Attributed to attack *AT8*. IoT data may be scattered in different physical locations, making them susceptible to physical attacks despite the the existence of the previously mentioned solutions. Therefore, there is a need of physical security measures for protecting IoT data at rest. This is because the above-mentioned solutions cannot prevent the physical damage of IoT objects along with their storage as well as data centres. Presently, several physical security solutions can be used to protect IoT data at rest, including but not limited to security guards, physical barriers, video surveillance, and locks. It is also wise to improve the efficiency of such physical security measures by integrating them with IoT technology due to the use of connected sensors and actuators. Intelligent monitoring, tampering alerts, perimeter protection, and facial recognition are some examples of this kind of integration.

(MT12) **Monitoring and auditing**: Attributed to attack *AT8*. Monitoring activities in the storage of IoT data in the cloud is of paramount importance to prevent data breaches [92]. Toward this end, several research efforts have been conducted, some of the most recent of which are described here. In [93], the authors propose a centralised monitoring technique for cloud applications used to monitor servers, agents, and files along with their configurations. To overcome the limitations of a centralised monitoring approach, which include scalability and most importantly single point of failure, this technique provides multi-level notifications, redundancy, and automatic healing. In [94], the authors propose a scalable distributed monitoring solution for clouds. This solution depends heavily on a scattered management tree which involves a set of parameters along with their protocols for data collection. Moreover, the authors reviewed the shortcomings of current intrusion detection solutions and also investigated the use of one of the emerging fields for securing virtual machines (VMs) in the cloud, known as virtual-machine-level intrusion detection. In [95], the authors propose a novel architecture in which the virtualisation technology can be integrated into the heart of cloud computing to carry out intrusion detection security utilising hypervisor performance metrics like packets transmitted/received, CPU utilisation, and read/write requests. The authors also illustrate and validate that malicious activities could happen, even when the attackers lack the knowledge of the

operating system which operates within the VMs. For the interested readers, other research proposals related to this topic can be found in [96,97].

(MT13) **Decommissioning**: Attributed to attack *AT1*. The process of proper decommissioning of IoT objects along with their data in the cloud is a fundamental requirement in IoT security, and its solutions can be broadly classified into two categories: (i) object-based solutions which focus on decommissioning of IoT objects and their on board data, and (ii) cloud-based solutions which concentrate on the destruction of IoT data in the cloud storage. Despite the importance of object-based decommission techniques for addressing security and privacy concerns like personal data breaches, there is a lack of state-of-the-art research conducted in this regard. Nevertheless, the Smart Card Alliance in [98] suggested two choices for decommissioning. Firstly, the objects can be reset to factory default mode. In this option, all data in objects will be deleted except for the basic security parameters. These objects can come back to life later. Secondly, a blacklist technique implemented on a server will be used to prevent blocked objects to re-join a network unless their statuses on the server have been changed.

(MT14) **Secure data migration**: Attributed to attacks *AT4* and *AT8*. Despite the importance of secure data migration solutions in preventing some threats and attacks (e.g., unauthorised access and linkage attacks), a few research works in the literature have been proposed. We briefly discuss them in the following.

In [99], the authors propose a secure data migration solution for migrating or transporting IoT data from one cloud storage service to another. To assure pre-migration authentication, this solution is equipped with mutual authentication composed of key splitting and sharing approaches. Having used a symmetric algorithm (Revest–Shamir–Adleman (RSA)) to encrypt migrated data, several security goals, such as confidentiality, integrity, and authenticity, are fulfilled. Two OpenStack servers were used to implement and validate the feasibility of this technique. In [100], the authors propose a simple and effective solution for securely migrating data between different cloud storage services. This technique depends heavily on the use of cryptography and steganography, and is known as Secure Cloud Migration Architecture using Cryptography and Steganography (SCMACS). To encrypt and decrypt migrated data in this technique, a shared key generated by a symmetric algorithm is used by both sender and receiver. The advantage of this approach stems from generating a dynamic value for the private key. The authors also developed a prototype to illustrate the feasibility of their technique based on HDFS. Other techniques for migrating data securely among different cloud storage can be found in [101–103].

An overview of countermeasures proposed IoT data at rest is presented in Table 13.

Table 13. A summary of the mitigation techniques proposed for IoT data at rest.

Implementation Techniques	Research Proposal	Year	Mechanism Used
Secure storage schemes	[48]	2015	Suggests a secure and scalable IoT storage technique that meets different non-functional requirements (e.g., flexibility, liability, and security).
	[50]	2016	Proposes a technique in which IoT data can be stored securely using cryptographic algorithms and several access control policies.
	[51]	2018	Proposes a flexible framework to address storing IoT data securely by merging cloud computing used to store non-time-sensitive data and fog computing used to store time-sensitive data.
	[53]	2016	Provides possible techniques to address some cloud computing issues like data breaches, unavailability, and reliability.
	[52]	2014	Proposes a file system based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) in which secure deletion as well as access to encrypted files in the cloud can be achieved.

Table 13. *Cont.*

Implementation Techniques	Research Proposal	Year	Mechanism Used
Access control	[60]	2017	Suggests a hybrid method composed of data encryption with fine-grained access technique and index encryption, which is suitable for a fog computing ecosystem.
	[61]	2016	Proposes a security model of attribute-based encryption with outsourced decryption called Chosen Ciphertext Attack (CCA), which is the best technique for IoT data protection in the cloud.
	[63]	2018	Proposes a general framework in which a fully secure leakage-resilient function encryption technique is constructed to prevent several attacks (e.g., side-channel attacks).
	[57]	2012	Discusses different solutions that can be used to protect user data, such as encryption, authentication interface, and multi-level virtualisation.
	[62]	2018	Suggests a novel technique to reinforce CP-ABE solutions to offer immunity against key-delegation abuse concern.
Distributed data storage	[85]	2014	Proposes a new type of Merkle hash tree to enhance effective integrity checking, secure file sharing without any alteration, and file content update.
	[104]	2011	Suggests a novel approach for a secure data repository service developed on a public cloud infrastructure to allow customers to securely share and store their sensitive data in the cloud.
	[87]	2015	Describes HDFS and its difficulty in preserving the security and privacy of Big Data.
	[88]	2015	Represents three techniques (Kerberos, name node, and algorithm) used to enhance HDFS security.
Recovery strategy	[10]	2017	Suggests a distributed cloud storage system based on a mini-cloud assumption used to replicate and upload IoT data among different data centres.
	[64]	2016	Suggests the distribution of local cloud computing resources to investigate the long-term evolution architecture shortcomings within radio access networks and proposes a new protocol for a memory replication.
	[65]	2013	Proposes a divide-and-conquer technique used to replicate the content in wireless mesh networks.
	[67]	2015	Suggests different local search algorithms and represents a new technique called Aurora used to apply such algorithms in HDFS with lower overhead.
	[66]	2013	Suggests a lightweight and scalable approach in which an object replication and placement technique in WMNs is achieved.
Transient data storage	[73]	2018	Proposes a technique for managing mass transient data in IoT applications, which consists of several components (e.g., transient data characterisation, data manager, and resource estimator).
	[74]	2014	Proposes a software architecture that facilitates the collection of sensor data in the IoT environment.
	[76]	2015	Proposes a distributed cloud-based storage system developed specifically for IoT data.
	[75]	2014	Proposes a new approach to utilize sensing capabilities in smart cities collect environmental data from different heterogeneous objects to be stored in a data storage system that supports Structured Query Language (SQL) and non SQL technologies.

Table 13. *Cont.*

Implementation Techniques	Research Proposal	Year	Mechanism Used
Anonymisation based solutions	[68]	2012	Suggests an anonymity-tree based technique suitable for IoT that reinforces multi-precision queries.
	[69]	2012	Proposes an enhanced fine-grained algorithm *k*-anonymity which re-evaluates the generalisation scale corresponding to the application domain.
	[71]	2008	Proposes a new privacy notation known as *t*-closeness in which the distribution of a feature in any class should be very close to the distribution of the feature in the whole table.
	[72]	2010	Proposes a privacy procedure based on information theory, the implementation of which depends on the post-randomisation method.
Searchable encryption	[78]	2011	Suggests some improvements in searchable symmetric encryption in terms of effective constructions and definitions.
	[79]	2008	Addresses the notation threshold privacy preserving keyword search (TPPKS) , identifies its security goals, and develops a TPPKS approach.
	[81]	2011	Proposes a multi-user searchable encryption approach which is more practical, and has a set of benefits over the popular techniques.
	[83]	2016	Proposes the first attribute-based keyword search approach equipped with an effective user revocation technique, offering fine-grained search authorisation.
Blockchain-based solutions	[89]	2018	Proposes a decentralised architecture based on blockchain technology in which the trust and integrity of IoT data among TPAs can be achieved.
	[7]	2017	Proposes a blockchain-based architecture to provide the integrity of IoT data among different TPAs.
	[90]	2017	Proposes a blockchain IoT data storage system which provides secure and permanent IoT data management.
	[91]	2018	Proposes a new IoT data storage system (known as Sapphire) based on blockchain technology. IoT data coming from different IoT devices constitutes objects with methods, IDs, features, and policies.
Monitoring and auditing	[96]	2014	Proposes an approach to deal with a huge amount of data to investigate for security monitoring.
	[97]	2015	Proposes a new public auditing technique based on Merkle hash tree known as MuR-DPA which integrates a new authenticated data structure (ADS).
	[95]	2014	Suggests a hypervisor-based cloud intrusion detection technique that does not need extra software installed in VMs which simultaneously provides more benefits compared to host-based intrusion-detection techniques.
	[94]	2013	Proposes a scalable monitoring approach for clouds to supervise their data in a distributed manner.
Deduplication schemes	[34]	2010	Suggests simple solutions which allow cross-user deduplication and, at the same time, minimise the danger of data leakage.
	[43]	2012	Proposes a secure data deduplication architecture for cloud storage.
	[45]	2013	Proposes a secure and effective storage service known as ClouDedup, which enables block-level deduplication as well as data confidentiality.
	[44]	2016	Proposes an approach based on attribute-based encryption used not only to deduplicate encrypted data stored in the cloud storage, but also to provide secure data access control.

