Privacy-Preserving Tools and Technologies
Government Adoption and Challenges

Prabowo, Sidik; Putrada, Aji Gautama; Oktaviani, Ikke Dian; Abdurohman, Maman; Janssen, Marijn; Nuha, Hilal Hudan; Sutikno, Sarwono

DOI
10.1109/ACCESS.2025.3540878

Publication date
2025

Document Version
Final published version

Published in
IEEE Access

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 15 January 2025, accepted 6 February 2025, date of publication 11 February 2025, date of current version 25 February 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3540878

SURVEY

Privacy-Preserving Tools and Technologies: Government Adoption and Challenges

SIDIK PRABOWO[1], (Student Member, IEEE), AJI GAUTAMA PUTRADA[1], (Member, IEEE), IKKE DIAN OKTAVIANI[1], (Graduate Student Member, IEEE), MAMAN ABDUROHMAN[1], (Member, IEEE), MARIJN JANSSEN[2], HILAL HUDAN NUHA[1], (Senior Member, IEEE), AND SARWONO SUTIKNO[3], (Member, IEEE)

[1]School of Computing, Telkom University, Bandung 40287, Indonesia
[2]Technology, Policy and Management, Delft University of Technology, 2628 CD Delft, The Netherlands
[3]School of Informatics Engineering, Institut Teknologi Sumatera, Lampung 35365, Indonesia

Corresponding author: Sidik Prabowo (prabowo@student.telkomuniversity.ac.id)

This work was supported by Telkom University Research and Community Services (PPM) through International Collaboration Scheme under Grant 514/PNLT3/PPM/2023.

ABSTRACT Understanding the landscape of privacy protection in governmental systems is crucial for ensuring the trustworthiness of public services and safeguarding citizens' sensitive data from breaches or misuse. Systematic mapping and synthesis of previous research can help identify existing privacy-preserving techniques, assess their effectiveness, and highlight areas for improvement, offering valuable insights for policymakers and practitioners. We aim to conduct a systematic literature review (SLR) of privacy-preserving tools and technologies, focusing on their adoption and governments' challenges. This study also uncovers emerging trends and future research directions, contributing to developing more robust privacy strategies tailored to government needs.Given its extensive reach and government-centric methodology, this evaluation distinguishes itself from previous research. Our work methodically synthesizes privacy-preserving tools and technologies from the distinct perspective of government roles, in contrast to previous assessments that concentrate narrowly on certain technologies or areas. Our findings offer a synthesis of the government's diverse roles in privacy preservation—regulator, enforcer, user, and service provider—and address existing concerns and key privacy-related technologies. Finally, we identify significant research opportunities, such as improving privacy-preserving mechanisms to strengthen the integrity of public services and mitigate the risks of data breaches and misuse.

INDEX TERMS Privacy, regulation, privacy-preserving mechanisms, government, systematic literature study.

I. INTRODUCTION

Privacy-preserving tools are essential for safeguarding sensitive information while maintaining the effectiveness of government operations.These tools, such as a platform for privacy preference (P3P), privacy-enhancement technologies (PETs), pseudonymization, cryptography (e.g., pretty good privacy (PGP), public key infrastructure (PKI), digital signatures), and other emerging technologies, are rapidly evolving and reshaping the landscape of privacy protection in government [1]. Although various PETs are available for government agencies, effectively addressing privacy requirements can pose challenges [2]. One of the main challenges is the changing business environment, which requires increased automation to protect privacy online. Government agencies are faced with the challenge of properly addressing privacy requirements in a global context. In the digital age, privacy and data protection have grown more complicated, necessitating a thorough strategy that considers the social, legal, technological, and economic aspects. The abundance of data generated by human actions necessitates reevaluating the rules controlling data access and analysis by

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

powerful organizations and governments, and this presents a vital concern for privacy.

Governments often rely on frameworks such as the Fair Information Practice Principles (FIPPs) to address these challenges, which provide a structured approach to privacy and data protection. FIPPs are a formalized model based on six protection goals, where these principles guide the design, implementation, and evaluation of privacy-preserving systems and practices. The six goals include transparency, which emphasizes the importance of informing individuals about data collection and processing activities; participation, which advocates for allowing individuals to control their personal information; purpose specification, which entails specifying the purposes for which data is collected and used; data minimization, which promotes gathering as little data as is required for the stated goals; data quality and integrity, which emphasizes the importance of ensuring accuracy and reliability of data; and security protections, which entail putting in place the necessary controls to guard against misuse, disclosure, and illegal access to data. Organizations and legislators can use these principles to guide the development and functioning of information systems and procedures by adhering to these protective aims.

The usability of privacy-preserving tools and technologies (PETs) in the public sector is a key factor determining their adoption and effectiveness [3]. Governments must prioritize user-friendly interfaces, clear instructions, and adequate training to ensure smooth integration and minimal workflow disruption. Government employees often encounter challenges when adopting and implementing these tools, yet there is no comprehensive overview of their typical obstacles. Usability is frequently cited as a major hurdle, as these technologies, though beneficial for safeguarding privacy and data, can be difficult to implement. Therefore, a systematic literature review is essential to explore the challenges and usability factors affecting the effective use of privacy-preserving tools in government.

This paper aims to conduct a systematic literature study (SLR) about government adoption and challenges related to privacy-preserving tools and technology. The first step is to define the research questions, which involves clarifying the specific inquiries or objectives that the systematic literature review aims to address, ensuring a clear focus and purpose for the study. Next, we explain that the search strategy entails devising a comprehensive and systematic approach to identify relevant literature, including specifying search terms, databases, and inclusion/exclusion criteria. Selecting and executing the data extraction involves systematically retrieving and recording relevant data from the selected studies, using standardized forms or templates to ensure consistency and completeness. Finally, our last step is synthesis, which involves analyzing and interpreting the extracted data to identify patterns, themes, and relationships, ultimately deriving meaningful insights and conclusions from the synthesized evidence.

Motivated by the increasing complexity of privacy challenges in government operations, this review takes a distinctive government-centric approach to synthesizing privacy-preserving tools and technologies. Unlike previous studies, which are often constrained to specific technologies or domains, our work systematically examines privacy mechanisms through the multifaceted roles of government—as regulator, enforcer, user, and service provider. To bridge the gap between technical capabilities and policy needs, we introduce a novel taxonomy that organizes privacy solutions based on their applications and underlying technologies. Furthermore, we explore cross-domain applications and identify critical research opportunities, focusing on scalability, usability, and regulatory alignment—key factors for effective government adoption. The following are our key contributions:

1) A mind map that synthesizes a body of knowledge on privacy-preserving mechanisms related to the government.
2) A qualitative synthesis of the government's roles and challenges.
3) An analysis of privacy-preserving mechanisms in the government with sub-implementations, advantages, and prospects.
4) A discussion of research opportunities and the future direction of privacy-preserving mechanisms related to the government.

The remainder of this paper is organized as follows: Section II discusses related survey papers and how our SLR fills the gap in state-of-the-art survey papers. Section III describes the SLR methodology. Section IV discusses three important contents: The search results of the SLR—the answer to the SLR's research question. Also, there is a discussion of future works. Lastly, Section V summarizes the important findings in our SLR.

II. RELATED WORKS

Several survey papers' content relates to privacy preservation mechanisms and the government. A privacy taxonomy that established a relationship between various data types and appropriate privacy-preserving mechanisms for those data types' characteristics was proposed by Cunhaet al. [4]. The taxonomy identifies open challenges and future directions, specifically developing novel privacy-preserving mechanisms. The paper's main concern is about data types. The SLR provided a comprehensive mapping between data types and privacy-preserving mechanisms. It also measured the strengths and weaknesses of each mechanism. However, the paper did not discuss the relationship with the government.

In a survey paper, Patil et al. [5] covered differential privacy techniques for data privacy and provided the foundational differential privacy algorithms for privacy-preserving data analysis. They identified state-of-the-art issues and future research directions. However, the paper primarily focuses on differential privacy, whereas various other privacy-preserving mechanisms exist and offer interesting capabilities. A comparison of the strengths and weaknesses of each method is a research opportunity.

A review of privacy-preserving Electronic Toll Collection (ETC) schemes, including their components, technologies, security features, privacy properties, and attacks on ETC systems (ETCS), was described in the work by Jolfaei et al. [6]. The paper provides comprehensive methods for privacy attacks surrounding ETCS. However, other fields such as IoT, healthcare, law, finance, and the web also possess problems concerning privacy preservation. There is a research opportunity for an SLR that discusses privacy concerns in various fields.

To address the problems with the pre-established voting technique, Priya et al. [7] built an online voting system using blockchain technology. They also implemented SHA 256 algorithm hashing for secure password hashing. The paper exercised the use of blockchain as a part of the privacy preservation mechanism, which is implemented in online voting and is related to the election of an eligible government. However, the paper lacks discussion about state-of-the-art methods, problems, and government roles in privacy preservation. There is a research opportunity to discuss the government's role in facing privacy preservation.

Wang et al. [8] conducted a thorough analysis of the current state of research and development trends regarding location privacy protection mechanisms in continuous location-based services (LBSs). The study classified five existing technologies and provided descriptions of their privacy efficiency, technological solutions, and application scenarios based on a timeline. The survey paper also outlined challenges for future research in location privacy protection. However, there are ample other research challenges and future directions due to government roles and different fields of concern.

In 2020, Yang et al. [9] examined privacy-preserving technology in machine learning applications, presented models for privacy-preserving protocols, and summarized the key technologies in this field. Models and methods for privacy-preserving machine learning protocols were presented in the article. Additionally, they addressed issues examining machine learning methods that protect privacy. However, the last few years have witnessed the emergence of state-of-the-art technologies, such as edge computing and federated learning. There is a research opportunity to discuss these technologies as privacy-preserving mechanisms that promote decentralization.

The main challenges raised by privacy constraints are discussed in the article by Carvalho et al. [10], along with the main approaches to overcome them, a review of the taxonomies of privacy-preserving mechanisms, a theoretical analysis of previous comparative studies, and several open issues. Unlike other research, the paper served as an in-depth discussion of the trade-offs between privacy protection and data utilization. However, the survey paper mainly discusses anonymization and perturbation techniques. On the other hand, there is a research opportunity to discuss different methods that maintain data utility, such as homomorphic encryption.

Shimona [11] briefly presented the privacy-preserving data mining (PPDM) techniques and other privacy preservation methods to prevent and safeguard the data from unauthorized parties. The paper presented PPDM techniques and other privacy preservation methods, the aim of which is to prevent unauthorized access to secured data. However, the paper is too brief as it discusses privacy preservation, specifically in data mining, and cites a limited number of 23 references.

Tanuwidjaja et al. [12] examined the most recent developments in privacy-preserving deep learning, assessed all available techniques, contrasted the benefits and drawbacks of each strategy, and discussed problems and obstacles in the field of privacy-preserving deep learning. This paper also mentioned that there is a tradeoff between privacy and performance. However, there is a need to discuss future challenges in combining deep learning techniques with other techniques that preserve data utility.

Kurupathi et al. [13] explained federated learning, a range of federated architectures, and various privacy-preserving mechanisms. The paper also illustrated how federated learning is an emerging field of study that could usher in a new era in artificial intelligence and machine learning. The paper discussed in-depth the types of federated learning, such as centralized, peer-to-peer, and decentralized federated learning. However, the paper did not discuss how federated learning and the government can mutually collaborate.

The survey study by Cui et al. [14] addressed the shortcomings of current approaches and future growth directions. It concentrated on various strategies to safeguard the private information of individuals on the blockchain and in recently emerging fields that combine blockchain technology. However, the paper did not discuss how blockchain and the government can mutually collaborate. Table 1 compares all related survey papers on privacy preservation mechanisms related to the government and displays research opportunities for our survey paper.

Recent privacy-preserving schemes have also demonstrated significant advancements in addressing privacy and trust in specific domains, like vehicular networks. For example, the Privacy-Preserving Reputation Updating Scheme (PPRU) focuses on safeguarding reputation updates in cloud-assisted vehicular networks. While PPRU is effective in its domain, it does not address the cross-domain challenges central to our review, such as integrating privacy technologies into government roles like regulation and service provision [15].

The Balancing Trust Management and Privacy Preservation (BTMPP) scheme balances privacy and trust management during emergency message dissemination in vehicular networks. However, BTMPP is narrowly focused on vehicular communication. In contrast, our review provides a broader perspective, exploring privacy-preserving tools in diverse sectors such as healthcare, IoT, and public administration [16].

Similarly, the Privacy-Preserving Trust Management Scheme (PPTM) for space-air-ground integrated vehicular networks excels in managing trust for emergency message dissemination. Nonetheless, its application remains confined to vehicular systems, whereas our review highlights challenges like scalability and usability pertinent to privacy technologies in government contexts [17].

A lightweight privacy-preserving scheme with efficient reputation management has also been proposed for mobile crowd-sensing in vehicular networks. This approach optimizes reputation management while reducing computational overhead. However, unlike this scheme, our review extends beyond specific domains to propose a taxonomy of privacy mechanisms that include blockchain, federated learning, and differential privacy to meet government-specific requirements [15].

Lastly, trust-based privacy management systems leveraging blockchain and smart contracts have been developed to secure vehicular network communications. While these systems efficiently classify vehicles based on trust levels, they are limited to vehicular systems. Our review, by contrast, emphasizes the generalizability of privacy-preserving tools across domains and their unique applicability in government operations [16].

III. RESEARCH METHODOLOGY

This study uses an SLR following multiple steps [18], [19]. The main stages are defining the research question, creating a search strategy, making a selection, and then carrying out data extraction and synthesis.

A. RESEARCH QUESTION

The initial stage of SLR is to define several research questions (RQs). This stage is important because the motivation of an SLR can be seen from its RQs [20]. We form three RQs to be answered in this SLR, namely:

- RQ1: What are government agencies' key roles and responsibilities in implementing and regulating privacy-preserving mechanisms?
- RQ2: What governmental ministries or departments across various sectors integrate privacy-preserving technologies to protect sensitive data while balancing transparency and accountability in data handling practices?
- RQ3: What are the current trends and innovations in privacy-preserving technologies utilized by and related to governments?

B. SEARCHING AND SELECTION STRATEGY

The searching and selection strategy includes two main activities: searching based on the inclusion criteria and selection based on the exclusion criteria. The search starts with applying the inclusion criteria, followed by scraping to gather several papers based on several specifications [253]. The inclusion criteria for this study are:

- Database: Google Scholar, ACM Digital Library, IEEExplore, Elsevier Scopus, Wiley Interscience, and BibSonomy.
- Title strings: "privacy-preserving mechanism" and "government."
- Keyword strings: "privacy-preserving mechanism," "government."
- Year: between 2006 and 2023.
- Language: English.
- Publication type: Journal, conference, and book chapter.
- Document type: PDF, HTML.

We have different title and keyword criteria strings to balance sensitivity and specificity. After scraping based on the inclusion criteria, the next stage is selection based on the exclusion criteria [21]. The first activity in selection excludes all closed-access research papers. Then, it is followed by excluding all duplicate titles. The next step is to exclude papers from non-selected publishers (ACM, IEEE, Elsevier, Wiley, MDPI, KoreaScience, Hindawi, Springer, HeinOnline, IGI-Global, arXiv, Sage, Taylor & Francis). After term analysis, we maintain the context of related terms by deleting papers whose titles and abstracts do not contain the expected terms. Finally, publication types that are not research articles and have unsuitable content should be excluded.

C. DATA EXTRACTION AND SYNTHESIS

In this SLR's data extraction and synthesis step, we thoroughly collect relevant information from selected studies to address the research objectives and answer key questions. This phase systematically extracts data elements such as important terms, keywords, and study characteristics, mined from methodology details, key findings, and other pertinent information identified during the screening and eligibility assessment stages.

Once data extraction is complete, we move on to the synthesis stage, where we analyze and interpret the extracted data to identify patterns, trends, and relationships within the literature. This involves organizing and categorizing the extracted data based on thematic similarities or theoretical frameworks, facilitating a structured approach to data synthesis. We employ qualitative synthesis techniques such as thematic analysis, content analysis, or meta-synthesis to derive meaningful insights and interpretations from the collected data. In the first stage, a broad synthesis of the body of knowledge is created and represented in a full-scale mind map.

During synthesis, we critically evaluate and compare the quality and relevance of the extracted data, considering factors such as problems, solutions, and potential future opportunities. This process involves synthesizing evidence from diverse sources to develop a coherent and nuanced understanding of the research topic, often through iterative refinement and validation of emerging themes and

TABLE 1. Related paper survey comparisons on privacy-preservation mechanisms related to the government.

Survey Paper	Discussion and Strength	Limitation	Scenario	Attributes
Cunha *et al.* [4]	Comprehensively maps data types and privacy-preserving mechanisms. It also measures the strengths and weaknesses of each mechanism.	The paper did not discuss the relationship between the mechanisms and the government.	Data Types	Anonymization, Usability*, Scalability*
Patil *et al.* [5]	A survey work that covered differential privacy mechanisms for data privacy and provided the ground-breaking differential privacy algorithms that allow for privacy-preserving data analysis.	The paper is too niche regarding differential privacy, whereas various other privacy-preserving mechanisms exist and offer interesting capabilities. A comparison of the strengths and weaknesses of each method is a research opportunity.	Differential Privacy	Differential Privacy , Scalability, Usability*
Jolfaei *et al.* [6]	A review of privacy-preserving ETC systems covered ETCS, security features, technology, and components. The report offers thorough strategies for privacy breaches related to ETCS.	Other fields such as IoT, healthcare, law, finance, and the web also possess problems concerning privacy preservation.	ETC Systems	Anonymization, Encryption, Usability*, Scalability*
Priya *et al.* [7]	The paper exercised the use of blockchain as a part of the privacy-preservation mechanism, which is implemented in online voting and is related to the election of an eligible government.	The paper lacks discussion about state-of-the-art methods, problems, and government roles in privacy preservation.	Blockchain Voting	Encryption, Usability*, Scalability*
Wang *et al.* [8]	The survey paper outlined challenges for future research in location privacy protection.	A research opportunity lies in ample other research challenges and future direction due to government roles and different fields of concern.	Location Privacy	Anonymization, Scalability, Usability*
Yang *et al.* [9]	A survey paper from 2020. Models and methods for privacy-preserving machine learning protocols were presented in the article. Additionally, it addressed issues still present in examining machine learning methods that protect privacy.	The last few years have witnessed the emergence of state-of-the-art technologies such as edge computing and federated learning.	Machine Learning	Differential Privacy, Scalability, Usability*
Carvalho *et al.* [10]	Unlike other research, the paper discussed the trade-offs between privacy protection and data utilization.	The survey paper mainly discusses anonymization and perturbation techniques. On the other hand, there is a research opportunity to discuss other methods that maintain data utility, such as homomorphic encryption.	Data Utilization	Anonymization, Usability*, Scalability*
Shimona [11]	Briefly presented the PPDM techniques and other privacy preservation methods to prevent and safeguard the data from unauthorized parties.	The paper is too brief as it just discusses privacy preservation in the field of data mining and cites 23 references.	Data Mining	Anonymization, Usability*, Scalability*
Tanuwidjaja *et al.* [12]	The authors reviewed the most recent advancements in privacy-preserving deep learning, assessed every technique, contrasted the benefits and drawbacks of each strategy, and addressed problems and obstacles in the field. Performance and privacy are subject to trade-offs, as this work also noted.	There is a need to discuss future challenges in combining deep learning techniques with other techniques that preserve data utility.	Deep Learning	Differential Privacy, Scalability
Kurupathi *et al.* [13]	The paper discussed the types of federated learning, such as centralized, peer-to-peer, and decentralized federated learning.	The paper did not discuss how federated learning and the government can mutually collaborate.	Federated Learning	Differential Privacy, Scalability, Usability*
Cui *et al.* [14]	The paper discussed privacy-preserving techniques for blockchain and their limitations. The paper suggested future directions for privacy protection in blockchain technology.	The paper did not discuss how blockchain and the government can collaborate.	Blockchain Privacy	Anonymization, Encryption, USability*, Scalability

interpretations. We create tables that merge and display the qualitative synthesis for a simple and vast understanding.

