IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 10, 2020, accepted August 21, 2020, date of publication September 11, 2020, date of current version September 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3023659

Privacy-Preserving Identifiers for IoT: A Systematic Literature Review

MAHDI AKIL[1], LEJLA ISLAMI[1], SIMONE FISCHER-HÜBNER[1], (Member, IEEE), LEONARDO A. MARTUCCI[1], AND ALBIN ZUCCATO[2]

[1]Computer Science Department, Karlstad University, 65188 Karlstad, Sweden
[2]ICA Gruppen AB, 17193 Solna, Sweden

Corresponding authors: Mahdi Akil (mahdi.akil@kau.se) and Lejla Islami (lejla.islamil@kau.se)

This work was supported by the Swedish Foundation for Strategic Research (SSF) Secure and Private Connectivity in Smart Environments (SURPRISE) Project.

ABSTRACT The Internet of Things (IoT) paves the way for smart applications such as in E-health, E-homes, transportation, or energy production. However, IoT technologies also pose privacy challenges for their users, as they allow the tracking and monitoring of the users' behavior and context. The EU General Data Protection Regulation (GDPR) mandates data controller to follow a data protection by design and default approach by implementing for instance pseudonymity for achieving data minimisation. This paper provides a systematic literature review for answering the question of what types of privacy-preserving identifiers are proposed by the literature in IoT environments for implementing pseudonymity. It contributes with classifications and analyses of IoT environments for which privacy-preserving identifiers have been proposed and of the pseudonym types and underlying identity management architectures used. Moreover, it discusses trends and gaps in regard to addressing privacy trade-offs.

INDEX TERMS Privacy, identity, pseudonym, anonymous credential, the IoT, systematic literature review.

I. INTRODUCTION

The Internet of Things (IoT) as a pervasive technology is now entangled in everyday life, from ''smart'' vehicles that communicate with each other and vacuum cleaners that create blueprints of homes to watches that track calories burnt and light bulbs controlled over the Internet. Its pervasiveness also implies that all data that are produced or handled by IoT devices can be used to directly or indirectly draw conclusions on personal behaviour and preferences. While some may appreciate the benefits of those inferences as they may result in personalized services, others may have concerns about the consequences of the collection and use of their personal data. The EU General Data Protection Regulation (GDPR) [1] mandates that data controllers should enforce Data Protection by Design by implementing appropriate technical and organisational measures, such as pseudonymisation, for complying with data-protection principles, such as data minimisation, effectively.

In this survey based on a systematic literature review (SLR), we review the scientific literature on the use of privacy-preserving identifiers implementing pseudonymity in identity management (IdM) systems for IoT, which were published in the ten years period from 2009 to 2019. Digital identifiers, such as X.509 certificates, are used to uniquely identify users or IoT devices. In contrast to X.509 certificates, privacy-preserving identifiers are information containers used to identify or authorise a user and/or a device without necessarily revealing the identity or other personal details of the device holders. Privacy-preserving identifiers can implement pseudonyms and allow IoT services to request no more than the necessary information needed to authorise pseudonymous users and/or their personal devices. Thereby they can minimize the amount of personal data that is collected and processed in compliance with the GDPR. Hence, this SLR addresses the following research question:

> *What types of privacy-preserving identifiers are proposed for IoT environments?*

For answering this research question, we have analyzed the landscape of IoT application environments and investigated the types of privacy-preserving identifiers employed, as well as, how they are used for implementing pseudonymity and thus data minimization. The main contributions of this

The associate editor coordinating the review of this manuscript and approving it for publication was P. K. Gupta.

SLR are including answers for the aforementioned research question:

- A classification and analysis of the IoT application areas using privacy-preserving identifiers.
- A classification and analysis of the use of privacy-preserving identifiers in IoT in regard to:
  - their degree of linkability across contexts
  - the IdM architectures used for implementing them.
  - means for accountability and/or re-identification.
- An analysis and discussion of trends, gaps and possible future research directions.

The remainder of this paper is structured as follows: Section II presents the basic background information about pseudonyms, identity management architectures and types of identifiers. Section III describes the methodology used for our SLR. Section IV then presents the main results of the SLR in terms of the provided analyses and classifications, before Section V summarises and assesses results in terms of observations, trends, gaps as well as limitations and related work. Section VI finally provides the main conclusions.

II. BACKGROUND

This section provides a short overview of pseudonym types, identity management architectures and identifier types, on which the classifications provided in this paper will build upon.

A. PSEUDONYMS

Privacy-preserving identifiers are implemented by pseudonyms as a means for enforcing data minimisation. A pseudonym can be defined as an "*identifier of a subject, which is different from the subject's real name*" [2]. The subject is the pseudonym holder, which can e.g. be a user or her device. A pseudonym can be used to authorise its holder, without the need for revealing her identity, and even allow to implement anonymous transactions. Also, accountability can be realised with respect to a pseudonym, allowing to re-identify the pseudonym holder in case of misuse [2].

Pfitzmann and Hansen [2] have provided a classification of pseudonym types according to their degree of linkability due to the use of a pseudonym across different contexts. As the types of pseudonyms that may be distinguished by the kind of context of use, they list:

- A person pseudonym, which is a substitute for the holder's real name (e.g. nickname, artist name);
- A role pseudonym, which is used by the pseudonym holder while performing a certain role;
- A relationship pseudonym, which is used by the pseudonym holder for transactions in relation to a specific other subject;
- A role-relationship pseudonym, which is used by the pseudonym holder in a certain role for transactions in relation to a certain other subject;
- A transaction pseudonym, which is used for only one transaction and can thus be used for making a transaction unlinkable with any other transaction using different transaction pseudonyms.

The linkability across different contexts due to the (re-)use of these pseudonyms can be presented as a lattice, as illustrated in [2]. The degree of unlinkability of transactions, and thus the degree of protecting against profiling of a subject's activities, is increasing the less often a pseudonyms is re-used for different transactions, and thus the smaller the context is in which the pseudonym is used. Person pseudonyms are used for transactions in different contexts have the highest degree of linkabilty. Stronger unlinkability is provided by role pseudonyms and relationship pseudonyms, which are only used in the context of a specific role or relationship, and the degree of unlinkability is even increased by role-relationship pseudonyms which are used in the context of a specific role and a specific relationship. Finally transaction pseudonyms provide full unlinkability and thus anonymity of transactions.

Pseudonyms may refer to one holder during its life time or may be as "transferable pseudonyms" transferable from one holder to another one or may refer as a "group pseudonym" to several holders. In IoT environments, identifiers or pseudonyms can be either used for users or for IoT devices that can be related to a user or user group. In the latter case, they constitute group pseudonyms, which usually still raise privacy risks, especially if the user group is small (resulting in a small anonymity set size). In the remainder of this article, we will use the terms "privacy-preserving identifiers" and "pseudonyms" interchangeably.

B. IdM ARCHITECTURE

Identity management is the process related to the life cycle of identifiers: from their (*a*) issuing and use to their (*b*) expiration or revocation. In this literature review, we classify an IdM architecture according to the availability of its component parts in charge of issuing privacy-preserving identifiers. In the results of our survey, we treat revocation separately from issuing in terms of IdM architecture (Sections IV-D and IV-E). A privacy-preserving IdM architecture is an architecture for IdM that handles pseudonyms and it is classified as follows in this literature review:

- *Centralized*. In centralized IdM architectures, a (non-empty) set of trusted third parties issues pseudonyms to end devices and may also revoke them. As in public-key infrastructure architecture, it is usually assumed that all participants share a common list of trusted third parties (the Certification Authorities (CAs)) and their certificates. Hence, it is in general possible to verify the validity of an identifier without direct interaction with an online trusted third party. The presence of an online trusted third party or parties is required in centralized architectures mainly for the generation and revocation of user credentials. An IdM that requires a service to be available to issue and validate pseudonyms is an example of a centralized IdM architecture.
- *Decentralized*. In decentralized IdM architectures, a (non-empty) set of trusted third party issues token

wallets to end devices. End devices use their token wallets to generate tokens (pseudonyms) with no interaction with a trusted third party. The verification of the validity of a pseudonym is also performed without any interaction with a third trusted party. An IdM in which end devices can issue their own pseudonyms without the participation of a central authority is decentralized.[1]

- *Fully Decentralized*. In fully decentralized IdM architectures there are no trusted third parties. End devices generate their own pseudonyms. The lack of a trust anchor means that trust relationships are established either offline or following a past evidence of behavior. An example of a fully decentralized IdM architecture is the web of trust model used in PGP.

C. IDENTIFIER TYPES

A pseudonym in a computer system is often implemented as a digital identifier. Digital identifiers can be instanced as random values, public keys, certificates (signed public keys), or anonymous credentials (also called privacy-preserving attribute-based credentials or Privacy-ABCs).

An anonymous credential is a cryptographic construction that enables the holder to authenticate without revealing information that can lead back to its holder's identity. Anonymous credentials can be constructed with either blind signatures [3] or zero-knowledge proofs of knowledge [4]. In short, the main difference between the two techniques can be summarized in the problem that they solve. Blind signatures provide an answer to the question ''how can one (a signer) sign something without seeing it?'' while zero-knowledge proofs answer the question ''how to prove that one knows the answer to a problem without telling the answer?''.

The details around the implementation of an anonymous credential based solution determine the type of pseudonym it outputs and its properties. For instance, the identity mixer (idemix), a zero-knowledge proof anonymous credential system based on CL-signatures [5], can be instantiated in multiple ways to output different types of pseudonyms [6]–[8].