Table 13. *Cont.*

Implementation Techniques	Research Proposal	Year	Mechanism Used
Secure data migration techniques	[99]	2017	Proposes a secure data migration approach to move the data from one cloud storage service to another.
	[101]	2015	Proposes a new architecture which enables secure data transportation from users to the cloud server providers.
	[103]	2018	Proposes a new framework for multi-tenant cloud migration used to fulfil data integrity and confidentiality.
	[102]	2016	Proposes an inter-cloud data migration technique which provides better security goals and quicker response time for transferring large files into cloud storage services.

5. Analysis of Security and Privacy Guidelines for IoT Data at Rest

This section first describes our derived guidelines as they relate to the involved stakeholders. Then, the overall guideline framework is presented with the links between guidelines, mitigation techniques, and attacks.

(G1) **Minimise data storage**: The GDPR has proposed six principles for the processing of personal data, among which is data minimisation. CSSs, under GDPR, should only store personal data required to achieve their processing purposes [105]. Two benefits are associated with this type of principle. One is that data breaches will be minimised, as unauthorised users will have access to a restricted amount of data. The other benefit is that data accuracy will be improved [106]. This guideline hence suggests that the amount of data stored either on objects or in the cloud should be minimised, and any segment of data that is not needed to execute a specific task should be removed from IoT storage [106]. For example, the authors in [14] state that raw data can be removed from storage once secondary contexts are extracted and, more importantly, all data must be de-identified. Three countermeasures, namely, *MT1*, *MT5*, and *MT8*, can be used to accomplish this guideline.

Reasoning: This guideline is proposed based on one of the Privacy by Design as well as Security by Design principles, which is the minimisation of data, proposed by Hoepman in [107] and Open Web Application Security Project (OWASP) [108], respectively. We do believe this guideline can be used by MAN, DEV, and PRV as they are directly involved in the production, deployment, and development of IoT objects. This can be done by allowing such objects to minimise the amount of data on them by deleting any segments of data that are not needed. It can also be used by CNS, since in the future IoT objects may be armed with dashboard settings, permitting data collection to be minimised. Table 14 represents the stakeholders who may utilize this guideline.

Table 14. The involved IoT stakeholders in G1.

MAN	DEV	PRV	CNS
✓	✓	✓	✓

(G2) **Minimise data retention**: In [109], the authors state that retaining data for a long time is associated with data breaches, since it gives an attacker an opportunity to try all of their hacking techniques to compromise it. Apart from data breaches, privacy risks may also be increased, according to [14]. This is because long retention periods may cause unauthorised secondary usage. This is why the GDPR has stated that sensitive data must be stored "no longer than is necessary for the purposes for which the personal data are processed" [105]. This guideline therefore suggests that data retention on IoT objects or in the cloud should be minimised as much as possible. This guideline can be implemented by *MT6*. All stakeholders who may use this guideline can be shown in Table 15.

Table 15. The involved IoT stakeholders in G2.

MAN	DEV	PRV	CNS
✓	✓	✓	✓

Reasoning: This guideline is proposed based on a minimisation principle suggested in Privacy by Design (Hoepman in [107]) as well as Security by Design (OWASPS in [108]) frameworks. It can be utilised by MAN to ensure that their objects are equipped with data retention rules. For DEV and PRV, this guideline can be implemented to ensure that IoT applications are engineered from the beginning to avoid keeping data longer than is required. CNS can also benefit from this guideline by deleting unnecessary data on their objects. All stakeholders who may use this guideline can be shown in Table 15.

(G3) **Distributed data storage**: To prevent a single point of failure in IoT applications and enhance their availability, this guideline suggests that IoT data should be stored in a distributed manner. However, the use of this guideline has associated trade-offs. On the one hand, it improves the availability of IoT applications and also reduces some privacy risks. For instance, the authors in [14] state that distributed data storage can be used to minimise privacy violations, since it prevents unauthorised access and secondary knowledge discovery. On the other hand, it opens doors for several attacks and threats like data leakage, as it increases the attack surface of IoT, according to [110]. Therefore, this guideline should be investigated with caution, and it can be implemented by *MT8*.

Reasoning: This guideline is suggested based on the aggregation principle proposed in the Privacy by Design framework (Hoepman in [107]). It can be utilised by MAN to assure that their IoT products have capabilities to store data in distributed environments. For PRV and DEV, it can be utilised to assure that their IoT applications and services are designed to store data in distributed environments by supporting distributed IoT architectures. Table 16 shows stakeholders who may utilize this guideline.

Table 16. The involved IoT stakeholders in G3.

MAN	DEV	PRV	CNS
✓	✓	✓	✗

(G4) **Encrypt data storage**: In [17], the ENISA expressed the importance of encrypted IoT data at rest to minimise privacy violations in the IoT. It is also worth mentioning that the Payment Card Industry Data Security Standard (PCI DSS) has forced all companies dealing with credit card information (e.g., Visa, Mastercard) to implement encryption techniques when storing data [111]. Moreover, PCI DSS explicitly prevents the use of storage encryption as provided by operating systems. This guideline thus suggests that the data of IoT applications should be stored in an encrypted manner either on IoT objects or in the cloud. Two protection measures (*MT2* and *MT7*) can be used to achieve this guideline.

Reasoning: This guideline is stated based on the hide principle proposed in the Privacy by Design framework (Hoepman in [107]). It can be utilised by MAN to assure that their IoT products have the ability to encrypt their stored data. Both PRV and DEV can integrate this guideline from the beginning into their IoT applications so that they always store their data in an encrypted format. CNS can also benefit from this guideline by enabling this feature if it comes with IoT products. Stakeholders involved in this guideline are represnted in Table 17.

Table 17. The involved IoT stakeholders in G4.

MAN	DEV	PRV	CNS
✓	✓	✓	✓

(G5) **Prevent data leakage**: Even if IoT data is stored in an encrypted form, it is still vulnerable to side-channel attacks. This can be happen for many reasons, such as weak encryption, hardware failure, and human error [53]. Therefore, this guideline suggests that IoT stakeholders like manufacturers and providers should implement suitable data leakage prevention techniques (e.g., Searchable Encryption (SE) techniques) by taking governments rules and industry standards into consideration. Six implementation techniques (*MT1*, *MT2*, *MT5*, *MT6*, *MT6*, and *MT12*) can be used to carry out this guideline.

Reasoning: This guideline is suggested based on the hide principle proposed in the Privacy by Design framework (Hoepman in [107]). MAN can integrate this guideline into their IoT products in order to be more resistant to side-channel attacks. It can also be utilised by PRV and DEV to assure that their IoT applications are engineered from the ground up to prevent data leakage. The involved stakeholders in this guideline are shown in Table 18.

Table 18. The involved IoT stakeholders in G5.

MAN	DEV	PRV	CNS
✓	✓	✓	✗

(G6) **Minimise data granularity**: "Granularity" here refers to the level of detail available and to be utilised. A concrete representation of data (e.g., a full address) is known as high granularity, while a summary view of data or a high-level representation of data is called low granularity (e.g., a dissemination of location), according to [112]. In this context, storing concrete data is always associated with high privacy risks compared to storing data at an abstract level, since it is composed of more data. Therefore, this guideline suggests that IoT systems should only store minimal data in which their functions can be maintained [14]. This guideline can be implemented by *MT1* and *MT7*.

Reasoning: This guideline is stated based on the minimisation principle suggested in Privacy by Design (Hoepman in [107]) as well as Security by Design (OWASPS in [108]) frameworks. It can be implemented by MAN to ensure that their products always collect and store information about their customers at a high level. Both DEV and PRV can also integrate this guideline into their IoT applications from the ground up to prevent identification attacks as they store data at an abstract level. Table 19 shows all stakeholders who may utilize this guideline.

Table 19. The involved IoT stakeholders in G6.

MAN	DEV	PRV	CNS
✓	✓	✓	✗

(G7) **Ensure data availability**: With the growth of the IoT, data will be generated at an unprecedented rate, as billions of objects will be connected to the Internet. Since most of these objects (e.g., actuators, sensors, thermostats) do not have on-board storage, their data must be stored in cloud data centres [10]. The availability of this data is a crucial requirement for many applications to achieve their tasks. This guideline therefore suggests that CSSs as well as IoT objects should implement efficient techniques (e.g., recovery strategies and DoS prevention) by which the availability of their data is guaranteed in case of natural disasters or some attacks. For instance, an attacker could flood a storage server with invalid data at very high rate in such a way that the storage server wastes most of its time validating the authenticity of data and therefore fails to respond to valid network traffic in a timely fashion [31]. This guideline can be implemented by two protection measures (*MT4* and *MT1*).

Reasoning: This guideline can be utilised by DEV, PRV, and MAN to ensure that their applications, services, and objects are always accessible by their authorised users. Table 20 shows all stakeholders who may utilize this guideline.

Table 20. The involved IoT stakeholders in G7.

MAN	DEV	PRV	CNS
✓	✓	✓	✗

(G8) **Location-based aggregation**: This guideline suggests that IoT applications should aggregate their data based on geographical boundaries. For instance, a query would be "how many medical objects are used in each city in Switzerland". The response to this question would be an aggregated value unique to each city. However, it is not necessary to gather details about individual medical objects, as it may lead to privacy breaches [113]. This guideline can be implemented by *MT8*.

Reasoning: This guideline is suggested based on aggregation principle proposed in the Privacy by Design framework (Hoepman in [107]). MAN and PRV can implement this guideline in their products and services so that they can aggregate their data based on geographical boundaries. Table 21 shows all stakeholders who may utilize this guideline.

Table 21. The involved IoT stakeholders in G8.

MAN	DEV	PRV	CNS
✓	✗	✓	✗

(G9) **Post-inform customers**: In a recently published survey by Eurobarometer, 67% of Europeans indicated that they were worried about their information and personal data that they offer online, since they lack control over it [22]. Toward this end, the GDPR was developed to give the individuals of the EU control over their personal data. This guideline thus suggests that IoT applications should always inform their users before storing or sharing data related to them. For instance, the GDPR states that the processing of personal individual data in business enterprises requires an explicit opt-in or consent from them, and several kinds of data will necessitate distinct consent [105]. This guideline can be implemented by *MT2*.