Snowballing, frequently employed in SLRs, involves a recursive literature search and examination process [22]. It begins with relevant articles obtained through our predefined search criteria. These articles are then scrutinized for additional references that might not have been captured in the initial search. This recursive process continues iteratively until no new articles are found. Snowballing is particularly valuable in SLRs as it helps identify seminal works, locate hard-to-find literature, and ensure comprehensive coverage of the research domain. However, we carefully consider the quality and relevance of each retrieved article to maintain the integrity of the review process.

Lastly, we identify gaps, inconsistencies, or areas of ambiguity in the literature, highlighting opportunities for further investigation or refinement of research questions to create a broad chance for quality future research.

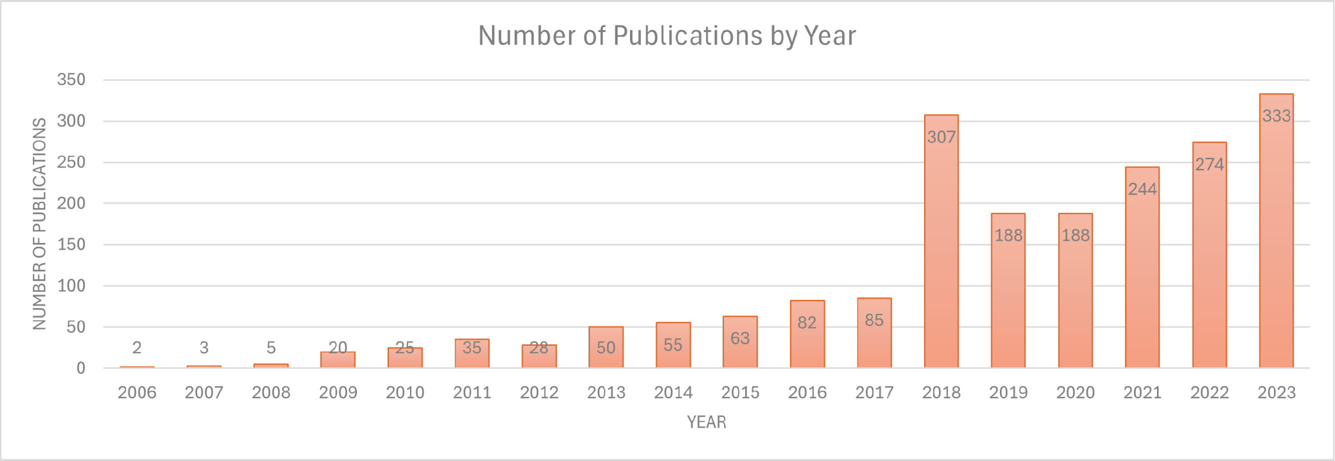


FIGURE 1. Number of papers per year on privacy-preserving mechanisms for governments.

TABLE 2. Number of articles in each step.

Step	Excluded	Remaining Number
Initial Number	–	980
Full Text Availability	−281	699
Duplication & Language	−10	689
Publisher Suitability	−300	389
Term Suitability	−107	282
Publication Type Suitability	−57	225
Content Suitability	−31	194
Snowballing	+29	223
Final Numbers	**−757**	**223**

IV. RESULT AND DISCUSSION

A. STUDY CHARACTERISTICS

1) STUDY SELECTION RESULTS

The SLR stage began with paper mining based on the inclusion criteria, which found 980 papers. The papers were then filtered using the exclusion criteria stage. Table 2 shows the number of excluded papers at every stage of the exclusion criteria [23]. After receiving the total number of papers, the amount gradually decreases as we scrutinize the availability of full text, duplication, and language suitability. We also limit the publisher of the selected journals to ensure the inclusion of high-quality and reputable sources.

Furthermore, we go deeper into the content of each paper by filtering papers that do not have the term that we have mined in the paper collection corpus. Again, we filter out survey papers as we search for technical discussions. The last step in the filtering is reading the summary of each paper and further filtering papers that are unsuitable to our desired topic. Lastly, we do snowballing, which adds the amount of paper by exploring newly found topics throughout the paper collection.

The exclusion criteria that rejected the largest number of papers is related to the accessibility issue. Some papers are not open access, linked to a dead link, or available through an unsafe website. The second one is content suitability. Several papers that passed all inclusion criteria turned out to have expanded, incomplete, or no novelty content. The third largest exclusion occurred in the publication type. Several studies did not comply with the inclusion criteria, including the publication type of datasets,*Powerpoints* presentations,or books.

2) THE NUMBER OF PAPERS PER YEAR

The search for papers using the website app.dimensions.ai resulted in 1,987 papers published between 2006 and 2023. Figure 1 shows the number of papers per year. The picture shows that the trend is increasing over the years. A total of 80.6% of the articles were published in the last seven years, which marks a rapid increase in the topic of privacy-preserving mechanisms for governments. A quadratic function obtained from the fitting method describes the trend line of the curve in the graph [24]. The following formula gives the function:

$$y = x^2 - 4010x + 4020025 \tag{1}$$

where y is the number of papers per year, while x is the year. The function has a coefficient of determination or $r^2 = 0.87$, which explains the function's proximity to the actual cumulative value–The r^2 has a value range of 0 to 1, where higher values show better proximation. This function can be useful for several reasons: prediction, understanding patterns, research investment planning, presentation, and comparison with other topics. For example, we can observe that the growth of our research interest is quadratic. Then, we can predict that the number of paper topics related to privacy-preservation concerning the government in 2024 will be approximately 361.

3) THE RESEARCH TOPICS

We tested the collected papers extensively to describe demographics on research topics in privacy-preserving mechanisms for governments. We use the VosViewer

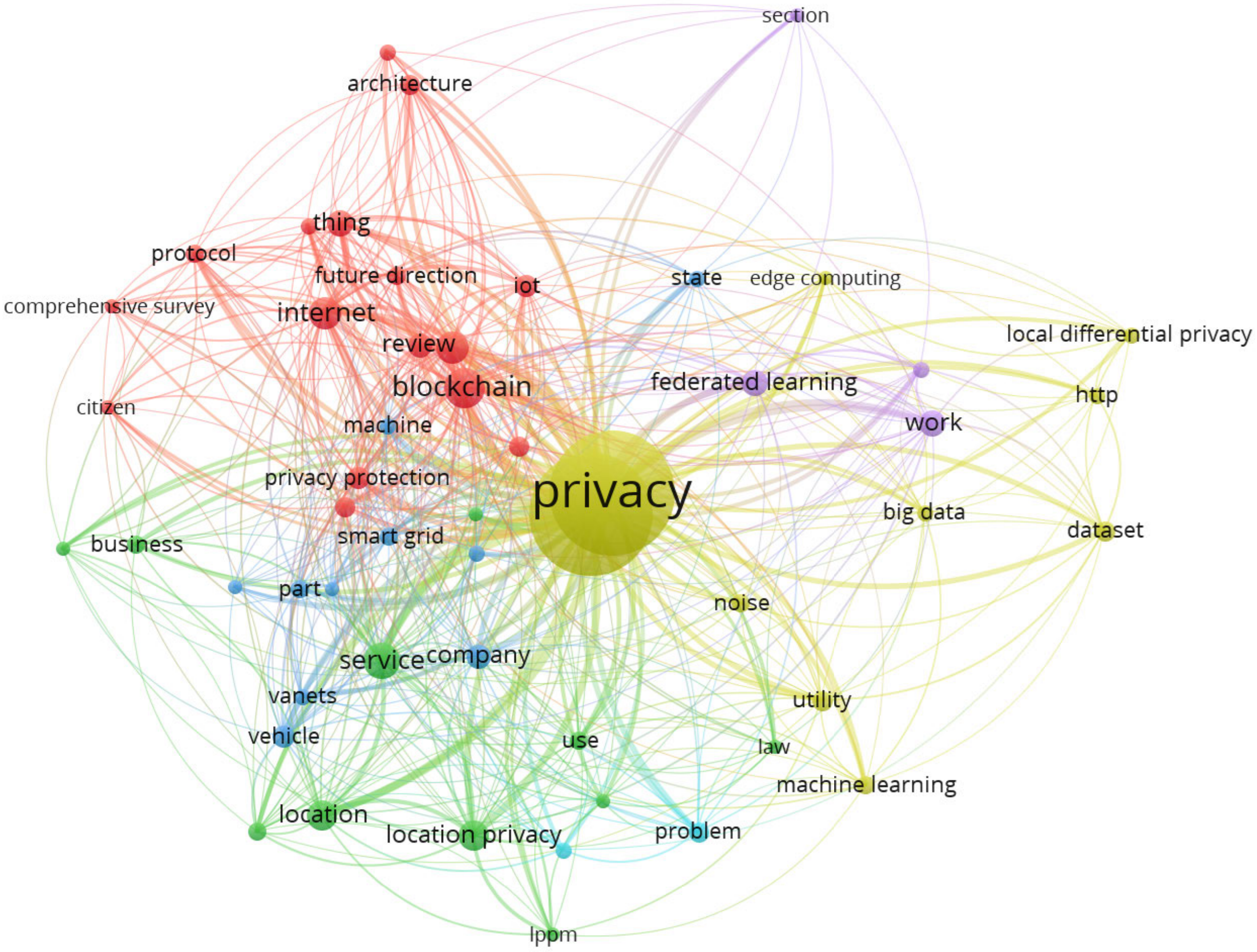


FIGURE 2. Research topics in privacy-preserving mechanisms for governments.

application [25] to find topics from the collected titles. We use binary counting as the counting method, then give a value of 10 for the minimum number of occurrences of a keyword. Then, we took the 60% terms with the highest relevance from the results obtained.

Of the 4,774 terms, 89 occur more than or equal to 10 times. The 60% terms with the highest relevance resulted in 53 terms. The results are shown in Figure 2. The two terms with the highest occurrence are ''blockchain'' and ''location privacy.'' Meanwhile, the two terms with the highest average publication year are ''federated learning'' and ''local differential privacy,'' representing the most up-to-date research.

4) THE PRIME TAXONOMY FOR PRIVACY-PRESERVING MECHANISMS OF THE GOVERNMENTS

Three primary dimensions are covered by the taxonomy created for the systematic literature review on government privacy-preserving mechanisms: the role of the government, the ministry or area of interest, and the underlying science and technology. The taxonomy offers a systematic framework for classifying and evaluating research articles based on these essential components. The government role dimension lists governments' different tasks and duties when putting privacy-preserving systems, regulating them, and using them. Research articles are categorized by the ministry or field of interest dimension according to the particular governmental ministries or sectors like healthcare, finance, or law enforcement that use privacy-preserving technologies.

Last, the underlying technology and science dimension groups articles based on the scientific and technological developments that propel privacy-preserving technologies like encryption, anonymization, security computation, and blockchain.By organizing research articles into these categories, the taxonomy facilitates a comprehensive exploration of the multifaceted landscape of privacy preservation within government contexts, enabling researchers to identify trends, gaps, and opportunities for further investigation and development.Figure 3 shows the prime taxonomy of this SLR.

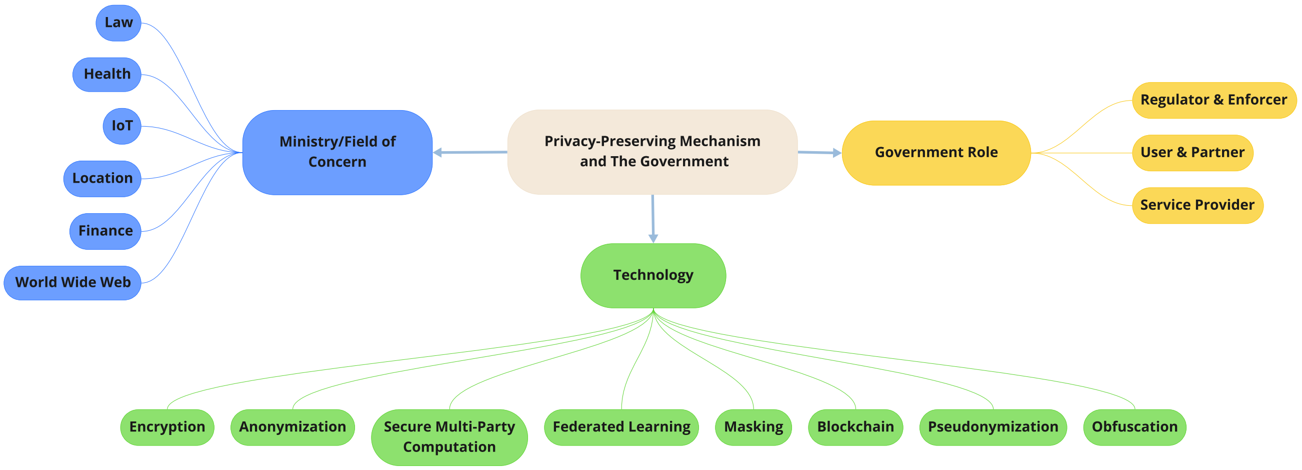


FIGURE 3. **The prime taxonomy of privacy-preserving mechanisms of the governments.**

B. THE GOVERNMENT'S ROLE IN PRIVACY PRESERVATION

This section answers RQ1, ''What are government agencies' key roles and responsibilities in implementing and regulating privacy-preserving mechanisms?''. In our 58 articles, the government has three important roles: user, regulator, or provider of privacy-preserving mechanisms for society. The following subsections discuss each role.

1) AS REGULATOR AND ENFORCER

Much research about privacy preservation has pointed out or mentioned that the government's involvement is paramount.

In one example, artificial intelligence (AI) technologies' heightened concerns over potential privacy infringements have prompted governments to enact stricter regulations to safeguard individuals' data from exploitation and misuse by AI systems [26].

In privacy preservation, the government plays a pivotal role as both a regulator and an enforcer, ensuring privacy rights are upheld and protected across various sectors and industries [27]. As a regulator, the government establishes and enforces privacy laws, regulations, and standards that dictate how personal data should be collected, used, shared, and protected [28]. Government regulation ensures data privacy and security, promotes interoperability and standardization, and fosters innovation while addressing concerns related to smart grid, healthcare data management, and financial transaction processing [29], [30], [31].

Furthermore, the government enforces privacy preservation by actively monitoring compliance with privacy laws and regulations, investigating complaints and breaches, and imposing sanctions or penalties on entities that fail to meet their privacy obligations [32]. Regulatory agencies tasked with privacy enforcement are crucial in holding organizations accountable for their data practices and ensuring that individuals' privacy rights are respected and upheld [33]. The government works to deter privacy violations through regulatory inspections, audits, and legal actions and to promote a culture of accountability in data handling [34].

By fulfilling its role as both regulator and enforcer of privacy preservation, the government helps create a trustworthy and privacy-respecting environment where individuals can confidently handle their data responsibly and lawfully [35]. Ultimately, the government's commitment to privacy preservation protects the equity of individual privacy rights, promotes consumer trust, and fosters innovation and growth in an increasingly data-driven society [36].

As a regulator of privacy preservation, we can take many examples. In smart homes, the government can regulate them by establishing guidelines for data privacy, cybersecurity standards, and interoperability protocols to ensure the safety and protection of individual personal information and the integrity of connected devices and systems [37]. In differential privacy, the government can mandate the use of differential privacy techniques by telecommunications companies to anonymize aggregate data used for statistical analysis, ensuring individual privacy protection while allowing meaningful insights to be derived from large datasets [38].

Many research implementations can be used to regulate privacy, such as game theory and privacy impact assessment (PIA). Game theory provides a framework for analyzing strategic interactions among stakeholders, facilitating the development of incentive mechanisms and enforcement strategies that incentivize compliance with privacy regulations and deter privacy violations [39]. Therefore, PIA is a methodical approach to detecting, evaluating, and reducing privacy concerns related to handling personal data for a project, system, or initiative.

PIA involves several key steps to identify and mitigate privacy risks in projects or initiatives. Firstly, it begins with scoping, where the purpose, goals, and scope of the assessment are defined, along with identifying relevant stakeholders [40].Next, information gathering involves collecting details about the project, including the data types, how it will be collected, used, and stored, and potential privacy risks [41]. After that, a risk assessment is carried out to determine the possibility and significance of privacy risks, considering elements like the sensitivity of data and the possible harm to persons [42]. The assessment identifies appropriate measures to mitigate or eliminate these risks, including implementing privacy-enhancing technologies, adjusting data handling practices, or updating policies and procedures [43]. After mitigation, the assessment results are documented in a report, which may include recommendations for ongoing monitoring and review to ensure continued compliance with privacy requirements [44]. Figure 4 shows the basic steps of executing PIA.

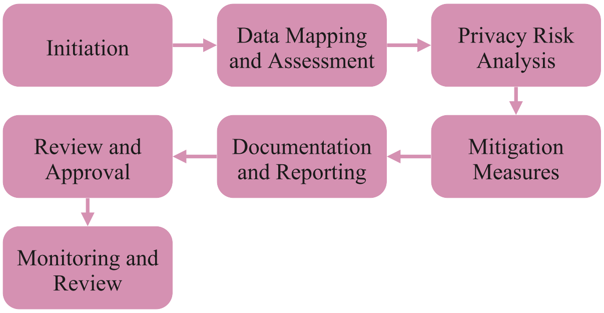


FIGURE 4. The basic steps in PIA.

Here is an example of a PIA demonstration: A new iPhone release and government regulations correlate with the necessity for compliance with privacy regulations such as differential privacy algorithms, prompting Apple to implement enhanced privacy features in its products to meet regulatory requirements and address growing privacy concerns among consumers [45].

Moreover, Governments utilize formal models to increase privacy protection by developing structured frameworks based on privacy principles and regulations, enabling systematic evaluation and enforcement of privacy-preserving measures across various domains and applications [46]. Genetic algorithms (GA) can be utilized in privacy regulation by optimizing the selection and enforcement of regulatory policies through iterative adaptation and evolution based on feedback from stakeholders and the changing privacy landscape [47].

2) AS USER AND PARTNER

In the landscape of privacy preservation, the government assumes the crucial roles of both user and partner, actively engaging with privacy-preserving mechanisms to protect citizens' sensitive information and foster a culture of privacy-conscious governance. Among other government roles in privacy preservation, the user's role provides the broadest discussion, covering several privacy preservation mechanisms and a variety of partners, each representing a different field of concern. Generally, the government employs privacy-preserving mechanisms to protect data privacy, including measuring privacy through an attacker's estimation error, ensuring robust protection against unauthorized disclosure of sensitive information [48].