III. METHODOLOGY

The methodology used to conduct this literature research follows Kitchenham *et al.* guidelines [9]. Their approach is based on an initial database to perform the initial search and, from there the subsequent selections are derived. Our initial search was performed on the ACM and IEEE publication databases. Besides, we used Web of Science as our indexing reference. Table 1 lists the type and URL addresses of the aforementioned database. Abiding to the guidelines in [9] and recommendations from [10], all the phases of information retrieval and review process were carefully documented.

[1]Decentralized IdM architectures are sometimes referred to as hybrid because of the presence of a trusted third party in the bootstrapping of the token wallets.

TABLE 1. Selected databases.

Database	Type	URL
IEEE Xplore	Digital Library	https://ieeexplore.ieee.org/Xplore/
ACM Digital Library	Digital Library	https://dl.acm.org/
Web of Science	Bibliographic Database	https://apps.webofknowledge.com

A. FORMALIZING THE RESEARCH QUESTION

The prime focus of this paper is to shed light and get a better overview of what kind of privacy-preserving identifiers are proposed in the literature, what level of privacy they provide and which approaches they take as part of technical IdM solutions. To keep the research heavily directed, our research question was carefully defined as:

> *What types of privacy-preserving identifiers are proposed for IoT environments?*

We answer this research question with a structured literature survey following the guidelines proposed by Kitchenham and Brereton [9]. We conducted a rigorous search for high-quality peer-reviewed research articles published in well-reputed sources in a ten-year period. The search strictly revolved around the research question, and the following concepts were initially used in the review protocol phase; privacy, privacy-preserving identifiers, IoT environments. This strategy bases the initial search on publication databases on well-defined search terms instead of relying on pre-selected set of publications to start the reviewing process. Figure 1 depicts the research topic in this literature review targeting the intersection of the three sub topics: privacy, identity and IoT environments.

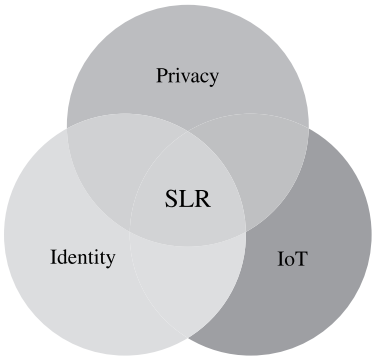


FIGURE 1. The scope of this SLR is in the intersection of privacy, identity and IoT.

B. SELECTION OF SOURCES

The databases should be selected based on the subject that they cover and the type of publications they index [11]. Hence, during the preparation phase, we selected publication databases and the respective search terms concerning the research question and the scope (Section III-A) Therefore, we started with two of the most digital libraries in the field that provide excellent coverage of the researched topic, which

together form an essential core of today's scientific research on electrical engineering and computing. ACM and IEEE are publishers and their search engines retrieve only publications released in their own journals, conference proceedings, etc. To expand our search scope, we included Web of Science, a bibliographical database that contains abstracts and citations from academic journal articles. These databases were chosen because they contain peer-reviewed articles, as well as, they enable the possibility of searching through logical expressions (keywords, titles, and/or abstracts). The selection of the defined databases listed in Table 1 influenced the retrieved publications towards the disciplines of computer science and information systems.

Each selected database was queried independently using the specified search terms and in the end, results were combined and duplicates were removed. Table 2 illustrates the number of publications yielded in each of the queried databases. Some of the retrieved publications appear in more than one database, hence the total number of publications without duplication is 617.

TABLE 2. Number of retrieved articles from each database (with duplications).

Database	IEEE Xplore	ACM Digital Library	Web of Science
# Hits	187	231	309

C. SEARCH STRING

During the querying phase, we used an automated search process for practical reasons [9]. The automated process allowed us to rely on well-picked search terms instead of a predefined set of publications, as the latter approach would not have been feasible due to authors' initial knowledge constraints related to the topic of interest. Therefore, we relied on the generic synonyms of the well-defined search terms to cover as many usage contexts as possible. The semantic equivalent search terms were identified from the areas of privacy, privacy-preserving identifiers, and IoT environments, which also define the areas where the retrieved publications should reside. Furthermore, all three database queries were limited only to the title, abstract, and subject terms of the papers. This was done on purpose to remove the irrelevant papers that mentioned the search terms only in the body text.

TABLE 3. Search string.

Search string	(privacy AND (identity OR identifier OR "identity management" OR idm OR certificate OR pseudonym OR "anonymous credential") AND ("internet of thing" OR iot OR "smart environment"))

The search string in Table 3 is slightly modified for each database. Therefore, search strings were adjusted (when needed) according to each database query syntax without altering the search space. More specifically, the "$" sign is not relevant in both IEEE and ACM since words are automatically stemmed there.

D. INCLUSION AND EXCLUSION CRITERIA

This section outlines the criteria that the retrieved publications went through in the initial search. In order to be included in the following screening phase, a publication has to comply with the following criteria:

- It must have gone through a peer-reviewed process. This criteria relates well with the selection of databases.
- Its publication date should be within the ten years period between 2009—2019.
- It has to describe or contain a proposal that includes privacy-preserving identifiers in IoT.
- It must be written in English.

E. SCREENING

During the primary selection, 727 articles were retrieved from the three databases. The majority of papers retrieved were conference proceedings or journal articles. The indicated number of the retrieved publications from each database shows that the search terms used for the queries were not too generic and did not catch many other disciplines apart from the researched field. At this stage, any duplicates retrieved from the databases were removed, and this aggregation resulted in 617 publications. Before conducting the initial screening process, all the retrieved publications were examined to check their correspondence with the research question and the quality criteria. Next, we read the titles, abstracts, and keywords of each publication to keep the ones relevant for the next screening phase [9]. In addition, we carefully checked whether they are within or outside the scope defined by the inclusion and exclusion criteria by reading other sections of the paper and in particular the abstract, conclusion, and discussion sections. As such, a small amount of the publications passed the primary screening phase due to several reasons. More precisely, the first article screening ended up with 109 articles discarding publications that had little relevance for our researched topic.

F. FINAL SELECTION

During the final screening process, we conducted a detail-oriented full-text reading of the remaining 109 articles and selected the 23 papers listed in Table 4. Table 5 shows the number of the selected publications from each database. The total number of the articles listed in Table 5 is more than 23 because most of the papers appeared in more than one of the databases. Figure 2 shows the distribution over the years of the selected publications, according to the publication date.

IV. RESULTS

After a brief overview of the privacy aspects addressed by the selected papers, this section provides an analysis and classification of the papers in terms of the IoT application environments in which pseudonyms are used as privacy-preserving identifiers (Section IV-B), the types of pseudonyms (Section IV-C), IdM architectures used for protecting privacy in IoT (Section IV-D), and how

TABLE 4. Retrieved results without duplication.

Year	Authors	Title (abbreviated)
2009	Armac et al. [12]	Privacy-Friendly smart environments
2012	Vinkovits et al. [13]	Anonymous networking meets real-world business req...
2013	Alcaide et al. [14]	Anonymous authentication for privacy-preserving IoT...
2013	Liang et al. [15]	EPS: An efficient and privacy-preserving service searching...
2015	Khemissa and Tandjaoui [16]	A lightweight authentication scheme for e-health applications...
2015	Neisse et al. [17]	An agent-based framework for informed consent in the...
2015	Skarmeta et al. [18]	A required security and privacy framework for smart objects
2015	Wang et al. [19]	2FLIP: A two-factor lightweight privacy-preserving auth....
2016	Alpár et al. [20]	New directions in IoT privacy using attribute-based auth...
2016	Kang et al. [21]	Location privacy attacks and defenses in cloud-enabled...
2016	Saxena et al. [22]	Authentication protocol for an IoT-enabled LTE network
2017	Bernabé et al. [23]	Holistic privacy-preserving identity management system for...
2017	Chowdhury et al. [24]	Holistic privacy-preserving identity management system...
2017	Shen et al. [25]	Privacy-preserving and lightweight key agreement protocol...
2017	Tunaru et al. [26]	Location-based pseudonyms for identity reinforcement in...
2017	Vijayakumar et al. [27]	Computationally efficient privacy preserving authentication...
2018	Kang et al. [28]	Privacy-preserved pseudonym scheme for fog computing...
2018	Sanchez et al. [29]	Integration of anonymous credential systems in IoT...
2018	Sanchez et al. [30]	Towards privacy preserving data provenance for the...
2019	Boussada et al. [31]	A lightweight privacy-preserving solution for IoT: the case...
2019	Li et al. [32]	Blockchain meets VANET: an architecture for identity and...
2019	Liu et al. [33]	Anonymous reputation system for IIOT-enabled retail...
2019	Zhu et al. [34]	Lightweight privacy preservation for securing large-scale...

TABLE 5. Number of selected publications from each database (with duplications).

Database	IEEE Xplore	ACM Digital Library	Web of Science
# Hits	16	3	20

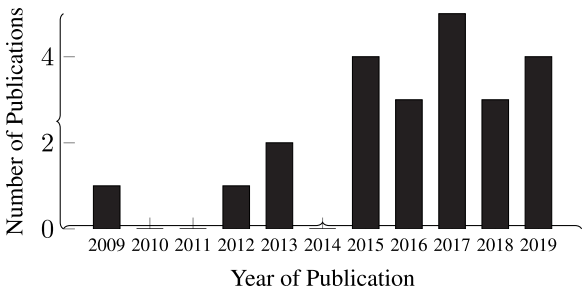


FIGURE 2. Number of selected publications according to the year of their publication.

is pseudonym revocation and re-identification handled (Section IV-E).

