REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
		START DATE	END DATE
MAY 2023	JOURNAL ARTICLE (POST PRINT)	SEPTEMBER 2019	JANUARY 2023

4. TITLE AND SUBTITLE

Privacy-Preservation Techniques for IoT: A Systematic Mapping Study

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
FA8750-19-C-0077	N/A	
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**
		R2R7

6. AUTHOR(S)

Damiano Torre, Anitha Chennamaneni, Alex Rodriguez

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Texas A&M University Central Texas
Department of Computer Information Systems
Killeen TX 76549

8.PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10.SPONSOR/MONITOR'S ACRONYM(S)	11.SPONSOR/MONITOR'SREPORT NUMBER(S)
Air Force Research Laboratory/RITGB 525 Brooks Road Rome NY 13441-4505	AFRL/RI	AFRL-RI-RS-TP-2023-023

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for Public Release; Distribution Unlimited. PA# AFRL-2022-4610
Date Cleared: 27-September-2022

13. **SUPPLEMENTARY NOTES**

14. ABSTRACT

The Internet of Things (IoT) is becoming a pervasive technology entangled in everyday life. The objective of IoT is to provide ubiquitous access to numerous devices and machines on service providers. However, IoT-based devices may expose a user to various privacy and security threats. Privacy-preservation techniques focus on securing any type of data transfer between different parties. We aim to deliver the current state of the art in terms of privacy-preservation techniques used for IoT devices that have been discussed in the literature. Therefore, we carried out a systematic identification of the privacy-preservation techniques for IoT devices that have been described in the cybersecurity domain. To do so, we followed rigorous guidelines to define our research protocol to increase the repeatability and reliability of our results. A set of ten research questions was created to drive the analysis of our study. This research work comprehensively analyzes and discusses the privacy-preservation techniques for IoT devices published in five different academic venues. We identified 260 studies, mostly published between 2017 and 2021, that were systematically selected from an initial set of 1394 papers. The most active research areas in privacy-preservation techniques for IoT devices discuss cryptography techniques to improve the authentication process to access IoT devices. The majority of authors presented privacy-preservation techniques for IoT that involved inventory privacy threats and discussed privacy interference attacks. We comprehensively analyze and discuss the trends, gaps, and possible future research directions of the privacy-preservation techniques used for IoT devices published in different academic venues.

15. **SUBJECT TERMS**

Privacy preservation, Internet of Things, systematic mapping study, privacy threats, privacy goals, privacy attacks.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	C. THIS PAGE		
U	U	U	SAR	24

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER *(Include area code)*
RICHARD BUTLER	N/A

STANDARD FORM 298 (REV. 5/2020)
Prescribed by ANSI Std. Z39.18

PREVIOUS EDITION IS OBSOLETE.

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 12 January 2023, accepted 12 February 2023, date of publication 14 February 2023, date of current version 22 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3245524

RESEARCH ARTICLE

Privacy-Preservation Techniques for IoT Devices: A Systematic Mapping Study

DAMIANO TORRE, (Member, IEEE), ANITHA CHENNAMANENI, (Member, IEEE), AND ALEX RODRIGUEZ

Department of Computer Information Systems, Texas A&M University Central Texas, Killeen, TX 76549, USA

Corresponding author: Damiano Torre (damiano.torre@tamuct.edu)

This work was supported in part by the Air Force Research Laboratory (AFRL) and Department of Homeland Security (DHS) Science and Technology (S&T) Directorate under Award FA8750-19-C-0077.

ABSTRACT The Internet of Things (IoT) is becoming a pervasive technology entangled in everyday life. The objective of IoT is to provide ubiquitous access to numerous devices and machines on service providers. However, IoT-based devices may expose a user to various privacy and security threats. Privacy-preservation techniques focus on securing any type of data transfer between different parties. We aim to deliver the current state of the art in terms of privacy-preservation techniques used for IoT devices that have been discussed in the literature. Therefore, we carried out a systematic identification of the privacy-preservation techniques for IoT devices that have been described in the cybersecurity domain. To do so, we followed rigorous guidelines to define our research protocol to increase the repeatability and reliability of our results. A set of ten research questions was created to drive the analysis of our study. This research work comprehensively analyzes and discusses the privacy-preservation techniques for IoT devices published in five different academic venues. We identified 260 studies, mostly published between 2017 and 2021, that were systematically selected from an initial set of 1394 papers. The most active research areas in privacy-preservation techniques for IoT devices discuss cryptography techniques to improve the authentication process to access IoT devices. The majority of authors presented privacy-preservation techniques for IoT that involved inventory privacy threats and discussed privacy interference attacks. We comprehensively analyze and discuss the trends, gaps, and possible future research directions of the privacy-preservation techniques used for IoT devices published in different academic venues.

INDEX TERMS Privacy preservation, Internet of Things, systematic mapping study, privacy threats, privacy goals, privacy attacks.

I. INTRODUCTION

In recent years, remarkable technological advancements have been made in the development of smart platforms. Various mobile devices are gaining popularity among users and business organizations. These mobile devices run applications that can bring considerable improvements in Internet-based services. People can work, communicate, shop, learn, entertain, control, and monitor anything from anywhere, at any time through many devices over the Internet. 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 [1]. However, these applications may expose a mobile user to various privacy and security threats. From the security and privacy perspectives, new commodities and advanced capabilities of mobile platforms are not thoroughly analyzed. Smart mobile devices are equipped with built-in sensors and are capable of providing different connectivity options [2]. The fundamental objective of IoT is to provide ubiquitous access to numerous devices and machines on service providers (SPs), covering many

The associate editor coordinating the review of this manuscript and approving it for publication was Shaohua Wan.

areas such as location-based services (LBS), smart home, smart city, E-Health, E-Learning, E-Business, etc [3]. IoT devices are pieces of hardware, such as sensors, actuators, gadgets, appliances, or machines, that are programmed for certain applications and can transmit data over the internet or other networks. They can be embedded into other mobile devices, industrial equipment, environmental sensors, medical devices, and more. While those devices may provide personalized services, they also introduce privacy-related concerns regarding the consequences of the collection and use of their personal data. Though IoT is a breakthrough innovative idea that will bring ease and comfort to human life, still it faces many challenges in its way to being widely accepted by the users [4]. The major challenge to IoT is the security and privacy of the user's [5]. In particular, a considerable amount of recent studies (i.e., [6], [7], [8], [9]) have been addressing the implementation of privacy laws that provide the appropriate technical and organizational measures, such as pseudonymisation, for complying with data-protection principles, such as data minimisation. Privacy can be defined as a method of protecting information that can be sensitive to any individual. The basic reason for privacy preservation (PP) is to prevent an intruder from learning more than the minimum required information regarding any specific individual either in the case of real-time or statistical data [10]. When it comes to IoT devices and solutions available commercially, privacy is often confused with security, and secure solutions are often marketed as privacy-preserving. Moreover, existing solutions and techniques mainly focus on securing the communication channel as well as authentication and authorization mechanisms [11]. Much less consideration is given to the preservation of privacy in the data collection, aggregation, storage, and retrieval processes [12]. To date, various PP strategies have been proposed by researchers to overcome certain privacy threats [10]. We identified several recent survey papers, which discuss PP techniques involving IoT devices [1], [2], [3], [10], [11], [13], [14]. However, to the best of our knowledge, no systematic literature reviews on PP techniques for IoT devices have been published.

A. RESEARCH OBJECTIVE AND CONTRIBUTIONS

The main research question guiding our work is the following: *What is the current state of the art in terms of PP techniques used for IoT devices?* To do so, we carried out a systematic identification of the PP techniques which have been used to preserve the privacy of users of IoT devices. Hence, this article aims to deliver a comprehensive summary of the PP techniques used for IoT devices that have been discussed in the literature. To achieve this goal, this paper explores the role of PP techniques for IoT devices by performing a Systematic Mapping Study (SMS) [15] as this is a research method that provides an objective procedure for identifying the quantity of existing research related to a research question. Performing an SMS has several benefits [16]: it gives a starting point for future research, and in the longer term, it provides a body of knowledge to the next generation of researchers. To carry out the SMS detailed in this paper, we followed the guidelines of Kitchenham and Charters [17]. These guidelines are admittedly for systematic literature reviews. However, they can be readily applied, and have been applied by others, when conducting systematic mapping studies [18]. Our SMS comprehensively analyses and discusses the trends, gaps, and possible future research directions of the PP techniques used for IoT devices published in different academic venues.

The main contributions of this paper are the following:

- By applying a systematic protocol, we present 260 primary study research papers where authors discuss novel PP techniques used for IoT devices. Those 260 were systematically selected from an initial set of 1394 research papers collected from five search engines (IEEE, ACM, Science Direct, Springer Link, and Web of Science).
- We report the findings and analysis for each one of the ten research questions that drive this research. Those findings can be used in future research directions.
- We review the different PP techniques, the PP techniques providing tool support, the PP goals studied, the IoT layers involved in the studied, the IoT devices most covered, privacy threats and attacks discussed by the authors, and the most frequently used evaluation metrics in the area of PP techniques for IoT devices, among others.
- We introduce the following new taxonomies: (a) eights PP techniques that can be used to secure the privacy of IoT devices, and (b) nine PP goals that were studied by the authors of the 260 primary studies.
- We provide the reference list of the 260 primary studies in order to provide a body of knowledge to the future researcher in the field of PP and IoT.

The rest of this paper is structured as follows. In section II we provide a brief discussion on related work. This is followed by a description of the SMS protocol we used [17]: the SMS planning (section III), the SMS execution (section IV), and the results (section V). A set of additional results are provided in section VI. Threats to validity are in section VII. Finally, section VIII draws the conclusions and provides directions for future works.

II. RELATED WORK

Several reviews of the literature on PP techniques have been published in recent years, some of them focusing on IoT devices. Table 1 provides the comparison of the nine research papers analyzed in this section. The first column *"Reference"* of the table provides a reference to each study. The second column *"Year"* indicates the year when the study was published. The third column *"Systematic"* shows if the study was conducted by following a systematic procedure. The fourth column *"Primary Studies"* indicates the number of primary studies discussing PP techniques for IoT devices considered by each study. The fifth column *"Main Goal"* shows the main goal of each paper. We discuss the selected studies next.

TABLE 1. Related work.

Reference	Year	Systematic	Primary Studies	Main Goal
Hassan et al. [10]	2020	×	7	Differential privacy techniques in CPSs scenarios.
Imtiaz et al. [11]	2019	×	14	Privacy preserving techniques for IoT devices involving sensors, computation and service since.
Khan et al. [2]	2019	×	59	Approaches used for preserving privacy in mobile crowdsensing applications.
Akil et al. [1]	2019	✓	39	Use of privacy-preserving identifiers implementing pseudonymity in identity management (IdM) systems.
Ali et al. [4]	2019	×	12	Privacy-preserving data aggregation techniques.
Desai et al. [14]	2019	×	50	Privacy related research in the Internet of Everything.
Abi Sen et al. [3]	2018	×	42	Privacy-preservation techniques in IoT.
Peng et al. [19]	2021	×	59	Security of smart contracts for IoT escosystems.
Wan et al. [20]	2020	×	28	Privacy and Security protocols.
This SMS	**2022**	✓	**260**	**Privacy-preservation techniques for IoT devices.**

Table 2 shows the coverage of the 10 research questions answered in this manuscript (see Section III) by the nine related works papers. The goal of Table 2 is to provide a summary of previous analyses in comparison to the analysis carried out in this work to highlight the novelty of this work. Notice that our study was built incrementally manner by considering the analyses conducted by the previous nine related works. In other words, we included all the analyses carried out by the nine previous related work and introduced new ones. As follows, we discuss the selected studies.

Hassan et al. [10] survey state-of-the-art work on differential privacy techniques in CPSs scenarios. They review previous survey articles on differential privacy and highlight important features of them by focusing more on the presenting practical aspects of differential privacy in CPSs. The authors provide a thorough survey of differential privacy and its implementation in CPSs and provide an extensive summary of the applications of differential privacy in CPSs. They finally survey the work done over the implementation of differential privacy in energy systems, transportation system, healthcare, and industrial IoT systems. Among a large set of research papers analyzed, only seven focus on Industrial IoT.

Imtiaz et al. [11] present an overview of privacy-preserving techniques for IoT along with the privacy threats addressed by each solution, their limitations, and known resistance to attacks on user privacy. For this work, the authors focus on IoT devices and services used for personal applications such as health care and smart home solutions. In particular, they discuss three components sensors, computation, and service since, since they have received much less attention in the literature. They consider privacy in communication protocols as outside the scope of their study.

Khan et al. [2] investigate the current approaches used for preserving privacy in mobile crowdsensing applications. They present a comprehensive and detailed classification of various privacy-preserving mechanisms that are provided along with a classification of task management in a mobile crowdsensing paradigm. After a generic description of mobile crowdsensing systems and their components, they discuss critical issues related to PP, such as task management, task assignment models, and incentive mechanisms. In addition, the authors discuss various mobile crowdsensing mechanisms available in the literature.

Akil et al. [1] present a systematic literature review on the use of privacy-preserving identifiers implementing pseudonymity in identity management systems for IoT published from 2009 to 2019. Privacy-preserving identifiers are information containers used to identify or authorize a user and/or a device without necessarily revealing the identity or other personal details of the device holders. The authors 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 authors finally provide a classification and analysis of the IoT application areas using privacy-preserving identifiers and a classification and analysis of the use of privacy preserving identifiers in IoT.

Ali et al. [4] discuss Privacy-Preserving Data Aggregation techniques and compare their performance as to guide the researcher to where efforts should be made to develop new privacy-preserving techniques for resource-constrained IoT. In addition, the authors provide an analysis of each mathematical operation involved in the different PP schemes.

Desai et al. [14] present a survey of privacy-related research in the Internet of Everything (IoE) enabled smart grid environment. The survey presents an analysis of privacy problems and their corresponding solutions by using privacy preserving schemes. In particular, the authors analyze and highlight the potential privacy concerns, categorize and review the existing solutions and summarize future research challenges in preserving user privacy for advanced metering infrastructures.

TABLE 2. Related work coverage of the research questions discussed in this paper.

Reference	RQ1	RQ2	RQ3	RQ4	RQ5	RQ6	RQ7	RQ8	RQ9	RQ10
Hassan et al. [10]	✓			✓	✓	✓	✓			
Imitaz et al. [11]	✓		✓	✓	✓					
Khan et al. [2]	✓			✓		✓	✓			
Akil et al. [1]	✓	✓	✓	✓			✓			
Ali et al. [13]	✓			✓	✓				✓	
Desai et al. [14]	✓			✓		✓	✓			
Abi Sen et al. [3]	✓			✓	✓		✓			
Peng et al. [19]	✓		✓	✓		✓	✓			✓
Wan et al. [20]	✓			✓	✓				✓	
This SMS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Abi Sen et al. [3] present an overview of PP techniques in IoT and alongside the tools used by researchers in the field. The authors of this paper separates security and privacy and focuses on the privacy approaches in the IOT environment. In addition, the authors review different approaches and techniques implementing preserving privacy in IoT.

Peng et al. [19] explore the vulnerabilities and attacks in smart contracts, which may seriously affect the stability of the IoT ecosystem. Specifically, the authors reviewed the security issues and solutions in the integration between smart contracts and the IoT systematically, they summarized and compared recent advances of the corresponding solutions toward the three aspects of security issues, and they finally outlined challenges and future research directions.

Wan et al. [20] summarize and analyze the recent advances in blockchain consensus protocols, by giving an explicit comparison of their performance and other critical particularities. This paper (a) reviews representative protocols according to specific classification, (b) provides a comparison of their qualitative and quantitative performance and other critical particularities with pros and cons, and (c) discusses future research trends in consensus studies.

A. DIFFERENCES BETWEEN THE RELATED WORK AND OUR SMS

None of the nine reviews above carried out a similar systematic study as we do in this manuscript. More precisely, our work differs from the current work in the following respects: (i) we retrieve and analyze a larger number of primary studies compared to the other studies; (ii) we follow a systematic procedure to carry out our study. No study, except the works of Akil et al. [1], followed a systematic procedure. Akil et al. [1] presented fewer research questions, retrieved fewer primary studies, and considered fewer search engines compared to our work; (iii) we focus only on PP techniques for IoT devices. Other studies also included primary studies that involved PP techniques for other types of systems (e.g., Hassan et al. [10] discuss PP techniques for CPSs); (iv) we report on primary studies published up to October 2021. The most recent review (among the studies presented in this section) discussed papers published up to 2020 (i.e., [10]; and (v) we provide a broader analysis including 10 research questions. Table 2 show how most of the nine studies include only analysis covering five research questions (i.e., RQ1, RQ4, RQ5, RQ6 and RQ7);).

To summarize, we were unable to find any research work that answers our main research question (see Introduction), which confirmed the need for an SMS about PP techniques for IoT devices. However, it is also important to note that published works related to our SMS are, in general, more informal literature surveys or comparisons with no defined research questions, no search process, no defined data extraction or data analysis processes. Instead, our SMS follows a strict, well-known protocol.

III. SMS PLANNING

We applied a structured and well-established review process, presented by Petersen et al. [15]. Figure 1 graphically illustrates the overall process, which consists of three main activities: (1) database search, (2) primary studies selection, and (3) data extraction.

A. OBJECTIVE

The main objective of this research focuses on the development of new PP techniques used for IoT devices. The research goal of this SMS is to map PP techniques, IoT devices, PP goals, privacy threats, privacy attacks, etc., from works published up to October 2021. Likewise, by providing an overview of techniques that are used to preserve the privacy of data used by IoT devices. We aim at helping the practitioners in the intersection of cybersecurity (specifically PP-related) and IoT that have to choose the tools that best meet their needs for research and practice throughout ten research questions. In addition to these questions, which provide the classification of proposed PP techniques for cross-application IoT-related domains, we also included a broader analysis discussing research gaps for heterogeneity of the surveyed techniques, evolution issues, and usability issues.