As a user of privacy-preserving technologies and practices, government agencies leverage encryption, anonymization, secure communication protocols, and other privacy-enhancing tools to safeguard sensitive data collected and managed during their operations. For example, the government employs privacy-preserving mechanisms such as secure multiparty computation (SMPC) in collaborative research initiatives, allowing multiple agencies to analyze sensitive data collectively while ensuring individual privacy and confidentiality [49]. Other research shows this mechanism can also prevent human trafficking [50]. Consequently, implementing privacy preservation measures in applications such as Mobility as a Service (MaaS) would enhance user privacy and data protection throughout the transportation ecosystem [51].

The government also leverages differential privacy techniques to anonymize and aggregate citizens' data for statistical analysis, ensuring individual privacy protection while enabling valuable insights derived from large-scale datasets [52].To balance data utility and privacy preservation, differential privacy techniques add precisely calibrated noise to query responses, ensuring that statistical results remain accurate while preventing the identification of individual data points [53]. Additionally, differential privacy techniques incorporate rigorous mathematical guarantees to quantify the level of privacy protection provided [54]. This guarantee ensures that the amount of noise added to query responses is carefully calibrated to achieve a desired privacy level while preserving the integrity and utility of the aggregated data [55].

On the other hand, open, collaborative networks, semantic technologies, and swarm coordination mechanisms can preserve privacy by enabling decentralized, distributed, and self-organizing systems that minimize the need for centralized data repositories and intermediaries, thus reducing the risk of unauthorized access or data breaches [56]. These technologies facilitate fine-grained access control and data labeling, ensuring that sensitive information is only shared with authorized entities and enhancing privacy protection.

The government partners in collaborative efforts to advance privacy preservation across sectors and industries, working with technology providers, academia, civil society organizations, and other stakeholders to develop and implement effective privacy solutions. In healthcare, they implement privacy-preserving measures in COVID-19 tracing efforts by utilizing techniques such as decentralized contact tracing apps, anonymized location data, and encryption protocols to protect individuals' privacy while effectively tracking and containing the spread of the virus [57].

It is also paramount for the government to use privacy preservation to protect electronic health records (EHRs) [58]. Then, decentralized mobile contact tracing applications add privacy by tracking and monitoring individuals' potential exposure to contagious diseases, such as COVID-19, without relying on centralized data storage or processing [59].

In the field of the smart grid, the government utilizes privacy-preserving technologies, implementing techniques such as homomorphic encryption to securely analyze energy consumption data while protecting the privacy of individual users' information [60]. The government can also harbor the protection of other privacy-sensitive data, such as firefighting data [61]. Such protection allows them to be used for forecasting or autoregression without revealing personal data [62].

The hoped outcome from the role as the user is that government agencies prioritize data protection through stringent and the government aims to protect citizens' sensitive information service provider laws and frameworks that govern personal data collection, storage, and processing, ensuring that individuals have control over how their information is used and shared. Government agencies employ encryption, anonymization, and other privacy-preserving technologies to safeguard sensitive data from unauthorized access or disclosure while fostering a culture of privacy awareness and accountability among employees and stakeholders.

3) AS SERVICE PROVIDER

As a service provider, the government aims to protect citizens' sensitive information while offering services that enhance privacy. The government offers citizens access to tools, resources, and initiatives designed to enhance their privacy and security in the digital realm. This may include the provision of secure communication channels and system decentralization. The government can also become a third-party privacy provider to extra government entities and offer certification or PIAs.

The government can offer secure communication channels as a privacy provider in computer networks, employing data encryption, authentication, and access control [63]. These steps safeguard users' personal information and mitigate the risk of unauthorized access or data breaches, including vehicle networks [64], [65]. It will also ensure privacy through urban message delivery on mobile devices, digital signage, public address systems, or social media platforms [66]. In addition to providing safe pathways, the government can also provide decentralization services, which can strengthen system resilience against single points of failure, support data sovereignty, and give people more control over their data [67].

The government can give certification programs and audits as third-party privacy providers to social media, guaranteeing adherence to privacy laws, encouraging openness in data handling procedures, and building user confidence in the platform's privacy safeguards. [68]. Another third-party service offers PIAs to private companies, nonprofit organizations, and educational institutions, which would help identify potential privacy risks [69].

Through its roles as a privacy preservation service provider, the government plays a critical role in fostering a privacy-respecting society by leveraging privacy-preserving technologies internally while offering privacy-enhancing services to the public. The government empowers citizens who can confidently control their data and navigate digital interactions. We synthesize the discussion in this subsection (government's role in privacy preservation). Table 3 shows the summary of that synthesis.

C. MINISTRIES INVOLVED IN PRIVACY PRESERVATION AND FIELD OF CONCERNS

1) LAW

As thoroughly discussed in the previous RQ, the government plays a pivotal role in privacy preservation through regulatory functions. It oversees developing and enforcing privacy laws and regulations governing data protection and privacy rights. The government is responsible for drafting, amending, and enacting laws safeguarding individuals' privacy rights and regulating personal data collection, use, and disclosure by government agencies, private organizations, and other entities.

Many privacy problems arise within the realms of country regulations. For example, the legality of activities within vulnerability markets may be subject to various laws and regulations related to cybersecurity, intellectual property, data protection, and computer crime, depending on the jurisdiction [70]. Hence, the disclosure of software vulnerabilities is often governed, particularly in the context of responsible disclosure programs and bug bounty programs, which may impact participants' activities in vulnerability markets.

On the other hand, the tension between regulating privacy and technological advancement becomes another problem. For instance, facial expression recognition conflicts between the potential benefits of innovative applications and the concerns over intrusive surveillance, data privacy, and the ethical implications of facial data collection and analysis [71]. Background noise or intentional masking methods may compromise the confidentiality of spoken communication, leading to concerns about privacy breaches or unintended disclosure of sensitive information within personal spaces [72].

A legal framework refers to a structured system of laws, regulations, policies, and procedures that govern a particular subject matter or area of activity within a society or organization. For example, the legal framework surrounding big data privacy establishes regulations, standards, and guidelines that govern the collection, processing, storage, sharing, and protection of personal data within the context of large-scale data analytics, ensuring compliance with privacy laws and safeguarding individuals' rights to privacy and data protection [73].

The General Data Protection Regulation (GDPR) is the data protection regulation aimed at safeguarding the privacy and rights of individuals within the European Union, which emphasizes many aspects. GDPR is built upon seven

TABLE 3. The summary of government roles in privacy preservation.

Government Role in Privacy Preservation	**Regulator & Enforcer**	**User & Partner**	**Service Provider**
Purpose	To establish and enforce clear rules and guidelines for data handling practices and protect individuals' privacy rights across sectors and industries.	To protect citizens' sensitive information and uphold privacy rights in government operations.	To provide citizens with tools and resources to enhance their privacy and security in the digital realm.
Key Activities	• Incentivization through game theory [39]. • Product audit through PIA [39]. • Regulation optimization through GA [47].	• Protect government-collected privacy-sensitive data [51]. • Employ SMPC, differential privacy, and secure communication protocols [52]. • Partners in collaborative efforts to advance privacy preservation across sectors and industries [57].	• Offer privacy services such as secure communication channels and system decentralization [64]. • Become a third-party privacy provider to extra-government entities to offer certification and PIAs [68].
Outcome	A regulatory framework that promotes responsible data stewardship and protects individuals' privacy rights in diverse contexts.	A privacy-respecting environment where government agencies prioritize data protection and uphold individuals' privacy rights.	Empowered citizens who can exercise greater control over their data and navigate digital interactions with confidence.

fundamental principles designed to govern the processing of personal data [74]. These principles include lawfulness, fairness, and transparency, ensuring that data processing activities are conducted lawfully, with fairness towards individuals whose data is being processed, and transparency regarding how their data is used [75]. The GDPR also strongly emphasizes purpose limitation, which states that personal information should only be gathered for clearly defined, acceptable objectives [76]. Then, data reduction promotes gathering only the information required to achieve the goal [77].

Furthermore, the principles underscore accuracy, requiring that personal data be accurate and updated [78]. Next, we have storage limitation, which is the fifth principle and states that data should not be stored longer than necessary [79]. Integrity and confidentiality are the focus of the second GDPR principle, which requires that personal data be processed with sufficient security, including defense against improper or unauthorized processing and against unintentional loss, destruction, or damage [80]. Accountability in GDPR regulates liability and compensation for data subjects due to GDPR violations [81]. These principles guide organizations to ensure compliance with GDPR and safeguard individuals' data protection and privacy rights. Figure 5 shows the seven principles of GDPR, and the article number of each principle is written in brackets.

Data minimization, transparency, and individual consent ensure blockchain applications and other technologies comply with privacy regulations by design and default while enabling secure and transparent data transactions [82]. In particular, homomorphic encryption is supported by GDPR's Article 5, which establishes principles linked to data processing since it permits data processing while protecting the privacy of individual data subjects [83].

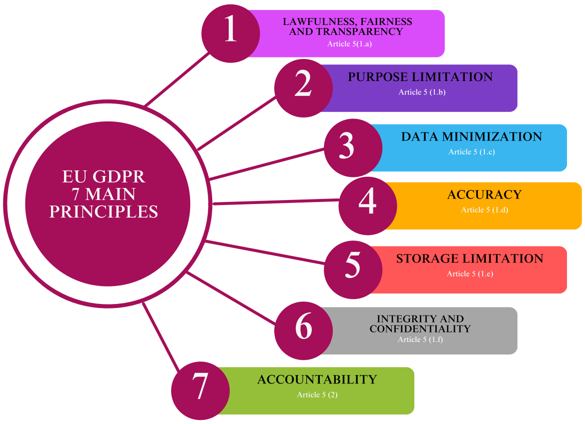


FIGURE 5. The seven principles of GDPR.

Furthermore, federated learning conforms to GDPR's focus on data reduction, purpose limitation, and data protection by design and default, as it entails training machine learning models across decentralized devices [84]. Federated learning correlates to the Internet of Things (IoT), enabling collaborative training across distributed IoT devices [85].

Furthermore, the Ministry of Law and Justice is involved in privacy preservation by interpreting and applying legal principles and precedents to privacy-related disputes and cases. As the guardian of legal interpretation and judicial oversight, the ministry provides legal guidance, opinions, and advisory services on privacy matters, clarifying the scope of privacy rights, defining legal obligations, and resolving legal disputes related to privacy violations.

2) HEALTHCARE

Privacy preservation in healthcare is prominent because it is driven by the increasing digitization of medical records, the proliferation of healthcare technologies, and the growing demand for personalized healthcare services. For example, privacy problems arise in healthcare tracing because of the risk of unauthorized access or disclosure of sensitive patient information, potential breaches of patient confidentiality, challenges in obtaining informed consent for data collection and sharing, and concerns about the accuracy, integrity, and security of health data collected and processed during tracing efforts [86].

Furthermore, in cloud-based EHR, issues may be related to data retention and secondary use of health data [87]. It also creates potential stigmatization or discrimination of individuals based on their health status or tracing history [88]. Centralized data storage risks privacy preservation as it creates a single point of failure and increases the likelihood of data breaches or unauthorized access [89]. Centralized data raises concerns about data monopolization and surveillance [90]. Privacy problems that may arise in healthcare activity recognition include concerns over the collection and analysis of sensitive health-related data without explicit patient consent, the potential for unintentional or unauthorized monitoring of individuals' activities, the risk of misinterpretation or misuse of activity data leading to stigmatization or discrimination, and challenges in ensuring the accuracy, security, and privacy of activity recognition systems and the data they generate [91].

Several advanced solutions have addressed healthcare privacy problems. Federated learning in healthcare ensures privacy by training machine learning models across distributed healthcare institutions' data silos [92]. It enables collaborative analysis while keeping sensitive patient data localized and secure [93]. Federated learning leverages edge computing by enabling machine learning model training to be performed locally on edge devices. It reduces the requirement for data transmission to centralized servers and facilitates collaborative learning while protecting privacy [94].

Furthermore, federated learning can collaborate with differential privacy in healthcare by aggregating locally trained machine learning models across distributed devices while adding carefully calibrated noise to the model updates [95]. Differential privacy preserves patient privacy rights by limiting identifying specific patient information and facilitating extracting insightful information from extensive healthcare databases. In addition to facilitating collaborative analysis of sensitive healthcare data, this guarantees the protection of individual privacy [96].

Federated learning can collaborate with blockchain in healthcare by utilizing blockchain's decentralized and immutable ledger to record and validate model updates from distributed healthcare institutions securely [97]. This ensures the collaborative learning process's transparency, integrity, and traceability while maintaining data privacy and security.

Several technologies have been implemented to enhance privacy in EHRs. By offering a decentralized, immutable ledger system for safely storing and exchanging sensitive patient data, blockchain technology in healthcare improves privacy [98]. It ensures data integrity and reduces the risk of unauthorized access or tampering [99]. Encryption and biometric authentication prevent unauthorized access to privacy-sensitive EHR privacy [100]. Homomorphic encryption in EHRs enables computation on encrypted data, preserving patient privacy while allowing for secure data analysis and sharing among authorized parties [101]. EHR solutions can be made less expensive by implementing efficient data encryption, access control mechanisms, and scalable infrastructure solutions to optimize costs [102].

Anonymization can collaborate with privacy preservation in healthcare by transforming personally identifiable information (PII) into non-identifiable data, such as pseudonyms or anonymized identifiers, before analysis or sharing [103]. This allows healthcare organizations to perform data analytics while minimizing the risk of re-identification and unauthorized access to sensitive patient information, safeguarding patient privacy and confidentiality.

Privacy auditing is crucial in healthcare to ensure compliance with regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA) and GDPR, assess the effectiveness of privacy controls and safeguards, detect and mitigate privacy breaches or unauthorized access to patient data, and maintain trust and confidence among patients and stakeholders in the confidentiality and security of their health information [104].

As a user of EHR privacy protection methods, the government plays a crucial role in safeguarding sensitive health information and upholding patient privacy rights within healthcare systems through the Ministry of Health. The Ministry of Health's oversight and administration rely on EHR systems to manage and analyze vast patient data collected from healthcare providers, clinics, and hospitals. The Ministry implements privacy protection methods such as access controls, encryption, anonymization, and audit trails within EHR systems to ensure data confidentiality, integrity, and security.

3) IoT

The ascent of IoT during the 2010s has ushered in numerous advantages, yet it has also precipitated a constellation of privacy concerns. The architecture of IoT integrates an array of disciplines, encompassing communication, embedded systems, big data, cloud computing, web programming, and data analytics [105]. A privacy problem in the communication of IoT devices is the potential interception or eavesdropping of sensitive data transmitted over insecure communication channels, leading to the disclosure of personal information [106]. In IoT gateways, the privacy problem lies in the potential vulnerability to data breaches or unauthorized access due to the aggregation and processing of sensitive information from multiple IoT devices [107].

IoT covers several fields of implementations, from smart home, smart city, and industrial IoT (IIoT) to agricultural IoT. In agricultural IoT, the privacy problem arises from the potential for location-based data to be used to infer sensitive information about agrarian activities, land ownership, or crop yields, leading to concerns over data privacy, confidentiality, and the potential for misuse or unauthorized access to farmers' data [108].

Advanced solutions have been implemented to preserve privacy in IoT, applying anonymization, federated learning, or authentication. By guaranteeing that each IoT device record is indistinguishable from at least k1 other records, Kanonymity protects IoT privacy by making it difficult for adversaries to identify particular users or devices from the gathered data [109]. The similarity between IoT and federated learning is that both aim to maintain data security and privacy while facilitating cooperative data analysis and model training across dispersed devices [110]. Oblivious identity management is related to privacy-preserving authentication methods, where users can prove their identity without revealing any unnecessary information about themselves [111].

Blockchain technology can enhance the privacy of IoT by providing a decentralized and tamper-resistant ledger for recording IoT device transactions and interactions [112]. Through blockchain, IoT data can be encrypted and securely stored in a distributed manner, reducing the risk of data breaches or unauthorized access, even in electronic vehicles [113]. Consensus procedures built into blockchain technology protect data integrity and transparency while giving consumers control over their data [114]. This decentralized approach mitigates the reliance on centralized authorities, thereby reducing the potential for single points of failure and enhancing the privacy and security of IoT ecosystems [115].

The Ministry of Interior or Home Affairs may be involved in regulating IoT deployments in critical infrastructure sectors such as smart cities, transportation systems, and public safety applications, where privacy concerns regarding surveillance, data collection, and data sharing are prominent. These ministries collaborate with other relevant government agencies, industry stakeholders, and civil society organizations to develop comprehensive privacy frameworks and regulatory mechanisms that address the evolving privacy challenges posed by IoT technologies.

4) LOCATION

Location privacy protects individuals' sensitive location information from unauthorized access, tracking, or disclosure [116]. It includes people's right to manage how their location data is collected, used, and shared, including their movement trajectories, proximity to particular locations, and real-time or historical geographic coordinates [117]. Location privacy is essential for safeguarding individuals' autonomy, safety, and security and mitigating risks related to surveillance, stalking, profiling, or other forms of privacy infringement based on their physical whereabouts [118].

LBSs are prone to privacy issues due to the inherently sensitive nature of location data and the potential for misuse, abuse, or unauthorized access to this information [119]. For example, Vehicle-to-Grid (V2G) technology lies in the potential for unauthorized access to sensitive vehicle and energy consumption data, compromising users' privacy and security [120]. Location privacy issues in COVID-19 tracing arise from concerns over collecting and potentially misusing individuals' precise location data for contact tracing purposes, raising questions about surveillance, data retention, and the erosion of privacy rights [121]. Figure 6 shows the most prominent LBSs and why location privacy has become the most outstanding field of concern compared to others.

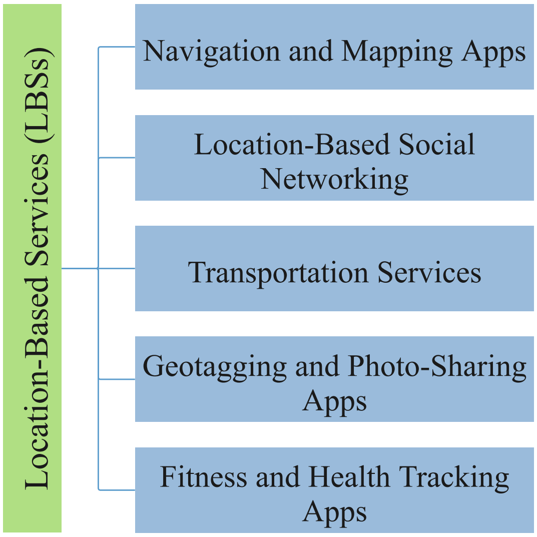

Location-Based Services (LBSs)
Navigation and Mapping Apps
Location-Based Social Networking
Transportation Services
Geotagging and Photo-Sharing Apps
Fitness and Health Tracking Apps

FIGURE 6. The most prominent LBSs.

Location data may be susceptible to data breaches, unauthorized access, or misuse by third parties, leading to privacy violations, identity theft, inference attacks, or other security risks for individuals whose location information is compromised [122]. An inference attack is a privacy attack where an adversary deduces sensitive information about an individual by analyzing seemingly innocuous or nonsensitive data [123].