The publications reviewed in this SLR discuss different aspects of privacy in IoT and embrace a variety of privacy-enhancing IdM solutions. The publications included in this SLR use pseudonyms in privacy-preserving applications and services such as authentication, authorisation, access control, reputation systems, bandwidth sharing, location, and identity protection, and provenance.

A. CLASSIFICATION SCHEME

The classification in the context of this survey is viewed as a "formal system for classifying multifaceted, complex phenomena according to a set of common conceptual domains and dimensions" [35]. Abiding by the guidelines of Petersen *et al.* [36], the classification scheme proposed here is a topic-specific classification scheme and the elicitation of the categories have emerged from analysing the contents of the reviewed publications. Therefore, each of these categories represents a property that each article was scrutinised against thus, capturing a wide knowledge about a set of artifacts (i.e., the IdM architecture, or the IoT application domain).

In that regard, all the selected articles can be classified depending on their solution space in the three main aspects of application domains, types of pseudonyms to which they are devoted, and system architecture. For instance, these categories are oriented towards different types of application domains, hence the types of pseudonyms that have been proposed in the articles are also different. As a result, most of the elicited categories that are presented below relate to the principle of an extended taxonomy with other types of derived pseudonyms from those described in section II. The relation of the classified privacy-preserving identifiers to other categories on the classification scheme will be discussed in more details in the discussion section. Consequently, this classification scheme allows us to also identify aspects that were unspecified, or partially addressed by the selected articles, which will be depicted in the following sections.

B. APPLICATION DOMAIN

With the progression of IoT, its deployment is becoming part of smart grids, smart cities, smart transportation or smart medical services. Due to continuing advances in the underlying technologies, which are summarized as IoT, different applications of IoT are converting the world and our society into a smart(er) one. This is important as the combination

of technology and humans in an application area have an impact on the properties of technology. Expectation and privacy requirements are defined upon use cases derived from the application domains. Also the EU General Data Protection Directive (GDPR) [1] takes a risk-based approach and stipulates that (privacy) requirements have to be formulated based on the processing activity (i.e. the use case) and the inherent risks. Hence, we have to assume mutual impact of the application domain and privacy requirements and solutions.

We have therefore classified the articles into their application domains (see Figure 3) as we present and motivate in the subsections below. Please note that this overview provides an indication of in which IoT application areas privacy-preserving solutions based on pseudonyms have been proposed by the scientific literature in the last 10 years. However, we have not used the application areas, such as VANET, E-home or E-health, as terms as part of the search string for restricting the scope of this SLR to papers to our research question that focuses more generally on IoT (see also Section V). Therefore, the classification in this section and figure 3 may not reflect all scientific work that has been conducted in those application areas.

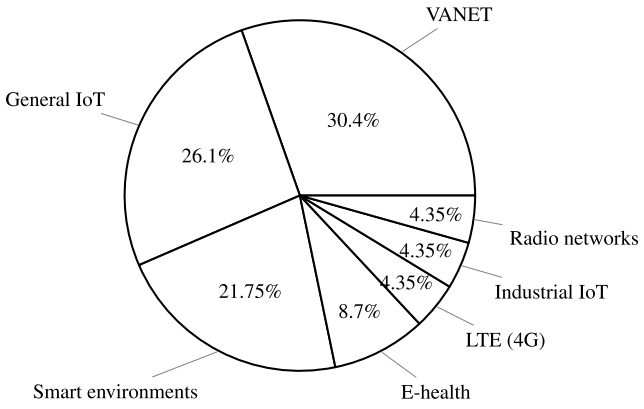


FIGURE 3. Application domain classification.

A noteworthy observation is that the application domains correlate well with the technological demands of the underlying concepts, meaning that if the presented solutions require some processing power, this has implications with respect to the use. IoT devices with low computation capabilities, like smart sensors, smart tags or similar, pose challenges for the development of advanced privacy-enhancing technical solutions due to the technical restrictions and have hardly been considered in the selected papers. Hence, application domains like logistics, retail or healthcare are hardly represented by the articles, even though we see from practice that those domains are currently heavily experimenting in projects and trials with IoT technology. VANETs (vehicular ad-hoc networks) and general IoT solutions, on the other hand, can have more powerful processing capabilities, and the articles in those domains are thus, as discussed below, involving more advanced technical privacy-preserving solutions that for instance involve anonymous credentials.

1) VANETs

A popular application domain in IoT is that of vehicular networks. A set of reviewed publications propose security and privacy improvements in VANETs [19], [21], [24], [25], [27], [28], [32]. Articles take different approaches to achieve authentication for vehicular networks while achieving different levels of privacy and unlinkability. [24] main focus is to address vehicle tracking by anonymizing vehicle names and the certificate issuing proxies to protect the real identity of the vehicle. Article [19], employs a decentralized certificate authority and depends on a two-factor authentication scheme to achieve conditional privacy. Both [19] & [27] depend on an efficient signature scheme based on bilinear pairings [37] to achieve their designed privacy goals and they employ a dynamic pseudo-identity that is utilized as time changes to preserve the identity of the vehicles. In [32] to solve the problems of centralization in the current VANET infrastructure, the authors design a blockchain-based architecture, by adopting a dynamic threshold encryption and k-anonymity unity (assuring that the number of vehicles at a certain measurable location is at least $k > 1$) to achieve identity and location privacy. Compared with different schemes, their solution is lightweight and enhances privacy-preservation and as well as achieves unlinkability. Two other articles [28] & [21] in this category shift the pseudonym management to the cloud (or fog) to overcome the vehicles' challenges of processing the massive information required for path planning, the internet of vehicles (IoV) is evolving into a cloud-enabled IoV [21] or fog-enabled IoV [28]. They tackle the identity and location privacy of vehicles by employing short-time context pseudonyms where vehicles change pseudonyms on context information. Vehicle to Grid communication in [25] is used to regulate interactions between electric vehicles (EVs) and the power grid to make better use of the energy storage capacity of EVs. The authors propose a lightweight key agreement authentication protocol that emphasizes strong privacy and security between EVs and smart grids implemented in the network.

2) SMART ENVIRONMENTS

Another application domain category that is considered in this survey is smart environments. In this category, we considered papers that deal with smart homes, smart buildings, smart cities, and more [12], [15], [17], [20], [29]. These are environments with versatile smart devices and objects integrated to bring convenience for the users while using them in their everyday life. As these environments continue to spread, new privacy and security challenges arise. In [12], the authors present E-home personalization and privacy protection services, enabling a user to select an identity and parts of personal data to disclose depending on the visited E-home. [15] propose a privacy-preserving service searching scheme that enables residents of a home to receive internet bandwidth from other cooperative nearby homes. It is worth mentioning that the majority of papers in this domain employ anonymous credentials that are mainly applied to preserve

users' privacy by minimizing the personal information disclosed and digital traces that are left while authenticating and transmitting various messages between users and devices or between devices themselves. We found that most of the proposed anonymous credential schemes are based on Idemix and thus use zero-knowledge proofs [38] for minimizing linkability and enabling selective disclosure of personal information [39]. For instance, in [12] the authors propose a system to disclose only necessary data to an E-home depending on the desired service. For that they created an identity management system where a user is provided with multiple unlinkable pseudonyms by a trusted CA and then the user can choose which pseudonym to disclose depending on the personal service required. Moreover, they give the user the option to generate her own pseudonym with specified attributes. Idemix is applied also in other articles where a user could prove to a verifier that she possesses some attributes without actually disclosing them and hence proving her identity while preserving her privacy. [12], [17], [20], [29].

3) E-HEALTH

Papers in this domain deal with E-health which is an important application of IoT that allows patients to be monitored remotely and enables medical intervention promptly [16], [31]. In [16] the authors propose an authentication scheme between the devices planted in the human body and the base station (mobile phone) in this situation. [31] introduces a novel crypto scheme called PKE-IBE that is based on the identity based cryptography, an asymmetric scheme that is used to eliminate the certificate management tasks [40]. Although this scheme encrypts and hides the user identity using elliptic curves and bilinear pairing [37], it provides high linkability as the same public key is used throughout the entire lifespan of the IoT device.

4) INDUSTRIAL IoT (IIoT)

IIoT consists of a global network of smart objects and it is expected to revolutionize the retail industry. IIoT is remodeling the retail industry for businesses, suppliers, and retailers to enhance operational efficiency and consumer experience. In IIoT-enabled retail marketing, reputation systems play a crucial part to boost mutual trust among industrial entities and build consumer confidence. Liu *et al.* [33] focus on reputation management in the consumer-retailer channel, where retailers can accumulate reputations from consumer feedbacks. To encourage consumers to post feedback without worrying about being tracked or retailed. They have developed an anonymous reputation system which provides privacy guarantees for consumers, and can be efficiently and securely integrated with a proof of stake blockchain retail systems.

5) 4G LONG TERM EVOLUTION (LTE) CELLULAR NETWORKS

LTE, a radio access technology, is the fourth generation (4G) cellular network. In comparison to 3G radio technologies, such as UMTS and CDMA2000, it offers higher resource capacity, lower cost at the customers' end, lower latency, and better quality of service and coverage. Deploying LTE in today's IoT settings and other large distributed systems, such as smart grid, transportation and telecommunication systems, is challenging as it requires managing a high volume of network traffic and providing different services to a large group of devices in a secure manner [22]. According to Saxena *et al.* [22] the authentication and key agreement protocol used in LTE networks doesn't support LTE-enabled IoT devices and this poses several security limitations and identity privacy problems. Therefore, they propose a new secure and efficient protocol that mitigates the object Id-theft, impersonation, man-in-the-middle attacks and more.