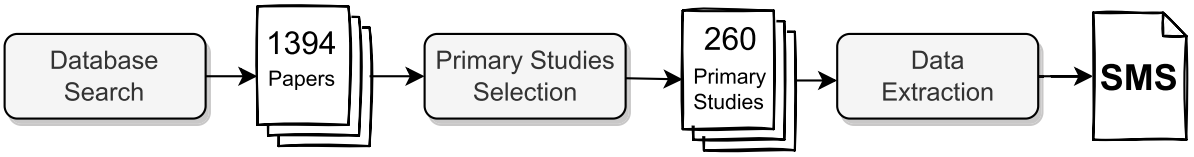

FIGURE 1. Overview of the systematic mapping study process.

TABLE 3. Research questions.

Research Question	Motivation
RQ1) What are the PP techniques used for IoT devices?	To discover the PP techniques used for IoT devices that research has focused upon, to reveal the PP techniques that are considered more important than others, as well as to identify opportunities for further research.
RQ2) What are the PP goals of the studied PP techniques?	To pinpoint the PP goals that research has focused upon, to reveal the goals that are considered more important than others.
RQ3) What type of affected IoT layers have been discussed?	To study the IoT layers that researchers has focused upon.
RQ4) What type of affected IoT devices have been considered?	To identify the IoT devices studied by the researchers in field.
RQ5) What type of privacy threats have been studied?	To highlight the privacy threats that research has focused upon, to reveal what are the ones considered more important than others.
RQ6) What type of privacy attacks have been analyzed?	To focus on the privacy attacks that research considered more important than others.
RQ7) What are the performance metrics used to evaluate PP techniques for IoT devices?	To find what are the metrics used for evaluating the performance of PP techniques used for IoT devices.
RQ8) What kind of research method has been adopted?	To determine if the field is generally more applied or more basic research as well as to identify opportunities for future research.
RQ9) What type of research has been conducted?	To determine the type of research that has been conducted: academic, industrial, or both academic and industrial.
RQ10) Are the PP techniques (i.e., the code of the algorithms) implemented and publicly available?	To discover how the PP techniques used for IoT devices are implemented, and to collect the ones that are publicly available.

B. RESEARCH QUESTIONS

Table 3 presents the research questions that drive this study along with the description of the motivations for each research question. To identify the current state of the art on PP techniques used for IoT devices, we considered ten research questions (RQs).

C. SEARCH STRATEGY

To carry out a search for primary studies we had to create search strings (SS), and decide the parts of the primary studies (papers) in which the search strings are looked for (the search fields). To create our search strings, we followed the procedure suggested by Brereton et al. [21]:

- Define the major terms;
- Identify alternative spellings, synonyms or related terms for major terms;
- Check the keywords in any relevant papers were already available;
- Use the Boolean OR to incorporate alternative spellings, synonyms or related terms;
- Use the Boolean AND to link the major terms.

TABLE 4. Search string.

Major terms	Alternative terms
Privacy-preservation	privacy-preservation OR privacy preservation OR privacy preserving
Technique	technique OR method OR approach OR algorithm
IoT	IoT OR Internet of Things
Device	device OR system

The major search terms were "Privacy-preservation", "Technique", "IoT", and "Device" and the alternative spellings, synonyms or terms related to the major terms are presented in Table 4.

We took into account several criteria when choosing the search string. Other search terms were tested, but owing to space restrictions, we are unable to describe all of them here. In the set of alternative search strings, we selected the following one as it allowed us to retrieve the largest number of useful papers, i.e., the largest number of papers focusing on PP techniques for IoT devices:

(privacy-preservation OR privacy preservation OR privacy preserving) AND (technique OR method OR approach OR algorithm) AND (IoT OR Internet of Things) AND (device OR system)

Up to October 2021, we did not impose any search limitations on publishing years. The SMS process started in August 2021 and was finished in June 2022. The five search engines Science Direct, IEEE Digital Library, ACM Digital Library, Springer Link, and Web of Science were employed using the aforementioned search string. The searches were limited to the following search fields: title, keywords and abstract.

D. INCLUSION AND EXCLUSION CRITERIA

In this section, we discuss the inclusion and exclusion criteria we used. We then discuss the process we followed to include primary studies in this SMS. The inclusion criteria were:

- Electronic Papers (EPs) discussing at least one PP technique for IoT devices;
- EPs written in English language;
- EPs published in peer-reviewed journals, international conferences, magazine, and workshops;
- EPs published up to October 2021.

The exclusion criteria were:

- EPs not discussing at least one PP technique for IoT devices;
- EPs that did not present a full-text paper (title, abstract, complete body of the article, and references) but were reduced to an abstract for instance;
- Duplicated EPs (e.g., returned by different search engines);
- EPs discussing PP techniques not meant for IoT devices.

E. DATA EXTRACTION STRATEGY

We extracted the data from the primary studies according to several criteria, which were directly derived from the research questions detailed in Table 3. Using each criterion to extract data required that we read the full text of each of the 260 primary studies. Once recorded, we collected data in a spreadsheet that represents our data form. We answered RQ1-RQ10 by collecting data from the execution of the four steps described in Table 5. Figure 2 shows the data model of the data collected. In total, we collected over 10000 answers for the ten research questions applied to the 260 primary studies identified by our systematic mapping study. In our data model, each *Electronic Paper*– which refers to the primary studies of this SMS– has an *ID* which is a unique code assigned to each paper, the *Year* when the paper was published, the name(s) of the *Authors*, the *Title* of the paper, the *Link* to access the paper, the application *Domain*, the *Search Engine* where the paper was identified (i.e., *IEEE*, *ACM*, *Web of Science*, *Springer Link*, and *Science Direct*), the *Type of Research* that was conducted (i.e.,*Academia*, *Industry*, *Academia/Industry*), the *Type of Venue* (i.e., *Journal*, *Conference*, or *Workshop*), the *Name of the Venue*, and according to [22] the *Research Method* applied in each paper:

- *Evaluation Research:* it investigates techniques that are implemented in practice and an evaluation of the technique is conducted. That means the paper shows how the technique is implemented in practice (solution implementation) and what are the consequences of the implementation in terms of benefits and drawbacks (implementation evaluation).
- *Validation Research:* it investigates the properties of a solution that has not yet been implemented in practice.
- *Proposal of Solution:* it proposes a solution to a problem and argues for its relevance, without a full-blown validation.
- *Philosophical Paper:* it sketches a new way of looking at things, a new conceptual framework, etc.
- *Opinion Paper:* it contains the author's opinion about what is wrong or good about something, how something should be done, etc.

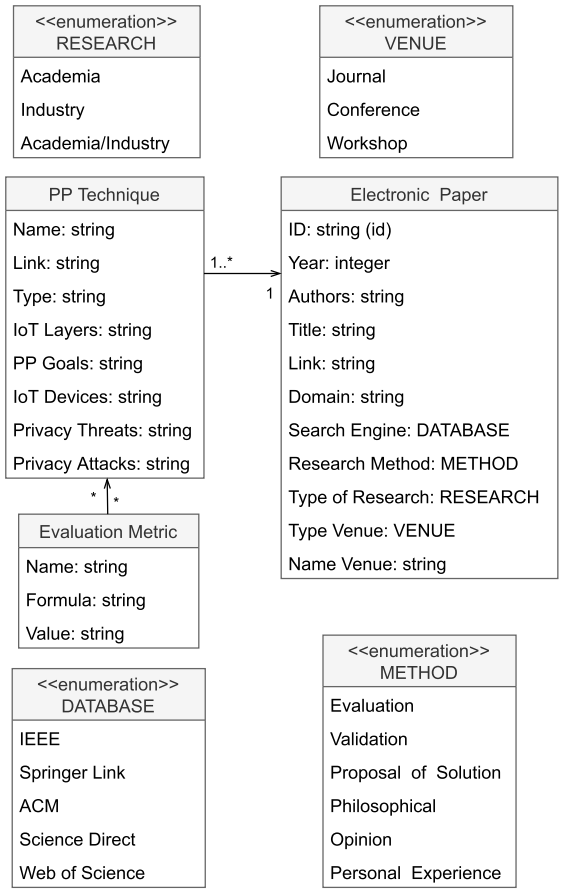

FIGURE 2. Data model of the collected answers.

- *Personal Experience Paper:* it emphasizes more on what and not on why.

In each paper, at least one *PP Technique* was implemented, and for each technique, we collected, its *Name*, the *Link* to access the source code (if available), the *Type* of solution implemented (for instance, homomorphic encryption, cryptography, blockchain, etc) in the PP technique, the *IoT Layers* covered, the *PP Goals* that were achieved, the *IoT Devices* involved the *Privacy Threats* considered, and the types of *Privacy Attacks* detected by the technique. To each technique we collected (if available) the *Evaluation Metrics* used during the evaluation of each paper.

IV. EXECUTION

The planning for this SMS with the five search engines began in August 2021 and was completed in June 2022. In this section we present the execution of the SS into the five search engines and the selection of primary studies according to the inclusion/exclusion criteria previously described. To document the review process with sufficient details [17], we describe the multi-step process of four steps we followed:

- First step (S1): the search string was used to search with the five search engines as mentioned earlier.

TABLE 5. Summary of primary studies selection.

Step	IEEE	ACM	Science Direct	Springer Link	Web of Science	Total
S1	264	113	49	313	655	**1394**
S2	229	101	37	187	334	**888**
S3	89	26	28	102	166	**411**
S4	58	12	21	77	92	**260**

- Second step (S2): we deleted the duplicates and obtained an initial set of studies by reading the title, abstract and keywords of all the papers obtained after SP1 while enforcing the inclusion and exclusion criteria.
- Third step (S3): we identified a set of studies by reading the introduction and conclusion of all the papers obtained after SP2 while enforcing the inclusion and exclusion criteria.
- Fourth step (S4): all the papers identified in SP3 were read in their entirety and the exclusion criteria were applied again. This resulted in the final set of 260 primary studies.

Table 5 breaks down the number of papers we have found by sub-phases. Row S1 in Table 5 shows the first results which were obtained by running the search string into the five search engines selected. The next two rows show the results obtained after applying S2 and S3 of the studies selection process. In the end (i.e., S4), we collected 260 primary studies for further analysis. The complete list of references of primary studies can be found in Table 7.

V. RESULTS

In order to achieve the goal of this study, i.e., addressing the research questions listed in Table 3, the 260 primary studies selected were classified according to the criteria detailed in section III, then the results of the SMS reported in this section show the answers to the ten research questions previously presented. A quantitative summary of the results for research questions RQ1-RQ10 is presented in Table 6. More details are provided in the following sub-sections.

A. PRIVACY-PRESERVATION TECHNIQUES (RQ1)

This section discusses the different PP techniques for IoT devices involved in the primary studies. As a result, we finally identified eight different PP techniques for IoT devices (see Table 7). As follows, we present the eight types of PP techniques for IoT devices that were used among the 260 primary studies. Notice that some of the following categories (i.e., Anonymization, Cryptography, and Dataflow) are refined with more specific sub-categories of privacy preservation techniques. Since this is a list of PP techniques from the primary studies we found, this list is not meant to exhaustively represent all the types of PP techniques that can be identified with IoT devices:

TABLE 6. Summary of the results.

Research Question	Answer	# Papers	Percent
RQ1: Privacy preservation Technique	Anonymization	31	11.9%
	Obfuscation	15	5.8%
	Multi-tier ML	5	1.9%
	Decentralized ML	10	3.8%
	Cryptography	154	59.2%
	Dataflow	51	19.6%
	Data summarization	6	2.3%
	Personal data stores	2	0.8%
RQ2: Privacy preservation Goals	Authentication	154	59.2%
	Authorization	17	6.5%
	Reputation system	6	2.3%
	Bandwidth sharing	5	1.9%
	Data provenance	9	3.5%
	E-health data communication	12	4.6%
	Access control	53	20.4%
	Location privacy	48	18.5%
	Identity privacy	77	29.6%
RQ3: IoT Layers	Perception layer	14	5.4%
	Network layer	251	96.5%
	Application layer	33	12.7%
RQ4: IoT Devices	General IoT	163	62.7%
	IoV	42	16.1%
	Mobile	13	5%
	IoMT	32	12.3%
	RFID	5	1.9%
	Wearable	7	2.7%
	Others	8	3.1%
RQ5: Privacy Threats	Tracking	72	27.7%
	Identification	124	47.7%
	Inventory	167	64.3%
	Profiling	65	25%
	Linkange	81	31.1%
RQ6: Privacy Attacks	Membership inference	6	2.3%
	Data inference	183	70.4%
	Attribute disclosure	76	29.2%
	Fingerprinting and Impersonation	69	26.5%
	Re-identification	51	19.6%
	Database reconstruction	40	15.4%
	Model stealing	5	1.9%
	Model inversion	12	4.6%
RQ7: Evaluation Metrics	Communication Cost	96	36.9%
	Computation Cost	136	52.3%
	Storage Cost	38	14.6%
	Success Rate	4	1.5%
	Error rate	10	3.8%
	MAE	4	1.5%
	Accuracy	6	2.3%
RQ8: Research Method	Evaluation Research	126	48.5%
	Validation Research	59	22.7%
	Proposal of Solution	85	32.7%
RQ9: Type of Research	Academia	227	87.3%
	Academia/Industry	40	15.4%
	Industry	3	1.1%
RQ10: Tool Support	Yes	9	3.5%
	No	251	96.5%

1) **Anonymization**: in general, data de-identification practices includes the removal of some sensitive attributes like names, gender, state codes, or identification numbers – commonly referred to as personally identifiable information. More sophisticated anonymization techniques are (a) *k-anonymity*: it

provides privacy protection by guaranteeing anonymity between k entries – each released data record will relate to at least k individuals in the collection even if the records are directly linked to external information [23], [24]; (b) *l-diversity*: it improves upon k-anonymity and provides protection against attribute inference attacks [25]. Each anonymized group of (generally k) users has at least l "well represented" sensitive attribute values; and (c) *t-closeness*: it improves upon its precedents and aims at limiting the distance between the probability distributions of sensitive attribute (SA) values within an anonymized group and SA values in the entire dataset [26].

2) **Obfuscation**: it entails making a design or system more complicated within a provided range, while also allowing the design or system to have the same functionality as the original [27].
3) **Multi-tier ML**: training openly available ML models on sensitive user data directly allows for data memorization. This technique proposes the introduction of multiple training levels, which can reduce the footprint of distinct and sensitive training data on output models. Semi-supervised knowledge aggregation techniques used often used in Multi-tier ML [28].
4) **Decentralized ML**: it offers a new computing paradigm for better privacy preservation. Instead of transmitting (potentially sensitive) user data to computation, a part of the computation is offloaded to end-user devices and each device contributes with partial updates to the system model [11].
5) **Cryptography**: it allows only the sender and intended recipient of a message to view its contents by applying homomorphic encryption techniques. The term is derived from the Greek word kryptos, which means hidden. Homomorphic encryption allows binary operations, such as addition and multiplication, on encrypted data directly, without the need of decrypting it in advance [29]. Homomorphic schemes are further classified as (a) *partially homomorphic encryption*: that supports limited operations like addition and multiplication as well as other operations on ciphertexts, but does not support arbitrary computation on ciphertexts [30]; and (b) *fully homomorphic encryption*: that supports multiplication and addition, and also support quadratic function and arbitrary computation on ciphertexts. Classifiers designed using this schema are privacy-preserving by nature and are better suited for real-world applications in terms of privacy guarantees because they support arbitrary computation [11].
6) **Dataflow**: it proposes the creation of dataflow models with respective permissions at different privacy level to ensure user privacy and transparent accountability. There are two main types of data flow models used to ensure privacy (a) *blockchain* which is used for verifiability and accountability of data collection, storage and access in IoT environments [31]; and (b) *privacy-based programming languages*, which require information flows and privileges to be declared beforehand, so all the data elements are attached to respective policies [32].
7) **Data summarization**: it is a process of creating a concise, yet informative, version of data to preserve the privacy of the original data. The terms concise and informative are quite generic and depend on application domains. Summarization has been extensively studied in many domains including text analysis, network traffic monitoring, financial domain, health sector, and many others [33]. The summary definition or utility is dependent on the purpose of using it; for example network traffic privacy preservation.
8) **Personal data stores**: they are services to let an individual store, manage and deploy their key personal data in a highly secure and structured way.[1] They give the user a central point of control for their personal information. The user's data attributes being managed by the service may be stored in a co-located repository, or they may be stored in multiple external distributed repositories, or a combination of both. Attributes from a personal data store may be accessed via another application. Users of the same personal data store instance may be allowed to selectively share sets of data with other users.

TABLE 7. Privacy-preservation techniques and primary studies.

Privacy-preservation technique	Primary studies
Anonymization (31 papers)	[34]–[64]
Obfuscation (15 papers)	[64]–[78]
Multi-tier ML (5 papers)	[79]–[83]
Decentralized ML (10 papers)	[78], [84]–[92]
Cryptography (154 papers)	[48], [51], [59], [62], [63], [76], [83], [85], [86], [92]–[236]
Dataflow (51 papers)	[61], [82], [83], [89], [101], [165], [216], [221], [223], [237]–[278]
Data summarization (6 papers)	[279]–[284]
Personal data stores (2 papers)	[285], [286]

Notice that Table 6 (second row, RQ1) shows a total number of 274 PP techniques rather than 260, which is the number of primary studies because there were papers that used more than one PP technique. More than half (59.2%) primary studies (154 out of 260) present PP techniques implementing cryptography schemes. The second most used PP techniques implemented involve Dataflow (19.6%). Table 7 shows the primary studies discussing the eight PP technique for IoT devices identified in this study.