Location privacy problems can also arise in crowdsourcing [124]. Crowdsourcing is obtaining contributions, ideas, or services from a large group of people, typically facilitated through online platforms or communities, to solve problems, gather information, or complete tasks [125]. There is a potential for individuals to inadvertently disclose their precise or sensitive location information when participating in crowd-based tasks or sharing location-tagged content [119]. This can lead to concerns over unauthorized tracking, surveillance, stalking, or the disclosure of personal routines or activities, posing risks to individuals' privacy and safety [126]. Additionally, crowdsourced location data may be susceptible to re-identification attacks [127]. Misuse by third parties is also possible for targeted advertising, profiling, or other invasive purposes [128]. These threats highlight the need for robust privacy safeguards and informed consent mechanisms in crowdsourcing platforms [129].

Mobile participatory sensing collects data from individuals' mobile devices, such as smartphones or wearable sensors, to gather information about participants' environment, behavior, or activities [130]. Mobile participatory sensing raises location privacy concerns by collecting data from individuals' mobile devices, including potentially sensitive location information [131].

One solution to maintaining location privacy is implementing a location privacy framework. A location privacy framework is a structured approach or principles designed to address privacy concerns about collecting, using, and disseminating location data in various applications and contexts [132]. This framework typically includes guidelines, policies, and technical mechanisms to protect individuals' location privacy rights while enabling the effective utilization of LBS or data-driven applications.

Many techniques, such as perturbation, anonymization, and obfuscation, have attempted to increase location privacy by blurring the location [133]. Perturbation techniques can provide privacy in road networks by adding noise or randomization to the location data of vehicles or individuals traversing the network [134]. Game theory can enhance location privacy by providing strategic frameworks for individuals or entities to make decisions that protect their privacy interests in the face of potential adversaries or competing interests [135]. For example, game-theoretic models can be used to analyze interactions between users and LBSs, where users aim to maximize their utility while minimizing the disclosure of sensitive location information.

Federated learning, which facilitates cooperative model training across dispersed devices, may offer a solution to the privacy preservation of LBS. Users' location data can be spread while maintaining local and decentralized control. Decentralization lessens the requirement for centralized data aggregation and lowers the possibility of sensitive location data being accessed without authorization or privacy violations [136].

Differential privacy can potentially preserve LBS privacy [137]. It can supplement location data or query results with precisely calibrated noise [138]. This mechanism ensures that individual users' contributions remain indistinguishable from the aggregate data [139]. It protects their privacy while enabling meaningful analysis and utilization of location information [140]. This strategy lessens the possibility of privacy violations or unauthorized tracking while preserving the usefulness of the data for location-based services (LBS) applications by preventing the identification of particular people or sensitive places from the gathered data [141].

The Ministry of Transportation and the Geospatial Information Agency are relevant to location-related privacy issues, particularly concerning the regulation of location tracking technologies in transportation systems such as Intelligent Transportation Systems (ITS), vehicle telematics, and LBSs for public transit, ensuring privacy safeguards for travelers' geolocation data.

5) FINANCE AND ECONOMY

It has become apparent in previous sections that the government is responsible for collecting big data containing various information, from healthcare to finance [142]. The main issues in privacy related to national finance and the economy revolve around the collection, storage, and utilization of sensitive financial data by government agencies, financial institutions, and businesses [143]. As digital transactions and online banking services become more common, worries about the possibility of illegal access, data breaches, identity theft, and financial fraud grow [144].

Financial safeguarding after COVID-19 mitigates economic vulnerabilities, protects livelihoods, and ensures resilience against future crises [145]. The threat of financial disruption can also come from social media, where social bots can spread rumors that harm national financial stability [146].

Decentralization can contribute to privacy preservation in economic data by distributing data storage and processing across multiple nodes or participants, reducing the concentration of sensitive information in centralized databases, and minimizing the risk of single points of failure or unauthorized access [147]. Individuals retain greater control over their data through decentralized systems such as blockchain or distributed ledger technology [148]. Then, cryptographic techniques ensure privacy and confidentiality while allowing for secure and transparent transactions or interactions [149]. Additionally, decentralization can foster trust and accountability by enabling consensus mechanisms and verifiable data integrity without relying on trusted intermediaries, enhancing privacy protections in economic transactions and data exchange [150].

The central bank can employ differential privacy to aggregate and analyze financial data from multiple banks while preserving the privacy of individual transactions and account holders [151]. The central bank can monitor economic indicators and extract insights by carefully calibrating noise into the aggregated data, all while maintaining the security of critical financial data. This will protect data privacy and make policymaking and financial oversight more efficient.

The Ministry of Finance plays a critical role in financial privacy preservation by formulating and enforcing policies, regulations, and standards that govern the collection, storage, and use of financial data. To ensure compliance with privacy laws and regulations, such as data protection acts or financial confidentiality statutes, it supervises the installation of safeguards for individuals' financial information. Additionally, the Ministry of Finance collaborates with financial institutions, regulatory bodies, and other stakeholders to develop secure frameworks for data sharing, transaction processing, and information exchange, balancing transparency and accountability with protecting individuals' privacy rights. Through oversight, guidance, and collaboration, the Ministry of Finance aims to foster trust, integrity, and confidence in financial systems while respecting individuals' privacy and confidentiality concerns.

6) WORLD WIDE WEB

The main privacy problem in the World Wide Web, particularly concerning the Semantic Web and web services, revolves around the pervasive collection, aggregation, and utilization of personal data across interconnected systems and applications. With the increasing adoption of semantic technologies and web services, vast amounts of user-generated data are generated and shared, and concerns about privacy, consent, and control are processed. Other matters around the web and the usage of smartphones have also become privacy concerns, including collaborative filtering and keystroke-based authentication.

Privacy threats from the semantic web arise primarily due to the extensive interlinking and sharing of structured data across various online platforms and databases [152]. Semantic technologies enable the seamless integration and aggregation of diverse datasets, facilitating sophisticated data analysis and knowledge discovery [153]. However, these interconnections also increase the risk of unintended data exposure and inference attacks, where adversaries can exploit semantic relationships to infer sensitive information about individuals or entities.

Privacy concerns in web services revolve around collecting, storing, and processing users' data across various online platforms and applications [154]. As web services interact with users and exchange information over the internet, there is a heightened risk of unauthorized access, data breaches, and privacy violations [155]. Users may be unaware of how much their data is being collected and utilized by web services, leading to concerns about transparency, consent, and control over personal information [156]. Furthermore, the aggregation and analysis of user data from multiple sources can enable profiling, targeted advertising, and other forms of surveillance, eroding individuals' privacy rights and autonomy online [157]. Additionally, inadequate security measures, weak authentication mechanisms, and vulnerabilities in web service infrastructure may expose sensitive user data to malicious actors, exacerbating privacy risks [158].

Privacy risks in collaborative filtering arise from collecting and analyzing users' data to generate recommendations, potentially exposing sensitive information and preferences to third parties or unauthorized access [159]. Collaborative filtering algorithms rely on large datasets of user interactions and preferences, raising concerns about the privacy and security of this data.

While offering a convenient and potentially more secure alternative to traditional password-based methods, Keystroken-based authentication also presents significant privacy threats [160]. By analyzing the timing, rhythm, and other behavioral aspects of users' typing patterns, keystroke-based authentication systems inherently collect sensitive biometric data that can uniquely identify individuals. However, this biometric data is highly personal and can reveal intimate details about users' identities, behaviors, and emotional states.

Knowledge-based schemes can generate tailored recommendations, search results, and content suggestions by analyzing users' browsing history, search queries, or interactions with online platforms without compromising users' privacy [161]. Anonymization, obfuscation, or differential privacy may protect the user's data throughout the process [162]. Furthermore, knowledge-based schemes can empower users with greater control over their online privacy by allowing them to customize their preferences, manage consent settings, and opt out of data collection practices that they find intrusive or undesirable to contribute to a more privacy-conscious web ecosystem.

The ministry related to privacy problems in the World Wide Web often includes the Ministry of Communications and Information Technology, which oversees regulations and standards for data protection, cybersecurity, and online privacy rights. The Ministry of Communication and Information Technology oversees privacy preservation in government internal web services and information systems by implementing robust security protocols, compliance with privacy regulations, and regular audits to enforce data protection measures.

We synthesized our comprehensive explanation of the problems, solutions, and ministries related to privacy preservation. Table 4 summarizes the synthesis.

D. PRIVACY-PRESERVING MECHANISMS AND UNDERLYING TECHNOLOGIES

This section summarizes the answers to RQ3, "What are the current trends and innovations in privacy-preserving technologies utilized by and related to governments?". Our SLR process found several research topics related to RQ3: Encryption and homomorphic encryption, anonymization, SMPC, tokenization, edge computing and federated learning, data masking, blockchain, pseudonymization, and obfuscation. We discuss each one of these research topics in the following subsections

1) ENCRYPTION, HOMOMORPHIC ENCRYPTION, AND SMPC

Encryption can increase privacy by encoding sensitive information so that it becomes unreadable to anyone who does not have the corresponding decryption key [163]. This process ensures that even if unauthorized parties intercept or access the encrypted data, they cannot decipher its contents without the proper key [164]. Individuals and organizations can safeguard the confidentiality and integrity of their information by implementing encryption techniques to prevent unauthorized access, surveillance, or interception [165]. Encryption is widely used in various contexts, including communication channels, storage systems, and data transmission, to safeguard sensitive data and mitigate the risk of unauthorized disclosure or exploitation [166].

Privacy preservation with encryption has reached benefits in many aspects of digital communication. Encrypting network messages enhances privacy by rendering the content

TABLE 4. Summary of the field of concerns and their relationship with technology solutions and ministries involved.

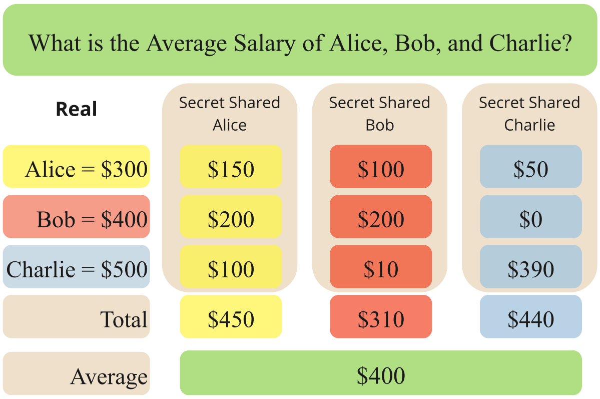
Domain	Cite	Privacy Problems	Advanced Solutions	Ministries Involved
Law	[84] [85]	• Unauthorized data access and data breaches • Tension between data advancement and privacy	• Legal frameworks • Privacy regulations, GDPR	• Ministry of Justice
Healthcare	[100] [102]	• Unauthorized access and data breaches to medical records • Threats in centralized EHR • PII in healthcare intelligence	• Federated learning in healthcare silos • Blockchain-based distributed EHR • Health data encryption • HIPAA compliance	• Ministry of Health
IoT	[109] [112]	• Insecure data communication • Data breaches • Unauthorized access to IoT devices	• Anonymization for IoT data • Oblivious authentication for IoT access • Federated learning and blockchain for decentralized IoT	• Ministry of Communication and Information Technology
Location	[116] [119]	• Location privacy issues in LBSs • Location privacy issues in crowdsourcing • Location privacy issues in mobile participatory sensing	• Promote location privacy frameworks • Applying privacy-preserving mechanisms to blur locations • Differential privacy on preserving data utilization	• Ministry of Transportation • Geospatial Information Agency
Finance and Economy	[147] [148]	• Financial disruption in the aftermath of COVID-19 • Financial disruption by social bots on social media • Identity theft, fraud, and breach on financial data	• Decentralized Finance • Differential privacy by the central bank	• Ministry of Finance
World Wide Web	[152] [154]	• Extensive interlinking in web semantics • Data breaches through web services • PII in collaborative filtering • Inference attack in key-stroke authentication	• Knowledge-based schemes for privacy-preserving recommendations • Anonymization techniques in web queries • User consent for a more privacy-conscious web ecosystem	• Ministry of Communications and Information Technology

indecipherable to unauthorized parties, protecting sensitive information from interception and unauthorized access [167]. Encrypting XML streams involves encoding the XML data to be unreadable without the appropriate decryption key, ensuring confidentiality and privacy during transmission and storage [168]. Encrypting email messages provides a privacy benefit by ensuring that the content of the emails remains confidential and secure from unauthorized access or interception during transmission, thereby safeguarding sensitive information shared via email [169]. Encryption improves privacy preservation in peer-to-peer communication by encrypting the sent data so that only the intended recipient has the decryption key [170]. This prevents unauthorized access or interception. Encryption may have negative aspects in privacy preservation compared to other privacy-preserving mechanisms.

Compared to differential privacy, one potentially negative aspect of using encryption for privacy is that it can sometimes hinder lawful access to data for legitimate purposes, such as law enforcement investigations or national security efforts [171]. Compared to anonymization, the potentially negative aspect of encryption as a privacy preservation technique is that it does not alter the underlying data itself; instead, it only secures the data during transmission or storage, meaning that if the encryption is compromised, the sensitive information could still be accessed or exposed [172].

Homomorphic encryption is pivotal in preserving privacy by enabling computations on encrypted data without decrypting it [173]. This groundbreaking technology allows sensitive data to remain encrypted throughout processing, mitigating the risk of exposure or unauthorized access to the raw information [174]. By maintaining confidentiality while enabling computations, homomorphic encryption facilitates secure data analysis, collaborative research, and outsourced computation tasks without compromising privacy. This feature is especially helpful in sensitive research, finance, and healthcare settings where data protection is crucial. In these situations, businesses can protect the integrity and security of sensitive data while getting important insights from encrypted data.

A single-party web search is a scenario where a user privately conducts a search query without revealing it to any other party [175]. It cannot facilitate collaborative search scenarios where multiple parties jointly compute search results while preserving the privacy of their queries. To maintain privacy, SMPC allows many parties to collaboratively calculate a function over their private inputs while guaranteeing that no participant learns anything beyond the computation's output [176].



What is the Average Salary of Alice, Bob, and Charlie?

Real	Secret Shared Alice	Secret Shared Bob	Secret Shared Charlie
Alice = $300	$150	$100	$50
Bob = $400	$200	$200	$0
Charlie = $500	$100	$10	$390
Total	$450	$310	$440
Average	$400		

FIGURE 7. A simple illustration to show how SMPC works.

The technology underlying SMPC relies on cryptographic protocols, such as secret sharing, and cryptographic primitives like homomorphic encryption [177]. By employing those technologies, SMPC enables secure communication and computation among multiple parties while preserving the privacy of their inputs [178]. SMPC plays a crucial role in secure collaboration supply chains by enabling various entities to collectively analyze and share sensitive data while preserving the privacy of each participant's proprietary information [179].

Figure 7 shows how SMPC works with a simple illustration. In this example, Alice, Bob, and Charlie have $300, $400, and $500 salaries, respectively. They want to know their salary average without revealing it to each other. This is an additive secret-sharing example. Each divides their salary into three parts with random proportions and shares those parts with other parties. For example, Alice divides her salary into $150, $100, and $50, then shares each piece with herself, Bob, and Charlie. After each party does the same thing, they total each piece. The result in this case is $450, $310, and $440 each, showing that neither salary is exposed. However, the average result is accurate, stating that their objective of calculating the average salary without exposing each salary to others has been achieved.

2) ANONYMIZATION AND DIFFERENTIAL PRIVACY

Some privacy preservation methods provide strong privacy guarantees but may compromise data utility by introducing significant noise or distortion into the data. On the other hand, anonymization methods mitigate privacy risks by transforming or removing identifying information from datasets while preserving their utility for analysis [180]. Differential privacy, k-anonymity, l-diversity, and t-closeness are all techniques aimed at anonymizing data to protect individual privacy while allowing for useful analysis.

Differential privacy focuses on injecting noise into the data or query replies to prevent specific individuals from being identified in a dataset. This ensures that the presence or absence of any individual's data has little effect on the results of searches [181].

Additionally, k-anonymity prevents the identification of individuals by hiding them inside larger groups by guaranteeing that each record in a dataset is indistinguishable from at least k-1 other records to certain quasi-identifiers [182]. By mandating that every set of documents with the same quasi-identifiers have different values for sensitive attributes, l-diversity extends k-anonymity and strengthens privacy against attribute disclosure attacks [183]. T-closeness refines k-anonymity by ensuring that the distribution of sensitive attribute values within each group is statistically close to the overall dataset, thereby reducing the risk of attribute inference attacks [184].

Several works have seen the improvement of anonymization through federated learning enhancement, randomized response, and big data implementation. Combining anonymization with federated learning involves leveraging anonymization techniques to obfuscate sensitive data before it is shared among participating entities in a federated learning framework, thereby enhancing privacy protection and enabling collaborative model training across distributed datasets [185]. Then, Randomized response involves respondents providing random or partially randomized responses to sensitive survey questions to enhance privacy [186].

Anonymization of big data introduces a layer of privacy protection by removing or obfuscating personally identifiable information, enabling analysis while mitigating the risk of individual re-identification [187].

Anonymization has planted specific roles in both anonymity networks and smart grids. Anonymization in anonymity networks obscures the origin and destination of network traffic, enhancing user privacy by preventing adversaries from linking network activities to specific individuals or entities [188]. Anonymization in smart grid systems helps protect the privacy of energy consumption data by removing personally identifiable information, enabling aggregate analysis while preserving individual users' anonymity [189].

Advancements in anonymization techniques have led to innovative approaches in various domains. In clustering-based anonymization, data points are grouped into clusters based on similarity and then anonymized collectively to preserve privacy while maintaining data utility [190]. Machine learning anonymization leverages advanced algorithms to automatically identify and anonymize sensitive information, offering efficient and scalable solutions for large datasets [191]. Incentive-based anonymization employs strategic decision-making principles to optimize the trade-off between privacy preservation and data accuracy, ensuring robust protection against privacy breaches in dynamic and adversarial environments [192].

Anonymization typically provides stronger privacy guarantees than perturbation and tokenization, where perturbation adds controlled noise to data [193]. On the other hand, tokenization's focus on efficiency degrades its privacy guarantees compared to anonymization [194]. Compared to blockchain, anonymization offers broader privacy protection by entirely concealing data subjects' identities, whereas blockchain may still expose transaction details [195].

3) EDGE COMPUTING AND FEDERATED LEARNING

Edge computing leverages edge devices' local processing and storage capabilities, such as smartphones, IoT devices, and edge servers [196]. The local platform performs data processing, application hosting, and efficient communication for data transmission to centralized servers [197]. This paradigm shift enables sensitive data to remain localized and under the control of the data owner, reducing privacy risks associated with data movement and storage in third-party systems [198]. Recent advancements in edge computing focus on optimizing resource allocation, workload scheduling, and security mechanisms to ensure efficient and secure data processing at the edge while preserving data privacy and confidentiality [199].

By facilitating cooperative model training across dispersed edge devices without requiring the sharing of raw data, federated learning expands on edge computing concepts [200]. Edge devices use their private data to train machine learning models locally in federated learning. They then regularly transmit updates to a central server, aggregating them to enhance the global model [201]. This decentralized approach to model training ensures data privacy and confidentiality, as raw data never leaves the edge devices, and only model updates are transmitted to the central server [202]. Recent research in federated learning explores techniques to enhance model convergence, communication efficiency, and privacy guarantees, including differential privacy-aware aggregation, secure model parameter updates, and adaptive sampling strategies for edge devices with heterogeneous data distributions [203].