6) COGNITIVE RADIO NETWORKS

The database-driven cognitive radio networks are viewed as an approach to using limited spectrum resources in large-scale IoT. Zhu *et al.* [34] propose a lightweight privacy-preserving location verification protocol for cognitive radio networks in which users don't need to provide their real identity and location information to the database and therefore, preventing the database from misusing the information.

7) GENERAL IoT

This category of articles presents a unified privacy-preserving solutions that can be used in many IoT application domains, including some of the domains listed above [13], [14], [18], [23], [26], [30]. Papers demonstrate their framework applicability in multiple scenarios in IoT. A common aspect of these models, is that rather than being specific application-driven models, they represent versatile IoT use cases, able to be integrated in the IoT ecosystem. The most common IoT use case treated in these articles is the smart city scenario [14], [18], [30]. One paper shifts the attention on building an anonymous reputation system [13]. These particular approaches provide a general degree of scalability and flexibility suitable for different IoT scenarios with similar security and privacy requirements [23], [14]. The diversity of the various application domains stems most likely from the wide spectrum of IoT-enabled services. [30] & [13] used idemix but with a non-interactive zero-knowledge proofs protocol which according to [30] signs data in a privacy-preserving manner where a user is not required to interact with a verifier in order to prove the possession of the claimed attributes. This provides a high level of unlinkability by allowing users to generate their own pseudonyms depending on the situation where the degree of unlinkability between the generated pseudonyms depends on a lot of factors that will be discussed in section IV-C. Tunaru *et al.* [26] take a different approach by employing a fully decentralized architecture where IoT devices can generate their pseudonyms locally based on different parameters in relative to other neighboring devices in wireless ad hoc networks.

C. PSEUDONYMS IN IoT ENVIRONMENTS

As described by [2] and outlined in section II-A, pseudonyms can be classified according to the context in which they are used and/or according to whether and how they may be revoked, e.g., for providing accountability. In the following subsections, we classify the surveyed papers according to these categories.

1) CLASSIFICATION ACROSS CONTEXTS

The environment and thus the context of IoT devices and their users are typically dynamically changing, which also allows implementing more fine-grained context-dependent security and privacy policies. Therefore, in addition to contexts discussed in [2] of the person, the relationship, role-relationship, and a transaction, for which a pseudonym can be used, we found that pseudonyms in IoT applications have also been defined and used across other contexts in our surveyed papers. In particular, the context of a time periods, the current session and location of an IoT user / device, or a combination of those with other contexts, have been used for exchanging pseudonyms and thus reducing their linkability. This has led to the following additional pseudonym types used in IoT environments: device pseudonyms, short-term pseudonyms, session pseudonyms, and location-based pseudonyms.

Below, we provide an overview of the implementation of different pseudonym types across contexts that were used in our surveyed papers:

- **Personal:** A personal pseudonym may provide anonymity on its first use but after multiple uses, it can be easily linked to the real id and hence these pseudonyms provide the lowest level of unlinkability. Personal pseudonyms were only used in one lightweight protocol. [31] defines a cryptographic scheme (PKE-IBE) based on identity-based cryptography for protection communication in E-health systems, in which a user's public key is used as a person pseudonym.
- **Device:** Device pseudonyms, which are unique for each device, are also used for lightweight protocols for the authentication of IoT devices. Device pseudonyms are equal personal pseudonyms in case of personal device usage, or group pseudonyms if a device is used by several users. In the latter case, they are providing protection that is increasing with the number of device users. Still, if used over a longer time period, the degree of linkability and risk of re-identification of users is usually high. [16] defines an authentication scheme for E-health, in which a device pseudonym is a result of a hash function using as input an id and a pre-shared secret value (shared between the device and a base station). [27] defines an authentication protocol for VANETS, in which cars obtain a pseudonym directly from a trusted third party. This device pseudonym is then used in the communication with other vehicles.
- **Relationship:** Two general IoT papers leverage anonymous credential systems which are based on idemix for implementing relationship pseudonyms [18], [30]. A user would first enroll with an identity provider and obtain an anonymous credential, and afterwards, the user will be able to generate her own partial identities, i.e. subset of personal attributes corresponding to relationship pseudonyms, for each service she would like to authenticate for. The derived partial identities are based on a set of chosen attributes by the user and therefore, allowing data minimization and selective disclosure which should provide unlinkability of the created partial identities unless partial identities used for different services could be linked via attributes that are jointly used for different partial identities.
- **Short-term:** As the name suggests, short-term (or short-lived) pseudonyms are typically used one or more times during a specified time period. And at all times that it is (re)used, it is linkable. pseudonyms are linkable for reasons of costs or efficiency (as reuse of pseudonyms for a time period reduces costs for obtaining a new one from an issuing party) or for reasons functionality requiring linkability (e.g. for reputation scoring). Since they are used for a short time, it is hard for malicious entities to link them to the real identity. Three VANET papers [21], [28], [32] and one general IoT paper [13] fall under this category. Lin *et al.* [32] divide the identity of a vehicle into multiple sub-pseudonyms created via dynamic threshold cryptography [41] that are periodically exchanged for preventing attackers from obtaining enough partial identities for deriving a vehicle's real identity. These sub-identities are used to upload Safety Beacon Messages (SBMs) to a blockchain while protecting privacy via pseudonymity. In addition, vehicular location privacy is protected, by uniting vehicles to upload SBMs by the way of k-anonymity [42]. Kang *et al.* [21] address location privacy issues with Cloud-enabled Internet of Vehicles by the use of short-term pseudonyms for broadcasting safety messages and the use of different VM identifiers to LBS requests, with regular synchronised changes of pseudonyms and exchange of VM identifiers by the vehicles and VM manager. Kang *et al.* [28] present another scheme for the time-limited use of pseudonyms for VANETs that allows a vehicle to change pseudonyms according to its own preferences. Vehicles may coordinate with others to change pseudonyms by sending messages to nearby vehicles indicating that it wants to change its pseudonym. The local authority is informed about the pseudonym change or that they may be changed on ''social hotspots'' or based on time-triggers. In the context of anonymous networking for IoT environments and for the implementation of an anonymous reputation scheme, [13] uses anonymous credentials for implementing pseudonyms, which are however used across organisations, for allowing to derive reputation scores, but changed regularly for enhancing privacy.

- **Session:** These are pseudonyms that are used throughout an entire session between the user and the service that the user wishes to communicate with. In these schemes even if the user is trying to authenticate for different services from the same service provider she will be required to use the same pseudonym for all the services she's using throughout the session. Five papers use session pseudonyms: VANETS [24], [25]. LTE [22]. general IoT applications [23] and smart environments [15]. Saxena *et al.* [22] and Shen *et al.* [25] assume that the user/device is already enrolled in a trusted authority and every time they want to authenticate for a session they will calculate their own temporary id which is mostly based on their original pseudo-id and the current timestamp. [15] uses public-keys as pseudonyms that are assigned to users by a CA. A new set of keys is used for every session, which constitute session pseudonyms. Bernabe *et al.* [23] propose the establishment of session pseudonyms for attribute-based anonymous authentication and authorization of IoT devices. Chowdry *et al.* [24] propose a similar approach for vehicular networks in which vehicles generate their own pseudonyms, that are used throughout a session, from a pre-installed permanent identifier.
- **Relation or Session:** These are pseudonyms that can either be used as session or relationship pseudonyms. They change after every session, but if a user wishes to use them for more than one service that is provided by the same service provider, she can use a different pseudonym for each service in every session. Thereby, the service provider will not be able to link the user of services within a session with the different pseudonyms for the same user. [12] & [17] use idemix to implement this type of pseudonyms by providing users with a pool of pseudonyms that users can choose from based on the service they want to use.
- **Location-based:** Location pseudonyms depend on the current location of a device and/or user and were only used in one paper for privacy protection in smart environments. [26] introduces pseudonyms for an IoT device that are locally generated with a hash function out of different sources of radio-location information as a security overlay to prevent impersonation attacks. There are two possibilities for ad-hoc location pseudonyms: (1) one global pseudonym per node based on global location information, connectivity information, device information; or (2) link-dependent pseudonyms in regard to each neighbor node based on a hash of link-dependent information (relative distance or relate clock drift with regard to a neighbour node).
- **Transaction Pseudonyms:** This type of pseudonyms was leveraged the most by the surveyed papers [14], [19], [20], [29], [33], [34] for all identified application domains except for E-health. Both [29] & [20] use transaction pseudonyms for privacy-preserving authentication and authorisation of IoT devices. Idemix attribute based credentials (idemix) involving IoT smart cards are empowering users to control what data their devices are disclosing and can implement transaction pseudonyms. In [29], IoT devices have a duality in their functionality that is the device will play both roles of a user and a verifier. Therefore, devices will be able to authenticate and as well as demonstrate their credentials in a privacy-preserving way. [34] presents a privacy-preserving protocol for securing Large-Scale Database-Driven Cognitive Radio Networks with Location verification, with which a trusted authority (TA) will provide the user with multiple distinct pseudo-ids, which are each used for one channel request only. In [19] transaction pseudonyms are employed in VANETs especially in the message exchange between the vehicles where for each message that a vehicle wants to send a new *dynamic pseudo-identity* will be generated, while in [14] they were used in a completely decentralized manner where each time a node wants to authenticate with data collectors a new zero-knowledge proof token will be generated to provide full unlinkability. In [33] transaction pseudonyms were used in an anonymous reputation system where their system is based on blockchain technology and leverages the proof of stake (PoS) consensus protocol. In this system, a user can leave multiple feedbacks for different products and neither the retailer nor the PoS reviewing system will be able to link two feedbacks to the same user.