[1] https://web.archive.org/web/20151001065833/https://mydex.org/understand-pds/

RQ1 answer: We coalesced a set of eight techniques used to protect the privacy of IoT devices. Cryptography is the most used PP technique for IoT devices.

B. PRIVACY-PRESERVATION GOALS (RQ2)

To answer RQ2, we use the nine categories identified by Akil et al. [1] in order to represent the PP goals that can be identified in literature (1) Privacy-enhancing *Authentication*, (2) Privacy-enhancing *Authorization*, (3) Privacy-enhancing *Reputation system*, (4) Privacy-enhancing *Bandwidth sharing*, (5) Privacy-preserving *Data provenance*, (6) Protection of *E-health data communication*, (7) *Access control*, (8) *Location privacy*, and (9) *Identity privacy*. Table 6 (fourth row, RQ2) presents the results of the PP goals most involved with the 260 primary studies. We shorten the names of the PP goals 1-6 to be able to fit them in Table 6. Most of the primary studies (154 out of 260, 59.2%) describe PP techniques used to ensure that communication over IoT devices takes place only between the right parties without disclosure of information to unauthorized parties. In other words, they focus on enhancing the authentication of of the users of IoT devices. Other PP goals that were covered by a large number of primary studies were identity privacy (29.6%), access control (20.4%), and location privacy (18.5%). Notice that Table 6 (third row, RQ2) shows a total number of 381 PP goals rather than 260, which is the number of primary studies because there were papers that covered more than one PP goal.

RQ2 answer: The majority of the primary studies focus on creating PP techniques used to improve the authentication process to access IoT devices. Other popular PP goals targeted by the authors are related to identity privacy, access control and location privacy.

C. IoT LAYERS (RQ3)

There are a lot of components that need to work together in order for the IoT devices to function as intended. The IoT architecture is a framework that defines these physical components, the functional organization and configuration of the network, operational procedures and the data formats to be used. There are many standards to reference IoT architecture as it encompasses a variety of technologies. In this paper, specifically in Table 6 (fourth row, RQ3), we consider the following three IoT layers [287]:

- **L1: perception layer** – consisting of the sensory devices collecting data. This is the physical layer of the architecture where the sensors and connected devices come into play as they gather various amounts of data as per the need of the device. Thi layer can be the edge devices, sensors, and actuators that interact with their environment.
- **L2: network layer** – responsible for collecting, aggregating, processing, and transmitting the data from the perception layer. In other words, the network layer's job consists of collecting all of these devices needs to be transmitted and processed. It connects these devices to other smart objects, servers, and network devices and it handles the transmission of all of the data.
- **L3: application layer** – consisting of all the applications and solutions driven by the sensory data that are available to the users. The application layer is what the user interacts with and what is responsible for delivering application-specific services to the user. This can be a smart home implementation, for example, where users tap a button in the app to turn on a coffee maker.

Almost every paper (96.5%) discussed PP techniques involving the Network layer, followed by the Application layer (12.7%) and Perception layer (5.4%).

RQ3 answer: The great majority of the primary studies present PP techniques for IoT devices involving the Network layer.

D. IoT DEVICES (RQ4)

The majority of the primary studies (163 out of 260, 62.7%) discussed PP techniques that were developed not to be used with specific IoT devices. "General IoT" is used as a generic category when the authors did not present a specific IoT device on which their PP technique could be applied. We finally identified a set of ten different types of IoT devices. Table 6 (fifth row, RQ4) presents the six IoT devices that were the most covered among the 260 primary studies and that was involved in at least five papers: 42 papers (16.1%) presented PP techniques for Internet of Vehicles (IoV) devices, 32 papers (12.3%) focused on Internet of Medical Things (IoMT) devices, 13 papers (5%) on Mobile devices, 7 papers (2.7%) on Wearable devices, and 5 papers (1.9%) on Radio-frequency identification (RFID) devices. The other IoT device types identified are: Fog-Based IoT (3 papers), Industrial IoT devices (2 papers), Internet of Underwater Things (IoUT) (2 papers), and Agricultural IoT devices (1 paper).

RQ4 answer: We identified a set of ten different categories of IoT devices. However, most of the authors did not discuss a specific IoT device to apply the discussed PP techniques.

E. PRIVACY THREATS (RQ5)

Table 6 (sixth row, RQ5) presents the privacy threats discussed by the authors of the 260 primary studies. Privacy Threat means any threat or connected series of threats to unlawfully use or publicly disclose private data misappropriated from a user for the purpose of demanding money, securities or other tangible or intangible property of value from the user.[2] In particular, a privacy threat occurs when an attacker is able to link a record owner to a sensitive attribute in a published data table. These are specified as record linkage, attribute linkage, and table linkage, respectively [288]. In this study, we identified a set of five privacy threats. Notice that the following list of privacy threats is obtained from the primary studies we found, this list is not meant to exhaustively

[2] https://www.lawinsider.com/

represent all the privacy threats of PP techniques for IoT devices. The privacy threats identified in this study are:

1) **Tracking**: it denotes the threat of determining an individual's physical location and recording it over time without authorization or consent. The attacker receive continuous updates of user location in real time, which can be used to identify the user's location routes, predict future locations, and/or frequently traveled routes with sufficient accuracy using a user's mobility patterns [289]. This privacy threat affects all three IoT layers.
2) **Identification**: it refers to the threat of associating a given identifier with an individual. For example, the attacker is able to gather sporadic updates of user location, which can be used to identify the user's frequently visited locations (such as home or work place) and these places can be used to disclose a user's identity [289]. This privacy threat affects L2.
3) **Inventory**: it mainly arises when there are limited communication capability of the sensor devices, which enables unauthorized access or collection of data. Unauthorized parties can also observe the communication pattern and deduce the presence of devices as well as their specification. In addition, inventories can give information on user preferences which may be exploited by burglars for targeted break-ins [11]. This privacy threat affects all three IoT layers.
4) **Profiling**: it focuses on the activity of profiling a given user. This threat often results in unwanted advertisements, price discrimination, or biased automatic decisions. This type of privacy threat may not have the required information to identify the user but can use the collected data to profile the user. For example, an attacker can identify which hospitals or religious places a user visits, or which places the user goes for shopping, and how often [289]. This privacy threat affects L2.
5) **Linkange**: it occurs when IoT platforms are exploited and correlated for record linkage that reveals user's identity. In particular, this concerns the combination of data collected from independent sources that can reveal information about individuals that they originally did not consent to reveal [290]. This privacy threat affects L2.
6) **Lifecycle**: it happens when there is a change in the owner of a given IoT device. IoT devices request the sizeable amount of personal data when the user purchase a new device. This data often can not be completely removed upon a memory wipe before transfer of a device to a different user [11]. This privacy threat affects L2.

167 out of 260 primary studies (64.3%) discussed PP techniques for IoT devices involving inventory threats. This was followed by identification threats (47.7%) and linkage threats (31.1%). Notice that Table 6 (seventh row, RQ6) shows a total number of 509 privacy threats rather than 260, which is the number of primary studies because there were papers that involved more than one privacy threat.

RQ5 answer: The majority of authors presented PP techniques for IoT that involved inventory privacy threats.

F. PRIVACY ATTACKS (RQ6)

Table 6 (seventh row, RQ6) presents the privacy attacks covered by the authors of the 260 primary studies. As follows, we present the definitions of the nine types of privacy attacks covered by the primary studies discussed in this paper. Since this is a list of privacy attacks from the primary studies we found, this list is not meant to exhaustively represent all the types of privacy attacks that can be identified with IoT devices:

1) **Membership inference**: it allows an attacker to query a trained machine learning (ML) model to predict whether or not a particular example was contained in the model's training dataset. In particular, the attacker can reveal whether or not a specific data record was used to train the ML model, given that the attacker has knowledge of the ML model and the individual data record [291].
2) **Data inference**: it tries to recover information about the data or queries by combining leakage with publicly-available information (e.g., census data or language statistics) and makes tailored queries to the system and observing the responses to see if any information about underlying records is leaked. The most well-known example of an inference attack is frequency analysis which is used to break classical ciphers [292]. This attack is commonly associated with encryption-based privacy-preserving solutions.
3) **Attribute disclosure**: it happens when an individual is linked to a particular record in the released table. In particular, attribute disclosure occurs when new information about some individuals is revealed, i.e., the released data makes it possible to infer the characteristics of an individual more precisely than it would be possible before the data release. For instance, an observer of a released table may incorrectly perceive that an individual's sensitive attribute takes a particular value, and behave accordingly based on the perception. This can harm the individual, even if the perception is incorrect [26]. This attack commonly uses linkage from multiple data sources to infer user information.
4) **Fingerprinting and Impersonation**: it is carried out when an adversary aims to seize the identity of a legitimate smart object, such as access credentials of the device, to act on behalf of the legitimate device (e.g., injecting fake data) that may be compromising privacy preference enforcement [293]. Device fingerprinting can be a privacy risk. For example, learning that someone owns an IoT blood sugar monitor or pacemaker

effectively reveals a diabetes or heart-disease diagnosis, respectively. Internet browsing habits are also subject to privacy breaches by website fingerprinting attacks using network traffic metadata. Network traffic metadata has also been used to perform user and device fingerprinting by a variety of techniques, including correlating IP ID header fields, clock skews from the TCP timestamp option, and hidden Markov models trained on Netflow data [294].

5) **Re-identification**: it involves an attacker that can use linkage to combine data from multiple collections to re-identify a record from outsourced, published or open data records [295]. Re-identification is a common type of attack that is often detected, for instance, in 1997 from the records released by a health insurance company, a voters list was used for reidentification of a government official's health record.
6) **Database reconstruction**: it aims at reconstructing a private dataset from public aggregate information such as statistical data that is published by agencies for research or information purposes. Typically, these datasets contain sensitive information about individuals, whose privacy needs to be protected. This may allow attackers to partial or full reconstruct the original database records, which may lead to the identification or unintended profiling of users of the targeted database [296].
7) **Model stealing**: an attacker with query access to a target model can steal its parameters or functionality. In other words, it works by querying the target model with samples and using the model responses to forge a replicated model [297]. This attack can serve different purposes: (a) it can copy an effective model at a low cost for its functionality, (b) it can copy the model to facilitate the design of other attacks (membership inference, adversarial examples, etc.) with a white-box set up, and (c) it can reveal sensitive information about the training data used for these models and can result in unintended profiling of users.
8) **Model inversion**: it is a type of privacy attack that tries to recover the training set given access only to a trained classifier [298]. By observing ML model predictions, model inversion attacks enable adversaries to extract underlying training data of the individuals [299]. A complete training set is not always extracted as a result of this attack, but, the attacker may extract an average representation of inputs that are similarly classified.

The majority of papers, 70.4% of them, discuss data inference attacks. Notice that Table 6 (seventh row, RQ6) shows a total number of 442 PP privacy attacks rather than 260, which is the number of primary studies because there were papers that involved more than one privacy attack.

RQ6 answer: The majority of the authors discussed privacy data interference attacks.

G. EVALUATION METRICS (RQ7)

Table 6 (eighth row, RQ7) presents the most used metrics that were calculated to evaluate the PP techniques for IoT devices. 52.3% of the authors of the primary studies used computation cost as a metric to evaluate the proposed PP techniques. The other most used evaluation metrics were communication cost (36.9%) and storage cost (14.6%). Other evaluation metrics used by the authors were error rate, accuracy, success rate, and mean absolute error (MAE). Notice that Table 6 shows a total number of 294 different evaluation metrics rather than 260, which is the number of selected primary studies because there were papers that used more than one evaluation metric.

RQ7 answer: Across primary studies, PP techniques for IoT devices are evaluated using a variety of metrics. Most primary studies evaluate PP techniques by calculating computation cost, communication cost, and storage cost.

H. RESEARCH METHOD (RQ8)

Table 6 (ninth row, RQ8) presents the results of the research type facet classification where 48.5% (126 of 260 papers) of the primary studies proposed evaluation research of new PP techniques for IoT devices, 32.7% (85 of 260 papers) presented solution papers, and 22.7% (59 of 260 papers) presented validation research. We did not find any personal experience paper, philosophical paper or opinion paper (0 for all of them). This suggests the field is about evaluating the PP techniques for IoT devices that have been proposed.

RQ8 answer: The majority of the authors presented the new PP techniques for IoT devices in practice and presented an evaluation of such techniques.

I. TYPE OF RESEARCH (RQ9)

Table 6 (tenth row, RQ9) shows that out of 260 primary studies selected, 227 of them (87.3%) presented research developed in academia, 40 papers (15.4%) proposed research that was either (a) developed in collaboration with an industry partner, or (b) was evaluated on industrial datasets, and only three papers were from the industry. In particular, those three research papers were carried out at: (1) Tobacco Zhejiang Industrial Ltd, China, (2) IDEMIA & EURECOM, France, and (3) Information Technologies Institute, Hellas.

RQ9 answer: The majority of primary studies present research that was developed in academia.

J. TOOL SUPPORT (RQ10)

Table 6 (eleventh row, RQ10) shows that only nine PP techniques for IoT devices are implemented and publicly available (3.5%). The remaining 261 primary studies representing the most significant number of publications (96.5%) did not share any source code. Table 8 presents the nine primary studies that share the implementation of the proposed PP techniques. In particular, the first column "Reference" indicates the reference of the primary study, the second column "PP technique" refers to the PP technique used to protect the privacy of IoT devices' users, the third column "IoT

Device'' describes the IoT device to which the technique was used. Finally, the fourth column ''Link'' provides the URL to access the code of the PP technique.

RQ10 answer: The great majority of the primary studies do not share the implementation of the PP techniques discussed. Only 9 out of 260 papers share the code implementation of their solutions.

VI. ADDITIONAL RESULTS

Table 9 shows the publication venues with the most significant number of papers among the primary studies. We present the venues where authors have published at least three articles. The 260 primary studies were published across 115 different venues. Out of 260 articles, 232 were journal articles (89.2%) and 28 conference papers (10.8%)

The distribution per year of the 260 primary studies is shown in Figure 3. Between 2016 and 2018, the number of publications slowly increased from 4 to 18 articles a year. We also notice that starting from 2017 until 2021, the number of papers considerably increased. There are no publications decreased in 2022 because the search was made at the end of 2021 (i.e., October 2021).

A. LESSONS LEARNED

In this paper, we answered 10 RQs to identify the state of the art of privacy-preservation techniques for IoT devices. As follows, we list the five lessons learned from the research conducted in this manuscript:

1) **Privacy-preservation techniques**. Protection against direct leakage, i.e., the privacy of training data, as well as indirect leakage, i.e., the privacy of parameters, are the main challenges to be addressed. For techniques where training data is exposed (direct leakage), cryptography encryption, more specifically homomorphic, seems to be successful in protecting private data during both collaborative and individual learning processes. Not surprisingly, cryptography resulted in being the most used PP technique for IoT devices. Further investigation may also be needed for other PP techniques, such as multi-tier ML, data summarization, and personal data stores.
2) **IoT Layers**. The network layer poses some general security problems related to data integrity and confidentiality, such as unauthorized access to networks, eavesdropping, confidentiality and integrity damage, DDoS attacks, and man-in-the-middle attacks [300]. Although existing network protocols implement highly secured measures, the great majority of the primary studies present PP techniques for IoT devices involving the network layer. One reason for this trend is that existing security mechanisms are not always applicable to IoT devices and may lead to creating barriers rather than connections between different machines. Therefore, the current research focuses on developing new methods applicable to improve security, interoperability, and coordination at the network layer of IoT devices.
3) **Evaluation metrics:** The evaluation metrics used across the 260 primary studies are not uniform. In particular, many papers only assess the computation cost of, and the result is one-sided (see results RQ7). Therefore, the primary studies that use a variety of different evaluation metric combinations to provide their research results are difficult to compare with one another.
4) **Reproducibility of experiments:** We collected the code implementation of only nine privacy-preservation techniques out of 260 primary studies (RQ10). In other words, we found that many papers on privacy-preservation techniques for IoT devices do not report adequate information on how to access the implementation of their source code. In addition, the majority of the primary studies did not present a clear methodology to fully understand their work (privacy-preservation techniques details, evaluation of the solution, etc.). We encourage researchers implementing privacy-preservation techniques for IoT devices to consider the aspect of reproducibility when designing and reporting their approaches. We believe that publicly sharing the code implementations of the privacy-preservation techniques would help other researchers quickly replicate the results of published research building upon those ideas.
5) **Industrial research:** As shown in RQ9, most of the primary studies were conducted in academia. There is an urgent need for privacy-preservation techniques for IoT devices developed based on current industry requirements and tested on industrial data.

VII. THREATS TO VALIDITY

This section describes the main threats to the validity of our SMS. In particular, publication bias, selection bias, inaccurate data extraction, and misclassification are the primary risks to the validity of an SMS like ours [301].

A. CONSTRUCT VALIDITY

The omission of pertinent research poses a significant hazard to an SMS. Therefore, two co-authors undertook a collaborative evaluation procedure with explicit exclusion and inclusion criteria and quality evaluation for research qualification and categorization to mitigate this threat.

B. INTERNAL VALIDITY

1) SEARCH STRINGS

we utilized generic terminology associated with PP techniques and IoT devices in our search queries. Then, to select the primary studies discussing the PP techniques for IoT devices, we strictly applied our inclusion and exclusion criteria.