Reasoning: This guideline is stated based on the inform principle proposed in the Privacy by Design framework (Hoepman in [107]). This guideline can be implemented by MAN to assure that their objects have the ability to infrom their customers about their data. PRV can also implement this guideline in their services so that they can notify users when they store personal data or sensitive data, and give users control over their data. Table 22 shows all stakeholders who may utilize this guideline.

Table 22. The involved IoT stakeholders in G9.

MAN	DEV	PRV	CNS
✓	✗	✓	✗

(G10) **Chain data aggregation**: This guideline suggests that data aggregation be accomplished on-the-go as data transfers from one object to another so that each object will have an opportunity to respond [14]. In this case, if there is a query (e.g., one which requires a count), any object can respond to it without the need of a centralised entity. This will give all objects the chance to respond to this query, and it will simultaneously improve the availability of the IoT [114]. This guideline can be implemented by *MT8*.

Reasoning: This guideline is proposed based on the aggregation principle proposed in the Privacy by Design framework (Hoepman in [107]). Both MAN and PRV can implement this guideline in their products and services so that they can aggregate their data while transferring data from one object to another. Table 23 shows all stakeholders who may utilize this guideline.

Table 23. The involved IoT stakeholders in G10.

MAN	DEV	PRV	CNS
✓	✗	✓	✗

(G11) **Time-period data aggregation**: This guideline suggests that IoT applications should store their data over a long period of time (i.e., days, months). This guideline will minimise the granularity of IoT data, which in turn reduces data breaches. For instance, it is wise to report the power consumption of a given building in aggregate form per week rather than on a daily basis [115]. This guideline can be implemented by *MT8*.

Reasoning: This guideline is stated based on the aggregation principle proposed in the Privacy by Design framework (Hoepman in [107]). It can be implemented by MAN to assure that their products are armed with techniques in which customers can decide when they want this product to aggregate data related to them. PRV can also integrate this guideline into their services so that they can aggregate over a long period of time. Table 24 shows all stakeholders who may utilize this guideline.

Table 24. The involved IoT stakeholders in G11.

MAN	DEV	PRV	CNS
✓	✗	✓	✗

(G12) **Ensure authorised access to IoT data**: The importance of providing solid techniques to control access to IoT data at rest derives from two primary factors. One is that an IoT object may need to communicate with other objects in order to share and access their data. This object must therefore only interact with authorised objects. The other factor is that different IoT objects may store their data in the CSSs which are only logically isolated, but in reality such data may be physically kept in the same data centre [116]. Overlooking access control mechanisms to IoT data at rest may lead to harmful consequences. For instance, the authors in [6] show that a thermostat deployed in a smart home depends heavily on a smoke detector's data to turn a heating system off in case of danger. However, sharing and accessing the smoke detector's data by unauthorised objects may place the whole smart home at risk. This guideline thus suggests that each IoT object or CSS should be armed with authorisation techniques (e.g., a role-based technique) through which all unauthorised requests are blocked or prevented. Three implementation techniques—*MT11*, *MT9*, and *MT3*—can be used to fulfil this guideline.

Reasoning: This guideline is suggested based on the principle of defence in depth proposed in the Security by Design framework (OWASPS [108]). This guideline can be implemented by MAN to ensure that their products are equipped with measures via which only authorised users can gain access to them. PRV as well as DEV can also integrate this guideline into their services and applications so that only legitimate users can gain access to their stored data. Table 25 shows all stakeholders who may utilize this guideline.

Table 25. The involved IoT stakeholders in G12.

MAN	DEV	PRV	CNS
✓	✓	✓	✗

(G13) **Remove or hide sensitive data**: This guideline suggests that IoT applications must first get rid of personally identifiable information and then store it. It is obvious that storing a data set along with its personally identifiable information will significantly increase the risk of privacy losses. For instance, the authors in [117] illustrate that a retailer, called Target, once received a complaint from a customer who was very disappointed, as company sent coupons for kids' clothes to his teenage

daughter. Nevertheless, the Target intentionally sent such coupons to the daughter since she was pregnant at that time. This type of inference may happen as a consequence of storing data along with its personally identifiable information, which in turn helps companies to conduct data mining on their customers' data. This guideline can be implemented by *MT5*.

Reasoning: This guideline is proposed based on the hide principle proposed in the Privacy by Design framework (Hoepman in [107]). MAN can integrate this guideline into their products to ensure that they have capabilities to de-identify personal data before storing it. It can also be implemented by both PRV and DEV to assure their applications and services are developed from the ground up so that they are capable of identifying personally identifiable information, and more importantly, de-identifying it before storing it. Table 26 shows all stakeholders who may utilize this guideline.

Table 26. The involved IoT stakeholders in G13.

MAN	DEV	PRV	CNS
✓	✓	✓	✗

(G14) **Search on encrypted data**: As several research efforts have expressed the importance of performing information retrieval on encrypted data to prevent data linkage attacks [17,18,21], this guideline suggests that IoT applications should be shielded with techniques (e.g., SE) that allow IoT applications to respond to any queries by searching encrypted data without revealing sensitive information. This guideline can be implemented by *MT7*.

Reasoning: This guideline is stated based on two principles, the first of which is the hide principle proposed in the Privacy by Design framework (Hoepman in [107]). The second principle is defence in depth, suggested in the Security by Design framework (OWASPS in [108]). MAN and PRV can implement this guideline in their objects and services to assure that these objects and services have the ability to search encrypted data in order to alleviate linkage attacks. Table 27 shows all stakeholders who may utilize this guideline

Table 27. The involved IoT stakeholders in G14.

MAN	DEV	PRV	CNS
✓	✗	✓	✗

(G15) **Provide data integrity across different platforms**: With the emergence of the IoT, different IoT applications—which may store their data on several platforms—may cooperate with each other to accomplish specific tasks or services. If the data integrity of a single IoT application in the cloud has been tampered with, there is a risk of dealing with unsecured applications [7]. This guideline therefore suggests that IoT objects as well as CSSs should be equipped with techniques in which the data integrity across different platforms must be checked. This guideline can be implemented by *MT10*.

Reasoning: This guideline is stated based on the not trust principle suggested in the Security by Design framework (OWASPS in [108]). This guideline can be implemented by MAN and PRV to ensure that their objects and services are capable of checking the integrity of the data they deal with. Table 28 shows all stakeholders who may utilize this guideline.

Table 28. The involved IoT stakeholders in G15.

MAN	DEV	PRV	CNS
✓	✗	✓	✗

(G16) **Securely share data with untrusted TPAs**: Securely sharing data among untrusted TPAs is of paramount importance for two reasons. One is that IoT systems will store their data on different CSSs due to their limited capabilities as well as the dynamic nature of this technology. The other reason is that it is unrealistic to assume that all cloud service providers are reliable as expected [118]. Thus, this guideline suggests that IoT systems should be armed with techniques in which such systems could store and share their data securely in different CSSs, even when some of these are not untrusted [91]. This guideline can be implemented by *MT10*.

Reasoning: This guideline is stated based on two principles, namely, the not trust and defence in depth principles suggested in the Security by Design framework (OWASPS in [108]). Both MAN and PRV can equip their objects and services with techniques through which such objects and services can share their data securely among untrusted TPAs. Table 29 shows all stakeholders who may utilize this guideline.

Table 29. The involved IoT stakeholders in G16.

MAN	DEV	PRV	CNS
✓	✗	✓	✗

*(G17)***Prevent physical access to data storage**: In [119], the authors state that physical attacks against traditional computers have become easier to carry out compared to logical attacks, since logical security measures have been significantly improved. Likewise, the IoT will suffer from physical attacks. This is because the IoT inherits most of the issues of the existing Internet and, most probably, increases them due to direct association with physical objects [4,21]. Hence, physical security in the IoT is crucial because logical security measures like firewalls, intrusion detection systems, and encryption cannot prevent physical attacks against IoT objects or data centres in the cloud. This guideline thus suggests that a barrier should be placed around IoT objects and data centres to prevent unauthorised physical access. This guideline can be implemented by *MT11*.

Reasoning: This guideline is proposed based on the control principle suggested in the Privacy by Design framework (Hoepman in [107]). This guideline can be utilised by MAN to equip their products with techniques to prevent physical tampering. PRV can also benefit from this guideline by storing data collected by their provided services in different data storage services, which may be located in environments over which they have control. Table 30 shows all stakeholders who may utilize this guideline.

Table 30. The involved IoT stakeholders in G17.

MAN	DEV	PRV	CNS
✓	✗	✓	✗

(G18) **Take precautions in case of natural disaster**: In [120], the authors stress the importance of taking precautions in case of natural catastrophe. Toward this end, they used three backup servers, the data of which must be stored in encrypted format. If something unusual occurs to the server, the secret key used to encrypt the data will be used again to decrypt it. This guideline suggests that CSSs should have recovery strategies used to get their data back in case of unusual situations. This guideline can be implemented by *MT4*.

Reasoning: This guideline is proposed based on the fail securely principle proposed in the Security by Design framework (OWASPS in [108]). This guideline can be utilised by all stakeholders (see Table 31) by implementing recovery techniques so that they have a copy of their data in case of natural disasters.

Table 31. The involved IoT stakeholders in G18.

MAN	DEV	PRV	CNS
✓	✓	✓	✓

(G19) **Minimise duplicated copies**: Unlike minimising data storage, which focuses on removing unnecessary segments of data not required to carry out a specific task before the storing phase, this guideline concentrates on minimising duplicate data in the cloud. This kind of data replication can occupy network bandwidth and may be stored in different data storage services, increasing the attack surface. Data duplication in the cloud derives from two main factors. One is that HDFS generates a great deal of duplicate data due to its replication mechanism [31]. The other factor is that different IoT objects may be deployed to monitor the same environment, which may generate duplicated copies of IoT data [121]. This guideline therefore suggests that cloud-based storage services should be equipped with a technique in which only one unique copy of duplicate data is stored [47]. This guideline can be implemented by *MT1*.