Federated learning has evolved significantly with several key advancements that enhance its applicability and effectiveness. Personalized federated recommendation systems leverage federated learning to provide customized recommendations to users while preserving their privacy [204]. Decentralization in federated learning shifts model training from centralized servers to edge devices, distributing computation and reducing communication overhead while ensuring data locality and privacy [205]. Generative online networks extend federated learning to generate synthetic data miming real data distribution [206].

Differential privacy and federated learning represent a powerful approach to privacy-preserving machine learning across distributed datasets [207]. By incorporating precisely calibrated noise into the model updates or query responses during the federated learning process, differential privacy guarantees the confidentiality of individual-level data [208]. Organizations can work together on machine learning projects without jeopardizing the privacy of their data contributors by including differential privacy in federated learning [209].

4) DATA MASKING

Data masking techniques protect sensitive information by substituting, transforming, or obfuscating sensitive data elements while preserving the dataset's overall structure and statistical properties [210]. Creating sophisticated masking algorithms, such as format-preserving encryption (FPE), tokenization, and perturbation techniques, has led to recent developments in data masking. These algorithms allow for creating datasets that preserve privacy and are appropriate for analysis while reducing the possibility of re-identification or inference attacks [72].

Technological developments in data masking have been crucial in improving security and privacy in mobile cloud and smart grid contexts. Data masking methods have evolved in the smart grid domain to protect sensitive information related to energy consumption, grid infrastructure, and user behavior [211]. Similarly, in the mobile cloud context, data masking techniques safeguard personal and sensitive data stored or processed in cloud-based applications and services accessed via mobile devices [212].

FPE and tokenization are methods used for masking sensitive data while maintaining its original format and preserving its usability. FPE is appropriate for systems that need data to follow certain forms, like credit card numbers or social security numbers, as it encrypts data while maintaining the same format for the ciphertext and the plaintext [213]. This allows organizations to encrypt sensitive information without redesigning their databases or systems. According to Hu et al. [214], tokenization substitutes randomly generated tokens or placeholder values for sensitive data. Since tokenization does not employ reversible techniques like encryption, it is not feasible to undo the operation and extract the original data from the token. Rather, tokens are linked to relevant sensitive data safely stored apart via a mapping table.

5) BLOCKCHAIN

Blockchain, a distributed ledger technology, enables secure and transparent recordkeeping of transactions across a network of nodes, offering cryptographic data integrity and immutability guarantees [215]. Recent advancements in blockchain-based privacy solutions focus on enhancing privacy protections while maintaining the core principles of transparency and accountability [216]. One approach involves the development of privacy-focused blockchain platforms, such as privacy-enhanced cryptocurrencies (e.g., Monero, Zcash), which incorporate advanced cryptographic techniques such as zero-knowledge proofs and ring signatures to obfuscate transaction details and protect user privacy [217]. These privacy-centric blockchain platforms offer users greater anonymity and fungibility of digital assets, mitigating the risk of transaction surveillance and financial profiling [218].

Blockchain technology holds significant potential for fostering smart communities by enabling secure, transparent, and efficient decentralized systems for various applications [219]. In smart cities, blockchain-based platforms can streamline urban planning, infrastructure management, and resource allocation processes by ensuring transparent and traceable decision-making processes [220]. In the smart grid, blockchain-enabled smart contracts can automate and enforce agreements between different parties, reducing administrative overhead and enhancing the reliability of transactions within the community [221]. By giving people ownership over their data and enabling safe, decentralized authentication methods, blockchain-based identity management systems in smart homes can improve security and privacy in smart communities [222].

Blockchain technology has the potential to revolutionize the automotive industry by introducing greater transparency, security, and efficiency in various aspects of vehicle operations and management. Blockchain-based platforms can facilitate secure and decentralized data sharing among vehicles, enabling real-time communication and collaboration for advanced driver assistance systems, autonomous driving, and vehicle-to-vehicle (V2V) communication [223]. Furthermore, by offering a safe and unchangeable platform for handling digital signatures and cryptographic keys, blockchain technology can improve the security and integrity of vehicle-to-infrastructure (V2I) communication and over-the-air software upgrades [224].

Blockchain technology in legal systems refers to applying blockchain principles and architectures to improve various aspects of the justice system, including legal processes, record-keeping, transparency, and security. One prominent application of blockchain in justice is the creation of tamper-proof and transparent records for legal documents, such as contracts, property titles, and court records [225]. Blockchain can help increase trust among stakeholders, improve the efficiency of legal processes, and reduce the risk of fraud or corruption [226]. Blockchain technology can improve care coordination, reduce administrative burdens, and enhance patient privacy. During the COVID-19 pandemic, blockchain technology has been explored for various purposes, including vaccine distribution and supply chain management [227]. Blockchain can help track vaccine production, distribution, and administration, ensuring transparency and accountability, even with drones [228]. Additionally, blockchain-based solutions can facilitate secure and tamper-proof authentication for medical devices, which may be crucial for public health efforts [229].

Blockchain technology offers promising applications in social networks and public safety, albeit in distinct ways. By leveraging decentralized networks and cryptographic techniques, blockchain-based social platforms empower users with greater data ownership and control, ensuring transparency, privacy, and security [230]. On the other hand, in public safety, blockchain can enhance trust, transparency, and accountability in various ways, including secure record-keeping of critical information such as emergency response protocols, crime data, and public health records [231].

When comparing blockchain with other privacy preservation mechanisms, blockchain technology provides transparency, immutability, and security. Still, it may fall short regarding privacy protection, especially in scenarios where sensitive information needs to be kept confidential. Conversely, differential privacy offers strong privacy guarantees by adding noise to data queries but may not provide the same level of transparency and auditability as blockchain [232].

Figure 8 shows the steps of a blockchain transaction, which implies the decentralized concept of the technology. A user initiates a transaction by creating a digital message containing information about the transfer, such as the sender, recipient, and amount [233]. The transaction is broadcast to the network of computers (nodes) running the blockchain software. Verified transactions are grouped into a block. Miners compete to solve the puzzle through a consensus mechanism, possibly hashing. The solution is broadcast to the network by the first miner to solve the challenge. Additional nodes within the network confirm the answer supplied by the victorious miner. At this point, the blockchain has verified and documented the transaction.

6) PSEUDONYMIZATION

Pseudonymization techniques involve replacing identifiable information with pseudonyms or aliases, thereby reducing the risk of re-identification while allowing data to remain useful for analysis and processing [234]. Recent advancements in pseudonymization focus on enhancing the effectiveness and usability of pseudonymization methods while addressing challenges such as data linkage, quality, and usability [235]. Advanced pseudonymization algorithms, such as cryptographic hashing, tokenization, and anonymization, offer robust privacy protections by irreversibly transforming identifiable data elements into pseudonyms, preventing direct

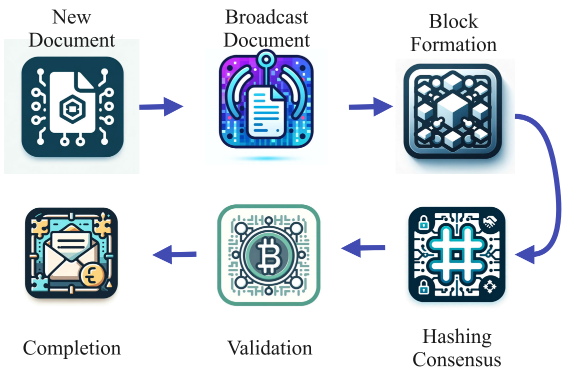


FIGURE 8. The steps of a blockchain transaction show the decentralized property of blockchain.

identification of individuals while preserving data integrity and utility [236].

Furthermore, research efforts explore context-aware pseudonymization approaches that adapt pseudonymization strategies based on the specific characteristics and requirements of the data and the intended use case, ensuring compatibility with diverse data types, formats, and privacy requirements [237]. Advancements in pseudonymization tools, standards, and best practices aim to promote interoperability, transparency, and accountability, enabling organizations and data processors to implement effective privacy safeguards while complying with regulatory requirements and privacy principles [238].

We discuss cryptographic hashing and Secure Hash Algorithm (SHA) as popular pseudonymization methods. Cryptographic hashing transforms input data of any length using a mathematical method into a fixed-length string of characters known as a hash value or hash code [239]. The National Security Agency (NSA) created the SHA family of cryptographic hash functions, frequently used for pseudonymization [240]. SHA algorithms generate hash values of fixed lengths, such as SHA256 or SHA512, which are considered secure and resistant to cryptographic attacks [241]. However, Cryptographic hashing of personally identifiable information (PII) like email or IP addresses is vulnerable due to the finite pre-image space, making identification attacks faster than brute-force methods [242].

7) OBFUSCATION

Obfuscation techniques aim to obscure or conceal sensitive information by modifying data representations or structures to retain the overall utility of the data while preventing individuals from directly identifying themselves. Obfuscation is similar to anonymization, masking, pseudonymization, and obfuscation. Their common goal is protecting sensitive data by altering or concealing its original form, thereby reducing the risk of unauthorized disclosure while preserving data utility. However, each harbors distinct techniques that differentiate each mechanism. Figure 9 illustrates the difference in the forms of a block diagram with a simple example.

Perturbation, noise injection, and data shuffling are techniques commonly employed in obfuscation to enhance privacy and protect sensitive information. To hide the underlying patterns and relationships, perturbation makes tiny, controlled changes or disturbances to the original data [243]. Examples of such disturbances include adding random noise or gently changing numerical values. Similarly, noise injection increases the amount of random or irrelevant data in the dataset, making it harder for adversaries to identify important information [244]. On the other hand, data shuffling reorganizes the order or structure of the data, mixing up the records or attributes to disguise any inherent patterns or correlations [245].

Obfuscation implementations are found in road networks and DNA data. Obfuscation in road networks involves techniques such as perturbation, where slight adjustments are made to the spatial coordinates of road segments or nodes, introducing noise to disrupt location-based patterns [246]. Additionally, data shuffling may be applied to alter the sequence or arrangement of road segments, making it difficult to discern specific routes or traffic patterns. In DNA data, obfuscation techniques aim to protect genetic information while maintaining its integrity for analysis [247]. Perturbation methods can involve introducing variations to individual nucleotide sequences or genetic markers, while data shuffling may rearrange the order of genetic sequences to conceal sensitive patterns or relationships. These obfuscation approaches help safeguard privacy in road networks and DNA data by obscuring sensitive information while preserving the overall structure and utility of the data.

The benefit of obfuscation is that it protects privacy by masking sensitive information while maintaining data utility. Unlike techniques such as anonymization, which may remove or generalize data attributes, obfuscation allows for the retention of detailed information while making it difficult to discern individual identities or patterns [248]. Furthermore, because obfuscation techniques are flexible, companies can customize the degree of privacy protection to meet their requirements. However, obfuscation may introduce challenges in maintaining data accuracy and consistency, as perturbation or data shuffling techniques can potentially impact the integrity of the original data. Furthermore, obfuscated data may still be susceptible to certain inference attacks or reverse engineering efforts, particularly if adversaries possess advanced analytical capabilities. Despite these limitations, obfuscation remains a valuable tool for balancing privacy concerns with the need for data utility in various domains.

E. REAL-WORLD SUCCESSFUL IMPLEMENTATIONS

Privacy-preserving techniques are essential for protecting sensitive data and guaranteeing its usefulness in various applications. To demonstrate the practical relevance and successful implementation of privacy-preserving technologies, we have

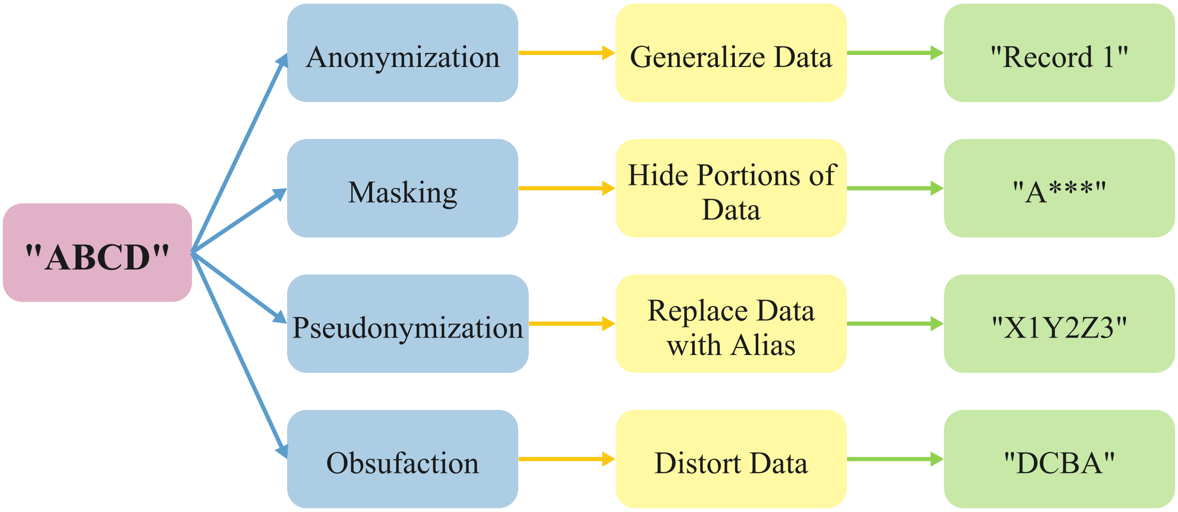


FIGURE 9. A simple example to illustrate the difference between anonymization, masking, pseudonymization, and obfuscation.

compiled a selection of real-world case studies across diverse domains. Table 5 illustrates how privacy-preserving mechanisms address domain-specific challenges while ensuring compliance with privacy and security requirements. From healthcare to vehicular networks, IoT-based smart cities, finance, and the public sector, these implementations highlight the adaptability and effectiveness of various privacy tools, including federated learning, blockchain, and secure multi-party computation.

Table 6 comprehensively synthesizes several prominent privacy-preserving methods, highlighting their advantages and disadvantages. By examining the pros and cons of each approach, stakeholders can make informed decisions regarding selecting and implementing appropriate privacy-preserving techniques. It showcases key factors such as the implementation context, success criteria, the privacy-preserving tools employed, and references to the original works. These cases provide valuable insights into how theoretical approaches to privacy preservation are translated into functional solutions across industries and domains. By highlighting these implementations, the paper underscores the tangible benefits and feasibility of adopting privacy-preserving technologies in real-world settings.

F. FUTURE DIRECTION AND OPEN ISSUES

1) AUTOMATED PIA FOR RAPID PRIVACY ENFORCEMENT

The need for PIAs in government research is paramount, serving as a crucial mechanism to evaluate and mitigate potential privacy risks associated with new policies, programs, and initiatives. By systematically assessing the impact of government actions on individuals' privacy rights and personal data, PIAs help identify privacy vulnerabilities, anticipate adverse effects, and implement appropriate safeguards to protect sensitive information. Furthermore, by guaranteeing that privacy issues are incorporated into decision-making processes and communicated to stakeholders, PIAs advance accountability, transparency, and public trust.

As government agencies increasingly rely on data-driven technologies and engage in data-intensive activities, conducting PIAs becomes essential to uphold privacy principles, comply with legal requirements, and uphold citizens' privacy rights in an evolving digital landscape.

Future research in PIA could focus on several key areas to make advancements in the field. Firstly, standardized frameworks and methodologies for conducting PIAs across different sectors and contexts are needed. This includes creating guidelines or best practices that organizations can follow to effectively assess the privacy implications of their activities and systems. Additionally, integrating automated or semi-automated tools into the PIA process could streamline and enhance efficiency, allowing organizations to conduct assessments more comprehensively and consistently. Moreover, the research could explore incorporating emerging technologies such as AI and machine learning into PIA frameworks, enabling more accurate risk assessments and proactive privacy protection measures. Finally, there is a growing recognition of the importance of stakeholder engagement and participatory approaches in PIA, suggesting opportunities for research into methodologies that facilitate collaboration and dialogue among various stakeholders to ensure that privacy concerns are effectively addressed.

2) ASSESSING RECENT IMPACTS OF GDPR ON THE REAL WORLD AND HARMONIZATION

The GDPR has significantly influenced data privacy practices worldwide since its implementation in 2018. As organizations grapple with GDPR compliance and adaptation

TABLE 5. Case studies of Real-World successful implementations of Privacy-Preserving technologies.

Domain	**Implementation**	**Success Factors**	**Privacy Tools Used**	**Reference**
Healthcare	Federated Learning to create predictive models across genomic and biomedical research institutions.	Enhanced predictive accuracy while preserving patient privacy.	Federated Learning, Blockchain.	Kuo *et al.* [249]
Vehicular Networks	Blockchain-based privacy-preserving record linkage for secure data integration in healthcare and national security applications.	Managed privacy in untrusted environments through secure data integration.	Blockchain, Secure Data Linkage.	Nóbrega*et al.* [250]
IoT/Smart Cities	Privacy-preserving crypto-system for e-healthcare IoT to protect sensitive patient data during transmission.	Ensured confidentiality and robustness against unauthorized access.	Chaos-based Encryption, Lightweight Cryptosystem.	Hamza *et al.* [251]
Finance	Multi-party computation (MPC) for privacy-preserving data aggregation in IoT-based systems.	Protected raw data while enabling secure aggregation in resource-constrained environments.	Secure Multi-Party Computation (MPC), Shamir's Secret Sharing.	Priya *et al.* [7]
Public Sector	Privacy-preserving machine learning framework (FLASH) for secure real-time analytics in sensitive data systems.	Enabled privacy-compliant analytics while ensuring strong security guarantees.	Secure Multi-Party Computation (MPC), Privacy-Preserving Machine Learning (PPML).	Byali *et al.* [252]

TABLE 6. Comparison of privacy-preserving techniques involved in the government.

Technique	Cite	Sub-technique/Implementation	Advantage	Disadvantage
Encryption	[170] [173]	Homomorphic Encryption	Enables computation on encrypted data without decryption	Computational overhead
	[175] [179]	SMPC	Enables computation on distributed data without revealing raw data	Communication overhead
Anonymization	[191] [192]	Differential Privacy	Provides rigorous privacy guarantees while allowing for accurate analysis	May impact data utility
		K-anonymity	Preserves privacy by generalizing data attributes	May lead to information loss
		L-diversity		
		T-closeness		
Edge Computing	[205] [209]	Federated Learning	Allows collaborative model training on decentralized data	Communication and synchronization overhead, privacy concerns
Data Masking	[211] [212]	Format-preserving Encryption	Preserves data format while protecting sensitive information	Limited protection against sophisticated attacks, loss of data fidelity
		Tokenization		
Blockchain	[222] [230]	Privacy-focused Cryptocurrencies	Enhances anonymity and fungibility of digital assets	Scalability issues, regulatory uncertainties, energy consumption
Pseudonymization	[237] [238]	Cryptographic Hashing	Protects individual identities without revealing real identities	Vulnerable to re-identification attacks
		Secure Hash Algorithms (SHA)		
Obfuscation	[247] [248]	Data Perturbation	Hides sensitive information by introducing randomness or distortion	May impact data utility
		Noise Injection		
		Data Shuffling		

to evolving data privacy standards, future research efforts should focus on several key areas to enhance effectiveness. Firstly, there is a need for empirical studies to assess the real-world impact of GDPR on individuals, businesses, and regulatory bodies. Understanding the challenges and benefits experienced by different stakeholders can inform potential amendments or clarifications to the regulation, ensuring its alignment with contemporary privacy concerns.