TABLE 8. PP techniques for IoT devices publicly available.

Reference	PP Technique	IoT Device	Link
[113]	Cryptography	Mobile	http://doi.ieeecomputersociety.org/10.1109//TSC.2016.2594071
[73]	Obfuscation	General IoT	https://github.com/TrishaDatta/PrivacyPreservingTrafficObfuscation
[88]	Decentralized ML	General IoT	https://github.com/OpenMined/PySyft
[138]	Cryptography	IoT	https://github.com/akirakanaoka/KUPEKS
[273]	Dataflow	Mobile	https://github.com/emsecurity/BPRF
[206]	Cryptography	General IoT	https://github.com/smx12345/code/blob/master/healthcareIET.pv
[225]	Cryptography	IoV	https://github.com/miracl/MIRACL/
[277]	Dataflow	IoMT	https://github.com/MohammadHosseinChinaei/Blockchain-based-Witnessing
[228]	Cryptography	Smart environment	https://github.com/miracl/MIRACL

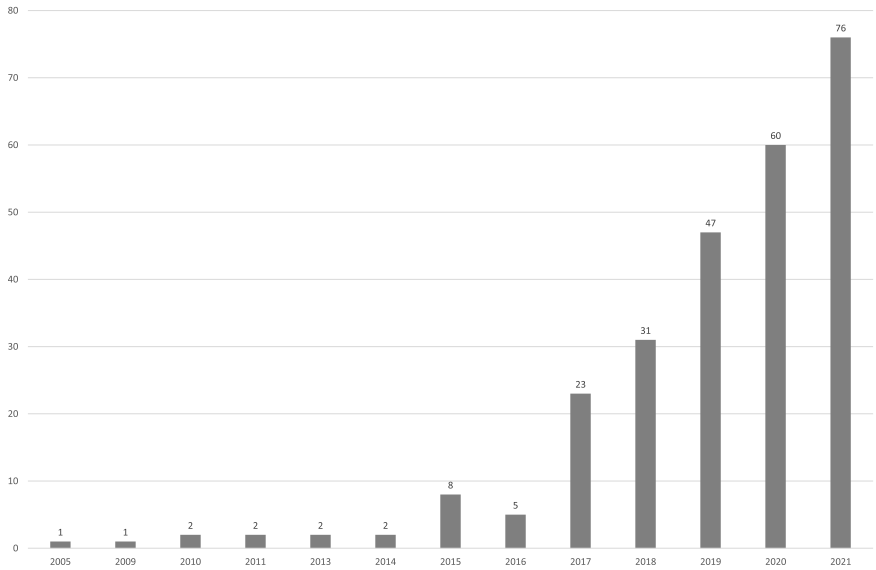

FIGURE 3. Number of primary studies per year.

2) PRIMARY STUDY SELECTION

the selection bias describes how the selection of the primary studies might skew the statistical analysis results. It is not feasible to thoroughly discuss every article that has been published about a given subject. We are aware that not all pertinent publications may have been included in our study. A study's inclusion or exclusion might be arbitrary. To mitigate this problem, the first two co-authors worked together to select the publications, employing predefined criteria to exclude research papers that were out of the scope of our study.

3) DATA EXTRACTION

missing or incorrectly interpreted information can be a problem when information is manually extracted from the primary studies. At the moment when we decided what was (and was not) pertinent to the scope of this study, during this procedure, there may have been a chance for subjectivity. The results could have been impacted by this interpretation. To ensure an unbiased data extraction process, we structured the selection of the papers, designed and followed a multi-phase procedure to execute the SMS, defined ten research questions in advance, and managed the selection of papers. Additionally, one co-author extracted the data from each study. In cases where the material was ambiguous or difficult to comprehend, a second co-author confirmed the data extraction. Any differences of opinion on the data extraction were settled during discussion meetings among all of the authors of this paper.

C. EXTERNAL VALIDITY

As it is impossible to completely cover every publication written on our topic, we acknowledge that some relevant

TABLE 9. Number of primary studies per venue.

Venue	#
Internet of Things (IEEE)	26
Access (IEEE)	22
Multimedia Tools and Applications (Springer)	15
The Journal of Supercomputing (Springer)	10
Cluster Computing (Springer)	9
Future Generation Computer Systems (Elsevier)	8
Personal and Ubiquitous Computing (Springer)	7
Computer Networks (Elsevier)	5
Transactions on Vehicular Technology (IEEE)	5
Journal of Network and Computer Applications (Elsevier)	5
Security and Communication Networks (Hindawi)	5
Transactions on Information Forensics and Security (IEEE)	4
Transactions on Network Science and Engineering (IEEE)	4
Information Sciences (Elsevier)	4
Science China Information Sciences (Springer)	4
SN Computer Science (Springer)	4
Computers & Security (Elsevier)	3
Transactions on Industrial Informatics (IEEE)	3
Transactions on Intelligent Transportation System (IEEE)	3
International Journal of Communication Systems (Wiley)	3
International Journal of Distributed Sensor Networks (SAGE)	3
Journal of Cloud Computing (Springer)	3
Journal of Parallel and Distributed Computing (Elsevier)	3
Neural Computing & Applications (Springer)	3
Sensors (MDPI)	3
The International Journal of Information Security (Springer)	3
Others	79

papers might not have been included. We used five search engines to collect journals, conferences and workshops proceedings that are relevant to PP techniques for IoT devices; we did not consider grey literature [17] (e.g., PhD theses, books) or unpublished results (e.g., technical reports) because these might affect the validity of our results because they were not peer-reviewed. Selection bias refers to the distortion of a statistical analysis owing to the criteria used to select publications.

D. RELIABILITY

The degree of our study's capacity to be replicated poses a threat to reliability and validity. The replication of this study is possible as long as all steps of the search process presented in Section III and shown in Figure 1 are followed. However, there may be discrepancies in the results due to probable disagreements over data extraction. To mitigate this issue, we described every step in our search process in detail provided a high-level summary of PP techniques used for IoT devices that can be used as a reference for classifying future PP-related studies.

VIII. CONCLUSION

In the last few years, researchers have proposed a sizable number of privacy preservation (PP) techniques for Internet of Things (IoT) devices. However, given that most research is represented by informal literature surveys or focusing on the presentation of new techniques, to the best of our knowledge, no systematic study on PP techniques for IoT devices has been published in the literature. In this paper, we report the findings of a Systematic Mapping Study (SMS) of the literature to determine and assess the current state of the art on PP techniques for IoT devices. The SMS was executed in accordance with well-accepted best practices [15], [17]. A total of 260 primary studies were chosen from an initial pool of 1394 publications gathered from five search engines (IEEE, ACM, Science Direct, Springer Link, and Web of Science) by adhering to a strict selection methodology guided by ten research questions. Following that, the primary studies were categorized using a number of criteria derived from those research questions.

By carrying out our thorough SMS, we have discovered many findings. We coalesced a set of eight techniques used to protect the privacy of IoT devices. The majority of the authors (59.2%) used cryptographic techniques to preserve the privacy of IoT devices. Most of PP techniques (96.5%) discussed in the primary studies do not share the implementation of the proposed solutions. Only 9 out of 260 papers (3.5%) share the code implementation of their solutions. The PP goals most studied by the authors of the primary studies focus on creating PP techniques used to improve the authentication process to access IoT devices (59.2%). Other popular PP goals targeted by the authors are related to identity privacy (29.6%), access control (20.4%), and location privacy (18.5%). We identified a set of nine different categories of IoT devices: Internet of Vehicles (IoV), Internet of Medical Things (IoMT), Mobile, Wearable, Radio-frequency identification (RFID), Fog-Based IoT, Industrial IoT, Internet of Underwater Things (IoUT), and Agricultural IoT. However, most of the authors did not discuss a specific IoT device to apply the discussed PP techniques. The majority of authors presented PP techniques for IoT devices that (a) involved inventory privacy threats (64.3%, 167 out of 260 papers), (b) discussed privacy data interference attacks (70.4%), (c) involved the network layer (96.5%), (d) was developed entirly in academia (87.3%), and (e) discussed techniques in practice and presented an evaluation of such techniques (48.5%). Across primary studies, PP techniques for IoT devices are evaluated using a variety of metrics. Most primary studies evaluate PP techniques by calculating computation cost (52.3%), communication cost (36.9%), and storage cost (14.6%). The number of primary studies identified has grown in recent years, especially after 2017. Comparing this outcome to earlier years makes it more clear; while 237 publications in total were published between 2017 and 2021, only 23 were published prior to 2016, an increase of more than ten times. This implies that the subject of PP techniques for IoT devices is very active right now, with many researchers engaged.

We consider this SMS to be pertinent for practice and research in developing PP techniques for IoT devices. In particular, PP developers may utilize the presented findings to determine which tools best suit their project's goals in terms of the evaluation metrics available and the IoT devices that will profit from the suggested PP techniques. Furthermore, the analysis of the results helps PP researchers and practitioners choose the tools for developing new PP techniques or choose a set of tools to work together during the PP techniques development process.

This SMS also identifies a number of issues and directions for further study. It may be especially useful in guiding new research with discussions of emerging PP techniques trends, such as personal data stores, data summarization, multi-tier machine learning, and decentralized machine learning, which have not yet been put into practice to protect the privacy of IoT devices. Additionally, as the majority of the initial research was carried out in academia, there is a pressing need for PP techniques for IoT devices to be created based on the most recent industry specifications.

ACKNOWLEDGMENT

The authors would like to thank Kyra Pitapit (Texas A&M University—Central Texas, Killeen, USA) for the help provided on the paper.

REFERENCES

[1] M. Akil, L. Islami, S. Fischer-Hubner, L. A. Martucci, and A. Zuccato, "Privacy-preserving identifiers for IoT: A systematic literature review," *IEEE Access*, vol. 8, pp. 168470–168485, 2020, doi: 10.1109/ACCESS.2020.3023659.

[2] F. Khan, A. Ur Rehman, J. Zheng, M. A. Jan, and M. Alam, "Mobile crowdsensing: A survey on privacy-preservation, task management, assignment models, and incentives mechanisms," *Future Gener. Comput. Syst.*, vol. 100, pp. 456–472, Nov. 2019, doi: 10.1016/j.future.2019.02.014.

[3] A. A. A. Sen, F. A. Eassa, K. Jambi, and M. Yamin, "Preserving privacy in Internet of Things: A survey," *Int. J. Inf. Technol.*, vol. 10, no. 2, pp. 189–200, Jun. 2018.

[4] I. Ali, E. Khan, and S. Sabir, "Privacy-preserving data aggregation in resource-constrained sensor nodes in Internet of Things: A review," *Future Comput. Informat. J.*, vol. 3, no. 1, pp. 41–50, Jun. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2314728817300594

[5] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: Threats and challenges," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2728–2742, 2014, doi: 10.1002/sec.795.

[6] O. Amaral, S. Abualhaija, D. Torre, M. Sabetzadeh, and L. C. Briand, "AI-enabled automation for completeness checking of privacy policies," *IEEE Trans. Softw. Eng.*, vol. 48, no. 11, pp. 4647–4674, Nov. 2022.

[7] D. Torre, M. Alférez, G. Soltana, M. Sabetzadeh, and L. C. Briand, "Modeling data protection and privacy: Application and experience with GDPR," *Softw. Syst. Model.*, vol. 20, no. 6, pp. 2071–2087, 2021, doi: 10.1007/s10270-021-00935-5.

[8] C. Perera, M. Barhamgi, A. K. Bandara, M. Ajmal, B. Price, and B. Nuseibeh, "Designing privacy-aware Internet of Things applications," *Inf. Sci.*, vol. 512, pp. 238–257, Feb. 2020, doi: 10.1016/j.ins.2019.09.061.

[9] P. Pullonen, J. Tom, R. Matulevicius, and A. Toots, "Privacy-enhanced BPMN: Enabling data privacy analysis in business processes models," *Softw. Syst. Model.*, vol. 18, no. 6, pp. 3235–3264, 2019, doi: 10.1007/s10270-019-00718-z.

[10] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 746–789, 1st Quart., 2019, doi: 10.1109/COMST.2019.2944748.

[11] S. Imtiaz, R. Sadre, and V. Vlassov, "On the case of privacy in the IoT ecosystem: A survey," in *Proc. Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2019, pp. 1015–1024, doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00177.

[12] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," *Future Gener. Comput. Syst.*, vol. 76, pp. 540–549, Nov. 2017, doi: 10.1016/j.future.2017.03.001.

[13] R. Ali, A. Ali, F. Iqbal, A. M. Khattak, and S. Aleem, "A systematic review of artificial intelligence and machine learning techniques for cyber security," in *Big Data and Security*, Y. Tian, T. Ma, and M. K. Khan, Eds. Singapore: Springer, 2019, pp. 584–593.

[14] S. Desai, R. Alhadad, N. Chilamkurti, and A. Mahmood, "A survey of privacy preserving schemes in IoE enabled smart grid advanced metering infrastructure," *Cluster Comput.*, vol. 22, no. 1, pp. 43–69, Mar. 2019.

[15] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *Proc. Electron. Workshops Comput.*, Jun. 2008, pp. 26–27. [Online]. Available: http://ewic.bcs.org/content/ConWebDoc/19543

[16] D. Budgen, M. Turner, P. Brereton, and B. A. Kitchenham, "Using mapping studies in software engineering," in *Proc. 20th Annu. Workshop Psychol. Program. Interest Group (PPIG)*, Lancaster, U.K., Sep. 2008, p. 20. [Online]. Available: http://ppig.org/library/paper/using-mapping-studies-software-engineering

[17] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele Univ. Durham Univ. Joint Rep., Tech. Rep. EBSE 2007-001, 2007. [Online]. Available: http://www.dur.ac.uk/ebse/resources/Systematic-reviews-5-8.pdf

[18] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Inf. Softw. Technol.*, vol. 55, pp. 2049–2075, Dec. 2013, doi: 10.1016/j.infsof.2013.07.010.

[19] K. Peng, M. Li, H. Huang, C. Wang, S. Wan, and K.-K.-R. Choo, "Security challenges and opportunities for smart contracts in Internet of Things: A survey," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12004–12020, Aug. 2021.

[20] S. Wan, M. Li, G. Liu, and C. Wang, "Recent advances in consensus protocols for blockchain: A survey," *Wireless Netw.*, vol. 26, pp. 5579–5593, Nov. 2020.

[21] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *J. Syst. Softw.*, vol. 80, no. 4, pp. 571–583, 2007, doi: 10.1016/j.jss.2006.07.009.

[22] R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: A proposal and a discussion," *Requir. Eng.*, vol. 11, no. 1, pp. 102–107, Mar. 2006, doi: 10.1007/s00766-005-0021-6.

[23] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002, doi: 10.1142/S0218488502001648.

[24] L. Sweeney, "Achieving K-anonymity privacy protection using generalization and suppression," *Int. J. Unc. Fuzz. Knowl. Based Syst.*, vol. 10, no. 5, pp. 571–588, 2002, doi: 10.1142/S021848850200165X.

[25] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Discovery From Data*, vol. 1, no. 1, p. 3, Mar. 2007, doi: 10.1145/1217299.1217302.

[26] N. Li, T. Li, and S. Venkatasubramanian, "T-closeness: Privacy beyond k-anonymity and l-diversity," in *Proc. IEEE 23rd Int. Conf. Data Eng.*, Apr. 2007, pp. 106–115, doi: 10.1109/ICDE.2007.367856.