Reasoning: This guideline is stated based on minimising the attack surface area principle suggested in the Security by Design framework (OWASPS in [108]). It can be utilised by both MAN and PRV to guarantee that their products and services only have one distinct copy of duplicate data, and most importantly that they are stored in different locations from their origin. Table 32 shows all stakeholders who may utilize this guideline.

Table 32. The involved IoT stakeholders in G19.

MAN	DEV	PRV	CNS
✓	✗	✓	✗

(G20) **Proper data destruction**: The secure destruction of IoT data either in IoT objects or in the cloud is a vital requirement to prevent different security and privacy issues (e.g., data leakage). On the one hand, the destruction of IoT objects along with their sensitive data is inevitable, since each IoT object will reach its end of life, and therefore its data must be destroyed properly [98]. In this case, this guideline suggests that each object should be equipped with a clear end-of-life technique in which this object can be disposed of or destroyed without exposing its sensitive data [122]. On the other hand, there are many reasons for the destruction of IoT data in the cloud. One is due to the termination of a contract with a provider in which a secure deletion of customer data must be accomplished [123]. Another reason is because of the compliance with GDPR in which people have the right not only to to access their personal data, but also to demand the destruction of their data [105]. In this case, this guideline suggests that data providers should delete and stop further use of users' personal data when they ask for their data to be forgotten.

Reasoning: This guideline is suggested based on the control principle suggested in the Security by Design framework (OWASPS in [108]). It can be utilised by MAN to ensure that their objects have the ability to destroy their data in a secure manner when they reach an end-of-life stage. PRV and DEV can also integrate this guideline into their services and applications in order to give their users control over their data, among which is the right for their data to be forgotten. Table 33 shows all stakeholders who may utilize this guideline.

Table 33. The involved IoT stakeholders in G20.

MAN	DEV	PRV	CNS
✓	✓	✓	✓

(G21) **Secure data migration**: Although most IoT systems transfer users' data to cloud storage services due to their limited capabilities in terms of memory and storage space, such systems may decide to migrate or transfer their data from one cloud storage service to another due to many factors (e.g., the lack of security and availability) [124]. This process of migrating or transporting data is known as data migration, and it must be carried out securely. That said, the lack of secure data migration when moving data from one CSS to another may open the door for many attacks and threats. For example, the authors in [125] state that if data migration is not accomplished systematically and properly, such data is susceptible to many attacks (e.g., unauthorised access). Hence, this guideline suggests that CSSs should be armed with techniques in which data migration among them should be carried out securely.

Reasoning: This guideline is stated based on the not trust services principle proposed in the Security by Design framework (OWASPS in [108]). It can be utilised by PRV when they transfer customers' data from one data storage service to another. MAN can also benefit from this guideline when moving their data (e.g., objects update) from one service to another. Table 34 shows all stakeholders who may utilize this guideline.

Table 34. The involved IoT stakeholders in G21.

MAN	DEV	PRV	CNS
✓	✗	✓	✗

(by G22) **Manage encryption keys**: To protect sensitive data, strong encryption is of paramount importance. Although several research proposals have been put forth to encrypt IoT data, the lack of a strong technique for managing the encryption keys is a common issue among them, which may lead to several vulnerabilities (e.g., unauthorised access). Moreover, the process of managing thousands of encryption keys within an IoT company is a challenge. This guideline therefore suggests that encryption keys must be kept on separate devices from the data they are used to encrypt. This kind of separation makes it harder for attackers to compromise data and its encryption keys at the same time [126].

Reasoning: This guideline is stated based on the defence in depth principle proposed in the Security by Design framework (OWASPS in [108]). This guideline can be implemented by both PRV and MAN to ensure the protection of users' data, since they separate encryption keys from encrypted data. Table 35 shows all stakeholders who may utilize this guideline.

Table 35. The involved IoT stakeholders in G22.

MAN	DEV	PRV	CNS
✓	✗	✓	✗

Figure 1 summarises the relationship between our proposed guidelines for IoT data at rest, followed by their suitable mitigation techniques and associated attack vectors.

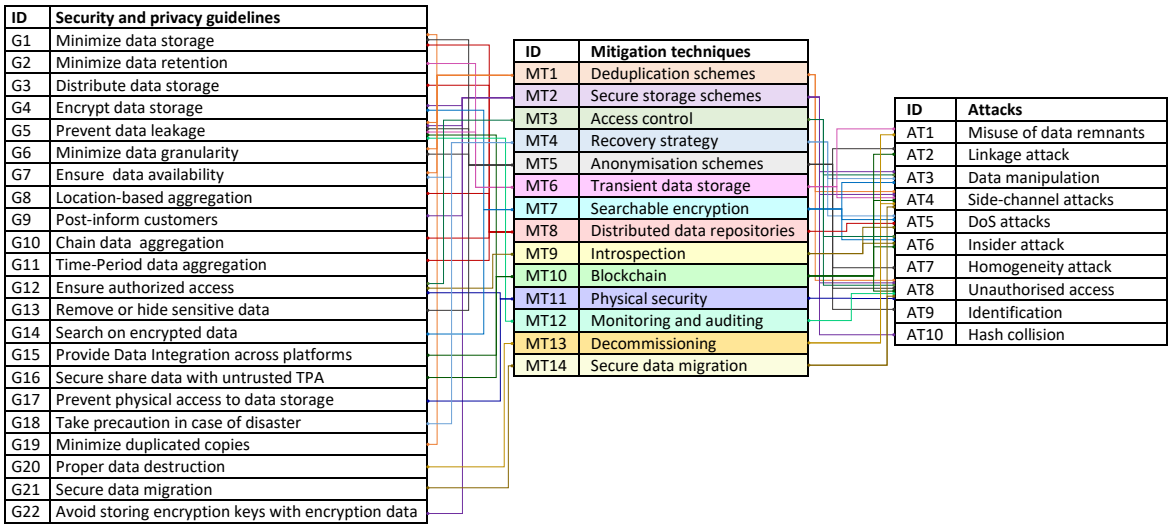

Figure 1. A summary of guidelines, stakeholders, attacks, and countermeasures for IoT data at rest. DoS: Denial of Service.

6. Discussion and Future Work

A summary of the previously mentioned research efforts is presented in Table 36, along with our intended objectives. It is not difficult to observe many limitations while going through them. Our research is therefore directed to overcome these shortcomings, which can be categorised as follows: (i) The absence of a comprehensive list of security and privacy guidelines for IoT data at rest, followed by for whom these guidelines are intended. (ii) The lack of suitable implementation techniques to implement such guidelines. (iii) The necessity of attack investigations related to IoT data at rest.

6.1. Recommendations for Future Work

In spite of considerable research efforts devoted to the IoT security domain, we can still suggest many issues that need to be addressed.

6.1.1. Protection against Insider Threats

Although some of previously mentioned protection measures (e.g., monitoring and incident response) can be used to mitigate malicious insider threats, such techniques can not fully protect IoT data at rest from such threats, as they are not designed specifically for this purpose. Therefore, there is a need to suggest a mechanism which can defend against insider threats in many IoT domains (e.g., e-healthcare organisations). This can be achieved by implementing preventive, detective, and reactive measures such as user behaviour analysis, policy-based frameworks, detection of anomalies in data access, and context-based access. Such techniques must be taken into account to avoid the impacts of malicious insiders in IoT data at rest. Toward this end, user behaviour analysis techniques have been proposed by a few researchers [127]. There are, however, many shortcomings in all the suggested approaches, and they therefore cannot be implemented in all IoT domains (e.g., the multi-cloud e-healthcare environment) to prevent malicious insiders, according to [24]. Hence, it is a challenge for researchers to design approaches which are suitable to investigate user behaviour and implement them to alleviate this threat, particularly in the e-healthcare environment. It is also possible that individuals who are in contact with patients could accidentally or intentionally alter the settings of IoT objects collecting health data, which may adversely impact the reply of healthcare organisations relating to patient care. It is therefore essential to develop an approach that can detect such a modification and at the same time notify health organisations about it so that they can turn back the changes in the settings.

Table 36. Comparison of research efforts presented in the literature.

Addressed Features		State-Of-The-Art Work							
		[14]	[15]	[16]	[17]	[18]	[19]	[21]	This Work
IoT security and privacy Guidelines	Minimise data storage	✓	✓	✓	✓	✓	✓	✗	✓
	Minimise data retention	✓	✗	✓	✓	✓	✗	✗	✓
	Encrypt data communication	✓	✓	✓	✓	✓	✓	✓	✗
	Secure boot process	✗	✗	✓	✓	✓	✓	✓	✗
	Hide data routing	✗	✗	✗	✓	✓	✓	✓	✗
	Reduce interference	✗	✓	✓	✓	✓	✓	✓	✗
	Distribute data storage	✓	✗	✗	✗	✗	✓	✗	✓
	Encrypt data storage	✓	✓	✓	✓	✓	✓	✗	✓
	Minimise data granularity	✓	✗	✗	✗	✗	✗	✗	✓
	Location-based aggregation	✓	✗	✗	✗	✗	✗	✗	✓
	Inform customers	✓	✓	✗	✓	✓	✓	✗	✓
	Chain data aggregation	✓	✗	✗	✗	✗	✗	✗	✓
	Time-period data aggregation	✓	✗	✗	✗	✗	✗	✗	✓
	Ensure authorised access	✗	✓	✓	✓	✓	✓	✓	✓
	Remove or hide sensitive data	✓	✓	✓	✓	✓	✓	✓	✓
	Search on encrypted data	✓	✗	✗	✓	✗	✓	✓	✓
	Provide data integrity across CSPs	✗	✗	✗	✗	✗	✗	✗	✓
	Secure share data with untrusted CSPs	✗	✗	✗	✗	✗	✗	✗	✓
	Minimise duplicated copies	✗	✗	✗	✗	✗	✗	✗	✓
	Prevent physical access	✗	✗	✓	✓	✗	✓	✗	✓
	Ensure data availability	✗	✗	✓	✓	✓	✓	✗	✓
	Proper data destruction	✗	✗	✗	✓	✗	✓	✗	✓
	Secure data migration between CSSs	✗	✗	✗	✗	✗	✗	✗	✓
	Void storing enc. keys with enc. data	✗	✗	✗	✗	✗	✗	✗	✓
Types of Guidelines	Privacy	✓	✓	✓	✓	✓	✓	✓	✓
	Security	✗	✓	✓	✓	✓	✓	✓	✓
Guidelines Intended for	Manufacturer	✗	✗	✓	✗	✓	✗	✓	✓
	Developer	✓	✓	✓	✓	✓	✓	✓	✓
	Customer	✗	✗	✓	✗	✗	✗	✓	✓
	Provider	✗	✗	✗	✗	✓	✗	✓	✓
Threats mitigated by guidelines		✗	✗	✗	✗	✗	✗	✓	✓
Technique to implement guidelines		✗	✗	✗	✗	✗	✗	✓	✓

Detection of anomalies in data access was investigated in [128]. The authors propose and design a novel technique capable of detecting, notifying, and responding to any anomalies inside Relational Database Management Systems (RDBMS). It is also capable of automatically creating and maintaining profiles of normal applications as well as end users. This process of keeping track of normal users and applications depends heavily on their communication with monitored RDBMS during the training stage. Then, it uses such profiles to identify malicious behaviour that sidetracks from normality. Nevertheless, several privacy issues may stem from monitoring the behaviour of end users. Therefore, a great deal of research is required to balance between security and privacy threats and end-user privacy.