D. IdM ARCHITECTURE

The type of IdM architecture necessarily falls in one of three categories: centralized, decentralized, or fully decentralized (see Section II-B). The IdM architecture category is often not clearly stated in most of our selected papers but it can be identified when analyzing their system architecture and protocols. For instance, a blockchain-based IdM may fall on either centralized or decentralized categories depending on how its ledger is maintained, kept and made available to its participants.

1) CENTRALIZED IdM ARCHITECTURES

Eleven publications [15], [16], [21], [22], [24], [27], [28], [31]–[34] propose solutions based on a central authority for issuing pseudonyms, i.e. they all include some sort of a centralized identity CA. The CA is a trusted third party responsible for generating and distributing credentials to its clients. Upon receiving a request from an authenticated, i.e., identified, client, the CA issues either one unique pseudonym [15], [16], [27], [31] or a set of unique pseudonyms [24], [28], [34]. Clients may then request new pseudonyms on demand.

This architectural setting requires the CA to be trusted by all clients not to disclose the link between pseudonyms and end users. Under this assumption, users' anonymity is preserved as long as the CA is not compromised. Depending on how the CA is implemented, its availability requirements may not be feasible for a specific

IoT environment with limited resources, as pointed out by Khemissa and Tandjaoui [16]. However, the CA is a logical central architectural point but not necessarily physically centralized. Kang *et al.* [28] suggest the use of a hierarchical CA architecture, with local CAs issuing pseudonyms to end users and synchronizing their lists of issued pseudonyms and end user identities with a central CA. The use of hierarchical CA architectures was proposed in [27] for vehicular networks.

Li *et al.* [32] and Liu *et al.* [33] proposals based on the use of blockchains also fall in the centralized IdM category. Even though the blockchains in the proposals are collectively maintained, they need to be always available to their participants in the proposed systems and therefore are classified as centralized IdM architectures.

The revocation of pseudonyms in a centralized IdM architecture requires a revocation server that keeps track of revoked identities and pseudonyms. In theory, the revocation process is straightforward. Upon identifying a misbehaving activity, the pseudonym is reported to the CA, which may add the pseudonym and other pseudonyms associated with the same end user to the revocation list of the revocation server. However, in practice, maintaining revocation lists especially regarding short-lived certificates is a long and on-going debate out of the scope of this SLR [43], [44].

2) DECENTRALIZED IdM ARCHITECTURES

Proposals based on decentralized IdM architectures do not require the intervention of a CA for the generation of pseudonyms. Nonetheless, they require a logical trust anchor, such as a CA, that links users to their long-term identifiers but at the same time has no control or oversight over short-term identifiers (pseudonyms) issued by end users. In short, decentralized IdM architectures assume that a CA is trusted to issue long-term identifiers but at the same time it is not trusted to link long-term to short-term identifiers. Solutions based on anonymous credentials (see Section II-C) fall into this IdM architecture category, which includes most of the articles and papers included in this SLR [12]–[14], [17], [18], [20], [23], [29], [30].

Idemix [38], an anonymous credential system based on zero-knowledge proofs of knowledge (see Section II-C), is the main building block in [12], [17], [18], [23], [29], [30]. In [12], [23], [29], idemix is used in user and/or device authentication and authorization in different IoT settings. Alpár *et al.* [20] and Vinkovits *et al.* [13] proposals on authentication and authorization of IoT devices require an unspecified anonymous credential system, which could be implemented with idemix but not necessarily, and Alcaide *et al.* [14] use Persiano and Visconti's anonymous credential system [45] instead of idemix. Neisse *et al.* [17] use idemix to set attribute based certificated in informed consent and Sanchez *et al.* [30] use anonymous credentials to design a provenance system for IoT. Skarmerta *et al.* [18] overview on security and privacy management standardization work in IoT also propose the use of idemix for generation of anonymous credentials.

Decentralized IdM architectures that do not make use of anonymous credentials were proposed for vehicular networks by Wang *et al.* [19] and Shen *et al.* [25]. In Wang *et al.*, the CA provides a unique identifier to a vehicle which is concatenated with a timestamp and then hashed to generate a pseudonym. In Shen *et al.*, a pseudonym is the output of a hash function with the following input: the vehicle's unique identifier $\oplus$ its previous pseudonym $\oplus$ a secret value shared between the vehicle and a central authority.

3) FULLY DECENTRALIZED IdM ARCHITECTURES

Tunaru *et al.* [26] is the only publication in our list with a fully decentralized IdM architecture. In their solution pseudonyms are generated locally using radio signal information, such as signal strength and round trip times, as input to a hash function.

TABLE 6. Classification of articles according to their pseudonym revocation/reidentification scheme.

Revocation/Identification	Implementation
through k out of N actors	with secret sharing, as in [32]
by a trusted party	in [17], [19], [21], [25], [27]–[31], [33]
by the user	with non-interactive zero-knowledge proofs of knowledge, as in [13]
by neighbour nodes	neighbours "securely guess" pseudonyms [26]
not possible / not specified	in [12], [14]–[16], [18], [20], [22]–[25]

E. REVOCABILITY AND RE-IDENTIFICATION

Pseudonyms can often be linked back to the pseudonym holder under certain conditions for pseudonym revocation or re-identification, in case of misuse for example. Table 6 provides a classification of the surveyed papers according to if and how pseudonymity can be revoked and/or pseudonym holders can be re-identified.

A simple revocation scheme involves a trusted party that has a one-to-one mapping of pseudonyms and pseudonym holders (e.g. [27]), or a Certification authority that can broadcast a revocation message [19] or a trusted party can retrieve the real identities via another protocol (e.g. via a built-in trapdoor). For instance, the anonymous credential systems in [46] (used in [30]) describes a revocation authority responsible for revoking credentials, which is a trusted authority who can de-anonymize presentation tokens under specific circumstances. These schemes usually require a single point of trust.

For distributing trust to k out of N actors (with $k \leq N$) that jointly must collude for re-identifying a pseudonym holder, secret sharing schemes have been used (see [32]). This approach must rely on the assumption that k nodes only collude in well-specified cases in which a re-identification is required. Other more advanced schemes cryptographically enable the re-identification of a pseudonym holder only in case of Sybil attacks (as e.g. in [33] if a user issues multiple reviews for the same retailer), or allow the pseudonym holder to prove the possession of a pseudonym

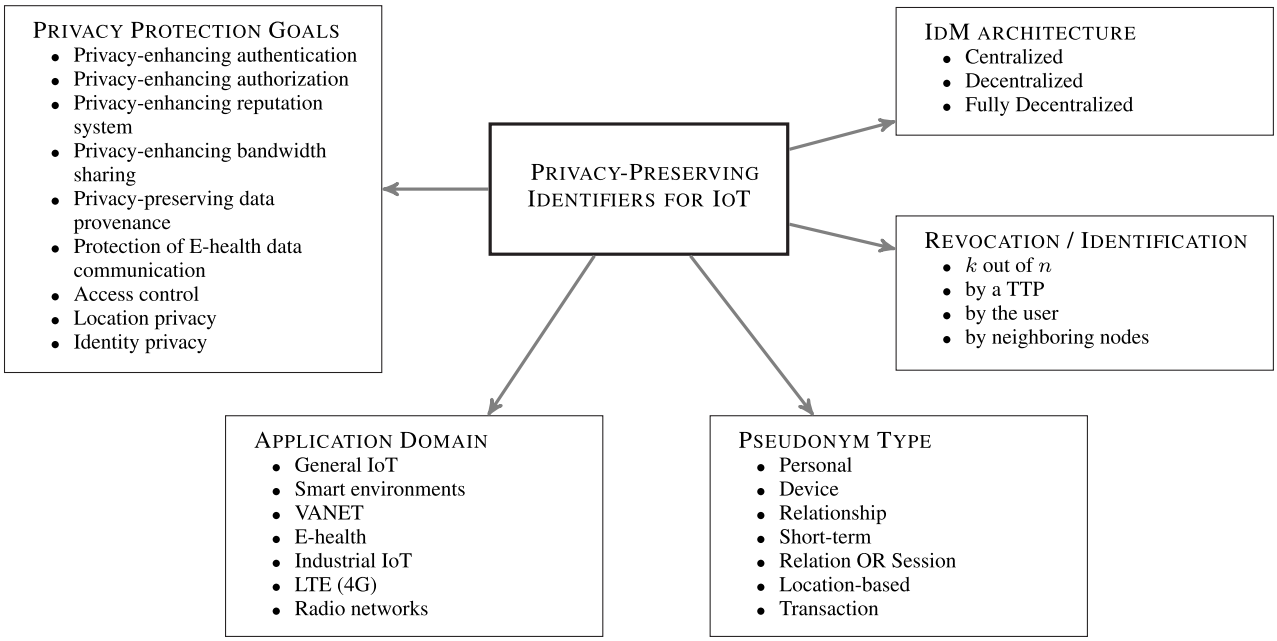


FIGURE 4. An overall summary of the SLR findings.

TABLE 7. Summary of properties in the selected publications.