[27] S. Bhunia and M. Tehranipoor, "Physical attacks and countermeasures," in *Hardware Security*, S. Bhunia and M. Tehranipoor, Eds. San Mateo, CA, USA: Morgan Kaufmann, 2019, pp. 245–290. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128124772000150

[28] N. Papernot, M. Abadi, U. Erlingsson, I. J. Goodfellow, and K. Talwar, "Semi-supervised knowledge transfer for deep learning from private training data," in *Proc. 5th Int. Conf. Learn. Represent., (ICLR)*, Apr. 2017, pp. 1–14. [Online]. Available: https://openreview.net/forum?id=HkwoSDPgg

[29] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: A survey," *Comput. Commun.*, vols. 91–92, pp. 17–28, Oct. 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366416302572
[30] R. Bendlin, I. Damgård, C. Orlandi, and S. Zakarias, "Semi-homomorphic encryption and multiparty computation," in *Advances in Cryptology EUROCRYPT 2011*, K. G. Paterson, Ed. Berlin, Germany: Springer, 2011, pp. 169–188.
[31] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT data management using BlockChain and trusted execution environment," in *Proc. IEEE Int. Conf. Inf. Reuse Integr. (IRI)*, Jul. 2018, pp. 15–22, doi: 10.1109/IRI.2018.00011.
[32] I. Zavalyshyn, N. O. Duarte, and N. Santos, "HomePad: A privacy-aware smart hub for home environments," in *Proc. IEEE/ACM Symp. Edge Comput. (SEC)*, Oct. 2018, pp. 58–73, doi: 10.1109/SEC.2018.00012.
[33] M. Ahmed, "Data summarization: A survey," *Knowl. Inf. Syst.*, vol. 58, no. 2, pp. 249–273, Feb. 2019, doi: 10.1007/s10115-018-1183-0.
[34] A. El Mougy and S. Sameh, "Preserving privacy in wireless sensor networks using onion routing," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Jun. 2018, pp. 1–6, doi: 10.1109/ISNCC.2018.8530968.
[35] Y. Sun, Z. Tian, Y. Wang, M. Li, S. Su, X. Wang, and D. Fan, "Lightweight anonymous geometric routing for Internet of Things," *IEEE Access*, vol. 7, pp. 29754–29762, 2019, doi: 10.1109/ACCESS.2019.2902621.
[36] B. D. Deebak, F. Al-Turjman, and A. Nayyar, "Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care," *Multimedia Tools Appl.*, vol. 80, no. 11, pp. 17103–17128, Nov. 2020, doi: 10.1007/s11042-020-10134-x.
[37] H. Hamadeh and A. Tyagi, "An FPGA implementation of privacy preserving data provenance model based on PUF for secure Internet of Things," *Social Netw. Comput. Sci.*, vol. 2, no. 2, p. 65, Apr. 2021, doi: 10.1007/s42979-020-00428-0.
[38] D. Liao, G. Sun, H. Li, H. Yu, and V. Chang, "The framework and algorithm for preserving user trajectory while using location-based services in IoT-cloud systems," *Cluster Comput.*, vol. 20, no. 3, pp. 2283–2297, 2017, doi: 10.1007/s10586-017-0986-1.
[39] W. Mahanan, W. A. Chaovalitwongse, and J. Natwichai, "Data anonymization: A novel optimal k-anonymity algorithm for identical generalization hierarchy data in IoT," *Service Oriented Comput. Appl.*, vol. 14, no. 2, pp. 89–100, Jun. 2020, doi: 10.1007/s11761-020-00287-w.
[40] K.-S. Wong and M. H. Kim, "Towards a respondent-preferred k I-anonymity model," *Frontiers Inf. Technol. Electron. Eng.*, vol. 16, no. 9, pp. 720–731, Sep. 2015, doi: 10.1631/FITEE.1400395.
[41] L. Fang, X. Cheng, L. Yang, and H. Wang, "Location privacy in mobile big data: User identifiability via habitat region representation," *J. Commun. Inf. Netw.*, vol. 3, no. 3, pp. 31–38, Sep. 2018, doi: 10.1007/s41650-018-0028-z.
[42] Y. A. Bangash, L.-F. Zeng, and D. Feng, "MimiBS: Mimicking base-station to provide location privacy protection in wireless sensor networks," *J. Comput. Sci. Technol.*, vol. 32, no. 5, pp. 991–1007, Sep. 2017, doi: 10.1007/s11390-017-1777-0.
[43] Y. Song and H. Tan, "Practical pairing-free sensor cooperation scheme for cloud-assisted wireless body area networks," *Cybersecurity*, vol. 3, no. 1, p. 21, Dec. 2020, doi: 10.1186/s42400-020-00061-7.
[44] Z. Qin, Y. Li, X. Ye, J. Zhou, M. Cao, and D. Chen, "ECAS: An efficient and conditional privacy preserving collision warning system in fog-based vehicular ad hoc networks," *CCF Trans. Netw.*, vol. 3, nos. 3–4, pp. 205–217, Dec. 2020, doi: 10.1007/s42045-020-00041-y.
[45] S. S. Rani, J. A. Alzubi, S. Lakshmanaprabu, D. Gupta, and R. Manikandan, "Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers," *Multimedia Tools Appl.*, vol. 79, no. 47, pp. 35405–35424, 2020, doi: 10.1007/s11042-019-07760-5.
[46] Z. Zhang, H. Wang, and Y. Gao, "C2MP: Chebyshev chaotic map-based authentication protocol for RFID applications," *Pers. Ubiquitous Comput.*, vol. 19, no. 7, pp. 1053–1061, Oct. 2015, doi: 10.1007/s00779-015-0876-6.
[47] P. M. Kumar and U. D. Gandhi, "Enhanced DTLS with CoAP-based authentication scheme for the Internet of Things in healthcare application," *J. Supercomput.*, vol. 76, no. 6, pp. 3963–3983, Jun. 2020, doi: 10.1007/s11227-017-2169-5.
[48] M. Shariq and K. Singh, "A novel vector-space-based lightweight privacy-preserving RFID authentication protocol for IoT environment," *J. Supercomput.*, vol. 77, no. 8, pp. 8532–8562, Aug. 2021, doi: 10.1007/s11227-020-03550-1.
[49] S. S. S. GhaemMaghami, A. Haghbin, and M. Mirmohseni, "Cryptanalysis and improvement of two new RFID protocols based on R-RAPSE," *J. Commun. Inf. Netw.*, vol. 2, no. 3, pp. 107–122, Sep. 2017, doi: 10.1007/s41650-017-0013-y.
[50] G. Sun, "Efficient location privacy algorithm for Internet of Things (IoT) services and applications," *J. Netw. Comput. Appl.*, vol. 89, pp. 3–13, Jul. 2017, doi: 10.1016/j.jnca.2016.10.011.
[51] I. Agadakos, J. Polakis, and G. Portokalidis, "Techu: Open and privacy-preserving crowdsourced GPS for the masses," in *Proc. 15th Annu. Int. Conf. Mobile Syst., Appl., Services*, Jun. 2017, pp. 475–487.
[52] A. R. Javed, M. U. Sarwar, S. ur Rehman, H. U. Khan, Y. D. Al-Otaibi, and W. S. Alnumay, "PP-SPA: Privacy preserved smartphone-based personal assistant to improve routine life functioning of cognitive impaired individuals," *Neural Process. Lett.*, pp. 1–18, Jan. 2021, doi: 10.1007/s11063-020-10414-5.
[53] B. Aslam, A. R. Javed, C. Chakraborty, J. Nebhen, S. Raqib, and M. Rizwan, "Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic," *Pers. Ubiquitous Comput.*, pp. 1–17, Jul. 2021, doi: 10.1007/s00779-021-01596-3.
[54] S. Jegadeesan, M. Azees, N. Ramesh Babu, U. Subramaniam, and J. D. Almakhles, "EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs)," *IEEE Access*, vol. 8, pp. 48576–48586, 2020, doi: 10.1109/ACCESS.2020.2977968.
[55] Y. Chung, S. Choi, and D. Won, "Anonymous authentication scheme for intercommunication in the Internet of Things environments," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 11, Nov. 2015, Art. no. 305785, doi: 10.1155/2015/305785.
[56] T. Gao, Y. Li, N. Guo, and I. You, "An anonymous access authentication scheme for vehicular ad hoc networks under edge computing," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 2, Feb. 2018, Art. no. 155014771875658, doi: 10.1177/1550147718756581.
[57] Y. Wang, Z. Tian, H. Zhang, S. Su, and W. Shi, "A privacy preserving scheme for nearest neighbor query," *Sensors*, vol. 18, no. 8, p. 2440, 2018, doi: 10.3390/s18082440.
[58] Y. Du, G. Cai, X. Zhang, T. Liu, and J. Jiang, "An efficient dummy-based location privacy-preserving scheme for Internet of Things services," *Information*, vol. 10, no. 9, p. 278, Sep. 2019, doi: 10.3390/info10090278.
[59] J. B. Bernabe, J. L. Hernandez-Ramos, and A. F. S. Gomez, "Holistic privacy-preserving identity management system for the Internet of Things," *Mobile Inf. Syst.*, vol. 2017, pp. 1–20, Aug. 2017, doi: 10.1155/2017/6384186.
[60] S. M. Soumyasri and R. Ballal, "An improved pillar K-means based protocol for privacy-preserving location monitoring in wireless sensor network," *Wireless Pers. Commun.*, vol. 101, no. 2, pp. 915–929, Jul. 2018, doi: 10.1007/s11277-018-5733-2.
[61] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications," *IEEE Access*, vol. 6, p. 17545–17556, 2018, doi: 10.1109/ACCESS.2018.2805837.
[62] Z. Ruan, W. Liang, D. Sun, H. Luo, and F. Cheng, "An efficient and lightweight source privacy protecting scheme for sensor networks using group knowledge," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 4, Apr. 2013, Art. no. 601462, doi: 10.1155/2013/601462.
[63] M. N. Esfahani, B. S. Ghahfarokhi, and S. Etemadi Borujeni, "End-to-end privacy preserving scheme for IoT-based healthcare systems," *Wireless Netw.*, vol. 27, no. 6, pp. 4009–4037, Aug. 2021, doi: 10.1007/s11276-021-02652-9.
[64] X. Zhang, H. Huang, S. Huang, Q. Chen, T. Ju, and X. Du, "A context-aware location differential perturbation scheme for privacy-aware users in mobile environment," *Wirel. Commun. Mob. Comput.*, vol. 2018, Aug. 2018, Art. no. 9173519, doi: 10.1155/2018/9173519.
[65] H. Cao, S. Liu, L. Wu, and Z. Guan, "SCRAPPOR: An efficient privacy-preserving algorithm base on sparse coding for information-centric IoT," *IEEE Access*, vol. 6, pp. 63143–63154, 2018, doi: 10.1109/ACCESS.2018.2876707.
[66] I. Ullah and M. A. Shah, "A novel model for preserving location privacy in Internet of Things," in *Proc. 22nd Int. Conf. Autom. Comput. (ICAC)*, Sep. 2016, pp. 542–547, doi: 10.1109/IConAC.2016.7604976.
[67] J. Wang, R. Zhu, and S. Liu, "A differentially private unscented Kalman filter for streaming data in IoT," *IEEE Access*, vol. 6, pp. 6487–6495, 2018, doi: 10.1109/ACCESS.2018.2797159.
[68] Z. Guan, Z. Lv, X. Sun, L. Wu, J. Wu, X. Du, and M. Guizani, "A differentially private big data nonparametric Bayesian clustering algorithm in smart grid," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2631–2641, Oct. 2020, doi: 10.1109/TNSE.2020.2985096.

[69] S. Ghane, A. Jolfaei, L. Kulik, K. Ramamohanarao, and D. Puthal, "Preserving privacy in the internet of connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5018–5027, Aug. 2021, doi: 10.1109/TITS.2020.2964410.

[70] W. Li, Y. Chen, H. Hu, and C. Tang, "Using granule to search privacy preserving voice in home IoT systems," *IEEE Access*, vol. 8, pp. 31957–31969, 2020, doi: 10.1109/ACCESS.2020.2972975.

[71] I. A. Khan, D. Pi, N. Khan, Z. U. Khan, Y. Hussain, A. Nawaz, and F. Ali, "A privacy-conserving framework based intrusion detection method for detecting and recognizing malicious behaviours in cyber-physical power networks," *Int. J. Speech Technol.*, vol. 51, no. 10, pp. 7306–7321, Oct. 2021, doi: 10.1007/s10489-021-02222-8.

[72] G. C. Polyzos and N. Fotiou, "Building a reliable Internet of Things using information-centric networking," *J. Reliable Intell. Environments*, vol. 1, no. 1, pp. 47–58, Jul. 2015, doi: 10.1007/s40860-015-0003-5.

[73] T. Datta, N. Apthorpe, and N. Feamster, "A developer-friendly library for smart home IoT privacy-preserving traffic obfuscation," in *Proc. Workshop IoT Secur. Privacy*, Aug. 2018, pp. 43–48, doi: 10.1145/3229565.3229567.

[74] J. Qiu, H. Li, J. Dong, and G. Feng, "A privacy-preserving cancelable palmprint template generation scheme using noise data," in *Proc. 2nd Int. Conf. Intell. Inf. Process.*, Jul. 2017, p. 29.

[75] G. Xu, H. Li, S. Xu, H. Ren, Y. Zhang, J. Sun, and R. H. Deng, "Catch you if you deceive me: Verifiable and privacy-aware truth discovery in crowdsensing systems," in *Proc. ASIA CCS 15th ACM Asia Conf. Comput. Commun. Secur.*, Oct. 2020, pp. 178–192.

[76] K. Owusu-Agyemeng, Z. Qin, H. Xiong, Y. Liu, T. Zhuang, and Z. Qin, "MSDP: Multi-scheme privacy-preserving deep learning via differential privacy," *Pers. Ubiquitous Comput.*, pp. 1–13, Feb. 2021, doi: 10.1007/s00779-021-01545-0.

[77] T. Zhang and Q. Zhu, "Distributed privacy-preserving collaborative intrusion detection systems for VANETs," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, no. 1, pp. 148–161, Mar. 2018, doi: 10.1109/TSIPN.2018.2801622.

[78] X. Cheng, Q. Luo, Y. Pan, Z. Li, J. Zhang, and B. Chen, "Predicting the APT for cyber situation comprehension in 5G-enabled IoT scenarios based on differentially private federated learning," *Secur. Commun. Netw.*, vol. 2021, pp. 1–14, Apr. 2021, doi: 10.1155/2021/8814068.

[79] L. Zhao, H. Huang, C. Su, S. Ding, H. Huang, Z. Tan, and Z. Li, "Block-sparse coding-based machine learning approach for dependable device-free localization in IoT environment," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3211–3223, Mar. 2021, doi: 10.1109/JIOT.2020.3019732.

[80] A. Nadian-Ghomsheh, B. Farahani, and M. Kavian, "A hierarchical privacy-preserving IoT architecture for vision-based hand rehabilitation assessment," *Multimedia Tools Appl.*, vol. 80, no. 20, pp. 31357–31380, Aug. 2021, doi: 10.1007/s11042-021-10563-2.

[81] C. X. Lu, B. Du, X. Kan, H. Wen, A. Markham, and N. Trigoni, "VeriNet: User verification on smartwatches via behavior biometrics," in *Proc. 1st ACM Workshop Mobile Crowdsensing Syst. Appl.*, Nov. 2017, pp. 68–73.

[82] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9463–9472, Jun. 2021, doi: 10.1109/JIOT.2020.2996590.

[83] P. Dey, S. K. Chaulya, and S. Kumar, "Secure decision tree twin support vector machine training and classification process for encrypted IoT data via blockchain platform," *Concurrency Comput., Pract. Exper.*, vol. 33, no. 16, Aug. 2021, Art. no. e6264, doi: 10.1002/cpe.6264.

[84] Y. Zhang, P. Zhang, Y. Luo, and L. Ji, "Towards efficient, credible and privacy-preserving service QoS prediction in unreliable mobile edge environments," in *Proc. Int. Symp. Reliable Distrib. Syst. (SRDS)*, Sep. 2020, pp. 309–318, doi: 10.1109/SRDS51746.2020.00038.

[85] Z. Xue, P. Zhou, Z. Xu, X. Wang, Y. Xie, X. Ding, and S. Wen, "A resource-constrained and privacy-preserving edge-computing-enabled clinical decision system: A federated reinforcement learning approach," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 9122–9138, Jun. 2021, doi: 10.1109/JIOT.2021.3057653.

[86] A. M. Elmisery, S. Rho, and M. Aborizka, "A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services," *Cluster Comput.*, vol. 22, no. S1, pp. 1611–1638, Jan. 2019, doi: 10.1007/s10586-017-1298-1.

[87] C. Dhasarathan, M. Kumar, A. K. Srivastava, F. Al-Turjman, A. Shankar, and M. Kumar, "A bio-inspired privacy-preserving framework for healthcare systems," *J. Supercomput.*, vol. 77, pp. 11099–11134, Mar. 2021, doi: 10.1007/s11227-021-03720-9.

[88] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "Federated learning for drone authentication," *Ad Hoc Netw.*, vol. 120, Sep. 2021, Art. no. 102574, doi: 10.1016/j.adhoc.2021.102574.

[89] D. Unal, M. Hammoudeh, M. A. Khan, A. Abuarqoub, G. Epiphaniou, and R. Hamila, "Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things," *Comput. Secur.*, vol. 109, Oct. 2021, Art. no. 102393, doi: 10.1016/j.cose.2021.102393.

[90] A. Ibarrondo, H. Chabanne, and M. Önen, "Banners: Binarized neural networks with replicated secret sharing," in *Proc. ACM Workshop Inf. Hiding Multimedia Secur.*, Jun. 2021, pp. 63–74.

[91] A. Basati and M. M. Faghih, "APAE: An IoT intrusion detection system using asymmetric parallel auto-encoder," *Neural Comput. Appl.*, vol. 35, no. 7, pp. 4813–4833, Mar. 2023.

[92] Z. Tan, H. Zhang, P. Hu, and R. Gao, "Distributed outsourced privacy-preserving gradient descent methods among multiple parties," *Secur. Commun. Netw.*, vol. 2021, pp. 1–16, Apr. 2021, doi: 10.1155/2021/8876893.

[93] C. Peng, M. Luo, H. Wang, M. K. Khan, and D. He, "An efficient privacy-preserving aggregation scheme for multidimensional data in IoT," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 589–600, Jan. 2022.

[94] L. Zhang, J. Wang, and Y. Mu, "Privacy-preserving flexible access control for encrypted data in Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 19, pp. 14731–14745, Oct. 2021, doi: 10.1109/JIOT.2021.3071553.

[95] Q. Yao, J. Ma, R. Li, X. Li, J. Li, and J. Liu, "Energy-aware RFID authentication in edge computing," *IEEE Access*, vol. 7, pp. 77964–77980, 2019, doi: 10.1109/ACCESS.2019.2922220.

[96] Q. Kong, R. Lu, F. Yin, and S. Cui, "Privacy-preserving continuous data collection for predictive maintenance in vehicular fog-cloud," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5060–5070, Aug. 2021, doi: 10.1109/TITS.2020.3011931.

[97] T. Wang, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu, and T. Hayajneh, "Preserving balance between privacy and data integrity in edge-assisted Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2679–2689, Apr. 2020, doi: 10.1109/JIOT.2019.2951687.

[98] R. Lu, "A new communication-efficient privacy-preserving range query scheme in fog-enhanced IoT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2497–2505, Apr. 2018, doi: 10.1109/JIOT.2018.2871204.

[99] H. Mahdikhani, R. Lu, Y. Zheng, J. Shao, and A. A. Ghorbani, "Achieving $O(\log^3 n)$ communication-efficient privacy-preserving range query in fog-based IoT," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5220–5232, Jun. 2020.