Second, studies should examine how GDPR interacts with cutting-edge technology like blockchain, AI, and IoT. These technologies present unique privacy challenges and opportunities, and their integration with GDPR frameworks requires careful consideration. Studies investigating the compatibility of GDPR principles with advanced data processing techniques and decentralized architectures can provide valuable insights into ensuring continued privacy protection in the digital age.

Furthermore, future research should explore the global implications of GDPR and its harmonization with other privacy regulations worldwide. As data flows transcend national borders, there is a growing need for international cooperation and standardization in privacy governance. Comparative analyses of GDPR with regulations like the California Consumer Privacy Act (CCPA), Indonesia's Personal Data Protection Regulation (UU PDP), Brazil's General Data ProVOLUME 1, 2020 21tection Law (LGPD), and the upcoming EU Data Governance Act can identify areas of convergence and divergence, facilitating a more cohesive global privacy framework. Ultimately, through interdisciplinary collaboration and empirical inquiry, future research endeavors can contribute to the ongoing evolution and refinement of GDPR, fostering a robust and adaptive data privacy landscape.

3) USER-CENTRIC PRIVACY-PRESERVING TECHNOLOGIES AND SERVICES

Research opportunities exist in developing and evaluating user-centric privacy-preserving technologies, such as privacy-enhancing tools, data anonymization techniques, and consent management platforms, that empower individuals to protect their privacy online. Studies could investigate user attitudes, perceptions, and behaviors towards privacy-enhancing services, exploring factors influencing adoption, usability, and effectiveness. Future research directions may involve examining the societal and economic impacts of the widespread adoption of privacy-preserving technologies and services, including their role in enhancing trust, fostering innovation, and promoting digital inclusion.

4) ADDRESSING LOCATION PRIVACY PROBLEMS IN THE EMERGENCE OF NEW DIMENSIONS IN LBSs

The future of location privacy research presents several significant challenges that necessitate innovative approaches and solutions. First, LBSs continue to proliferate and become more sophisticated, such as the emergence of IoT-based LBSs. This makes ensuring robust privacy protection mechanisms increasingly complex. Second, the dynamic nature of privacy threats requires continuous adaptation and enhancement of privacy-preserving techniques to keep pace with evolving privacy risks and regulatory landscapes. For example, consider the evolving landscape of mobile applications that utilize geolocation data. The privacy dangers connected to gathering and using location data are becoming more complex and multidimensional as new features and capabilities, such as location-based advertising and real-time tracking, are added to these apps.

Furthermore, changes in regulatory frameworks, such as updates to data protection laws like GDPR or CCPA, may require developers to adjust their privacy practices and implement more robust privacy-preserving mechanisms. Therefore, continuous adaptation and enhancement of privacy techniques are essential to address emerging threats and comply with evolving regulations in location privacy. Addressing these challenges will require interdisciplinary collaboration, technological innovation, and proactive policy measures to safeguard individuals' location privacy effectively.

5) THE COLLABORATION OF PETs AND DECENTRALIZATION

We have discussed blockchain as a decentralization technique in the privacy preservation mechanism. While blockchain is widely adopted as a decentralization technique, it typically provides minimal confidentiality in privacy protection. On the other hand, we have shown that anonymization, homomorphic encryption, and various PETs have brought significant success in safeguarding privacy-sensitive data.

Future research on the collaboration between PETs and decentralization holds significant promise for advancing privacy preservation in various domains. One avenue of exploration involves examining how decentralized systems, such as blockchain networks, can integrate PETs to enhance privacy while maintaining the benefits of decentralization, such as data autonomy and resilience against central points of failure. Additionally, researchers may develop novel PETs tailored specifically for decentralized environments, addressing challenges such as scalability, interoperability, and governance. Furthermore, investigating the synergies between PETs and emerging decentralized technologies, such as federated learning and decentralized identifiers (DIDs), could lead to innovative approaches for preserving privacy in distributed ecosystems while empowering individuals with greater control over their data.

6) ADVANCED TECHNIQUES IN BALANCING PRIVACY PROTECTION AND DATA UTILITY

We have discussed the many powers and disadvantages of various PETs. Increasing data utilization often involves sharing or analyzing more data, which can lead to a greater risk of privacy breaches. Conversely, prioritizing privacy protection may involve limiting data access or obfuscating information, hindering data utilization for analysis or decision-making purposes. Anonymization is more oriented toward privacy protection than data utilization. On the other hand, federated learning is more geared towards data utilization than privacy protection. It isn't easy to balance data utility and privacy protection for future research. Anonymization and data masking are two examples of privacy-preserving approaches that face significant challenges in balancing privacy protection with data value. Future research can explore methods to enhance data utility while maintaining strong privacy guarantees, including advanced anonymization algorithms that minimize information loss and innovative data masking techniques that preserve data fidelity.

V. CONCLUSION

This study proposes an SLR that conducts an in-depth discussion of three research questions, mainly about government roles in privacy-preserving mechanisms, ministries involved in and concerning matters, and advancements in privacy-preserving technologies utilized by and related to governments. Our study shows that the government plays three main roles related to privacy preservation: regulator and enforcer, user and partner, and service provider. Then, several main issues arise from our in-depth article review: law, healthcare, IoT, location, finance and economy, and the World Wide Web. The ministries involved consist of The Ministry of Law and Justice, The Ministry of Health, The Ministry of Internal Affairs, The Ministry of Transportation and The Agency of Geospatial Information, The Ministry of Treasury, and The Ministry of Communications and Information.

Our literature search shows that several solutions exist related to privacy preservation. Encryption has brought advances in computation and communication in the forms of homomorphic encryption and SMPC. Differential privacy is a very popular sub-technique of anonymization, where k-anonymity, l-diversity, and t-closeness are also formidable implementations. Federated learning has been the spearhead of edge computing advancements. Data masking is a complementary method to anonymization where, instead of altering or generalizing data attributes, sensitive information is replaced with fictional or modified values while preserving the overall structure and format of the dataset. Blockchain is the most popular among others in finance and healthcare data. Lastly, pseudonymization and obfuscation are two methods that replace identifiable information with pseudonyms and obscure or distort the data, respectively.

Our critical analysis shows five main research gaps in privacy-preserving mechanisms related to the government. First, PIA is vital to the government's role as regulator and enforcer. It ensures that privacy risks associated with policies, regulations, and enforcement actions are systematically identified, evaluated, and mitigated, safeguarding individuals' privacy rights and fostering trust in government data practices. Second, integrating regulatory and technological approaches in privacy preservation is paramount, as it allows for comprehensive and adaptive strategies that address legal requirements and technical challenges, thereby promoting effective and sustainable privacy protections in an evolving digital landscape. Third, user-centric privacy-preserving technologies and services should take the highlight for future research because prioritizing user preferences, needs, and consent is essential for promoting individual autonomy, trust, and accountability in data-driven environments, ultimately empowering users to exercise greater control over their personal information and privacy choices. Fourth, we have identified the emergence of popular topics: law, healthcare, IoT, location, finance and economy, and the World Wide Web. Addressing them and synthesizing interdisciplinary innovation should not be neglected. Fifth, we have discussed several privacy-preserving mechanisms, where some demonstrate immense advantages. However, research opportunities exist to perfect the methods above by increasing computational efficiency and preventing information loss.

TABLE 7. Abbreviations.

Abbreviation	Full form
ABE	Attribute-based encryption
AI	Artificial Intelligence
CCPA	California Consumer Privacy Act
DIDs	decentralized identifiers
DNA	Deoxyribonucleic Acid
EHRs	Electronic health records
ETC	Electronic Toll Collection
ETCS	ETC systems
FIPPs	Fair Information Practice Principles
FPE	Format-preserving encryption
GA	Genetic algorithms
GDPR	General Data Protection Regulation
HE	Homomorphic encryption
HIPAA	Health Insurance Portability and Accountability Act
IIoT	industrial IoT
IoMT	Internet of Medical Things
IoT	Internet of Things
ITS	Intelligent Transportation System
IPS	Indoor positioning systems
LBS	location-based service
LBSNs	Location-based social networks
LGPD	Brazil's General Data Protection Law
MaaS	Mobility as a Service
P3P	Platform for privacy preference
PET	Privacy-enhancing technology
PGP	Pretty good privacy
PIA	Privacy impact assessment
PII	personally identifiable information
PKI	public key infrastructure
PPDM	privacy-preserving data mining
ring-LWE	Lattice-based cryptography ring-learning with errors
SHA	Secure Hash Algorithms
SLR	Systematic literature review
SMPC	Secure multi-party computation
V2I	vehicle-to-infrastructure
V2G	Vehicle-to-Grid
V2V	vehicle-to-vehicle
V2X	vehicle-to-everything

VI. ABBREVIATIONS

Table 7 presents a comprehensive compilation of abbreviations relevant to privacy preservation within governmental contexts. These abbreviations facilitate clear communication and understanding of complex concepts, particularly privacy regulation and enforcement. By providing a reference guide, this table can assist researchers and practitioners in navigating the diverse landscape of privacy preservation initiatives undertaken by government entities.

ACKNOWLEDGMENT

The authors hope that this research will strengthen the privacy preservation related to governments. They also thank TU Delft for their support and accommodation throughout the research.

REFERENCES

[1] S. Lahlou, "Identity, social status, privacy and face-keeping in digital society," *Social Sci. Inf.*, vol. 47, no. 3, pp. 299–330, Sep. 2008.

[2] S. Pearson, "Privacy management and accountability in global organisations," in *Proc. IFIP PrimeLife Int. Summer School Privacy Identity Manage. Life*, Jan. 2014, pp. 33–52.

[3] M. Keshk, B. Turnbull, E. Sitnikova, D. Vatsalan, and N. Moustafa, "Privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems," *IEEE Access*, vol. 9, pp. 55077–55097, 2021.

[4] M. Cunha, R. Mendes, and J. P. Vilela, "A survey of privacy-preserving mechanisms for heterogeneous data types," *Comput. Sci. Rev.*, vol. 41, Aug. 2021, Art. no. 100403.

[5] S. Patil and K. Parmar, "Differential privacy mechanisms: A state-of-the-art survey," in *Proc. 4th Int. Conf. Futuristic Trends Netw. Comput. Technol. (FTNCT)*. Cham, Switzerland: Springer, 2022, pp. 1049–1060.

[6] A. A. Jolfaei, A. Boualouache, A. Rupp, S. Schiffner, and T. Engel, "A survey on privacy-preserving electronic toll collection schemes for intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 9, pp. 8945–8962, Sep. 2023.

[7] P. Priya, S. Girubalini, B. Lakshmi Prabha, B. Pranitha, and M. Srigayathri, "A survey on privacy preserving voting scheme based on blockchain technology," in *Proc. IoT Smart Syst. (CTIS)*, vol. 2. Cham, Switzerland: Springer, 2022, pp. 267–283.

[8] X. Wang, P. Shi, J. Li, Y. Yang, F. Yang, H. Yu, and J. Wang, "Privacy-preserving mechanisms of continuous location queries based on LBS: A comprehensive survey," in *Proc. 27th Int. Conf. Autom. Comput. (ICAC)*, Sep. 2022, pp. 1–6.

[9] R. Yang, "Survey on privacy-preserving machine learning protocols," in *Proc. 3rd Int. Conf. Mach. Learn. Cyber Secur. (ML4CS)*, Guangzhou, China. Cham, Switzerland: Springer, Jan. 2020, pp. 417–425.

[10] T. Carvalho, N. Moniz, P. Faria, and L. Antunes, "Survey on privacy-preserving techniques for microdata publication," *ACM Comput. Surv.*, vol. 55, no. 14s, pp. 1–42, Dec. 2023.

[11] S. Shimona, "Survey on privacy preservation technique," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, Feb. 2020, pp. 64–68.

[12] H. C. Tanuwidjaja, R. Choi, and K. Kim, "A survey on deep learning techniques for privacy-preserving," in *Proc. 2nd Int. Conf. Mach. Learn. Cyber Secur. (ML4CS)*, Xi'an, China. Cham, Switzerland: Springer, Jan. 2019, pp. 29–46.

[13] S. R. Kurupathi and W. Maaß, "Survey on federated learning towards privacy preserving AI," in *Proc. Comput. Sci. Inf. Technol. (CSIT)*, Sep. 2020, pp. 1–19.

[14] Y. Cui, B. Pan, and Y. Sun, "A survey of privacy-preserving techniques for blockchain," in *Proc. 5th Int. Conf. Artif. Intell. Secur. (ICAIS)*, New York, NY, USA. Cham, Switzerland: Springer, 2019, pp. 225–234.

[15] Y. Cheng, J. Ma, Z. Liu, Y. Wu, K. Wei, and C. Dong, "A lightweight privacy preservation scheme with efficient reputation management for mobile crowdsensing in vehicular networks," *IEEE Trans. Dependable Secure Comput.*, vol. 20, pp. 1771–1788, 2023.

[16] R. Li, Z. Liu, Y. Ma, Y. Xia, Y. Cheng, L. Wan, and J. Ma, "RPPM: A reputation-based and privacy-preserving platoon management scheme in vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 6, pp. 6147–6160, Jun. 2024.

[17] Z. Liu, J. Weng, J. Guo, J. Ma, F. Huang, H. Sun, and Y. Cheng, "PPTM: A privacy-preserving trust management scheme for emergency message dissemination in space-air-ground-integrated vehicular networks," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 5943–5956, Apr. 2022.

[18] S. F. Pane and M. S. Amrullah, "Systematic literature review: Analisa sentimen masyarakat terhadap penerapan peraturan ETLE," *J. Appl. Comput. Sci. Technol.*, vol. 4, no. 1, pp. 65–74, Jul. 2023.

[19] A. Amjad, P. Kordel, and G. Fernandes, "The systematic review in the field of management sciences," *Zeszyty Naukowe. Organizacja i Zarządzanie/Politechnika Śląska*, vol. 2023, no. 170, pp. 9–35, Jan. 2023.

[20] R. E. S. Santos and F. Q. B. Da Silva, "Motivation to perform systematic reviews and their impact on software engineering practice," in *Proc. ACM/IEEE Int. Symp. Empirical Softw. Eng. Meas.*, Oct. 2013, pp. 292–295.

[21] D. Tod, "Inclusion and exclusion criteria," *Conducting Systematic Rev. Sport, Exercise, Phys. Activity*, vol. 2019, pp. 55–66, Jan. 2019.

[22] K. R. Felizardo, E. Mendes, M. Kalinowski, É. F. Souza, and N. L. Vijaykumar, "Using forward snowballing to update systematic reviews in software engineering," in *Proc. 10th ACM/IEEE Int. Symp. Empirical Softw. Eng. Meas.*, Sep. 2016, pp. 1–6.

[23] A. P. Kurniati, O. Johnson, D. Hogg, and G. Hall, "Process mining in oncology: A literature review," in *Proc. 6th Int. Conf. Inf. Commun. Manage. (ICICM)*, Oct. 2016, pp. 291–297.

[24] Y.-H. Tseng, Y.-I. Lin, Y.-Y. Lee, W.-C. Hung, and C.-H. Lee, "A comparison of methods for detecting hot topics," *Scientometrics*, vol. 81, no. 1, pp. 73–90, Oct. 2009.

[25] A. Kirby, "Exploratory bibliometrics: Using VOSviewer as a preliminary research tool," *Publications*, vol. 11, no. 1, p. 10, Feb. 2023.

[26] L. Alzubaidi et al., "Towards risk-free trustworthy artificial intelligence: Significance and requirements," *Int. J.*, vol. 2023, pp. 1–41, Oct. 2023.

[27] H. Zhang, Y. Shu, P. Cheng, and J. Chen, "Privacy and performance trade-off in cyber-physical systems," *IEEE Netw.*, vol. 30, no. 2, pp. 62–66, Mar. 2016.

[28] T. Sharon and B.-J. Koops, "The ethics of inattention: Revitalising civil inattention as a privacy-protecting mechanism in public spaces," *Ethics Inf. Technol.*, vol. 23, no. 3, pp. 331–343, Sep. 2021.

[29] W. Ali, I. U. Din, A. Almogren, and B.-S. Kim, "A novel privacy preserving scheme for smart grid-based home area networks," *Sensors*, vol. 22, no. 6, p. 2269, Mar. 2022.

[30] T. W. Chim, S.-M. Yiu, V. O. K. Li, L. C. K. Hui, and J. Zhong, "PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 85–97, Jan. 2015.

[31] M. Alazab, T. R. Gadekallu, and C. Su, "Guest editorial: Security and privacy issues in industry 4.0 applications," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6326–6329, Sep. 2022.

[32] X. Zhang, S. Ji, and T. Wang, "Differentially private releasing via deep generative model (Technical Report)," 2018, *arXiv:1801.01594*.

[33] F. Abbas, U. Rajput, and H. Oh, "PRISM: Privacy-aware interest sharing and matching in mobile social networks," *IEEE Access*, vol. 4, pp. 2594–2603, 2016.

[34] A. Abeliuk, G. Berbeglia, and P. Van Hentenryck, "Bargaining mechanisms for one-way games," *Games*, vol. 6, no. 3, pp. 347–367, Sep. 2015.

[35] S. Wang, L. Shi, Q. Hu, J. Zhang, X. Cheng, and J. Yu, "Privacy-aware data trading," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3916–3927, 2021.

[36] D. Pujol and A. Machanavajjhala, "Equity and privacy: More than just a tradeoff," *IEEE Secur. Privacy*, vol. 19, no. 6, pp. 93–97, Nov. 2021.

[37] Y. Zhang, Y. Qu, L. Gao, T. H. Luan, X. Zheng,S. Chen, and Y. Xiang, "APDP: Attack-proof personalized differential privacy model for a smart home," *IEEE Access*, vol. 7, pp. 166593–166605, 2019.

[38] R. Danger, "Differential privacy: What is all the noise about?" 2022, *arXiv:2205.09453*.

[39] M. Chessa, J. Großklags, and P. Loiseau, "A game-theoretic study on non-monetary incentives in data analytics projects with privacy implications," in *Proc. IEEE 28th Comput. Secur. Found. Symp.*, Jul. 2015, pp. 90–104.

[40] D. Georgiou and C. Lambrinoudakis, "Data protection impact assessment (DPIA) for cloud-based health organizations," *Future Internet*, vol. 13, no. 3, p. 66, Mar. 2021.

[41] R. Meis and M. Heisel, "Systematic identification of information flows from requirements to support privacy impact assessments," in *Proc. 10th Int. Joint Conf. Softw. Technol. (ICSOFT)*, vol. 2, Jul. 2015, pp. 1–10.

[42] F. Zarrabi, I. Wagner, and E. Boiten, "Changes in conducting data protection risk assessment and after GDPR implementation," 2023, *arXiv:2304.11876*.

[43] H. J. Pandit, "A semantic specification for data protection impact assessments (DPIA)," in *Proc. 18th Int. Conf. Semantic Syst. (SEMANTiCS)*, Vienna, Austria. Amsterdam, The Netherlands: IOS Press, Sep. 2022, p. 36.

[44] K. Wadhwa, "Privacy impact assessment reports: A report card," *Info*, vol. 14, no. 3, pp. 35–47, May 2012.