6.1.2. Need for Legislation

In the literature, a huge number of issues related to IoT data are described poorly, and they need more investigation. For instance, customers would often like to know what type of data is collected and stored by their smart objects before purchasing them, which is not possible at this time. Moreover, customers may also want to know how their data stored either in the objects or in the cloud are protected. This kind of information is not generally offered. Therefore, it is also wise to give customers the chance to reconfigure their privacy choices or preferences in IoT objects, in a similar way as smartphones. For instance, Google, in the mobile context (e.g., Android), has designed a dashboard technique that gives users more control over their personal data. The appropriate implementation of such dashboard techniques will provide customers more precise ways to regulate what data they want to share and when and how their personal information is gathered and used [129]. Nevertheless, further investigation is required, since the the current approaches are not mature enough for standardisation, nor are they designed specifically for the IoT.

6.1.3. The Necessity of Common Intercloud Architecture

Despite the benefit of common intercloud architecture (e.g., OpenStack, which offers APIs and a framework for cloud systems) in which different clouds can coordinate, share, and manage their functionalities to provide services, it still lacks a common standard, which impedes its interoperability. Toward this end, a handful of research proposals have been conducted [130–132]. In [131], the authors propose a model that integrates different services to ease intercloud interaction between different platforms so as to display all available services. However, a great deal of effort is required to create a graphical user interface to offer a common management platform.

6.1.4. The Distribution of the Cloud Infrastructure over the Edge Computing

A new emerging technology known as edge computing has been proposed by CISCO [133] as an intermediate layer between IoT objects and cloud computing. The main objective behind this technology is to scatter the cloud infrastructure over the edge layer, making it closer to IoT objects and users. Several advantages in terms of bandwidth and latency that improve service quality come as a result of this closeness. It is expected that the IoT may benefit from edge cloud computing so as to achieve some desired requirements like performance and security. To this point, several research proposals are required to develop efficient security techniques based on edge computing technology. Apart from required security solutions, a few questions have still been raised and need to be addressed, for instance, how to develop a trust model between IoT objects and fog nodes in such a highly scattered IoT environment.

6.2. Limitations of the Study and Threats to Validity

In this paper, we propose a framework of security and privacy guidelines for IoT data at rest and for whom these guidelines are intended, as well as their appropriate countermeasures. However, such guidelines and their protection measures are not absolute, nor can they guarantee the protection of IoT data at rest for three reasons. One is that new vulnerabilities are continuously being disclosed, which indicates there is a necessity to monitor, review, and maintain IoT security and privacy guidelines for IoT data at rest as well as best practices developed for particular environments and use cases (e.g., healthcare) on a regular basis. Another reason is that the IoT paradigm is enabled by several technologies (e.g., middleware, sensors, and communication protocols such as secure video steaming in [134]), and, certainly, new emerging technologies related to how to either store or process IoT data at rest will be introduced. New security and privacy guidelines are therefore of paramount importance to avoid IoT data breaches. Unfortunately, these rules are breakable due to the advancements of hacking tools as well as the level of knowledge used by the adversaries. The other reason is that the success of our suggested framework of security and privacy guidelines for IoT data at rest depends

heavily on their implementation. Thus, the poor implementation of such countermeasures may lead to data breaches.

6.3. Conclusions

Because of the unexpected growth of connected sensors and network infrastructure, the dawn of the IoT in which several applications like smart cars, smart buildings, and smart grids can interact with each other to make our lives simpler and more productive is approaching. The IoT is a beneficial ecosystem that offers different solutions like the Amazon Echo; nevertheless, at the same time, the risk associated with data breaches can also be enormous. Therefore, in this paper we conducted an in-depth analysis of IoT data at rest to identify its possible attacks and alleviate its associated risks. Toward this end, we propose a framework of security and privacy guidelines for IoT data at rest that can be used by IoT stakeholders who may utilise such guidelines to build secure IoT systems from the ground up, and therefore enhance security and privacy by design. This framework also shows the link between guidelines, mitigation techniques, and attacks. More importantly, we discuss our derived guidelines as they relate to the involved stakeholders, and we also give a "reasoning" under which each guideline is stated based on one or two principles of either Security by Design or Privacy by Design frameworks. Furthermore, we briefly discuss several limitations of our framework, an example of which is the poor implementation of protection measures. Finally, we suggest some open challenges needing further investigation.

In the future, we will propose a step-by-step methodology of how our suggested guidelines can be implemented by developers from the early stages of their IoT systems so that the poor implementation of such guidelines can be mitigated.

Author Contributions: Conceptualisation, H.A.A., N.A.N. and D.K.; Investigation, H.A.A.; Methodology, H.A.A.; Supervision, H.A.A., N.A.N. and D.K; Validation, N.A.N., A.C. and D.K.; Writing—original draft, H.A.A.; Writing—review & editing, H.A.A., N.A.N., A.C. and D.K.

Funding: This work received funding by the European Union's Horizon 2020 Research and Innovation Programme through the GHOST project (https://www.ghost-iot.eu/) under Grant Agreement No. 740923 and AVENUE project (https://h2020-avenue.eu/) under Grant Agreement No. 769033. This paper reflects only the authors' views; the European Union is not liable for any use that may be made of the information contained herein.

Conflicts of Interest: The authors declared no conflict of interest.

References

1. Terzi, D.S.; Terzi, R.; Sagiroglu, S. A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Int. Things J.* **2017**, *4*, 1250–1258.
2. Rodic-Trmcic, B.; Labus, A.; Bogdanovic, Z.; Despotovic-Zrakic, M.; Radenkovic, B. Development of an IoT system for students' stress management. *Facta Univ. Ser. Electron. Energ.* **2018**, *31*, 329–342. doi:10.2298/fuee1803329r. [CrossRef]
3. Jain, R. Internet 3.0: Ten Problems with Current Internet Architecture and Solutions for the Next Generation. In Proceedings of the MILCOM 2006, Washington, DC, USA, 23–25 October 2006; pp. 1–9. doi:10.1109/MILCOM.2006.301995. [CrossRef]
4. Akram Abdul-Ghani, H.; Konstantas, D.; Mahyoub, M. A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*. doi:10.14569/IJACSA.2018.090349. [CrossRef]
5. Saleem, J.; Hammoudeh, M.; Raza, U.; Adebisi, B.; Ande, R. IoT standardisation: Challenges, perspectives and solution. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems—ICFNDS '18, Amman, Jordan, 26–27 June 2018; ACM Press: New York, NY, USA, 2018; pp. 1–9. doi:10.1145/3231053.3231103. [CrossRef]
6. Mohsen Nia, A.; Jha, N.K. A Comprehensive Study of Security of Internet-of-Things. *IEEE Trans. Emerg. Top. Comput.* **2016**, *5*, 586–602. [CrossRef]