[100] H. Mahdikhani, R. Lu, J. Shao, and A. Ghorbani, "Using reduced paths to achieve efficient privacy-preserving range query in fog-based IoT," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4762–4774, Mar. 2021, doi: 10.1109/JIOT.2020.3029472.

[101] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2017, pp. 1–6, doi: 10.1109/ANTS.2017.8384164.

[102] 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, doi: 10.1109/HPCC/SmartCity/DSS.2018.00104.

[103] H. Qin, H. Wang, X. Wei, L. Xue, and L. Wu, "Privacy-preserving wildcards pattern matching protocol for IoT applications," *IEEE Access*, vol. 7, pp. 36094–36102, 2019, doi: 10.1109/ACCESS.2019.2900519.

[104] A. Tewari and B. B. Gupta, "A robust anonymity preserving authentication protocol for IoT devices," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2018, pp. 1–5, doi: 10.1109/ICCE.2018.8326282.

[105] A. Arfaoui, S. Cherkaoui, A. Kribeche, S. M. Senouci, and M. Hamdi, "Context-aware adaptive authentication and authorization in Internet of Things," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6, doi: 10.1109/ICC.2019.8761830.

[106] J. Liu, H. Cao, Q. Li, F. Cai, X. Du, and M. Guizani, "A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing," 2018, *arXiv:1804.01822*.

[107] C. Guo, R. Zhuang, Y. Jie, K.-K. R. Choo, and X. Tang, "Secure range search over encrypted uncertain IoT outsourced data," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1520–1529, Apr. 2019, doi: 10.1109/JIOT.2018.2845106.

[108] F. Rezaeibagha, Y. Mu, K. Huang, L. Zhang, and X. Huang, "Secure and privacy-preserved data collection for IoT wireless sensors," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17669–17677, Dec. 2021, doi: 10.1109/JIOT.2021.3082150.
[109] A. Rasheed, R. R. Hashemi, A. Bagabas, J. Young, C. Badri, and K. Patel, "Configurable anonymous authentication schemes for the Internet of Things (IoT)," in *Proc. IEEE Int. Conf. RFID (RFID)*, Apr. 2019, pp. 1–8, doi: 10.1109/RFID.2019.8719256.
[110] N. I. Yekta and R. Lu, "PQuery: Achieving privacy-preserving query with communication efficiency in Internet of Things," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2017, pp. 1–5, doi: 10.1109/VTCFall.2017.8288344.
[111] Z. A. Abduljabbar, H. Jin, A. Ibrahim, Z. A. Hussien, M. A. Hussain, S. H. Abbdal, and D. Zou, "Secure biometric image retrieval in IoT-cloud," in *Proc. IEEE Int. Conf. Signal Process., Commun. Comput. (ICSPCC)*, Aug. 2016, pp. 1–6.
[112] T. Kumar, A. Braeken, M. Liyanage, and M. Ylianttila, "Identity privacy preserving biometric based authentication scheme for naked healthcare environment," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–7, doi: 10.1109/ICC.2017.7996966.
[113] W. Wang, P. Xu, L. T. Yang, and J. Chen, "Cloud-assisted key distribution in batch for secure real-time mobile services," *IEEE Trans. Serv. Comput.*, vol. 11, no. 5, pp. 850–863, Sep./Oct. 2018, doi: 10.1109/TSC.2016.2594071.
[114] J. Zhang, Y. Zong, C. Yang, Y. Miao, and J. Guo, "LBOA: Location-based secure outsourced aggregation in IoT," *IEEE Access*, vol. 7, pp. 43869–43883, 2019, doi: 10.1109/ACCESS.2019.2908429.
[115] N. Kaaniche, E. Jung, and A. Gehani, "Efficiently validating aggregated IoT data integrity," in *Proc. IEEE 4th Int. Conf. Big Data Comput. Service Appl. (BigDataService)*, Mar. 2018, pp. 260–265, doi: 10.1109/BigDataService.2018.00046.
[116] U. Khadam, M. M. Iqbal, S. Jabbar, and S. A. Shah, "Data aggregation and privacy preserving using computational intelligence," *IEEE Internet Things Mag.*, vol. 4, no. 2, pp. 60–64, Jun. 2021, doi: 10.1109/IOTM.0001.2000010.
[117] J. Zouari, M. Hamdi, and T.-H. Kim, "A privacy-preserving homomorphic encryption scheme for the Internet of Things," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 1939–1944, doi: 10.1109/IWCMC.2017.7986580.
[118] Q. Wang, L. Huang, S. Chen, and Y. Xiang, "Blockchain enables your bill safer," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14162–14171, Aug. 2022.
[119] V. Beltran, J. A. Martinez, and A. F. Skarmeta, "User-centric access control for efficient security in smart cities," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2017, pp. 1–6, doi: 10.1109/GIOTS.2017.8016287.
[120] B. A. Alzahrani and K. Mahmood, "Provable privacy preserving authentication solution for Internet of Things environment," *IEEE Access*, vol. 9, pp. 82857–82865, 2021, doi: 10.1109/ACCESS.2021.3086735.
[121] E. Yaacoub, K. Abualsaud, T. Khattab, and A. Chehab, "Secure transmission of IoT mHealth patient monitoring data from remote areas using DTN," *IEEE Netw.*, vol. 34, no. 5, pp. 226–231, Sep. 2020, doi: 10.1109/MNET.011.1900627.
[122] P. Punithavathi and S. Geetha, "Partial DCT-based cancelable biometric authentication with security and privacy preservation for IoT applications," *Multimedia Tools Appl.*, vol. 78, no. 18, pp. 25487–25514, Sep. 2019, doi: 10.1007/s11042-019-7617-1.
[123] R. Sendhil and A. Amuthan, "Contextual fully homomorphic encryption schemes-based privacy preserving framework for securing fog-assisted healthcare data exchanging applications," *Int. J. Inf. Technol.*, vol. 13, no. 4, pp. 1545–1553, Aug. 2021.
[124] N. Chikouche, P.-L. Cayrel, E. H. M. Mboup, and B. O. Boidje, "A privacy-preserving code-based authentication protocol for Internet of Things," *J. Supercomput.*, vol. 75, no. 12, pp. 8231–8261, Dec. 2019, doi: 10.1007/s11227-019-03003-4.
[125] X. Li, J. Li, S. Yiu, C. Gao, and J. Xiong, "Privacy-preserving edge-assisted image retrieval and classification in IoT," *Frontiers Comput. Sci.*, vol. 13, no. 5, pp. 1136–1147, Oct. 2019, doi: 10.1007/s11704-018-8067-z.
[126] Y. Alshboul, A. A. R. Bsoul, M. AL Zamil, and S. Samarah, "Cybersecurity of smart home systems: Sensor identity protection," *J. Netw. Syst. Manage.*, vol. 29, no. 3, p. 22, Jul. 2021, doi: 10.1007/s10922-021-09586-9.
[127] N. Sasikaladevi and D. Malathi, "Privacy preserving light weight authentication protocol (LEAP) for WBAN by exploring Genus-2 HEC," *Multimedia Tools Appl.*, vol. 78, no. 13, pp. 18037–18054, Jul. 2019, doi: 10.1007/s11042-019-7149-8.
[128] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan, and M. Dasgupta, "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography," *J. Supercomput.*, vol. 77, no. 2, pp. 1114–1151, Feb. 2021, doi: 10.1007/s11227-020-03318-7.
[129] H. Zhong, Y. Geng, J. Cui, Y. Xu, and L. Liu, "A weight-based conditional privacy-preserving authentication scheme in software-defined vehicular network," *J. Cloud Comput.*, vol. 9, no. 1, p. 54, Dec. 2020, doi: 10.1186/s13677-020-00198-3.
[130] Q. Wang, C. Feng, Y. Xu, H. Zhong, and V. S. Sheng, "A novel privacy-preserving speech recognition framework using bidirectional LSTM," *J. Cloud Comput.*, vol. 9, no. 1, p. 36, Dec. 2020, doi: 10.1186/s13677-020-00186-7.
[131] Q. Huang, L. Wang, and Y. Yang, "DECENT: Secure and fine-grained data access control with policy updating for constrained IoT devices," *World Wide Web*, vol. 21, no. 1, pp. 151–167, 2018, doi: 10.1007/s11280-017-0462-0.
[132] G. Spathoulas, G. Theodoridis, and G.-P. Damiris, "Using homomorphic encryption for privacy-preserving clustering of intrusion detection alerts," *Int. J. Inf. Secur.*, vol. 20, no. 3, pp. 347–370, Jun. 2021, doi: 10.1007/s10207-020-00506-7.
[133] M. Qi and J. Chen, "Secure authenticated key exchange for WSNs in IoT applications," *J. Supercomput.*, vol. 77, no. 12, pp. 13897–13910, Dec. 2021, doi: 10.1007/s11227-021-03836-y.
[134] D. Lee and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree," *Multimedia Tools Appl.*, vol. 80, nos. 26–27, pp. 34517–34534, Nov. 2021, doi: 10.1007/s11042-020-08776-y.
[135] Y. Chen, H. Liu, B. Wang, B. Sonompil, Y. Ping, and Z. Zhang, "A threshold hybrid encryption method for integrity audit without trusted center," *J. Cloud Comput.*, vol. 10, no. 1, pp. 1–14, Dec. 2021, doi: 10.1186/s13677-020-00222-6.
[136] S. Singh and V. K. Chaurasiya, "Mutual authentication scheme of IoT devices in fog computing environment," *Cluster Comput.*, vol. 24, no. 3, pp. 1643–1657, Sep. 2021, doi: 10.1007/s10586-020-03211-1.
[137] Y. Tu, G. Yang, J. Wang, and Q. Su, "A secure, efficient and verifiable multimedia data sharing scheme in fog networking system," *Cluster Comput.*, vol. 24, no. 1, pp. 225–247, Mar. 2021, doi: 10.1007/s10586-020-03101-6.
[138] H. Anada, A. Kanaoka, N. Matsuzaki, and Y. Watanabe, "Key-updatable public-key encryption with keyword search (or: How to realize PEKS with efficient key updates for IoT environments)," *Int. J. Inf. Secur.*, vol. 19, no. 1, pp. 15–38, Feb. 2020, doi: 10.1007/s10207-019-00441-2.
[139] R. Madhusudhan and R. Shashidhara, "A novel DNA based password authentication system for global roaming in resource-limited mobile environments," *Multimedia Tools Appl.*, vol. 79, nos. 3–4, pp. 2185–2212, Jan. 2020, doi: 10.1007/s11042-019-08349-8.
[140] T.-Y. Wu, Z. Lee, L. Yang, J.-N. Luo, and R. Tso, "Provably secure authentication key exchange scheme using fog nodes in vehicular ad hoc networks," *J. Supercomput.*, vol. 77, no. 7, pp. 6992–7020, Jul. 2021, doi: 10.1007/s11227-020-03548-9.
[141] S. A. Eftekhari, M. Nikooghadam, and M. Rafighi, "Robust session key generation protocol for social Internet of Vehicles with enhanced security provision," *J. Supercomput.*, vol. 77, no. 3, pp. 2511–2544, Mar. 2021, doi: 10.1007/s11227-020-03363-2.
[142] A. A. Alamr, F. Kausar, J. Kim, and C. Seo, "A secure ECC-based RFID mutual authentication protocol for Internet of Things," *J. Supercomput.*, vol. 74, no. 9, pp. 4281–4294, Sep. 2018, doi: 10.1007/s11227-016-1861-1.
[143] O. El Mouaatamid, M. Lahmer, and M. Belkasmi, "A scalable group authentication scheme based on combinatorial designs with fault tolerance for the Internet of Things," *Social Netw. Comput. Sci.*, vol. 1, no. 4, p. 234, Jul. 2020, doi: 10.1007/s42979-020-00247-3.
[144] I. Memon and Q. A. Arain, "Dynamic path privacy protection framework for continuous query service over road networks," *World Wide Web*, vol. 20, no. 4, pp. 639–672, 2017, doi: 10.1007/s11280-016-0403-3.
[145] T. Khalid, A. N. Khan, M. Ali, A. Adeel, A. ur Rehman Khan, and J. Shuja, "A fog-based security framework for intelligent traffic light control system," *Multimedia Tools Appl.*, vol. 78, no. 17, pp. 24595–24615, Sep. 2019, doi: 10.1007/s11042-018-7008-z.

[146] M. P. Gopinath, G. S. Tamizharasi, L. Kavisankar, R. Sathyaraj, S. Karthi, S. L. Aarthy, and B. Balamurugan, "A secure cloud-based solution for real-time monitoring and management of internet of underwater things (IOUT)," *Neural Comput. Appl.*, vol. 31, no. S1, pp. 293–308, Jan. 2019, doi: 10.1007/s00521-018-3774-9.

[147] T. Senthilnathan, P. Prabu, R. Sivakumar, and S. Sakthivel, "An enhancing reversible data hiding for secured data using shuffle block key encryption and histogram bit shifting in cloud environment," *Cluster Comput.*, vol. 22, no. S5, pp. 12839–12847, Sep. 2019, doi: 10.1007/s10586-018-1765-3.

[148] G. Ramu, "A secure cloud framework to share EHRs using modified CP-ABE and the attribute Bloom filter," *Educ. Inf. Technol.*, vol. 23, no. 5, pp. 2213–2233, Sep. 2018, doi: 10.1007/s10639-018-9713-7.

[149] R. Zhang, H. Ma, Y. Lu, and Y. Li, "Provably secure cloud storage for mobile networks with less computation and smaller overhead," *Sci. China Inf. Sci.*, vol. 60, no. 12, Dec. 2017, Art. no. 122104, doi: 10.1007/s11432-016-0038-6.

[150] S. Rana and D. Mishra, "An authenticated access control framework for digital right management system," *Multimedia Tools Appl.*, vol. 80, pp. 25255–25260, Apr. 2021, doi: 10.1007/s11042-021-10813-3.

[151] V. Kalaivani, "Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications," *Pers. Ubiquitous Comput.*, pp. 1–11, Mar. 2021, doi: 10.1007/s00779-021-01546-z.

[152] A. Elkhalil, J. Zhang, and R. Elhabob, "An efficient heterogeneous blockchain-based online/offline signcryption systems for Internet of Vehicles," *Cluster Comput.*, vol. 24, no. 3, pp. 2051–2068, Sep. 2021, doi: 10.1007/s10586-021-03246-y.

[153] A. Alghafis, N. Munir, and M. Khan, "An encryption scheme based on chaotic Rabinovich–Fabrikant system and S8 confusion component," *Multimedia Tools Appl.*, vol. 80, no. 5, pp. 7967–7985, Feb. 2021, doi: 10.1007/s11042-020-10142-x.

[154] D. Singh, B. Kumar, S. Singh, S. Chand, and P. K. Singh, "RCBE-AS: Rabin cryptosystem–based efficient authentication scheme for wireless sensor networks," *Pers. Ubiquitous Comput.*, pp. 1–22, Jul. 2021, doi: 10.1007/s00779-021-01592-7.

[155] K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," *Int. J. Inf. Secur.*, vol. 19, no. 1, pp. 129–146, Feb. 2020, doi: 10.1007/s10207-019-00464-9.

[156] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Inf. Sci.*, vol. 527, pp. 493–510, Jul. 2020, doi: 10.1016/j.ins.2019.01.070.

[157] S. S. Moni and D. Manivannan, "A scalable and distributed architecture for secure and privacy-preserving authentication and message dissemination in VANETs," *Internet Things*, vol. 13, Mar. 2021, Art. no. 100350, doi: 10.1016/j.iot.2020.100350.

[158] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," *Future Gener. Comput. Syst.*, vol. 76, pp. 540–549, Nov. 2017, doi: 10.1016/j.future.2017.03.001.

[159] K. Fan, H. Xu, L. Gao, H. Li, and Y. Yang, "Efficient and privacy preserving access control scheme for fog-enabled IoT," *Future Gener. Comput. Syst.*, vol. 99, pp. 134–142, Oct. 2019, doi: 10.1016/j.future.2019.04.003.

[160] J. Lu, F. Nan, Y. Huang, C.-C. Chang, Y. Du, and H. Tian, "Privacy-preserving public auditing for secure data storage in fog-to-cloud computing," *J. Netw. Comput. Appl.*, vol. 127, pp. 59–69, Dec. 2018, doi: 10.1016/j.jnca.2018.12.004.

[161] M. A. Azad, S. Bag, F. Hao, and K. Salah, "M2M-REP: Reputation system for machines in the Internet of Things," *Comput. Secur.*, vol. 79, pp. 1–16, Nov. 2018, doi: 10.1016/j.cose.2018.07.014.

[162] J. Lin, J. Niu, H. Li, and M. Atiquzzaman, "A secure and efficient location-based service scheme for smart transportation," *Future Gener. Comput. Syst.*, vol. 92, pp. 694–704, Mar. 2019, doi: 10.1016/j.future.2017.11.030.

[163] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving fusion of IoT and big data for e-health," *Future Gener. Comput. Syst.*, vol. 86, pp. 1437–1455, Sep. 2018, doi: 10.1016/j.future.2018.01.003.

[164] J. Hao, C. Huang, J. Ni, H. Rong, M. Xian, and X. S. Shen, "Fine-grained data access control with attribute-hiding policy for cloud-based IoT," *Comput. Netw.*, vol. 153, pp. 1–10, Apr. 2019, doi: 10.1016/j.comnet.2019.02.008.

[165] Y. Zhao, Y. Liu, A. Tian, Y. Yu, and X. Du, "Blockchain based privacy-preserving software updates with proof-of-delivery for Internet of Things," *J. Parallel Distrib. Comput.*, vol. 132, pp. 141–149, Oct. 2019, doi: 10.1016/j.jpdc.2019.06.001.