[45] F. Ayala-Gomez, I. Horppu, E. Gulbenkoglu, V. Siivola, and B. Pejó, "Revenue attribution on iOS 14 using conversion values in F2P games," 2021, *arXiv:2102.08458*.

[46] S.-E. Tbahriti, C. Ghedira, B. Medjahed, M. Mrissa, and D. Benslimane, "How to enhance privacy within DaaS service composition?" *IEEE Syst. J.*, vol. 7, no. 3, pp. 442–454, Sep. 2013.

[47] A. Bourass, S. Cherkaoui, and L. Khoukhi, "Secure optimal itinerary planning for electric vehicles in the smart grid," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3236–3245, Dec. 2017.

[48] D. Rebollo-Monedero, J. Parra-Arnau, C. Diaz, and J. Forné, "On the measurement of privacy as an attacker's estimation error," *Int. J. Inf. Secur.*, vol. 2013, no. 12, pp. 129–149, 2013.

[49] X. Li and G. Sun, "A solution to privacy preservation in publishing human trajectories," *KSII Trans. Internet Inf. Syst.*, vol. 14, no. 8, pp. 3328–3349, 2020.

[50] D. Edge, W. Yang, K. Lytvynets, H. Cook, C. Galez-Davis, H. Darnton, and C. M. White, "Design of a privacy-preserving data platform for collaboration against human trafficking," 2020, *arXiv:2005.05688*.

[51] Z. Garroussi, A. Legrain, S. Gambs, V. Gautrais, and B. Sansò, "Data privacy for mobility as a service," 2023, *arXiv:2310.10663*.

[52] F. Fioretto and P. V. Hentenryck, "Constrained-based differential privacy: Releasing optimal power flow benchmarks privately: Releasing optimal power flow benchmarks privately," in *Proc. Int. Conf. Integr. Constraint Program., Artif. Intell., Oper. Res.*, Delft, The Netherlands, 2018, pp. 215–231.

[53] D. B. Smith, K. Thilakarathna, and M. A. Kaafar, "More flexible differential privacy: The application of piecewise mixture distributions in query release," 2017, *arXiv:1707.01189*.

[54] A. Biswas and G. Cormode, "Verifiable differential privacy," 2022, *arXiv:2208.09011*.

[55] A. Biswas and G. Cormode, "Interactive proofs for differentially private counting," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2023, pp. 1919–1933.

[56] F. P. Appio, M. G. C. A. Cimino, A. Lazzeri, A. Martini, and G. Vaglini, "Fostering distributed business logic in open collaborative networks: An integrated approach based on semantic and swarm coordination," *Inf. Syst. Frontiers*, vol. 20, no. 3, pp. 589–616, Jun. 2018.

[57] A. De Carli, M. Franco, A. Gassmann, C. Killer, B. Rodrigues, E. Scheid, D. Schoenbaechler, and B. Stiller, "WeTrace—A privacy-preserving mobile COVID-19 tracing approach and application," 2020, *arXiv:2004.08812*.

[58] Z. Amin, A. Anjum, A. Khan, A. Ahmad, and G. Jeon, "Preserving privacy of high-dimensional data by l-diverse constrained slicing," *Electronics*, vol. 11, no. 8, p. 1257, Apr. 2022.

[59] L. Bedogni, S. K. Rumi, and F. D. Salim, "Modelling memory for individual re-identification in decentralised mobile contact tracing applications," in *Proc. ACM Interact.*, vol. 5, Mar. 2021, pp. 1–21.

[60] I. Vergara-Laurens, D. Méndez, L. G. Jaimes, and M. A. Labrador, "A-PIE: An algorithm for preserving privacy, quality of information, and energy consumption in participatory sensing systems," *Pervasive Mobile Comput.*, vol. 32, pp. 93–112, Oct. 2016.

[61] H. H. Arcolezi, J.-F. Couchot, S. Cerna, C. Guyeux, G. Royer, B. A. Bouna, and X. Xiao, "Forecasting the number of firefighter interventions per region with local-differential-privacy-based data," *Comput. Secur.*, vol. 96, Sep. 2020, Art. no. 101888.

[62] N. U. Sheikh, H. J. Asghar, F. Farokhi, and M. A. Kaafar, "Do auto-regressive models protect privacy? Inferring fine-grained energy consumption from aggregated model parameters," *IEEE Trans. Services Comput.*, vol. 15, no. 6, pp. 3198–3209, Nov. 2022.

[63] J. Ning, X. Huang, G. S. Poh, S. Xu, J.-C. Loh, J. Weng, and R. H. Deng, "Pine: Enabling privacy-preserving deep packet inspection on TLS with rule-hiding and fast connection establishment," in *Proc. 15th Eur. Symp. Res. Comput. Secur. (ESORICS)*, Jan. 2020, pp. 3–22.

[64] R. Hussain and H. Oh, "Identity-exchange based privacy preserving mechanism in vehicular networks," *J. Korea Inst. Inf. Secur. Cryptol.*, vol. 24, no. 6, pp. 1147–1157, Dec. 2014.

[65] T. Giannetsos and I. Krontiris, "Securing V2X communications for the future: Can PKI systems offer the answer?" in *Proc. 14th Int. Conf. Availability, Rel. Secur.*, Aug. 2019, pp. 1–8.

[66] S. Chang, H. Zhu, M. Dong, K. Ota, X. Liu, and X. Shen, "Private and flexible urban message delivery," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 4900–4910, Jul. 2016.

[67] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, "Hyperconnected network: A decentralized trusted computing and networking paradigm," *IEEE Netw.*, vol. 32, no. 1, pp. 112–117, Jan. 2018.

[68] A. Viejo, J. Castella-Roca, and G. Rufián, "Preserving the user's privacy in social networking sites," in *Trust, Privacy, and Security in Digital Business*. Berlin, Germany: Springer-Verlag, 2013.

[69] H. Jameel Asghar and D. Kaafar, "Averaging attacks on bounded noise-based disclosure control algorithms," 2019, *arXiv:1902.06414*.

[70] I. Vakilinia and S. Sengupta, "Vulnerability market as a public-good auction with privacy preservation," *Comput. Secur.*, vol. 93, Jun. 2020, Art. no. 101807.

[71] R.-J. Yew and A. Xiang, "Regulating facial processing technologies: Tensions between legal and technical considerations in the application of Illinois BIPA," in *Proc. ACM Conf. Fairness, Accountability, Transparency*, Jun. 2022, pp. 1017–1027.

[72] S. A. Anand, P. Walker, and N. Saxena, "Compromising speech privacy under continuous masking in personal spaces," in *Proc. 17th Int. Conf. Privacy, Secur. Trust (PST)*, Aug. 2019, pp. 1–10.

[73] S. Wang, L. Bonomi, W. Dai, F. Chen, C. Cheung, C. S. Bloss, S. Cheng, and X. Jiang, "Big data privacy in biomedical research," *IEEE Trans. Big Data*, vol. 6, no. 2, pp. 296–308, Jun. 2020.

[74] A. Cormack, "An introduction to the GDPR (v3)," *IDPro Body Knowl.*, vol. 1, no. 5, pp. 1–13, 2021. [Online]. Available: https://bok.idpro.org/article/11/galley/246/view/

[75] G. Malgieri, "The concept of fairness in the GDPR: A linguistic and contextual interpretation," in *Proc. Conf. Fairness, Accountability, Transparency*, Jan. 2020, pp. 154–166.

[76] M. Abdurohman, S. Prabowo, A. G. Putrada, I. D. Oktaviani, H. H. Nuha, D. W. Jacob, and M. Janssen, "A privacy-preserving smart body scale with K-Means anonymization towards GDPR-compliant IoT," in *Proc. Int. Conf. Electr., Commun. Comput. Eng. (ICECCE)*, Dec. 2023, pp. 1–6.

[77] S. Prabowo, A. G. Putrada, I. D. Oktaviani, and M. Abdurohman, "Camera-based smart lighting system that complies with Indonesia's personal data protection act," in *Proc. Int. Conf. Advancement Data Sci., E-learning Inf. Syst. (ICADEIS)*, Aug. 2023, pp. 1–6.

[78] O. Amaral, M. I. Azeem, S. Abualhaija, and L. C. Briand, "NLP-based automated compliance checking of data processing agreements against GDPR," *IEEE Trans. Softw. Eng.*, vol. 49, no. 9, pp. 4282–4303, Sep. 2023.

[79] D. Peloquin, M. DiMaio, B. Bierer, and M. Barnes, "Disruptive and avoidable: GDPR challenges to secondary research uses of data," *Eur. J. Human Genet.*, vol. 28, no. 6, pp. 697–705, Jun. 2020.

[80] M. Knockaert and N. D. Vos, "Ethical, legal and privacy considerations for adaptive systems," in *Engineering Data-Driven Adaptive Trust-based E-Assessment Systems*. Cham, Switzerland: Springer, Oct. 2019, pp. 267–296.

[81] C. Camardi, "Liability and accountability in the 'digital'relationships," in *Privacy and Data Protection in Software Services*. Venice, Italy: ARCA—Ca'Foscari, 2022, pp. 25–34.

[82] S. Panda, D. Jena, and P. Das, "A blockchain-based distributed authentication system for healthcare," *Int. J. Healthcare Inf. Syst. Inform.*, vol. 16, no. 4, pp. 1–14, 2021.

[83] Y. Xu, Z. Chen, and H. Zhong, "Privacy-preserving double auction mechanism based on homomorphic encryption and sorting networks," 2019, *arXiv:1909.07637*.

[84] H. Wang, A. Li, B. Shen, Y. Sun, and H. Wang, "Federated multi-view spectral clustering," *IEEE Access*, vol. 8, pp. 202249–202259, 2020.

[85] A. F. Parker, T. Grønli, and M. Younas, "A game of fog and mirrors: Privacy in the world of Internet of Things," in *Proc. MobiWIS*, Jan. 2021, pp. 163–174.

[86] M. Franco, B. Rodrigues, C. Killer, E. J. Scheid, A. D. Carli, A. Gassmann, D. Schönbächler, and B. Stiller, "WeTrace: A privacy-preserving tracing approach," *J. Commun. Netw.*, vol. 23, no. 5, pp. 374–389, Oct. 2021.

[87] L. D. Martino, Q. Ni, D. Lin, and E. Bertino, "Multi-domain and privacy-aware role based access control in eHealth," in *Proc. 2nd Int. Conf. Pervasive Comput. Technol. Healthcare*, Jan. 2008, pp. 131–134.

[88] H. Lin, J. Shao, C. Zhang, and Y. Fang, "CAM: Cloud-assisted privacy preserving mobile health monitoring," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 985–997, Jun. 2013.

[89] Q. Wang and S. Qin, "A hyperledger fabric-based system framework for healthcare data management," *Appl. Sci.*, vol. 11, no. 24, p. 11693, Dec. 2021.

[90] Y. Yang, X. Li, N. Qamar, P. Liu, W. Ke, B. Shen, and Z. Liu, "MedShare: A novel hybrid cloud for medical resource sharing among autonomous healthcare providers," *IEEE Access*, vol. 6, pp. 46949–46961, 2018.

[91] S. Samarah, M. Gh. Al Zamil, A. F. Aleroud, M. Rawashdeh, M. F. Alhamid, and A. Alamri, "An efficient activity recognition framework: Toward privacy-sensitive health data sensing," *IEEE Access*, vol. 5, pp. 3848–3859, 2017.

[92] C. Ju, R. Zhao, J. Sun, X. Wei, B. Zhao, Y. Liu, H. Li, T. Chen, X. Zhang, D. Gao, B. Tan, H. Yu, C. He, and Y. Jin, ''Privacy-preserving technology to help millions of people: Federated prediction model for stroke prevention,'' 2020, *arXiv:2006.10517*.

[93] M. M. A. Aziz, M. M. Anjum, N. Mohammed, and X. Jiang, ''Generalized genomic data sharing for differentially private federated learning,'' *J. Biomed. Informat.*, vol. 132, Aug. 2022, Art. no. 104113.

[94] S. M. Karunarathne, N. Saxena, and M. K. Khan, ''Security and privacy in IoT smart healthcare,'' *IEEE Internet Comput.*, vol. 25, no. 4, pp. 37–48, Jul. 2021.

[95] O. Choudhury, A. Gkoulalas-Divanis, T. Salonidis, I. Sylla, Y. Park, G. Hsu, and A. Das, ''Differential privacy-enabled federated learning for sensitive health data,'' 2019, *arXiv:1910.02578*.

[96] Y. Xia, T. Zhu, X. Ding, H. Jin, and D. Zou, ''Heterogeneous differential privacy for vertically partitioned databases,'' *Concurrency Comput., Pract. Exper.*, vol. 33, no. 8, p. e5607, Apr. 2021.

[97] A. Lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, A. Vidyarthi, A. Alkhayyat, and W. Wang, ''Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare,'' *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 664–672, Feb. 2023.

[98] J. Liu, W. Jiang, R. Sun, A. K. Bashir, M. D. Alshehri, Q. Hua, and K. Yu, ''Conditional anonymous remote healthcare data sharing over blockchain,'' *IEEE J. Biomed. Health Informat.*, vol. 27, no. 5, pp. 2231–2242, May 2023.

[99] A. A. Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, ''MediBchain: A blockchain based privacy preserving platform for healthcare data,'' in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*, Jan. 2017, pp. 534–543.

[100] F. Kausar, ''Iris based cancelable biometric cryptosystem for secure healthcare smart card,'' *Egyptian Informat. J.*, vol. 22, no. 4, pp. 447–453, Dec. 2021.

[101] P. Deshmukh, ''Design of cloud security in the EHR for Indian healthcare services,'' *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 29, no. 3, pp. 281–287, Jul. 2017.

[102] B. Qureshi, ''An affordable hybrid cloud based cluster for secure health informatics research,'' *Int. J. Cloud Appl. Comput.*, vol. 8, no. 2, pp. 27–46, Apr. 2018.

[103] S. U. Bazai, J. Jang-Jaccard, and R. Wang, ''Anonymizing k-NN classification on MapReduce,'' in *Proc. Int. Conf. Mobile Netw. Manag.* Cham, Switzerland: Springer, Jan. 2018, pp. 364–377.

[104] Z. Li and E. J. Pino, ''D&D: A distributed and disposable approach to privacy preserving data analytics in user-centric healthcare,'' in *Proc. IEEE 12th Conf. Service-Oriented Comput. Appl. (SOCA)*, Nov. 2019, pp. 176–183.

[105] E. S. Saputra, A. G. Putrada, and M. Abdurohman, ''Selection of vape sensing features in IoT-based gas monitoring with feature importance techniques,'' in *Proc. 4th Int. Conf. Informat. Comput. (ICIC)*, Oct. 2019, pp. 1–5.

[106] T. Le and S. Shetty, ''Artificial intelligence-aided privacy preserving trustworthy computation and communication in 5G-based IoT networks,'' *Ad Hoc Netw.*, vol. 126, Mar. 2022, Art. no. 102752.

[107] S. Demir, Ş. Şimşek, S. Gür, and A. Levi, ''Secure and privacy preserving IoT gateway for home automation,'' *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108036.

[108] Q. Yan, J. Lou, M. C. Vuran, and S. Irmak, ''Scalable privacy-preserving geo-distance evaluation for precision agriculture IoT systems,'' *ACM Trans. Sensor Netw.*, vol. 17, no. 4, pp. 1–30, Nov. 2021.

[109] J. Guo, M. Yang, and B. Wan, ''A practical privacy-preserving publishing mechanism based on personalized k-Anonymity and temporal differential privacy for wearable IoT applications,'' *Symmetry*, vol. 13, no. 6, p. 1043, Jun. 2021.

[110] M. Kamal, I. Rashid, W. Iqbal, M. H. Siddiqui, S. Khan, and I. Ahmad, ''Privacy and security federated reference architecture for Internet of Things,'' *Frontiers Inf. Technol. Electron. Eng.*, vol. 24, no. 4, pp. 481–508, 2023.

[111] R. T. Moreno, J. B. Bernabé, J. García-Rodríguez, T. K. Frederiksen, M. Stausholm, N. Martínez, E. Sakkopoulos, N. S. Ponte, and A. Skármeta, ''The olympus architecture—Oblivious identity management for private user-friendly services,'' *Sensors*, vol. 20, no. 3, p. 945, Feb. 2020.

[112] Q. Kong, R. Lu, F. Yin, and S. Cui, ''Blockchain-based privacy-preserving driver monitoring for MaaS in the vehicular IoT,'' *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3788–3799, Apr. 2021.

[113] M. Ali, A. Anjum, A. Anjum, and M. A. Khan, ''Efficient and secure energy trading in Internet of Electric Vehicles using IOTA blockchain,'' in *Proc. IEEE 17th Int. Conf. Smart Communities, Improving Quality Life Using ICT, IoT AI (HONET)*, Dec. 2020, pp. 87–91.

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

[115] H. Farooq, A. Altaf, F. Iqbal, J. C. Galán, D. G. Aray, and I. Ashraf, ''DrunkChain: Blockchain-based IoT system for preventing drunk driving-related traffic accidents,'' *Sensors*, vol. 23, no. 12, p. 5388, Jun. 2023.

[116] I. Rodhe, C. Rohner, and E. C.-H. Ngai, ''On location privacy and quality of information in participatory sensing,'' in *Proc. 8h ACM Symp. QoS Secur. Wireless Mobile Netw.*, Oct. 2012, pp. 55–62.

[117] Q. Lyu, Y. Ishimaki, and H. Yamana, ''Privacy-preserving recommendation for location-based services,'' in *Proc. IEEE 4th Int. Conf. Big Data Analytics (ICBDA)*, Mar. 2019, pp. 98–105.

[118] G. Theodorakopoulos, E. Panaousis, K. Liang, and G. Loukas, ''On-the-fly privacy for location histograms,'' *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 566–578, Jan. 2020.

[119] G. Kaur and R. Gupta, ''A study on location based services and TTP based privacy preserving techniques,'' in *Proc. Int. Conf. Adv. Comput. Commun. (ICACC)*, Oct. 2021, pp. 1–5.

[120] K. Park, Y. Park, A. K. Das, S. Yu, J. Lee, and Y. Park, ''A dynamic privacy-preserving key management protocol for V2G in social Internet of Things,'' *IEEE Access*, vol. 7, pp. 76812–76832, 2019.

[121] C. Monroe, F. Tazi, and S. Das, ''Location data and COVID-19 contact tracing: How data privacy regulations and cell service providers work in tandem,'' 2021, *arXiv:2103.14155*.

[122] G. Theodorakopoulos, R. Shokri, C. Troncoso, J.-P. Hubaux, and J.-Y. L. Boudec, ''Prolonging the hide-and-seek game: Optimal trajectory privacy for location-based services,'' in *Proc. 13th Workshop Privacy Electron. Soc.*, Nov. 2014, pp. 73–82.

[123] W. Zhang, B. Jiang, M. Li, and X. Lin, ''Privacy-preserving aggregate mobility data release: An information-theoretic deep reinforcement learning approach,'' *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 849–864, 2022.

[124] M. Kim, Y. Park, and P. B. Dighe, ''Privacy-preservation using group signature for incentive mechanisms in mobile crowd sensing,'' *J. Inf. Process.*, vol. 15, no. 5, pp. 1036–1054, Oct. 2019.