7. Liu, B.; Yu, X.L.; Chen, S.; Xu, X.; Zhu, L. Blockchain Based Data Integrity Service Framework for IoT Data. In Proceedings of the 2017 IEEE International Conference on Web Services (ICWS), Honolulu, HI, USA, 25–30 June 2017; pp. 468–475. doi:10.1109/ICWS.2017.54. [CrossRef]
8. ENISA European Union Agency For Network and Information Security. *Towards Secure Convergence of Cloud and IoT*; Technical Report; ENISA European Union Agency For Network and Information Security: Iraqion, Greece, 17 September 2018.
9. Cirani, S.; Ferrari, G.; Veltri, L. Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview. *Algorithms* **2013**, *6*, 197–226. [CrossRef]
10. Kumar, A.; Narendra, N.C.; Bellur, U. Uploading and replicating internet of things (IoT) data on distributed cloud storage. In Proceedings of the 2016 IEEE 9th International Conference on Cloud Computing, CLOUD, San Francisco, CA, USA, 27 June–2 July 2017; pp. 670–677.
11. Riahi Sfar, A.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. *Digit. Commun. Netw.* **2018**, *4*, 118–137, doi:10.1016/j.dcan.2017.04.003. [CrossRef]
12. Kim, D.; Choi, J.Y.; Hong, J.E. Evaluating energy efficiency of Internet of Things software architecture based on reusable software components. *Int. J. Distrib. Sens. Netw.* **2017**, *13*. doi:10.1177/1550147716682738. [CrossRef]
13. Russell, B.; Lingenfelter, D.; Abhiraj, K.S.; Manfredi, A.; Anderson, G.; Mordeno, A.; Bell, M.; Mukherjee, V.; Bhat, G.; Naslund, M.; et al. *Security Guidance for Early Adopters of the Internet of Things (IoT)*; Technical Report; Cloud Security Alliance Publishing: Seattle, WA, USA, April 2015.
14. Perera, C.; McCormick, C.; Nuseibeh, B. Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms. In Proceedings of the IoT'16, Stuttgart, Germany, 7–9 November 2016.
15. Broadband Internet Technical Advisory Group. *Internet of Things (IoT) Security and Privacy Recommendations: A Uniform Agreement Report*; Technical Report; Broadband Internet Technical Advisory Group: November 2016. Available online: https://www.bitag.org/documents/ (accessed on 29 March 2019).
16. OWASP. IoT Security Guidance. Available online: https://www.owasp.org/index.php/IoT_Security_Guidance (accessed on 29 March 2019).
17. ENISA. *Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures*; Technical Report; ENISA: November 2017, Available online: https://doi.org/10.2824/03228 (accessed on 29 March 2019).
18. Australia, I.A. Internet of Things Security Guideline. Available online: https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf (accessed on 29 March 2019).
19. IoT Security Foundation. IoT Security Compliance Framework. IoT Security Foundation: Best Practice User. 2017. Available online: https://www.iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf (accessed on 29 March 2019).
20. Trusted Computing Group. TPM Main Specification. 2011. Available online: https://trustedcomputinggroup.org/resource/tpm-main-specification/ (accessed on 29 March 2019).
21. Abdul-Ghani, H.A.; Konstantas, D. A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective. *J. Sens. Actuator Netw.* **2019**, *8*, 38. doi:10.3390/jsan8020022. [CrossRef]
22. SeeUnity. The Main Differences between the DPD and the GDPR and How to Address Those Moving Forward. 2017. Available online: https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf (accessed on 29 March 2019).
23. Chiarelli, D. *The Convergence of GDPR, the HIPAA Security Rule, and Part 11 on US Clinical Research*; Technical Report; Kinetiq: 2018. Available online: https://www.clinicalleader.com/doc/the-convergence-of-gdpr-the-hipaa-security-rule-and-part-on-us-clinical-research-0001 (accessed on 29 March 2019).
24. Ahmed, A.; Latif, R.; Latif, S.; Abbas, H.; Khan, F.A. Malicious insiders attack in IoT based Multi-Cloud e-Healthcare environment: A Systematic Literature Review. *Multimed. Tools Appl.* **2018**, *77*, 21947–21965. doi:10.1007/s11042-017-5540-x. [CrossRef]
25. Securitymetrics. *An Introduction to HIPAA Compliance*; Technical Report; Securitymetrics: Orem, UT, USA, 2013.
26. Industrial Internet Consortium. *The Industrial Internet of Things Volume G1: Reference Architecture IIRA*; Industrial Internet Consortium: Needham, MA, USA, 2017.

27. Zhang, M.; Raghunathan, A.; Jha, N.K. Trustworthiness of medical devices and body area networks. *Proc. IEEE* **2014**, *102*, 1174–1188. [CrossRef]
28. Li, C.; Raghunathan, A.; Jha, N. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In Proceedings of the 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2011, Columbia, MO, USA, 13–15 June 2011; pp. 150–156.
29. Cherdantseva, Y.; Hilton, J. A reference model of information assurance & security. In Proceedings of the 2013 International Conference on Availability, Reliability and Security, ARES 2013, Regensburg, Germany, 2–6 September 2013; pp. 546–555. doi:10.1109/ARES.2013.72. [CrossRef]
30. Aleisa, N.; Renaud, K. Privacy of the Internet of Things: A Systematic Literature Review. *arXiv* **2017**, arXiv:1611.03340. doi:10.24251/HICSS.2017.717.
31. Yu, S.; Guo, S. *Big Data Concepts, Theories, and Applications*; Springer International Publishing: Cham, Switzerland, 2016; pp. 1–437. doi:10.1007/978-3-319-27763-9.
32. Grobauer, B.; Walloschek, T.; Stöcker, E. Understanding cloud computing vulnerabilities. *IEEE Secur. Privacy* **2011**, *9*, 50–57. doi:10.1109/MSP.2010.115. [CrossRef]
33. OWASP. *The Ten Most Critical Web Application Security Risks*; Technical Report; OWASP: 2010. Available online: https://www.hkcert.org/my_url/en/guideline/18061501 (accessed on 29 March 2019).
34. Harnik, D.; Pinkas, B.; Shulman-Peleg, A. Side Channels in Cloud Services: Deduplication in Cloud Storage. *IEEE Secur. Privacy Mag.* **2010**, *8*, 40–47. doi:10.1109/MSP.2010.187. [CrossRef]
35. Masdari, M.; Jalali, M. A survey and taxonomy of DoS attacks in cloud computing. *Secur. Commun. Netw.* **2016**, *9*, 3724–3751. doi:10.1002/sec.1539. [CrossRef]
36. IBM-Security. *2016 Cyber Security Intelligence Index*; Technical Report; IBM: 2016. Available online: https://sloangroups.mit.edu/secmat/blog/ibm-x-force (accessed on 29 March 2019).
37. EY. *Managing Insider Threat a Holistic Approach to Dealing with Risk from Within*; Technical Report; EY: 2015. Available online: https://www.ey.com/Publication/vwLUAssets/EY-managing-insider-threat-june-13-2016/ (accessed on 29 March 2019).
38. Kaaniche, N.; Laurent, M. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. *Comput. Commun.* **2017**, *111*, 120–141. doi:10.1016/j.comcom.2017.07.006. [CrossRef]
39. Kaaniche, N. Cloud Data Storage Security Based on Cryptographic Mechanisms. Ph.D. Thesis, Institut National des Télécommunications, 2014. Available online: https://tel.archives-ouvertes.fr/tel-01146029/document (accessed on 29 March 2019).
40. Rittinghouse, J.; Ransome, J. *Cloud Computing Implementation, Management, and Security*; CRC Press: Boca Raton, FL, USA, 2010; p. 340.
41. Stevens, M.; Lenstra, A.; de Weger, B. Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 1–22. doi:10.1007/978-3-540-72540-4_1.
42. Daum, M.; Lucks, S. Hash Collisions (The Poisoned Message Attack). In *Eurocrypt 2005 Rump Session*; 2005. Available online: http://ljk.imag.fr/membres/Jean-Guillaume.Dumas/Enseignements/ProjetsCrypto/MD5-Collisions/ (accessed on 29 March 2019).
43. Rashid, F.; Miri, A.; Woungang, I. A secure data deduplication framework for cloud environments. In Proceedings of the 2012 Tenth Annual International Conference on Privacy, Security and Trust, Paris, France, 16–18 July 2012; pp. 81–87. doi:10.1109/PST.2012.6297923. [CrossRef]
44. Yan, Z.; Wang, M.; Li, Y.; Vasilakos, A.V. Encrypted Data Management with Deduplication in Cloud Computing. *IEEE Cloud Comput.* **2016**, *3*, 28–35. doi:10.1109/MCC.2016.29. [CrossRef]
45. Puzio, P.; Molva, R.; Onen, M.; Loureiro, S. ClouDedup: Secure Deduplication with Encrypted Data for Cloud Storage. In Proceedings of the 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, Bristol, UK, 2–5 December 2013; pp. 363–370. doi:10.1109/CloudCom.2013.54. [CrossRef]
46. Xu, J.; Chang, E.C.; Zhou, J. Weak leakage-resilient client-side deduplication of encrypted data in cloud storage. In Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security—ASIA CCS '13, Hangzhou, China, 8–10 May 2013; ACM Press: New York, NY, USA, 2013; p. 195. doi:10.1145/2484313.2484340. [CrossRef]
47. Shin, Y.; Koo, D.; Hur, J. A Survey of Secure Data Deduplication Schemes for Cloud Storage Systems. *ACM Comput. Surv.* **2017**, *49*, 1–38. doi:10.1145/3017428. [CrossRef]