[166] S. Gupta, B. L. Parne, and N. S. Chaudhari, "ISAG: IoT-enabled and secrecy aware group-based handover scheme for e-health services in M2M communication network," *Future Gener. Comput. Syst.*, vol. 125, pp. 168–187, Dec. 2021, doi: 10.1016/j.future.2021.06.038.

[167] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT," *Comput. Netw.*, vol. 133, pp. 141–156, Mar. 2018, doi: 10.1016/j.comnet.2018.01.036.

[168] B. D. Deebak and F. AL-Turjman, "Lightweight authentication for IoT/cloud-based forensics in intelligent data computing," *Future Gener. Comput. Syst.*, vol. 116, pp. 406–425, Mar. 2021, doi: 10.1016/j.future.2020.11.010.

[169] C. Zhang, L. Zhu, C. Xu, K. Sharif, X. Du, and M. Guizani, "LPTD: Achieving lightweight and privacy-preserving truth discovery in CIoT," *Future Gener. Comput. Syst.*, vol. 90, pp. 175–184, Jan. 2019, doi: 10.1016/j.future.2018.07.064.

[170] M. Barni, T. Bianchi, D. Catalano, M. D. Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, and A. Piva, "Privacy-preserving fingercode authentication," in *Proc. 12th ACM Workshop Multimedia Secur.*, Sep. 2010, pp. 231–240.

[171] K. Singh, P. Saini, S. Rani, and A. K. Singh, "Authentication and privacy preserving message transfer scheme for vehicular ad hoc networks (VANETs)," in *Proc. 12th ACM Int. Conf. Comput. Frontiers*, May 2015, p. 58.

[172] M. Liu, H. Hu, H. Xiang, C. Yang, L. Lyu, and X. Zhang, "Clustering-based efficient privacy-preserving face recognition scheme without compromising accuracy," *ACM Trans. Sens. Netw.*, vol. 17, no. 3, pp. 31:1–31:27, 2021, doi: 10.1145/3448414.

[173] A. Bhargav-Spantzel, A. C. Squicciarini, and E. Bertino, "Establishing and protecting digital identity in federation systems," in *Proc. Workshop Digit. Identity Manage.*, Nov. 2005, pp. 11–19.

[174] Q. Kong, R. Lu, M. Ma, and H. Bao, "Achieve location privacy-preserving range query in vehicular sensing," *Sensors*, vol. 17, no. 8, p. 1829, Aug. 2017, doi: 10.3390/s17081829.

[175] Q. Kong, R. Lu, H. Bao, and M. Ma, "A privacy-preserving sensory data sharing scheme in Internet of Vehicles," *Future Gener. Comput. Syst.*, vol. 92, pp. 644–655, Mar. 2019, doi: 10.1016/j.future.2017.12.003.

[176] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, "Efficient certificateless aggregate signature with conditional privacy preservation in IoV," *IEEE Syst. J.*, vol. 15, no. 1, pp. 245–256, Mar. 2021, doi: 10.1109/JSYST.2020.2966526.

[177] C. Lai, G. Li, and D. Zheng, "SPSC: A secure and privacy-preserving autonomous platoon setup and communication scheme," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 9, Sep. 2021, Art. no. e3982, doi: 10.1002/ett.3982.

[178] 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, doi: 10.1155/2019/9126376.

[179] A. Punitha and J. M. L. Manickam, "Privacy preservation and authentication on secure geographical routing in VANET," *J. Experim. Theor. Artif. Intell.*, vol. 29, no. 3, pp. 617–628, May 2017, doi: 10.1080/0952813X.2016.1212103.

[180] H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," *IEEE Access*, vol. 6, pp. 30049–30059, 2018, doi: 10.1109/ACCESS.2018.2844373.

[181] E. Yang, V. S. Parvathy, P. P. Selvi, K. Shankar, C. Seo, G. P. Joshi, and O. Yi, "Privacy preservation in edge consumer electronics by combining anomaly detection with dynamic attribute-based re-encryption," *Mathematics*, vol. 8, no. 11, p. 1871, Oct. 2020.

[182] Z. Benyamina, K. Benahmed, and F. Bounaama, "ANEL: A novel efficient and lightweight authentication scheme for vehicular ad hoc networks," *Comput. Netw.*, vol. 164, Dec. 2019, Art. no. 106899, doi: 10.1016/j.comnet.2019.106899.

[183] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "A novel anonymous mutual authentication protocol with provable link-layer location privacy," *IEEE Trans. Veh. Technol.*, vol. 58, no. 3, pp. 1454–1466, Mar. 2009, doi: 10.1109/TVT.2008.925304.

[184] H. Zhao, J. Yan, X. Luo, and X. Gua, "Privacy preserving solution for the asynchronous localization of underwater sensor networks," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 6, pp. 1511–1527, Nov. 2020, doi: 10.1109/JAS.2020.1003312.

[185] J.-H. Im, S.-Y. Jeon, and M.-K. Lee, "Practical privacy-preserving face authentication for smartphones secure against malicious clients," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2386–2401, 2020, doi: 10.1109/TIFS.2020.2969513.
[186] M. V. Babu, J. A. Alzubi, R. Sekaran, R. Patan, M. Ramachandran, and D. Gupta, "An improved IDAF-FIT clustering based ASLPP-RR routing with secure data aggregation in wireless sensor network," *Mobile Netw. Appl.*, vol. 26, no. 3, pp. 1059–1067, Jun. 2021, doi: 10.1007/s11036-020-01664-7.
[187] J. Feng, L. T. Yang, Q. Zhu, and K.-K.-R. Choo, "Privacy-preserving tensor decomposition over encrypted data in a federated cloud environment," *IEEE Trans. Depend. Secure Comput.*, vol. 17, no. 4, pp. 857–868, Jul. 2020, doi: 10.1109/TDSC.2018.2881452.
[188] Z.-C. Liu, L. Xiong, T. Peng, D.-Y. Peng, and H.-B. Liang, "A realistic distributed conditional Privacy- preserving authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 26307–26317, 2018, doi: 10.1109/ACCESS.2018.2834224.
[189] A. Alamer, "An efficient group signcryption scheme supporting batch verification for securing transmitted data in the Internet of Things," *J. Ambient Intell. Humanized Comput.*, pp. 1–18, Jun. 2020, doi: 10.1007/s12652-020-02076-x.
[190] Z. Wang and H. Xie, "Privacy-preserving meter report protocol of isolated smart grid devices," *Wireless Commun. Mobile Comput.*, vol. 2017, pp. 1–8, Jun. 2017, doi: 10.1155/2017/2539673.
[191] G. Wang, R. Lu, and Y. L. Guan, "Achieve privacy-preserving priority classification on patient health data in remote eHealthcare system," *IEEE Access*, vol. 7, pp. 33565–33576, 2019, doi: 10.1109/ACCESS.2019.2891775.
[192] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in VANET," *Inf. Sci.*, vol. 476, pp. 211–221, Feb. 2019, doi: 10.1016/j.ins.2018.10.021.
[193] F. O. Çatak and A. F. Mustacoglu, "CPP-ELM: Cryptographically privacy-preserving extreme learning machine for cloud systems," *Int. J. Comput. Intell. Syst.*, vol. 11, no. 1, pp. 33–44, 2018, doi: 10.2991/ijcis.11.1.3.
[194] L. Liu, H. Quan, X. Liu, and Y. Zhang, "Lightweight handover authentication with location privacy-preserving in mobile wireless networks," *Int. J. Embed. Syst.*, vol. 7, nos. 3–4, pp. 280–288, 2015, doi: 10.1504/IJES.2015.072374.
[195] J. Zhang, Y. Zhao, J. Wu, and B. Chen, "LVPDA: A lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled IoT," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4016–4027, May 2020, doi: 10.1109/JIOT.2020.2978286.
[196] H. Gunasinghe and E. Bertino, "PrivBioMTAuth: Privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 4, pp. 1042–1057, Apr. 2018, doi: 10.1109/TIFS.2017.2777787.
[197] H. J. Jo, I. S. Kim, and D. H. Lee, "Efficient and privacy-preserving metering protocols for smart grid systems," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1732–1742, May 2016, doi: 10.1109/TSG.2015.2449278.
[198] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for Internet of Vehicles deployment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5535–5548, Mar. 2020, doi: 10.1109/TVT.2020.2981934.
[199] S. O. Ogundoyin and I. A. Kamil, "PAASH: A privacy-preserving authentication and fine-grained access control of outsourced data for secure smart health in smart cities," *J. Parallel Distrib. Comput.*, vol. 155, pp. 101–119, Sep. 2021, doi: 10.1016/j.jpdc.2021.05.001.
[200] X. Yang, X. Yi, I. Khalil, Y. Zeng, X. Huang, S. Nepal, X. Yang, and H. Cui, "A lightweight authentication scheme for vehicular ad hoc networks based on MSR," *Veh. Commun.*, vol. 15, pp. 16–27, Jan. 2019, doi: 10.1016/j.vehcom.2018.11.001.
[201] J. S. Alshudukhi, B. A. Mohammed, and Z. G. Al-Mekhlafi, "Conditional privacy-preserving authentication scheme without using point multiplication operations based on elliptic curve cryptography (ECC)," *IEEE Access*, vol. 8, pp. 222032–222040, 2020, doi: 10.1109/ACCESS.2020.3044961.
[202] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, Sep. 2010, doi: 10.1109/TPDS.2010.14.
[203] M. Fal Sadikin and M. Kyas, "IMAKA-tate: Secure and efficient privacy preserving for indoor positioning applications," *Int. J. Parallel, Emergent Distrib. Syst.*, vol. 30, no. 6, pp. 447–463, Nov. 2015, doi: 10.1080/17445760.2015.1058939.
[204] M. Sun, R. Yang, and L. Hu, "A secure distributed machine learning protocol against static semi-honest adversaries," *Appl. Soft Comput.*, vol. 102, Apr. 2021, Art. no. 107095, doi: 10.1016/j.asoc.2021.107095.
[205] S. K. Ocansey, W. Ametepe, X. W. Li, and C. Wang, "Dynamic searchable encryption with privacy protection for cloud computing," *Int. J. Commun. Syst.*, vol. 31, no. 1, Jan. 2018, Art. no. e3403, doi: 10.1002/dac.3403.
[206] M. Shuai, L. Xiong, C. Wang, and N. Yu, "Lightweight and privacy-preserving authentication scheme with the resilience of desynchronisation attacks for WBANs," *IET Inf. Secur.*, vol. 14, no. 4, pp. 380–390, Jul. 2020, doi: 10.1049/iet-ifs.2019.0491.
[207] P. Devi, S. Sathyalakshmi, and D. V. Subramanian, "An optimal Meta-heuristic optimization based ElGamal public key cryptosystem for privacy in IoT environment," *Int. J. Syst. Assurance Eng. Manage.*, pp. 1–11, Jun. 2021, doi: 10.1007/s13198-021-01173-0.
[208] S. Zhang, S. Ray, R. Lu, Y. Zheng, and J. Shao, "Preserving location privacy for outsourced most-frequent item query in mobile crowdsensing," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 9139–9150, Jun. 2021, doi: 10.1109/JIOT.2021.3056442.
[209] Y. Zhao, L. T. Yang, and J. Sun, "Privacy-preserving tensor-based multiple clusterings on cloud for industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2372–2381, Apr. 2019, doi: 10.1109/TII.2018.2871174.
[210] Z. Guan, Y. Zhang, L. Zhu, L. Wu, and S. Yu, "EFFECT: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid," *Sci. China-Inf. Sci.*, vol. 62, no. 3, Mar. 2019, Art. no. 32103, doi: 10.1007/s11432-018-9451-y.
[211] S. Fu, J. Ma, H. Li, and Q. Jiang, "A robust and privacy-preserving aggregation scheme for secure smart grid communications in digital communities," *Secur. Commun. Netw.*, vol. 9, no. 15, pp. 2779–2788, Oct. 2016, doi: 10.1002/sec.1188.
[212] X. Dong, L. Wei, H. Zhu, Z. Cao, and L. Wang, "EP^{2}DF: An efficient privacy-preserving data-forwarding scheme for service-oriented vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 580–591, Feb. 2011.
[213] M. A. Al-Shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and A. S. Al-Hiti, "LSWBVM: A lightweight security without using batch verification method scheme for a vehicle ad hoc network," *IEEE Access*, vol. 8, pp. 170507–170518, 2020, doi: 10.1109/ACCESS.2020.3024587.
[214] U. Rajput, F. Abbas, H. Eun, and H. Oh, "A hybrid approach for efficient privacy-preserving authentication in VANET," *IEEE Access*, vol. 5, pp. 12014–12030, 2017, doi: 10.1109/ACCESS.2017.2717999.
[215] N. Saxena and B. J. Choi, "Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1438–1452, Jul. 2016, doi: 10.1109/TIFS.2016.2532840.
[216] B. L. Nguyen, E. L. Lydia, M. Elhoseny, I. V. Pustokhina, D. A. Pustokhin, M. M. Selim, G. N. Nguyen, and K. Shankar, "Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data," *Comput., Mater. Continua*, vol. 65, no. 1, pp. 87–107, 2020.
[217] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice," *J. Netw. Comput. Appl.*, vol. 122, pp. 50–60, Nov. 2018, doi: 10.1016/j.jnca.2018.07.017.
[218] W. Tang, J. Ren, K. Zhang, D. Zhang, Y. Zhang, and X. S. Shen, "Efficient and privacy-preserving fog-assisted health data sharing scheme," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 6, pp. 68:1–68:23, 2019, doi: 10.1145/3341104.
[219] F. M. Salem and A. S. Ali, "SOS: Self-organized secure framework for VANET," *Int. J. Commun. Syst.*, vol. 33, no. 7, May 2020, Art. no. e4317, doi: 10.1002/dac.4317.
[220] A. Yang, D. Boshoff, Q. Hu, G. P. Hancke, X. Luo, J. Weng, K. Mayes, and K. Markantonakis, "Privacy-preserving group authentication for RFID tags using bit-collision patterns," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11607–11620, Jul. 2021, doi: 10.1109/JIOT.2021.3059047.
[221] B. Sheng and Q. Li, "Verifiable privacy-preserving sensor network storage for range query," *IEEE Trans. Mobile Comput.*, vol. 10, no. 9, pp. 1312–1326, Sep. 2011, doi: 10.1109/TMC.2010.236.
[222] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102354, doi: 10.1016/j.jisa.2019.06.010.

[223] Z. Guan, X. Lu, W. Yang, L. Wu, N. Wang, and Z. Zhang, "Achieving efficient and privacy-preserving energy trading based on blockchain and ABE in smart grid," *J. Parallel Distrib. Comput.*, vol. 147, pp. 34–45, Jan. 2021, doi: 10.1016/j.jpdc.2020.08.012.

[224] S. Zhao, F. Li, H. Li, R. Lu, S. Ren, H. Bao, J.-H. Lin, and S. Han, "Smart and practical privacy-preserving data aggregation for fog-based smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 521–536, 2021, doi: 10.1109/TIFS.2020.3014487.

[225] L. Chen, J. Zhou, Y. Chen, Z. Cao, X. Dong, and K.-K.-R. Choo, "PADP: Efficient privacy-preserving data aggregation and dynamic pricing for Vehicle-to-Grid networks," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 7863–7873, May 2021, doi: 10.1109/JIOT.2020.3041117.

[226] I. Ali, T. Lawrence, A. A. Omala, and F. Li, "An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11266–11280, Oct. 2020, doi: 10.1109/TVT.2020.3008781.

[227] C. Ma, K. Xue, and P. Hong, "Distributed access control with adaptive privacy preserving property for wireless sensor networks," *Secur. Commun. Netw.*, vol. 7, no. 4, pp. 759–773, Apr. 2014, doi: 10.1002/sec.777.

[228] E. Vahedi, M. Bayat, M. R. Pakravan, and M. R. Aref, "A secure ECC-based privacy preserving data aggregation scheme for smart grids," *Comput. Netw.*, vol. 129, pp. 28–36, Dec. 2017, doi: 10.1016/j.comnet.2017.08.025.

[229] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, "Proximity-based security techniques for mobile users in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2089–2100, Dec. 2013, doi: 10.1109/TIFS.2013.2286269.

[230] 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, 2017, doi: 10.1007/s10586-017-0848-x.

[231] M. Zhou, Y. Zheng, Y. Guan, L. Peng, and R. Lu, "Efficient and privacy-preserving range-max query in fog-based agricultural IoT," *Peer Peer Netw. Appl.*, vol. 14, no. 4, pp. 2156–2170, Jul. 2021, doi: 10.1007/s12083-021-01179-2.

[232] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Inf. Sci.*, vol. 479, pp. 567–592, Apr. 2019, doi: 10.1016/j.ins.2018.02.005.

[233] I. Ali, Y. Chen, N. Ullah, R. Kumar, and W. He, "An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1278–1291, Feb. 2021, doi: 10.1109/TVT.2021.3050399.

[234] H. Tan, S. Xuan, and I. Chung, "HCDA: Efficient pairing-free homographic key management for dynamic cross-domain authentication in VANETs," *Symmetry*, vol. 12, no. 6, p. 1003, Jun. 2020, doi: 10.3390/sym12061003.

[235] I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in VANETs," *Veh. Commun.*, vol. 22, Apr. 2020, Art. no. 100228, doi: 10.1016/j.vehcom.2019.100228.