Year	Ref.	Application	Pseud. Type	Arch.	Privacy Protection Goal
2009	[12]	Smart env.	relation / session	Dec.	privacy-enhancing authentication & authorisation
2012	[13]	General IoT	short-term	Dec.	privacy-enhancing authentication, authorisation, reputation system
2013	[14]	General IoT	transaction	Dec.	privacy-enhancing authentication & authorisation
2013	[15]	Smart env.	session	Cen.	privacy-enhancing bandwidth sharing, location, identity privacy
2015	[16]	E-health	device	Cen.	lightweight privacy-enhancing authentication
2015	[17]	Smart env.	relation / session	Dec.	privacy-enhancing authentication & authorisation
2015	[18]	General IoT	relationship	Dec.	privacy-enhancing authentication & access control
2015	[19]	VANET	transaction	Dec.	location & identity privacy
2016	[20]	Smart env.	transaction	Dec.	privacy-enhancing authentication & authorisation
2016	[21]	VANET	short-term	Cen.	location privacy
2016	[22]	LTE (4G)	session	Cen.	privacy-enhancing authentication & authorisation
2017	[23]	General IoT	session	Dec.	privacy-enhancing authentication & authorisation
2017	[24]	VANET	session	Cen.	location & identity privacy
2017	[25]	VANET	session	Dec.	location & identity privacy
2017	[26]	General IoT	location	FullyD.	privacy-enhancing authentication & identity privacy
2017	[27]	VANET	device	Cen.	location privacy
2018	[28]	VANET	short-term	Cen.	location privacy
2018	[29]	Smart env.	transaction	Dec.	privacy-enhancing authentication & authorisation
2018	[30]	General IoT	relationship	Dec.	privacy-preserving data provenance
2019	[31]	E-health	person	Cen.	protection of E-health data communication
2019	[32]	VANET	short-term	Cen.	location & identity privacy
2019	[33]	Industrial IoT	transaction	Cen.	privacy-enhancing reputation system
2019	[34]	Radio net.	transaction	Cen.	location & identity privacy

with zero-knowledge [13]. [26] allows to "securely guess" pseudonyms of trusted neighbors or to allow nodes to 'securely guess" pseudonyms of trusted neighbors.

F. SUMMARY

Figure 4 illustrates the overall findings of the SLR. It contains the identified privacy protection goals, application domains, pseudonym types, IdM architecture used and the mechanisms for revocation / identification in the analysed literature. Table 7 shows the classification of each paper according to IoT application domains, pseudonym types and IdM architecture used in relation to the privacy protection goals that were stated in these papers. It allows to compare the IdM solutions chosen in terms of pseudonym types and architecture for the different application domains and protection goals.

V. DISCUSSION

In this section, we provide reflections regarding the use of privacy-enhancing identifiers in application domains before

we discuss trends and gaps that are apparent from the surveyed literature. Finally, we present limitations and discuss how our survey differs from related work.

A. APPLICATION DOMAIN SPECIFIC ASPECTS

We have seen that the application domains have an impact on the inherent assumptions of what the privacy-preserving identifiers can and have to accomplish. We find that it could be interesting for easier use to explicitly define and analyse the requirements originating from the application domain, also considering related technical capabilities and limitations. The availability of processors with high computational capabilities in IoT applications in VANETs or through the use of smart cards (as e.g. proposed in [29]) allows devices to perform more complex operations which are for instance needed for privacy-preserving decentralised approaches based on anonymous credentials. However, our survey includes also one proposal [27] that employs device pseudonyms for VANETs, which due to their linkability provide low privacy protection. Hence, as is shown in Table 7 as well, even for an application domain such as VANETs with the consistent privacy protection goal of protecting location privacy, the technical solutions in terms of pseudonym types and IdM architecture for achieving these goals differ considerably. The same observation is true for other domains, such as e.g. the smart environment domain.

Especially for practical applications, it can be relevant to show system designers what privacy risks could be addressed by applying what types of privacy preservation identifiers for a given application domain and its given technical capabilities, and thus to provide guidance on how to achieve privacy by design for that domain.

Due to the computational and architectural demands of the suggested IdM privacy-preserving mechanisms, not much consideration for the privacy of low computational devices, e.g. smart sensors, smart tags, have been considered in the reviewed literature over the past 10 years. An exemption for instance are [31] & [16] proposing a light-weight authentication protocol for sensor node device pseudonyms for E-health applications, probably also as for the processing of medical data, appropriate means for privacy protection are legally required in Europe and many other countries. Initial trials with those technologies in retail privacy-preserving identifiers (in the form of anonymous credentials). In application domains that depend on low performance devices, such as smart tags or sensors, the devices and users usually have to rely on lightweight privacy solutions and on a centralised approach with third parties to issuing their credentials. Hence, unsurprisingly, IoT applications including devices with high computational capabilities enable a more enhanced solution with higher privacy protection. and supply chain and early research work on RFID privacy (see e.g. [47]) have shown a clear need for privacy-enhancing mechanisms for the whole life-cycle of smart tags in these and other application domains. Given a continuous interest in retail and supply chain IoT applications, we think that research efforts on privacy-preserving identifiers for IoT in those and also in other application domains with restricted technical capabilities should be increased.

B. CHOICES OF PSEUDONYM TYPES

Different types of pseudonyms were proposed in the scientific literature in dependence of the technical capabilities that are also impacted by the application domain. In this section, we briefly list the aspects that motivate the choice of pseudonym types for IoT by the scientific literature.

Personal or device pseudonyms that are linkable, provide low privacy protection are mostly used for light-weight protocols, e.g. for E-health applications [16], [31] with sensors with low computational capabilities.

Transaction pseudonyms based on anonymous credentials require more complex cryptographic operations which usually result in performance-trade-offs, and often require extra equipment, such as smart cards, which not all IoT devices can utilise. They were mainly proposed for General IoT applications. Only one paper proposes transaction pseudonyms [19] for VANETS, which could be for the reason that for car collision detection pseudonyms need to be linkable at least for a short period of time. Also, the issuing of a set of one-time use credentials is costly. Therefore, a compromise between privacy protection on one side and costs and performance on the other side is usually made by using short-term pseudonyms, session pseudonyms, or relationship pseudonyms.

Session pseudonyms are mostly used where services require some degree of linkability for optimal operation, whereas role or relationship pseudonyms are typically proposed for applications requiring limited linkability, such as anonymous reputation systems for IoT environments. Relationship pseudonyms for general IoT applications implemented by anonymous credentials were also proposed allowing the user to define partial identities for different communication partners. Location-based pseudonyms were only proposed in [26] and are thus rarely used.

C. CHOICES OF IdM ARCHITECTURES

Our results show that literature is equally divided in relation to the selection of an IdM architecture in relation to the issuing of privacy-preserving identifiers between centralized and decentralized IdM architectures. As summarized in Table 7, 11 publications contain proposals that require the participation of a trusted third party, like a CA, for pseudonym issuing or distribution and 11 other publications propose decentralized IdM architectures, in which users or devices generate pseudonyms on their own using as input an unique identifier (provided to them by a trusted third party). Only one paper describes a fully decentralized IdM architecture [26].

Even though the number of publications found in each category does not allow for a proper statistical analysis, it is possible to identify an overall trend towards the publication of proposals based on centralized IdM architectures in the 2009–2019 period, with all but one publications in this category appearing after 2015 (with four of those in 2019 alone).

A possible explanation for such a trend is the tendency to incorporate technologies from the state-of-the-art in design of solutions for a given problem, such as blockchains [32], [33], or application scenarios in which a trusted third party already exists or can be easily envisioned, such as a transit authority or a car manufacture in VANET scenarios.

In contrast, publications based on decentralized IdM architectures are more fairly distributed over the ten year period covered in our survey. Nine out of the 11 publications classified under decentralized IdM architectures are based on anonymous credential systems. The idea of anonymous credentials was first conceptualized in the 1980s by Chaum [3], and made practical in the 2000s following the works of Brands [48] and Camenisch and Lysyanskaya [38], which are the foundations of Microsoft's IdM U-prove and idemix, respectively. However, up to this date, anonymous credential systems never gained popularity among end users, and remain a niche topic.

D. TRENDS AND GAPS

Throughout this section, we discuss current trends and gaps for the research field of privacy-preserving identifiers for IoT that we observed while surveying the selected articles and we also point out the need for future research and actions.

1) ANONYMOUS CREDENTIAL SYSTEMS DEPLOYMENT

In the course of this survey, anonymous credential systems could be identified as one of the means leveraged by most of the publications to deal with privacy concerns in different application domains. Nine publications leverage the anonymous credential systems with eight publications [12], [13], [17], [18], [20], [23], [29], [30] relying on the notion of identity mixer (idemix) [38] and one [14] relying on Persiano and Viscontis anonymous credential system [45] to achieve anonymity, data minimization, unlinkability and selective disclosure. Moreover, most of the papers falling in this category follow the decentralized architecture and give users the ability to generate their own pseudonyms without intervention from a CA. However, in practice, anonymous credential systems based on idemix have hardly been in use yet, and therefore also the practical exploitation of the research results based on idemix needs further actions.

2) PRIVACY-PRESERVING IDENTIFIERS FOR VANETs

VANETs could be identified as the one application domain discussed by a big number of the reviewed papers, seven papers [19], [21], [24], [25], [27], [28], [32]. The fact that much research is conducted in this application domain, underscores the significance of more unlinkability in vehicular communication systems, but also the significance of identifying potential trade-offs by implementing different types of pseudonyms. As both location and information privacy, in general, are at stake in these systems, privacy-preserving identifiers for vehicular communication systems will be an area that is in need of further research in the future, especially when it comes to emerging autonomous car technologies.

3) USABLE PSEUDONYM CONFIGURATIONS AND TRADE-OFFS

Different types of pseudonyms may cause privacy trade-offs, e.g., with utility, costs and/or performance, or even safety, as mentioned in section V-B. Many papers do however not discuss how trade-off decisions were made. Moreover, while privacy-preserving identifiers are within the scope of the surveyed papers, the usability aspect of configuring them and making trade-off decisions is not specifically discussed by them. Usability of configuring pseudonymity schemes securely or in compliance with user preferences may however turn out to be a great research challenge, as discussed in [49] for the case of configuring secret sharing for achieving pseudonymity.