48. Jiang, H.; Shen, F.; Chen, S.; Li, K.C.; Jeong, Y.S. A secure and scalable storage system for aggregate data in IoT. *Future Gener. Comput. Syst.* **2015**, *49*, 133–141. [CrossRef]
49. Kumar, A.; Lee, B.G.; Lee, H.; Kumari, A. Secure storage and access of data in cloud computing. In Proceedings of the 2012 International Conference on ICT Convergence (ICTC), Jeju Island, Korea, 15–17 October 2012; pp. 336–339. doi:10.1109/ICTC.2012.6386854. [CrossRef]
50. Bokefode, J.D.; Bhise, A.S.; Satarkar, P.A.; Modani, D.G. Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption. *Procedia Comput. Sci.* **2016**, *889*, 43–50. [CrossRef]
51. Fu, J.S.; Liu, Y.; Chao, H.C.; Bhargava, B.K.; Zhang, Z.J. Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4519–4528. doi:10.1109/TII.2018.2793350. [CrossRef]
52. Fu, Z.; Cao, X.; Wang, J.; Sun, X. Secure storage of data in cloud computing. In Proceedings of the 2014 10th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2014, Kitakyushu, Japan, 27–29 August 2014; pp. 783–786. doi:10.1109/IIH-MSP.2014.199. [CrossRef]
53. Rao, B.T.; Vurukonda, N. A study on data storage security issues in cloud computing. *Procedia Comput. Sci.* **2016**, *92*, 128–135.
54. Liu, H.; Wang, H.; Chen, Y. Ensuring data storage security against frequency-based attacks in wireless networks. In *Distributed Computing in Sensor Systems*, Springer: Berlin/Heidelberg, Germany, 2010; Volume LNCS 6131, pp. 201–215. doi:10.1007/978-3-642-13651-1_15. [CrossRef]
55. Storer, M.W.; Greenan, K.M.; Miller, E.L.; Voruganti, K. POTSHARDS: Secure Long-Term Storage Without Encryption. In Proceedings of the 2007 USENIX Annual Technical Conference, Santa Clara, CA, USA, 17–22 June 2007; pp. 143–156.
56. Jayant, D.B.; Swapnaja, A.U.; Sulabha, S.A.; Dattatray, G.M. Analysis of DAC MAC RBAC Access Control based Models for Security. *Int. J. Comput. Appl.* **2014**, *104*, 6–13. doi:10.5120/18196-9115. [CrossRef]
57. Wang, J.K.; Jia, X. Data security and authentication in hybrid cloud computing model. In Proceedings of the 2012 IEEE Global High Tech Congress on Electronics, Shenzhen, China, 18–20 November 2012.
58. Sandhu, R.; Coyne, E.; Feinstein, H.; Youman, C. Role-based access control models. *Computer* **1996**, *29*, 38–47. [CrossRef]
59. Sandhu, R.; Bhamidipati, V. The ASCAA principles for next-generation role-based access control. In Proceedings of the ARES 2008—3rd International Conference on Availability, Security, and Reliability, Barcelona, Spain, 4–7 March 2008. doi:10.1109/ARES.2008.211.
60. Xiao, M.; Zhou, J.; Liu, X.; Jiang, M. A hybrid scheme for fine-grained search and access authorization in fog computing environment. *Sensors* **2017**, *17*, 1423. [CrossRef] [PubMed]
61. Zuo, C.; Shao, J.; Wei, G.; Xie, M.; Ji, M. CCA-secure ABE with outsourced decryption for fog computing. *Future Gener. Comput. Syst.* **2016**, *78*, 730–738. doi:10.1016/j.future.2016.10.028. [CrossRef]
62. Jiang, Y.; Susilo, W.; Mu, Y.; Guo, F. Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 720–729. [CrossRef]
63. Yu, Z.; Au, M.H.; Xu, Q.; Yang, R.; Han, J. Towards leakage-resilient fine-grained access control in fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 763–777. [CrossRef]
64. Abdelwahab, S.; Hamdaoui, B.; Guizani, M.; Znati, T. Replisom: Disciplined Tiny Memory Replication for Massive IoT Devices in LTE Edge Cloud. *IEEE Internet Things J.* **2016**, *3*, 327–338. doi:10.1109/JIOT.2015.2497263. [CrossRef]
65. Al-Arnaout, Z.; Fu, Q.; Frean, M. A divide-and-conquer approach for content replication in WMNs. *Comput. Netw.* **2013**, *57*, 3914–3928. doi:10.1016/j.comnet.2013.09.016. [CrossRef]
66. Al-Arnaout, Z.; Fu, Q.; Frean, M. Exploiting graph partitioning for hierarchical replica placement in WMNs. In Proceedings of the 16th ACM International Conference on Modeling, Analysis & Simulation of Wireless and Mobile Systems—MSWiM '13, Barcelona, Spain, 3–8 November 2013; ACM Press: New York, NY, USA, 2013; pp. 5–14. doi:10.1145/2507924.2507928. [CrossRef]
67. Zhang, Q.; Zhang, S.Q.; Leon-Garcia, A.; Boutaba, R. Aurora: Adaptive Block Replication in Distributed File Systems. In Proceedings of the 2015 IEEE 35th International Conference on Distributed Computing Systems, Columbus, OH, USA, 29 June–2 July 2015; pp. 442–451. doi:10.1109/ICDCS.2015.52. [CrossRef]
68. Liu, W.; Fang, B.; Yin, L.; Yu, X. A tree based location privacy approach against multi-precision continuous attacks in the internet of things. *J. Inf. Comput. Sci.* **2012**, *9*, 1807–1819.

69. Xu, Y.; Qin, X.; Yang, Z.; Yang, Y.; Huang, C. An algorithm of k-anonymity for data releasing based on fine-grained generalization. *J. Inf. Comput. Sci.* **2012**, *9*, 3071–3080.
70. Machanavajjhala, A.; Kifer, D.; Gehrke, J.; Venkitasubramaniam, M. Diversity: Privacy Beyond k-Anonymity. *ACM Trans. Knowl. Discov. Data* **2007**, *9*, 3071–3080. [CrossRef]
71. Li, N.; Li, T.; Venkatasubramanian, S. t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. In Proceedings of the 2007 IEEE 23rd International Conference on Data Engineering, Istanbul, Turkey, 11–15 April 2007; pp. 106–115. doi:10.1109/ICDE.2007.367856. [CrossRef]
72. Rebollo-Monedero, D.; Forné, J.; Domingo-Ferrer, J. From t-Closeness-like privacy to postrandomization via information theory. *IEEE Trans. Knowl. Data Eng.* **2010**, *22*, 1623–1636. [CrossRef]
73. Narendra, N.C.; Nayak, S.; Shukla, A. Managing large-scale transient data in IoT systems. In Proceedings of the 2018 10th International Conference on Communication Systems and Networks, COMSNETS 2018, Bengaluru, India, 3–7 January 2018; Volume 2018, pp. 565–568. doi:10.1109/COMSNETS.2018.8328274. [CrossRef]
74. Cecchinel, C.; Jimenez, M.; Mosser, S.; Riveill, M. An Architecture to Support the Collection of Big Data in the Internet of Things. In Proceedings of the 2014 IEEE World Congress on Services, Anchorage, AK, USA, 27 June–2 July 2014; pp. 442–449. doi:10.1109/SERVICES.2014.83. [CrossRef]
75. Fazio, M.; Puliafito, A.; Villari, M. IoT4S: A new architecture to exploit sensing capabilities in smart cities. *Int. J. Web Grid Serv.* **2014**, *10*, 114. doi:10.1504/IJWGS.2014.060255. [CrossRef]
76. Narendra, N.C.; Koorapati, K.; Ujja, V. Towards Cloud-Based Decentralized Storage for Internet of Things Data. In Proceedings of the 2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, India, 25–27 November 2015; pp. 160–168. doi:10.1109/CCEM.2015.9. [CrossRef]
77. Gentry, C. Fully homomorphic encryption using ideal lattices. In Proceedings of the 41st Annual ACM Symposium on Symposium on Theory of Computing—STOC '09, Bethesda, MD, USA, USA, 31 May–2 June 2009; p. 169. doi:10.1145/1536414.1536440. [CrossRef]
78. Curtmola, R.; Garay, J.; Kamara, S.; Ostrovsky, R. Searchable symmetric encryption: Improved definitions. *J. Comput. Secur.* **2011**, *19*, 895–934. doi:10.3233/JCS-2011-0426. [CrossRef]
79. Wang, P.; Wang, H.; Pieprzyk, J. Threshold Privacy Preserving Keyword Searches. In *SOFSEM 2008: Theory and Practice of Computer Science*; Springer: Berlin/Heidelberg, Germany, 2008. doi:10.1007/978-3-540-77566-9_56.
80. Wang, P.; Wang, H.; Pieprzyk, J. An efficient scheme of common secure indices for conjunctive keyword-based retrieval on encrypted data. In *Information Security Applications*; Springer: Berlin/Heidelberg, Germany, 2009; Volume LNCS 5379, pp. 145–159. doi:10.1007/978-3-642-00306-6_11.
81. Yang, Y.; Lu, H.; Weng, J. Multi-User Private Keyword Search for Cloud Computing. In Proceedings of the 2011 IEEE Third International Conference on Cloud Computing Technology and Science, Athens, Greece, 29 November–1 December 2011.
82. Cheung, L.; Newport, C. Provably secure ciphertext policy ABE. In Proceedings of the 14th ACM Conference on Computer and Communications Security—CCS '07, Alexandria, VA, USA, 29 October–2 November 2007; ACM Press: New York, NY, USA, 2007.
83. Sun, W.; Yu, S.; Lou, W.; Hou, Y.T.; Li, H. Protecting Your Right: Verifiable Attribute-Based Keyword Search with Fine-Grained Owner-Enforced Search Authorization in the Cloud. *IEEE Trans. Parallel Distrib. Syst.* **2016**, *27*, 1187–1198. [CrossRef]
84. Sun, W.H.; Yu, S.C.; Lou, W.J.; Hou, Y.T.; Li, H. Protecting Your Right: Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud. In Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 226–234.
85. Shu, J.; Shen, Z.; Xue, W. Shield: A stackable secure storage system for file sharing in public storage. *J. Parallel Distrib. Comput.* **2014**, *74*, 2872–2883. doi:10.1016/j.jpdc.2014.06.003. [CrossRef]
86. Ambade, A.D.; Pansare, J.R. Securing Data Storage System for Internet of Things Using Key Aggregate Cryptosystem. *Int. J. Sci. Eng. Res.* **2017**, *8*, 31.
87. Adluru, P.; Datla, S.S.; Zhang, X. Hadoop eco system for big data security and privacy. In Proceedings of the 2015 Long Island Systems, Applications and Technology, Farmingdale, NY, USA, 1 May 2015; pp. 1–6. doi:10.1109/LISAT.2015.7160211. [CrossRef]