[236] S. Doss, J. Paranthaman, S. Gopalakrishnan, A. Duraisamy, S. Pal, B. Duraisamy, C. L. Van, and D.-N. Le, "Memetic optimization with cryptographic encryption for secure medical data transmission in IoT-based distributed systems," *Comput., Mater. Continua*, vol. 66, no. 2, pp. 1577–1594, 2021.

[237] P. Kumar, R. Kumar, G. Srivastava, G. P. Gupta, R. Tripathi, T. R. Gadekallu, and N. N. Xiong, "PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2326–2341, Jul. 2021, doi: 10.1109/TNSE.2021.3089435.

[238] A. Alharthi, Q. Ni, and R. Jiang, "A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET," *IEEE Access*, vol. 9, pp. 87299–87309, 2021, doi: 10.1109/ACCESS.2021.3086225.

[239] A. Alsaafin, I. A. Qasse, M. A. Talib, and Q. Nasir, "Lightweight blockchain-based system for Internet of Things security," in *Proc. SoutheastCon*, Mar. 2020, pp. 1–8.

[240] Q. Zhang, Y. Zhang, C. Li, C. Yan, Y. Duan, and H. Wang, "Sport location-based user clustering with privacy-preservation in wireless IoT-driven healthcare," *IEEE Access*, vol. 9, pp. 12906–12913, 2021, doi: 10.1109/ACCESS.2021.3051051.

[241] D. E. Majdoubi, H. El Bakkali, and S. Sadki, "Towards smart blockchain-based system for privacy and security in a smart city environment," in *Proc. 5th Int. Conf. Cloud Comput. Artif. Intell., Technol. Appl. (CloudTech)*, Nov. 2020, pp. 1–7, doi: 10.1109/CloudTech49835.2020.9365905.

[242] W. Yang, S. Wang, G. Zheng, J. Yang, and C. Valli, "A privacy-preserving lightweight biometric system for Internet of Things security," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 84–89, Mar. 2019, doi: 10.1109/MCOM.2019.1800378.

[243] B. S. Egala, S. Priyanka, and A. K. Pradhan, "SHPI: Smart healthcare system for patients in ICU using IoT," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst., (ANTS)*, Dec. 2019, pp. 1–6, doi: 10.1109/ANTS47819.2019.9118084.

[244] R. Goyat, G. Kumar, M. Alazab, M. Conti, M. K. Rai, R. Thomas, R. Saha, and T.-H. Kim, "Blockchain-based data storage with privacy and authentication in Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14203–14215, Aug. 2022.

[245] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "An efficient selective miner consensus protocol in blockchain oriented IoT smart monitoring," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Feb. 2019, pp. 1135–1142, doi: 10.1109/ICIT.2019.8754936.

[246] G. S. Aujla and A. Jindal, "A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 491–499, Feb. 2021, doi: 10.1109/JSAC.2020.3020655.

[247] S. Li, T. Qin, and G. Min, "Blockchain-based digital forensics investigation framework in the Internet of Things and social systems," *IEEE Trans. Computat. Social Syst.*, vol. 6, no. 6, pp. 1433–1441, Dec. 2019, doi: 10.1109/TCSS.2019.2927431.

[248] A. Rahman, M. J. Islam, F. A. Sunny, and M. K. Nasir, "DistBlockSDN: A distributed secure blockchain based SDN-IoT architecture with NFV implementation for smart cities," in *Proc. 2nd Int. Conf. Innov. Eng. Technol. (ICIET)*, Dec. 2019, pp. 1–6.

[249] W. Lv, S. Wu, C. Jiang, Y. Cui, X. Qiu, and Y. Zhang, "Towards large-scale and privacy-preserving contact tracing in COVID-19 pandemic: A blockchain perspective," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 282–298, Jan. 2022, doi: 10.1109/TNSE.2020.3030925.

[250] C. Patsonakis, S. Terzi, I. Moschos, D. Ioannidis, K. Votis, and D. Tzovaras, "Permissioned blockchains and virtual nodes for reinforcing trust between aggregators and prosumers in energy demand response scenarios," in *Proc. IEEE Int. Conf. Environ. Electr. Eng. IEEE Ind. Commercial Power Syst. Eur. (EEEIC/I&CPS Eur.)*, Jun. 2019, pp. 1–6.

[251] R. Singh, T. Ahmed, A. K. Singh, P. Chanak, and S. K. Singh, "SeizSClas: An efficient and secure Internet-of-Things-Based EEG classifier," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6214–6221, Apr. 2021, doi: 10.1109/JIOT.2020.3030821.

[252] G. Ali, "xDBAuth: Blockchain based cross domain authentication and authorization framework for Internet of Things," *IEEE Access*, vol. 8, pp. 58800–58816, 2020, 2020, doi: 10.1109/ACCESS.2020.2982542.

[253] J. Ranjith and K. Mahantesh, "Blockchain-based knapsack system for security and privacy preserving to medical data," *Social Netw. Comput. Sci.*, vol. 2, no. 4, p. 245, Jul. 2021, doi: 10.1007/s42979-021-00568-x.

[254] Y. Liu, J. Zhang, and J. Zhan, "Privacy protection for fog computing and the Internet of Things data based on blockchain," *Cluster Comput.*, vol. 24, no. 2, pp. 1331–1345, Jun. 2021, doi: 10.1007/s10586-020-03190-3.

[255] C. Lin, D. He, S. Zeadally, N. Kumar, and K.-K.-R. Choo, "SecBCS: A secure and privacy-preserving blockchain-based crowdsourcing system," *Sci. China Inf. Sci.*, vol. 63, no. 3, pp. 1–14, Mar. 2020, doi: 10.1007/s11432-019-9893-2.

[256] A. H. Sodhro, S. Pirbhulal, M. Muzammal, and L. Zongwei, "Towards blockchain-enabled security technique for industrial Internet of Things based decentralized applications," *J. Grid Comput.*, vol. 18, no. 4, pp. 615–628, Dec. 2020, doi: 10.1007/s10723-020-09527-x.

[257] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology," *J. Supercomput.*, vol. 77, no. 8, pp. 7916–7955, 2021, doi: 10.1007/s11227-020-03570-x.

[258] M. Altulyan, L. Yao, S. S. Kanhere, X. Wang, and C. Huang, "A unified framework for data integrity protection in people-centric smart cities," *Multimedia Tools Appl.*, vol. 79, nos. 7–8, pp. 4989–5002, Feb. 2020, doi: 10.1007/s11042-019-7182-7.

[259] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–14, Dec. 2020, doi: 10.1186/s13673-020-0214-5.

[260] C.-Y. Yang, C.-T. Huang, Y.-P. Wang, Y.-W. Chen, and S.-J. Wang, "File changes with security proof stored in cloud service systems," *Pers. Ubiquitous Comput.*, vol. 22, no. 1, pp. 45–53, Feb. 2018, doi: 10.1007/s00779-017-1090-5.

[261] K. Shi, L. Zhu, C. Zhang, L. Xu, and F. Gao, "Blockchain-based multimedia sharing in vehicular social networks with privacy protection," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 8085–8105, Mar. 2020, doi: 10.1007/s11042-019-08284-8.

[262] P. Kumar, G. P. Gupta, and R. Tripathi, "TP2SF: A trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning," *J. Syst. Archit.*, vol. 115, May 2021, Art. no. 101954, doi: 10.1016/j.sysarc.2020.101954.

[263] A. Ouaddah, "A blockchain based access control framework for the security and privacy of IoT with strong anonymity unlinkability and intractability guarantees," *Adv. Comput.*, vol. 115, pp. 211–258, Jan. 2019, doi: 10.1016/bs.adcom.2018.11.001.

[264] S. Badr, I. A. Gomaa, and E. Abd-Elrahman, "Multi-tier blockchain framework for IoT-EHRs systems," in *Proc. 9th Int. Conf. Emerg. Ubiquitous Syst. Pervasive Netw. (EUSPN) 8th Int. Conf. Current Future Trends Inf. Commun. Technol. Healthcare (ICTH)/Affiliated Workshops*, Nov. 2018, pp. 159–166.

[265] A. S. Patil, R. Hamza, A. Hassan, N. Jiang, H. Yan, and J. Li, "Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101958, doi: 10.1016/j.cose.2020.101958.

[266] A. R. Shahid, N. Pissinou, L. Njilla, S. Alemany, A. Imteaj, K. Makki, and E. Aguilar, "Quantifying location privacy in permissioned blockchain-based Internet of Things (IoT)," in *Proc. 16th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services*, Nov. 2019, pp. 116–125.

[267] P. Shrestha and N. Saxena, "Hacksaw: Biometric-free non-stop Web authentication in an emerging world of wearables," in *Proc. 13th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jul. 2020, pp. 13–24.

[268] Y.-L. Gao, X.-B. Chen, G. Xu, W. Liu, M.-X. Dong, and X. Liu, "A new blockchain-based personal privacy protection scheme," *Multimedia Tools Appl.*, vol. 80, no. 20, pp. 30677–30690, Aug. 2021.

[269] C. Patel, "IoT privacy preservation using blockchain," *Inf. Secur. J., Global Perspective*, vol. 31, no. 5, pp. 566–581, 2021.

[270] J. Noh, S. Jeon, and S. Cho, "Distributed blockchain-based message authentication scheme for connected vehicles," *Electronics*, vol. 9, no. 1, p. 74, Jan. 2020.

[271] L. Fang, Y. Wu, C. Wu, and Y. Yu, "A nonintrusive elderly home monitoring system," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2603–2614, Feb. 2021, doi: 10.1109/JIOT.2020.3019270.

[272] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019, doi: 10.1109/ACCESS.2019.2936575.

[273] H. J. Jo and W. Choi, "BPRF: Blockchain-based privacy-preserving reputation framework for participatory sensing systems," *PLoS ONE*, vol. 14, no. 12, pp. 1–23, Dec. 2019, doi: 10.1371/journal.pone.0225688.

[274] A. F. M. S. Akhter, M. Ahmed, A. F. M. S. Shah, A. Anwar, and A. Zengin, "A secured privacy-preserving multi-level blockchain framework for cluster based VANET," *Sustainability*, vol. 13, no. 1, p. 400, Jan. 2021.

[275] P. Lv, L. Wang, H. Zhu, W. Deng, and L. Gu, "An IoT-oriented privacy-preserving publish/subscribe model over blockchains," *IEEE Access*, vol. 7, pp. 41309–41314, 2019, doi: 10.1109/ACCESS.2019.2907599.

[276] S. Zou, J. Xi, H. Wang, and G. Xu, "CrowdBLPS: A blockchain-based location-privacy-preserving mobile crowdsensing system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4206–4218, Jun. 2020, doi: 10.1109/TII.2019.2957791.

[277] M. H. Chinaei, H. H. Gharakheili, and V. Sivaraman, "Optimal witnessing of healthcare IoT data using blockchain logging contract," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 10117–10130, Jun. 2021, doi: 10.1109/JIOT.2021.3051433.

[278] S. Singh, D. Satish, and S. R. Lakshmi, "Ring signature and improved multi-transaction mode consortium blockchain-based private information retrieval for privacy-preserving smart parking system," *Int. J. Commun. Syst.*, vol. 34, no. 14, Sep. 2021, Art. no. e4911, doi: 10.1002/dac.4911.

[279] Q. Yaseen and Y. Jararweh, "Building an intelligent global IoT reputation and malicious devices detecting system," *J. Netw. Syst. Manage.*, vol. 29, no. 4, p. 45, Oct. 2021, doi: 10.1007/s10922-021-09611-x.

[280] V. Prabhakaran and A. Kulandasamy, "Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection," *Neural Comput. Appl.*, vol. 33, no. 21, pp. 14459–14479, Nov. 2021, doi: 10.1007/s00521-021-06085-5.

[281] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things," *Pers. Ubiquitous Comput.*, pp. 1–14, Jun. 2021, doi: 10.1007/s00779-021-01583-8.

[282] W. M. Kang, S. Y. Moon, and J. H. Park, "An enhanced security framework for home appliances in smart home," *Hum.-Centric Comput. Inf. Sci.*, vol. 7, no. 1, pp. 1–12, Dec. 2017, doi: 10.1186/s13673-017-0087-4.

[283] C. Zhang, C. Li, and J. Zhang, "A secure privacy-preserving data aggregation model in wearable wireless sensor networks," *J. Electr. Comput. Eng.*, vol. 2015, Jan. 2015, Art. no. 104286, doi: 10.1155/2015/104286.

[284] D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 1, pp. 316–326, Jan. 2014, doi: 10.1109/JBHI.2013.2268897.

[285] S. K. Sood, "Mobile fog based secure cloud-IoT framework for enterprise multimedia security," *Multimedia Tools Appl.*, vol. 79, nos. 15–16, pp. 10717–10732, Apr. 2020, doi: 10.1007/s11042-019-08573-2.

[286] Z. Xu, R. Gu, T. Huang, H. Xiang, X. Zhang, L. Qi, and X. Xu, "An IoT-oriented offloading method with privacy preservation for cloudlet-enabled wireless metropolitan area networks," *Sensors*, vol. 18, no. 9, p. 3030, Sep. 2018, doi: 10.3390/s18093030.

[287] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. Comput. Intell. Secur.*, Dec. 2013, pp. 663–667, doi: 10.1109/CIS.2013.145.

[288] T. Menzies, E. Kocagüneli, L. Minku, F. Peters, and B. Turhan, "How to keep your data private," in *Sharing Data and Models in Software Engineering*, T. Menzies, E. Kocagüneli, L. Minku, F. Peters, and B. Turhan, Eds. Boston, MA, USA: Morgan Kaufmann, 2015, pp. 165–196. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780124172951000163

[289] M. J. Gajjar, "Sensor security and location privacy," in *Mobile Sensors and Context-Aware Computing*, M. J. Gajjar, Ed. San Mateo, CA, USA: Morgan Kaufmann, 2017, pp. 223–265. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128016602000094

[290] N. Madaan, M. A. Ahad, and S. M. Sastry, "Data integration in IoT ecosystem: Information linkage as a privacy threat," *Comput. Law Secur. Rev.*, vol. 34, no. 1, pp. 125–133, Feb. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364917301358

[291] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 3–18, doi: 10.1109/SP.2017.41.

[292] M. Naveed, S. Kamara, and C. V. Wright, "Inference attacks on property-preserving encrypted databases," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2015, pp. 644–655, doi: 10.1145/2810103.2813651.

[293] G. Sagirlar, B. Carminati, and E. Ferrari, "Decentralizing privacy enforcement for Internet of Things smart objects," *Comput. Netw.*, vol. 143, pp. 112–125, Oct. 2018, doi: 10.1016/j.comnet.2018.07.019.

[294] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the smart home: Privacy attacks and defenses on encrypted IoT traffic," 2017, *arXiv:1708.05044*.

[295] A. Narayanan, J. Huey, and E. W. Felten, *A Precautionary Approach to Big Data Privacy*. Dordrecht, The Netherlands: Springer, 2016, pp. 357–385.

[296] J. Abowd, L. Alvisi, C. Dwork, S. Kannan, A. Machanavajjhala, and J. Reiter, "Privacy-preserving data analysis for the federal statistical agencies," 2017, *arXiv:1701.00752*.

[297] Y. Shen, X. He, Y. Han, and Y. Zhang, "Model stealing attacks against inductive graph neural networks," 2021, *arXiv:2112.08331*.

[298] K. Wang, Y. Fu, K. Li, A. Khisti, R. S. Zemel, and A. Makhzani, "Variational model inversion attacks," in *Proc. Neural Inf. Process. Syst. 34, Annu. Conf. Neural Inf. Process. Syst. (NeurIPS)*, M. Ranzato, A. Beygelzimer, Y. N. Dauphin, P. Liang, and J. W. Vaughan, Eds., Dec. 2021, pp. 9706–9719. [Online]. Available: https://proceedings.neurips.cc/paper/2021/hash/50a074e6a8da4662ae0a29edde722179-Abstract.html

[299] N. Carlini, C. Liu, Ú. Erlingsson, J. Kos, and D. Song, "The secret sharer: Evaluating and testing unintended memorization in neural networks," 2018, *arXiv:1802.08232*.

[300] 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.

[301] D. I. K. Sjoeberg, "A survey of controlled experiments in software engineering," *IEEE Trans. Softw. Eng.*, vol. 31, no. 9, pp. 733–753, Sep. 2005, doi: 10.1109/TSE.2005.97.

DAMIANO TORRE (Member, IEEE) received the B.Sc. degree from the University of Bari, Italy, in 2009, the M.Sc. degree from the University of Castilla-La Mancha, Spain, in 2011, and the Ph.D. degree from Carleton University, Canada, in 2018. He is currently an Associate Research Scientist with the Department of Computer Information Systems, Texas A&M University Central Texas, USA. He is involved in a research project with U.S. agencies. His research interests include computer science, and more specifically on software engineering, cybersecurity, artificial intelligence, model-driven engineering, and empirical software engineering. Prior to coming to the USA, he was a Research Associate at the University of Luxembourg, from 2018 to 2021. He regularly serves on the organizing/program committees of ISSRE and QRS and satellite events of EMSE, ICSE, and ASE.

ANITHA CHENNAMANENI (Member, IEEE) received the Ph.D. degree in business administration with a major in information systems and a minor in computer science from The University of Texas at Arlington. She is currently the Chair and an Associate Professor of computer information systems with Texas A&M University Central Texas. Her research interests include cybersecurity, machine learning, the Internet of Things, artificial intelligence, data analytics, digital forensics, information privacy, and knowledge management.

ALEX RODRIGUEZ is currently pursuing the bachelor's degree in business administration for computer information systems with Texas A&M University Central Texas. He was worked with Texas A&M University Central Texas as a Student Worker and currently focused on his academics and personal programming projects.