Most of the surveyed papers do not analyse any potential trade-offs of the implemented pseudonym types that build upon the principles of ''unlinkability'' and ''high-performance'' and most of the proposals do not discuss any potential privacy trade-offs that could arise from the use of one-time or short-term use of pseudonyms in terms of costs or performance either. However, the potential discrepancy between desired privacy protection and the cost of issuing short-term (or session or relationship pseudonyms) may be very relevant, in particular for VANETS for instance which are often using short-term pseudonyms.

4) ADDRESSING SYBIL ATTACKS

Another privacy goal that is an important prerequisite for improving users' privacy and anonymity is resilience towards Sybil attacks. Only two of the revised publications address or mitigate Sybil attacks in their proposals. [27] is the only paper in the VANET domain that mitigates Sybil attacks even though prevention against Sybil attacks is arguably a priority topic in VANET, as it prevents vehicles from using multiple pseudonyms at the same time, which could compromise the functionality and safety of the system. In [33] the authors developed an anonymous reputation system which provides protection against Sybil attacks in order to prevent self-ratings. The low number of papers addressing Sybil attacks shows that the area of Sybil-free identifiers is not extensively studied and still needs to be further researched in the context of IoT environments.

5) PSEUDONYM RE-IDENTIFICATION AND REVOCATION SCHEMES

Several articles did not discuss or specify any pseudonym revocation or re-identification scheme. In case of short-lived pseudonyms, this can be due to the reason that revocation is not required, as the pseudonyms will anyhow expire after a short time period (see e.g. [22]). Several of the papers that use anonymous credential schemes based on attribute based credential (e.g. [12], [18], [20]) could include a revocation authority or inspector as defined by the ABC4Trust architecture, but may for the sake of enhanced privacy and ''unconditional'' pseudonymity restrain from integrating a back-door

for re-identification. For device pseudonyms (e.g. [16]), revocation and re-identification are easily possible and therefore do not need discussion. While on most schemes revocation or re-identification of the pseudonym holder rely on a trusted party, more advanced schemes that require less trust and provide more control for accountability (e.g. the approach proposed by Weber [50] enabling controlled and step-wise re-identification of transaction pseudonyms) are not widely in use yet and need further attention. An exception is the more recent work by [32] involving secret sharing diving the trust to n out of k actors, where $n \leq k$.

E. LIMITATIONS

This SLR strictly followed the Kitchenham *et al.* [9] guidelines as defined in Section III. A survey scope includes only publications selected after a set of predefined key terms. In our SLR, we didn't include specific IoT applications in our keywords (see Table 3), such as VANET, E-health, and E-home. This may have filtered out publications within the scope of our SLR that do not mention or include in their title, abstract, or keywords the more general terms ''internet of thing'', ''IoT'' or ''smart environment''. On the other hand, this design decision allows us to get a better overview of IoT applications for which privacy-preserving identifiers have been proposed, without any bias that could be incurred by including specific IoT applications in our search terms.

The retrieving process sets the filters to match the search terms in title, abstract and keywords and not in full text. These criteria limited the retrieval of publications that mention the queried search terms in the body text or use other terms to refer to privacy-preserving identifiers. To reduce the probability of missing articles due to the latter, for the search query we included different terms that are used by the research community to refer to privacy-preserving identifiers. Moreover, some publications were discarded in the screening process as they do not to specify the type of privacy-preserving identifiers they propose.

Furthermore, the retrieval process in our SLR is not exhaustive because of the pre-selection of publication databases. Therefore, articles published in other scientific databases were not included in our survey. In addition, the ten-year time window (2009—2019) means that relevant articles published outside this period are also not included. This decision was based on the fact that IoT is a fast evolving and emerging technology, and therefore the most recent research activities and trends are far more relevant than past ones.

F. RELATED WORK

There have been other surveys conducted on IoT privacy and security research. Trnka *et al.* [51], focus on the security domain of IoT, presenting existing research in the areas of authentication, authorization, and identity management. They summarize the state of the art of security at the application layer, device management, and access rule enforcement since 2013. Seliem *et al.* [52] review the privacy challenges and issues in IoT environments and discuss privacy-preserving proposed solutions. They analyse and point out major privacy concerns such as identification, tracking, monitoring, and profiling. In the end, the authors provide several IoT application scenarios where personal data can be breached. A different approach is taken by [53], in which they survey Sybil attacks and defense schemes in IoT. In addition, the authors identify challenges and future directions for Sybil defenses in IoT.

Zhu and Badr [54] review existing blockchain-based sovereign identity solutions and identify challenges in building identity management systems for the Internet of Things. Furthermore, they compare existing traditional identity management initiatives in terms of IoT special characteristics. At the end, the authors analyze the blockchain-based identity management solutions proposed by the academia in the last years and identify the main features of them.

Even though research has been conducted in IoT privacy and security, existing related surveys focus rather on authentication or access control for IoT in general. However in contrast to our work, they do not survey and analyse the use and role of privacy-preserving identifiers for achieving privacy for IoT environments. Moreover, in contrast to previous work, our article also contributes to a new extended taxonomy for pseudonym types for IoT environments.

VI. CONCLUSION

This literature review has discussed the state of the research of 23 publications with the purpose of analysing what types of privacy-preserving identifiers are proposed for IoT environments. Based on scrutinizing the publications in terms of the employed types of pseudonyms in specific application areas of IoT, one main contribution of this survey is a new classification of pseudonym types across different IoT contexts, which extends the classification by Pfitzmann and Hansen [2] with location, short-term, session, and device pseudonym types. The papers reviewed have also been analysed and classified in terms of common characteristics, such as the IoT application domains, IdM architectures and pseudonym revocation and reidentification schemes and analysed trends, gaps and possible research directions.

This SLR underlined that depending on the application domain, technical capabilities and protection goals, trade-offs need to be made when choosing the type of pseudonyms and IdM solutions between privacy and performance, costs, safety, and security. Nonetheless, for some application domains, such as for VANETs, a range of different pseudonym types and IdM solutions were proposed by the surveyed papers for the same goal of protecting location privacy, often without discussing the involved trade-offs. Hence it remains unclear how far trade-off decisions were made based on well-informed choices. The authors therefore advocate further work on privacy by design guidelines for implementing pseudonymity for different IoT application domains, which support developers and researchers to choose

pseudonym types and thus to make appropriate trade-off decisions.

Implementing privacy in combination with other protection goals and making privacy trade-offs when implementing pseudonymity for IoT are also relevant for further open research challenges that we identified: Areas such as usability of configuring privacy-preserving identifiers and their potential trade-offs have not been a focus of research in the reviewed articles. To close this gap, more research on the usability of configuring pseudonyms with different privacy trade-offs should be further researched in the context of different application areas of IoT. Moreover, another significant issue refers to the potential lack of pseudonymity solutions for IoT addressing Sybil attacks, which leads to the need for future efforts to provide means of implementing privacy-preserving identifiers in IoT environments that are Sybil-free.

REFERENCES

[1] C. of the European Union and E. Parliament, "Regulation (EU) 2016/679 of the European parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation)," *Off. J. Eur. Union*, vol. L119, no. 1, pp. 1–88, 2016.

[2] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," TU Dresden, Dresden Germany, Tech. Rep. V0.34, 2010.

[3] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*. Boston, MA, USA: Springer, 1983, pp. 199–203.

[4] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," *J. Cryptol.*, vol. 1, no. 2, pp. 77–94, Jun. 1988.

[5] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2001, pp. 93–118.

[6] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich, "How to win the clonewars: Efficient periodic n-times anonymous authentication," in *Proc. 13th ACM Conf. Comput. Commun. Secur. CCS*, 2006, pp. 201–210.

[7] C. Andersson, M. Kohlweiss, L. A. Martucci, and A. Panchenko, "A self-certified and sybil-free framework for secure digital identity domain buildup," in *Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks*. Berlin, Germany: Springer, 2008, pp. 64–77.

[8] L. A. Martucci, M. Kohlweiss, C. Andersson, and A. Panchenko, "Self-certified sybil-free pseudonyms," in *Proc. 1st ACM Conf. Wireless Netw. Secur. WiSec*, 2008, pp. 154–159.

[9] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Inf. Softw. Technol.*, vol. 55, no. 12, pp. 2049–2075, Dec. 2013.

[10] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quart.*, vol. 26, pp. 13–23, Jun. 2002.

[11] S. Rumsey, *How to Find Information: A Guide for Researchers*. New York, NY, USA: McGraw-Hill, 2008.

[12] I. Armac, A. Panchenko, M. Pettau, and D. Retkowitz, "Privacy-friendly smart environments," in *Proc. 3rd Int. Conf. Next Gener. Mobile Appl., Services Technol.*, Sep. 2009, pp. 425–431.

[13] M. Vinkovits, E. Elmasllari, and C. Pastrone, "Anonymous networking meets real-world business requirements," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 451–457.

[14] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target-driven applications," *Comput. Secur.*, vol. 37, pp. 111–123, Sep. 2013.

[15] X. Liang, K. Zhang, R. Lu, X. Lin, and X. Shen, "EPS: An efficient and privacy-preserving service searching scheme for smart community," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3702–3710, Oct. 2013.

[16] H. Khemissa and D. Tandjaoui, "A lightweight authentication scheme for E-health applications in the context of Internet of Things," in *Proc. 9th Int. Conf. Next Gener. Mobile Appl., Services Technol.*, Sep. 2015, pp. 90–95.