88. Saraladevi, B.; Pazhaniraja, N.; Paul, P.V.; Basha, M.S.; Dhavachelvan, P. Big Data and Hadoop-a Study in Security Perspective. *Procedia Comput. Sci.* **2015**, *50*, 596–601. doi:10.1016/J.PROCS.2015.04.091. [CrossRef]
89. Huang, Z.; Su, X.; Zhang, Y.; Shi, C.; Zhang, H.; Xie, L. A decentralized solution for IoT data trusted exchange based-on blockchain. In Proceedings of the 2017 3rd IEEE International Conference on Computer and Communications, ICCC 2017, Chengdu, China, 13–16 December 2017; doi:10.1109/CompComm.2017.8322729.
90. Shafagh, H.; Burkhalter, L.; Hithnawi, A.; Duquennoy, S. Towards Blockchain-based Auditable Storage and Sharing of IoT Data. In Proceedings of the 2017 on Cloud Computing Security Workshop, Dallas, TX, USA, 3 November 2017; pp. 45–50.
91. Xu, Q.; Aung, K.M.M.; Zhu, Y.; Yong, K.L. A Blockchain-Based Storage System for Data Analytics in the Internet of Things. **2018**, *715*, 119–138.
92. Gholami, A.; Laure, E. Big Data Security and Privacy Issues in the CLOUD. *Int. J. Netw. Secur. Its Appl.* **2016**, *8*, 59–79. doi:10.5121/ijnsa.2016.8104. [CrossRef]
93. Anand, M. Cloud Monitor: Monitoring Applications in Cloud. In Proceedings of the 2012 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, India, 11–12 October 2012; pp. 1–4. doi:10.1109/CCEM.2012.6354603. [CrossRef]
94. Brinkmann, A.; Fiehe, C.; Litvina, A.; Luck, I.; Nagel, L.; Narayanan, K.; Ostermair, F.; Thronicke, W. Scalable Monitoring System for Clouds. In Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing, Dresden, Germany, 9–12 December 2013; pp. 351–356.
95. Nikolai, J.; Wang, Y. Hypervisor-based cloud intrusion detection system. In Proceedings of the 2014 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 3–6 February 2014; pp. 989–993. doi:10.1109/ICCNC.2014.6785472. [CrossRef]
96. Marchal, S.; Jiang, X.; State, R.; Engel, T. A Big Data Architecture for Large Scale Security Monitoring. In Proceedings of the 2014 IEEE International Congress on Big Data, Washington, DC, USA, 27–30 October 2014; pp. 56–63. doi:10.1109/BigData.Congress.2014.18. [CrossRef]
97. Liu, C.; Ranjan, R.; Yang, C.; Zhang, X.; Wang, L.; Chen, J. MuR-DPA: Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud. *IEEE Trans. Comput.* **2015**, *64*, 2609–2622. doi:10.1109/TC.2014.2375190. [CrossRef]
98. Alliance, A.S.C. Embedded Hardware Security for IoT Applications. A Smart Card Alliance Internet of Things Security Council White Paper. 2017. Available online: https://hospitalitytech.com/smart-card-alliance-whitepaper-securing-internet-things (accessed on 4 April 2019).
99. Sushma, M.; Jaidhar, C.D.; Gudisagar, C.; Sahoo, B.R. Secure data migration between cloud storage systems. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017, Manipal, Karnataka, India, 13–16 September 2017; pp. 2208–2212. doi:10.1109/ICACCI.2017.8126173. [CrossRef]
100. Shen, Q.; Zhang, L.; Yang, X.; Yang, Y.; Wu, Z.; Zhang, Y. SecDM: Securing Data Migration between Cloud Storage Systems. In Proceedings of the 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, Sydney, Australia, 12–14 December 2011; pp. 636–641.
101. Dhamija, A.; Dhaka, V. A novel cryptographic and steganographic approach for secure cloud data migration. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, Delhi, India, 8–10 October 2015; pp. 346–351.
102. Khalil, I.; Hababeh, I.; Khreishah, A. Secure inter cloud data migration. In Proceedings of the 2016 7th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 5–7 April 2016; pp. 62–67.
103. Manikandasaran, S.S.; Raja, S. Security Architecture for multi-Tenant Cloud Migration. *Int. J. Future Comput. Commun.* **2018**, *7*, 42–45. doi:10.18178/ijfcc.2018.7.2.518. [CrossRef]
104. Kumbhare, A.G.; Simmhan, Y.; Prasanna, P. Designing a Secure Storage Repository for Sharing Scientific Datasets using Public Clouds. In Proceedings of the DataCloud-SC '11 Proceedings of the Second International Workshop on Data Intensive Computing in the Clouds, Seattle, WA, USA, 14 November 2011; pp. 31–40.
105. European Parliament and Council of the European Union. General Data Protection Regulation (GDPR)—Final Text Neatly lArranged. Available online: https://gdpr-info.eu/ (accessed on 4 April 2019).

106. Spiekermann, S.; Cranor, L.F. Engineering privacy. *IEEE Trans. Softw. Eng.* **2009**, *35*, 67–82. doi:10.1109/TSE.2008.88. [CrossRef]
107. Hoepman, J.H. Privacy Design Strategies. Avilable online: https://link.springer.com/chapter/10.1007/ (accessed on 4 April 2019).
108. OWASP_Foundation. *Security by Design Principles*; OWASP: Los Angeles, CA, USA, 2016.
109. Kotzanikolaou, P. Data retention and privacy in electronic communications. *IEEE Secur. Privacy* **2008**, *6*, 46–52. doi:10.1109/MSP.2008.114. [CrossRef]
110. Xu, Z.; Martin, K.; Kotnik, C.L. A Survey of Security Services and Techniques in Distributed Storage Systems. Technical Report; The Steering Committee of The World Congress in Computer Science, Computer˜.... 2010. Available online: https://pdfs.semanticscholar.org/eb63/3dd51c5ef339dfba3030df1526d9f9039b63.pdf (accessed on 4 April 2019).
111. PICDSS. *Requirements and Security Assessment Procedures Document Changes*; Technical Report; PCI Security Standards Council: Wakefield, MA, USA, 2016.
112. Beynon-Dames, P. Database and expert systems applications. *Eng. Appl. Artif. Intell.* **1996**, *9*, 575. doi:10.1016/0952-1976(96)84165-0. [CrossRef]
113. Ma, Y.; Guo, Y.; Tian, X.; Ghanem, M. Distributed Clustering-Based Aggregation Algorithm for Spatial Correlated Sensor Networks. *IEEE Sens. J.* **2011**, *11*, 641–648. doi:10.1109/JSEN.2010.2056916. [CrossRef]
114. Lindsey, S.; Raghavendra, C.; Sivalingam, K.M. Data gathering algorithms in sensor networks using energy metrics [PEGASIS]. *IEEE Trans. Parallel Distrib. Syst.* **2002**, *13*, 924–935. [CrossRef]
115. Danezis, G.; Domingo-Ferrer, J.; Hansen, M.; Hoepman, J.H.; Le Métayer, D.; Tirtea, R.; Schiffner, S. Privacy and Data Protection by Design—From Policy to Engineering. ENISA: 2015. Available online: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (accessed on 4 April 2019).
116. Vanitha, M.; Kavitha, C. Secured data destruction in cloud based multi-tenant database architecture. In Proceedings of the 2014 International Conference on Computer Communication and Informatics: Ushering in Technologies of Tomorrow, Today, ICCCI 2014, Coimbatore, India, 3–5 January 2014; pp. 1–6. doi:10.1109/ICCCI.2014.6921774. [CrossRef]
117. Han, J.; Pei, J.; Kamber, M. Data Mining: Concepts and Techniques. Available online: https://www.sciencedirect.com/book/9780123814791/data-mining-concepts-and-techniques (accessed on 4 April 2019).
118. Azzedin, F.; Ghaleb, M. Internet-of-Things and Information Fusion: Trust Perspective Survey. *Sensors* **2019**, *19*, 1929. [CrossRef] [PubMed]
119. Weingart, S.H. Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses. In *Cryptographic Hardware and Embedded Systems—CHES 2000*; Springer: Berlin/Heidelberg, Germany, 2000; pp. 302–317. doi:10.1007/3-540-44499-8_24.
120. Terzi, D.S.; Terzi, R.; Sagiroglu, S. A survey on security and privacy issues in big data. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 202–207. doi:10.1109/ICITST.2015.7412089. [CrossRef]
121. Luan, T.H.; Cai, L.X.; Chen, J.; Shen, X.S.; Bai, F. Engineering a distributed infrastructure for large-scale cost-effective content dissemination over urban vehicular networks. *IEEE Trans. Veh. Technol.* **2014**, *63*, 1419–1435. doi:10.1109/TVT.2013.2251924. [CrossRef]
122. Department of Homeland Security (DHS). *Strategic Principles for Securing the IoT (version 1.0)*; Technical Report; U.S. Department of Homeland Security: Washington, DC, USA, 2016.
123. Cloud Standards Customer Council. Security for Cloud Computing 10 Steps to Ensure Success. Cloud Standards Customer Council: Needham, MA, USA, 2015.
124. Mungole, A.J.; Dhore, M.P. Techniques of Data Migration in Cloud Computing. *IEEE Access* **2016**, *36*, 36–38.
125. Kushwah, V.S. A Security approach for Data Migration in Cloud Computing. *Int. J. Sci. Res. Publ.* **2013**, *3*, 1–8.
126. Kumar, P.R.; Raj, P.H.; Jelciana, P. Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Comput. Sci.* **2018**, *125*, 691–697. doi:10.1016/j.procs.2017.12.089. [CrossRef]
127. Claycomb, W.R.; Nicoll, A. Insider threats to cloud computing: Directions for new research challenges. In Proceedings of the International Computer Software and Applications Conference, Izmir, Turkey, 16–20 July 2012; pp. 387–394. doi:10.1109/COMPSAC.2012.113. [CrossRef]
128. Sallam, A.; Bertino, E.; Hussain, S.R.; Landers, D.; Lefler, R.M.; Steiner, D. DBSAFE—An Anomaly Detection System to Protect Databases From Exfiltration Attempts. *IEEE Syst. J.* **2017**, *11*, 483–493. [CrossRef]

129. Federal Trade Commission. IoT Privacy & Security in a Connected World; Technical Report. Available online: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (accessed on 4 April 2019).
130. Shan, C.; Heng, C.; Xianjun, Z. Inter-cloud operations via NGSON. *IEEE Commun. Mag.* **2012**, *50*, 82–89. [CrossRef]
131. Sotiriadis, S.; Bessis, N.; Petrakis, E.G.M. An inter-cloud architecture for future internet infrastructures. In *Adaptive Resource Management and Scheduling for Cloud Computing*; Springer: Cham, Switzerland, 2014; Volume 8907, pp. 206–216.
132. Borylo, P. Intercloud: Solving Interoperability and Communication in a Cloud of Clouds (Frahim, J., et al; 2016) [Book Review]. *IEEE Commun. Mag.* **2017**, *55*, 6. doi:10.1109/mcom.2017.7876847. [CrossRef]
133. Cisco. The Internet of Things Reference Model. In Proceedings of the Internet of Things World Forum, Chicago, IL, USA, 14–16 October 2014; pp. 1–12.
134. Venčkauskas, A.; Morkevicius, N.; Bagdonas, K.; Damaševičius, R.; Maskeliūnas, R. A lightweight protocol for secure video streaming. *Sensors* **2018**, *18*, 1554. doi:10.3390/s18051554. [CrossRef] [PubMed]