[17] R. Neisse, G. Baldini, G. Steri, Y. Miyake, S. Kiyomoto, and A. R. Biswas, "An agent-based framework for informed consent in the Internet of Things," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Dec. 2015, pp. 789–794.

[18] A. Skarmeta, J. L. Hernandez-Ramos, and J. Bernal Bernabe, "A required security and privacy framework for smart objects," in *Proc. ITU Kaleidoscope, Trust Inf. Soc. (K-)*, Dec. 2015, pp. 1–7.

[19] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET," *IEEE Trans. Veh. Technol.*, vol. 65, no. 2, pp. 896–911, Feb. 2016.

[20] G. Alpár, L. Batina, L. Batten, V. Moonsamy, A. Krasnova, A. Guellier, and I. Natgunanathan, "New directions in IoT privacy using attribute-based authentication," in *Proc. ACM Int. Conf. Comput. Frontiers CF*, 2016, pp. 461–466.

[21] J. Kang, R. Yu, X. Huang, M. Jonsson, H. Bogucka, S. Gjessing, and Y. Zhang, "Location privacy attacks and defenses in cloud-enabled Internet of vehicles," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 52–59, Oct. 2016.

[22] N. Saxena, S. Grijalva, and N. S. Chaudhari, "Authentication protocol for an IoT-enabled LTE network," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–20, Dec. 2016.

[23] J. B. Bernabé, J. L. H. Ramos, and A. F. Gómez-Skarmeta, "Holistic privacy-preserving identity management system for the Internet of Things," *Mobile Inf. Syst.*, vol. 2017, Jan. 2017, Art. no. 6384186.

[24] M. Chowdhury, A. Gawande, and L. Wang, "Secure information sharing among autonomous vehicles in NDN," in *Proc. 2nd Int. Conf. Internet Things Design Implement.*, Apr. 2017, pp. 15–26.

[25] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2526–2536, Aug. 2018.

[26] I. Tunaru, B. Denis, and B. Uguen, "Location-based pseudonyms for identity reinforcement in wireless ad hoc networks," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC Spring)*, May 2015, pp. 1–5.

[27] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Cluster Comput.*, vol. 20, no. 3, pp. 2439–2450, Sep. 2017.

[28] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported Internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2627–2637, Aug. 2018.

[29] J. L. C. Sanchez, J. B. Bernabe, and A. F. Skarmeta, "Integration of anonymous credential systems in IoT constrained environments," *IEEE Access*, vol. 6, pp. 4767–4778, 2018.

[30] J. L. Canovas Sanchez, J. B. Bernabe, and A. F. Skarmeta, "Towards privacy preserving data provenance for the Internet of Things," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 41–46.

[31] R. Boussada, M. E. Elhdhili, and L. A. Saidane, "A lightweight privacy-preserving solution for IoT: The case of E-health," in *Proc. IEEE 20th Int. Conf. High Perform. Comput. Commun., IEEE 16th Int. Conf. Smart City, IEEE 4th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Jun. 2018, pp. 555–562.

[32] H. Li, L. Pei, D. Liao, G. Sun, and D. Xu, "Blockchain meets VANET: An architecture for identity and location privacy protection in VANET," *Peer Peer Netw. Appl.*, vol. 12, no. 5, pp. 1178–1193, Sep. 2019.

[33] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous reputation system for IIoT-enabled retail marketing atop pos blockchain," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3527–3537, Jun. 2019.

[34] R. Zhu, L. Xu, Y. Zeng, and X. Yi, "Lightweight privacy preservation for securing large-scale database-driven cognitive radio networks with location verification," *Secur. Commun. Netw.*, vol. 2019, pp. 1–12, May 2019.

[35] E. H. Bradley, L. A. Curry, and K. J. Devers, "Qualitative data analysis for health services research: Developing taxonomy, themes, and theory," *Health Services Res.*, vol. 42, no. 4, pp. 1758–1772, Aug. 2007.

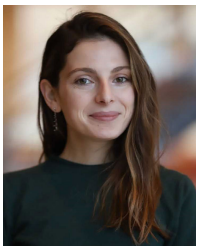
[36] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015.

[37] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 380–400, 2nd Quart., 2012.

[38] J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in *Proc. 9th ACM Conf. Comput. Commun. Secur.*, 2002, pp. 21–30.

[39] S. Brands, "A technical overview of digital credentials," *Available Online*, vol. 20, pp. 145–148, Feb. 2002.
[40] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1984, pp. 47–53.
[41] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive secret sharing or: How to cope with perpetual leakage," in *Proc. Annu. Int. Cryptol. Conf.*, Berlin, Germany: Springer, 1995, pp. 339–352.
[42] L. Sweeney, "k-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 2002.
[43] R. L. Rivest, "Can we eliminate certificate revocation lists," in *Proc. Int. Conf. Financial Cryptogr.* Berlin, Germany: Springer, 1998, pp. 178–183.
[44] S. Eskandarian, E. Messeri, J. Bonneau, and D. Boneh, "Certificate transparency with privacy," *Proc. Privacy Enhancing Technol.*, vol. 2017, no. 4, pp. 329–344, Oct. 2017.
[45] G. Persiano and I. Visconti, "An efficient and usable multi-show non-transferable anonymous credential system," in *Proc. Int. Conf. Financial Cryptogr.*, Springer, 2004, pp. 196–211.
[46] J. Camenisch, I. Krontiris, A. Lehmann, G. Neven, C. Paquin, and K. Rannenberg, "H2. 1—ABC4trust architecture for developers," *Heartbeat*, vol. 2, p. 1, Nov. 2012.
[47] A. Juels, "RFID security and privacy: A research survey," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 381–394, Feb. 2006.
[48] S. Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. Cambridge, MA, USA: MIT Press, 2000.
[49] E. Framner, S. Fischer-Hübner, T. Lorünser, A. S. Alaqra, and J. S. Pettersson, "Making secret sharing based cloud storage usable," *Inf. Comput. Secur.*, vol. 27, no. 5, pp. 647–667, Nov. 2019.
[50] S. G. Weber, *Multilaterally Secure Pervasive Cooperation: Privacy Protection, Accountability and Secure Communication for the Age of Pervasive Computing*, vol. 9. Amsterdam, The Netherlands: IOS Press, 2012.
[51] M. Trnka, T. Cerny, and N. Stickney, "Survey of authentication and authorization for the Internet of Things," *Secur. Commun. Netw.*, vol. 2018, pp. 1–17, Jun. 2018.
[52] M. Seliem, K. Elgazzar, and K. Khalil, "Towards privacy preserving IoT environments: A survey," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–15, Nov. 2018.
[53] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372–383, Oct. 2014.
[54] X. Zhu and Y. Badr, "A survey on blockchain-based identity management systems for the Internet of Things," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1568–1573.

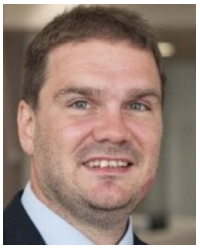
MAHDI AKIL received the bachelor's degree in computer science from Lebanese International University, Lebanon, in 2015, and the master's degree in networks and security from the Sapienza University of Rome, Italy, in 2018. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Karlstad University, Sweden. His research interests include security and privacy in vehicular ad hoc networks and smart environments.



LEJLA ISLAMI received the M.Sc. degree in cybersecurity from the Tallinn University of Technology, and the M.Sc. degree in cybersecurity from the University of Tartu, Estonia. She is currently pursuing the Ph.D. degree in computer science with Karlstad University, Sweden. Her research interests include investigating users perceptions on privacy trade-offs of vehicular communication systems, HCI, usable privacy, the IoT, cybersecurity, and nationwide cyber awareness.

SIMONE FISCHER-HÜBNER (Member, IEEE) received the Diploma degree in computer science (law), in 1988, and the Ph.D. and Habilitation degrees in computer science from the University of Hamburg, Germany, in 1992 and 1999, respectively. She has been a Full Professor with Karlstad University, Sweden, since 2000, where she is currently the Head of the Privacy and Security Research Group. She is also a Scientific Coordinator with the EU H2020 Marie Skłodowska-Curie ITN Privacy & Us. She has contributed as a Partner with the CyberSec4Europe, PAPAYA, CREDENTIAL, PRISMACLOUD, A4Cloud, SmartSociety, PrimeLife, PRIME, FIDIS, and Bugyo EU projects. Her research interests include cyber security, privacy-enhancing technologies, and usable privacy and security. She is a Swedish IFIP TC 11 Representative and a member of the Advisory Board Swedish Civil Contingency Agency's Cyber Security Council. She serves as the Vice Chair for the IEEE Sweden Computer/Software Engineering Chapter.

LEONARDO A. MARTUCCI received the Diploma and master's degrees in electrical engineering from the University of São Paulo, in 2000 and 2002, respectively, and the Ph.D. degree in computer science from Karlstad University, in 2009. He was a Postdoctoral Research Fellow with Linköping University, a Principal Investigator with the Center for Advanced Security Research Darmstadt, and a Postdoctoral Researcher with Technische Universität Darmstadt, Germany. He is currently an Associate Professor with Karlstad University and a Senior Member with the Privacy and Security Research Group.



ALBIN ZUCCATO received the master's degree in wirtschaftsinformatik from TU Wien and the Ph.D. degree in information security management from Karlstad University. He has been in information and IT security, since 1997. He has experience with the financial industry, public sector, cloud services, retail, telecom industry, and international research projects. He has worked in various management roles. He is currently a Senior Manager in IT security and IT privacy with ICA Gruppen AB. He is also a CISSP, a CISA, an ISO 27001 Lead Implementer, and a Lead Auditor certified.