[125] H. To and C. Shahabi, ''Location privacy in spatial crowdsourcing,'' in *Handbook of Mobile Data Privacy*. Cham, Switzerland: Springer, 2018.

[126] Z. Shao, H. Wang, Y. Zou, Z. Gao, and H. Lv, ''From centralized protection to distributed edge collaboration: A location difference-based privacy-preserving framework for mobile crowdsensing,'' *Secur. Commun. Netw.*, vol. 2021, pp. 1–18, Sep. 2021.

[127] L. Wang, D. Zhang, D. Yang, B. Y. Lim, X. Han, and X. Ma, ''Sparse mobile crowdsensing with differential and distortion location privacy,'' *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2735–2749, 2020.

[128] J. Bou Abdo, T. Bourgeau, J. Demerjian, and H. Chaouchi, ''Extended privacy in crowdsourced location-based services using mobile cloud computing,'' *Mobile Inf. Syst.*, vol. 2016, pp. 1–13, Jul. 2016.

[129] H. To, G. Ghinita, and C. Shahabi, ''A framework for protecting worker location privacy in spatial crowdsourcing,'' in *Proc. VLDB Endowment*, vol. 7, Jun. 2014, pp. 919–930.

[130] D. H. T. That, I. S. Popa, K. Zeitouni, and C. Borcea, ''PAMPAS: Privacy-aware mobile participatory sensing using secure probes,'' in *Proc. 28th Int. Conf. Sci. Stat. Database Manage.*, Jul. 2016, pp. 1–12.

[131] I. S. Popa, D. H. T. That, K. Zeitouni, and C. Borcea, ''Mobile participatory sensing with strong privacy guarantees using secure probes,'' *GeoInformatica*, vol. 25, pp. 533–580, Dec. 2019.

[132] I. Garitano, S. Fayyad, and J. Noll, ''Multi-metrics approach for security, privacy and dependability in embedded systems,'' *Wireless Pers. Commun.*, vol. 81, no. 4, pp. 1359–1376, Apr. 2015.

[133] A. S. Chauhan, A. Cuzzocrea, L. Fan, J. D. Harvey, C. K. Leung, A. G. M. Pazdor, and T. Wang, ''Predictive big data analytics for service requests: A framework,'' *Proc. Comput. Sci.*, vol. 198, pp. 102–111, Aug. 2022.

[134] M. Wang, H. Jiang, P. Zhao, J. Li, J. Liu, G. Min, and S. Dustdar, ''RoPriv: Road network-aware privacy-preserving framework in spatial crowdsourcing,'' *IEEE Trans. Mobile Comput.*, vol. 23, no. 3, pp. 2351–2366, Mar. 2023.

[135] R. Shokri, G. Theodorakopoulos, and C. Troncoso, "Privacy games along location traces: A game-theoretic framework for optimizing location privacy," *ACM Trans. Privacy Secur.*, vol. 19, no. 4, pp. 1–31, Feb. 2017.

[136] Q. Wang and K. Yang, "Privacy-preserving data fusion for traffic state estimation: A vertical federated learning approach," 2024, *arXiv:2401.11836*.

[137] L. Yan, H. Wang, Z. Wang, T. Wu, W. Fu, and X. Zhang, "Differentially private timestamps publishing in trajectory," *Electronics*, vol. 12, no. 2, p. 361, Jan. 2023.

[138] H. To, G. Ghinita, L. Fan, and C. Shahabi, "Differentially private location protection for worker datasets in spatial crowdsourcing," *IEEE Trans. Mobile Comput.*, vol. 16, no. 4, pp. 934–949, Apr. 2017.

[139] B. Li, H. Zhu, and M. Xie, "Releasing differentially private trajectories with optimized data utility," *Appl. Sci.*, vol. 12, no. 5, p. 2406, Feb. 2022.

[140] A. Héon, R. Sheatsley, Q. Burke, B. Hoak, E. Pauley, Y. Beugin, and P. McDaniel, "Systematic evaluation of geolocation privacy mechanisms," 2023, *arXiv:2309.06263*.

[141] L. Wang, D. Zhang, D. Yang, B. Y. Lim, and X. Ma, "Differential location privacy for sparse mobile crowdsensing," in *Proc. IEEE 16th Int. Conf. Data Mining (ICDM)*, Dec. 2016, pp. 1257–1262.

[142] Z. Chen, Y. Li, S. Zhang, J. Zhou, J. Zhou, C. Bao, and D. Yu, "A framework for cost-effective and self-adaptive LLM shaking and recovery mechanism," 2024, *arXiv:2403.07283*.

[143] M. A. P. Chamikara, P. Bertok, D. Liu, S. Camtepe, and I. Khalil, "Efficient privacy preservation of big data for accurate data mining," *Inf. Sci.*, vol. 527, pp. 420–443, Jul. 2020.

[144] A. Abadi, B. Doyle, F. Gini, K. Guinamard, S. K. Murakonda, J. Liddell, P. Mellor, S. J. Murdoch, M. Naseri, H. Page, G. Theodorakopoulos, and S. Weller, "Starlit: Privacy-preserving federated learning to enhance financial fraud detection," 2024, *arXiv:2401.10765*.

[145] X. Cheng, H. Yang, A. S. Krishnan, P. Schaumont, and Y. Yang, "KHOVID: Interoperable privacy preserving digital contact tracing," 2020, *arXiv:2012.09375*.

[146] S. Thakur and J. G. Breslin, "Rumour prevention in social networks with layer 2 blockchains," *Social Netw. Anal. Mining*, vol. 11, no. 1, p. 104, Dec. 2021.

[147] G. Tian, "The unique informational efficiency of the competitive mechanism in economies with production," *Social Choice Welfare*, vol. 26, no. 1, pp. 155–182, Jan. 2006.

[148] P. Ferraro, C. King, and R. Shorten, "Distributed ledger technology for smart cities, the sharing economy, and social compliance," *IEEE Access*, vol. 6, pp. 62728–62746, 2018.

[149] V. Bobinaite, M. Di Somma, G. Graditi, and I. Oleinikova, "The regulatory framework for market transparency in future power systems under the web-of-cells concept," *Energies*, vol. 12, no. 5, p. 880, Mar. 2019.

[150] E. Bao, D. Gao, X. Xiao, and Y. Li, "Communication efficient and differentially private logistic regression under the distributed setting," in *Proc. 29th ACM SIGKDD Conf. Knowl. Discovery Data Mining*, Aug. 2023, pp. 69–79.

[151] N. Wu, F. Farokhi, D. Smith, and M. A. Kaafar, "The value of collaboration in convex machine learning with differential privacy," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2020, pp. 304–317.

[152] A. Rezgui, A. Rouguettaya, and Z. Malik, "Enforcing privacy on the semantic web," *Inf. Secur. Ethics.*, vol. 2008, pp. 3713–3727, Jan. 2008.

[153] A. Rezgui, A. Bouguettaya, and M. Eltoweissy, "SemWebDL: A privacy-preserving semantic web infrastructure for digital libraries," *Int. J. Digit. Libraries*, vol. 4, no. 3, pp. 171–184, Nov. 2004.

[154] S.-E. Tbahriti, C. Ghedira, B. Medjahed, and M. Mrissa, "Privacy-enhanced web service composition," *IEEE Trans. Services Comput.*, vol. 7, no. 2, pp. 210–222, Apr. 2014.

[155] A. Rezgui, A. Bouguettaya, and Z. Malik, "A reputation-based approach to preserving privacy in web services," in *Proc. Int. Workshop. Technol. E-Services*, Jan. 2003, pp. 91–103.

[156] K. Mivule, "Data swapping for private information sharing of web search logs," *Proc. Comput. Sci.*, vol. 114, pp. 149–158, Jun. 2017.

[157] J. Castellá-Roca, A. Viejo, and J. Herrera-Joancomartí, "Preserving user's privacy in web search engines," *Comput. Commun.*, vol. 32, no. 14, pp. 1541–1551, 2009.

[158] K. Hawkey, "Privacy concerns for web logging data," in *Web Technologies: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Global, 2010.

[159] W. Ahmad and A. Khokhar, "An architecture for privacy preserving collaborative filtering on web portals," in *Proc. 3rd Int. Symp. Inf. Assurance Secur.*, Aug. 2007, pp. 273–278.

[160] M. Nauman, T. Ali, and A. Rauf, "Using trusted computing for privacy preserving keystroke-based authentication in smartphones," *Telecommun. Syst.*, vol. 52, no. 4, pp. 2149–2161, Apr. 2013.

[161] D. Sánchez, J. Castellà-Roca, and A. Viejo, "Knowledge-based scheme to create privacy-preserving but semantically-related queries for web search engines," *Inf. Sci.*, vol. 218, pp. 17–30, Jan. 2013.

[162] F. A. Aponte-Novoa, D. Povedano Álvarez, R. Villanueva-Polanco, A. L. S. Orozco, and L. J. G. Villalba, "On detecting cryptojacking on websites: Revisiting the use of classifiers," *Sensors*, vol. 22, no. 23, p. 9219, Nov. 2022.

[163] Y. Yang, X. Xiao, X. Cai, and W. Zhang, "A secure and privacy-preserving technique based on contrast-enhancement reversible data hiding and plaintext encryption for medical images," *IEEE Signal Process. Lett.*, vol. 27, pp. 256–260, 2020.

[164] Y.-B. Son, J.-H. Im, H.-Y. Kwon, S.-Y. Jeon, and M.-K. Lee, "Privacy-preserving peer-to-peer energy trading in blockchain-enabled smart grids using functional encryption," *Energies*, vol. 13, no. 6, p. 1321, Mar. 2020.

[165] H. Ren, G. Xu, H. Qi, and T. Zhang, "PriFR: Privacy-preserving large-scale file retrieval system via blockchain for encrypted cloud data," in *Proc. IEEE IEEE 9th Int. Conf. Big Data Secur. Cloud (BigDataSecurity) Int. Conf. High Perform. Smart Comput., (HPSC) IEEE Int. Conf. Intell. Data Secur. (IDS)*, May 2023, pp. 16–23.

[166] F. P. Calmon, M. Varia, and M. Médard, "On information-theoretic metrics for symmetric-key encryption and privacy," in *Proc. 52nd Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2014, pp. 889–894.

[167] Z. Liu, E. Tromer, and Y. Wang, "Group oblivious message retrieval," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, May 2022, pp. 753–783.

[168] J.-Y. Huang, W.-C. Hong, P.-S. Tsai, and I.-E. Liao, "A model for aggregation and filtering on encrypted XML streams in fog computing," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 5, May 2017, Art. no. 155014771770415.

[169] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Digital forensics vs. anti-digital forensics: Techniques, limitations and recommendations," 2021, *arXiv:2103.17028*.

[170] Z. Zali, E. Aslanian, M. H. Manshaei, M. R. Hashemi, and T. Turletti, "Peer-assisted information-centric network (PICN): A backward compatible solution," *IEEE Access*, vol. 5, pp. 25005–25020, 2017.

[171] K. Nguyen, J. Krumm, and C. Shahabi, "Spatial privacy pricing: The interplay between privacy, utility and price in geo-marketplaces," in *Proc. 28th Int. Conf. Adv. Geographic Inf. Syst.*, Nov. 2020, pp. 263–272.

[172] G. Rudin, "Walling off privacy: Apple's neuralhash controversy, the ecpa, the fourth amendment, and encryption," *Colo. Tech. LJ*, vol. 21, p. 337, Jul. 2023.

[173] S. A. Bhat, N.-F. Huang, I. B. Sofi, and M. Sultan, "Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability," *Agriculture*, vol. 12, no. 1, p. 40, Dec. 2021.

[174] R. Gupta and A. K. Singh, "Differential and access policy based privacy-preserving model in cloud environment," *J. Web Eng.*, vol. 21, no. 3, pp. 609–632, Feb. 2022.

[175] A. Viejo, J. Castellá-Roca, O. Bernado, and J. M. Mateo-Sanz, "Single-party private web search," in *Proc. 10th Annu. Int. Conf. Privacy, Secur. Trust*, Jul. 2012, pp. 1–8.

[176] M. A. Mustafa, S. Cleemput, A. Aly, and A. Abidin, "An MPC-based protocol for secure and privacy-preserving smart metering," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT-Europe)*, Sep. 2017, pp. 1–6.

[177] A. G. Putrada and M. Abdurohman, "Increasing the security of RFID-based classroom attendance system with Shamir secret share," *Int. J. Inf. Commun. Technol. (IJoICT)*, vol. 6, no. 1, pp. 10–22, Jun. 2020.

[178] I. Gupta, R. Gupta, A. K. Singh, and R. Buyya, "MLPAM: A machine learning and probabilistic analysis based model for preserving security and privacy in cloud environment," *IEEE Syst. J.*, vol. 15, no. 3, pp. 4248–4259, Sep. 2021.

[179] S. Barkataki and H. Zeineddine, "On achieving secure collaboration in supply chains," *Inf. Syst. Frontiers*, vol. 17, no. 3, pp. 691–705, Jun. 2015.

[180] S. Tripathy and S. K. Mohanty, "MAPPCN: Multi-hop anonymous and privacy-preserving payment channel network," in *Proc. Conf. Financial Cryptography Data Secur.* Cham, Switzerland: Springer, Jan. 2020, pp. 481–495.

[181] T. Mimoto, H. Yokoyama, T. Nakamura, T. Isohara, M. Hashimoto, R. Kojima, A. Hasegawa, and Y. Okuno, "Privacy-preserving correlation coefficient," *IEICE Trans. Inf. Syst.*, vol. E106.D, no. 5, pp. 868–876, 2023.

[182] S. Sakthivel and N. Vinotha, "An intellectual optimization of k-anonymity model for efficient privacy preservation in cloud platform," *J. Intell. Fuzzy Syst.*, vol. 45, no. 1, pp. 1497–1512, Jul. 2023.

[183] L. Yao, Z. Chen, H. Hu, G. Wu, and B. Wu, "Sensitive attribute privacy preservation of trajectory data publishing based on l-diversity," *Distrib. Parallel Databases*, vol. 39, no. 3, pp. 785–811, Sep. 2021.

[184] W. Ren, K. Ghazinour, and X. Lian, "KT-safety: Graph release via k-anonymity and t-closeness (technical report)," 2022, *arXiv:2210.17479*.

[185] O. Choudhury, A. Gkoulalas-Divanis, T. Salonidis, I. Sylla, Y. Park, G. Hsu, and A. Das, "Anonymizing data for privacy-preserving federated learning," 2020, *arXiv:2002.09096*.

[186] D. Le Quoc, M. Beck, P. Bhatotia, R. Chen, C. Fetzer, and T. Strufe, "Privacy preserving stream analytics: The marriage of randomized response and approximate computing," 2017, *arXiv:1701.05403*.

[187] C. Eyupoglu, M. A. Aydin, A. H. Zaim, and A. Sertbas, "An efficient big data anonymization algorithm based on chaos and perturbation techniques," *Entropy*, vol. 20, no. 5, p. 373, May 2018.

[188] C. Kocaoğullar, D. Hugenroth, M. Kleppmann, and A. R. Beresford, "Pudding: Private user discovery in anonymity networks," 2023, *arXiv:2311.10825*.

[189] K. S. Adewole and V. Torra, "DFTMicroagg: A dual-level anonymization algorithm for smart grid data," *Int. J. Inf. Secur.*, vol. 21, no. 6, pp. 1299–1321, Dec. 2022.

[190] A. Majeed, S. Khan, and S. O. Hwang, "Toward privacy preservation using clustering based anonymization: Recent advances and future research outlook," *IEEE Access*, vol. 10, pp. 53066–53097, 2022.

[191] A. Majeed, S. Khan, and S. O. Hwang, "Group privacy: An underrated but worth studying research problem in the era of artificial intelligence and big data," *Electronics*, vol. 11, no. 9, p. 1449, Apr. 2022.

[192] Y. Li, H. Song, Y. Zhao, N. Yao, and N. Wang, "Anonymous data reporting strategy with dynamic incentive mechanism for participatory sensing," *Secur. Commun.*, vol. 2021, pp. 1–20, Jun. 2021.

[193] S. Venkatasubramanian, "Measures of anonymity," in *Privacy-Preserving Data Mining*. New York, NY, USA: Springer, Jan. 2008, pp. 81–103.

[194] Z. Zhang, D. H. Yum, and M. Shin, "PARS: Privacy-aware reward system for mobile crowdsensing systems," *Sensors*, vol. 21, no. 21, p. 7045, Oct. 2021.

[195] M. Dehez-Clementi, J.-C. Deneuville, E. Lochin, and J. Lacan, "BEAT-traffic: A blockchain-enabled infrastructure for anonymous-yet-traceable traffic reporting," in *Proc. 53rd Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Jun. 2023, pp. 100–107.

[196] A. G. Putrada, M. Abdurohman, D. Perdana, and H. H. Nuha, "EdgeSL: Edge-computing architecture on smart lighting control with distilled KNN for optimum processing time," *IEEE Access*, vol. 11, pp. 64697–64712, 2023.

[197] U. Jayasinghe, G. M. Lee, Á. MacDermott, and W. S. Rhee, "TrustChain: A privacy preserving blockchain with edge computing," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–17, Jul. 2019.

[198] M. Djatmiko, D. Schatzmann, X. Dimitropoulos, A. Friedman, and R. Boreli, "Federated flow-based approach for privacy preserving connectivity tracking," in *Proc. 9th ACM Conf. Emerg. Netw. Exp. Technol.*, Dec. 2013, pp. 429–440.

[199] A. Fitwi, Y. Chen, and S. Zhu, "PriSE: Slenderized privacy-preserving surveillance as an edge service," in *Proc. IEEE 6th Int. Conf. Collaboration Internet Comput. (CIC)*, Dec. 2020, pp. 125–134.

[200] J. Feng, C. Rong, F. Sun, D. Guo, and Y. Li, "PMF: A privacy-preserving human mobility prediction framework via federated learning," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 4, no. 1, pp. 1–21, Mar. 2020.

[201] F. Wang, H. Zhu, R. Lu, Y. Zheng, and H. Li, "A privacy-preserving and non-interactive federated learning scheme for regression training with gradient descent," *Inf. Sci.*, vol. 552, pp. 183–200, Apr. 2021.

[202] K. Mandal and G. Gong, "PrivFL: Practical privacy-preserving federated regressions on high-dimensional data over mobile networks," in *Proc. ACM SIGSAC Conf. Cloud Comput. Secur. Workshop*, Nov. 2019, pp. 57–68.

[203] W. Wang, G. Yang, L. Bao, K. Ma, and H. Zhou, "A privacy-preserving crowd flow prediction framework based on federated learning during epidemics," *Secur. Commun. Netw.*, vol. 2022, pp. 1–20, Oct. 2022.

[204] S. Luo, Y. Xiao, X. Zhang, Y. Liu, W. Ding, and L. Song, "PerFedRec++: Enhancing personalized federated recommendation with self-supervised pre-training," 2023, *arXiv:2305.06622*.

[205] A. S. Alahmed, G. Cavraro, A. Bernstein, and L. Tong, "Operating-envelopes-aware decentralized welfare maximization for energy communities," in *Proc. 59th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2023, pp. 1–8.

[206] Z. Zhang, H. Wang, Z. Fan, J. Chen, X. Song, and R. Shibasaki, "GOF-TTE: Generative online federated learning framework for travel time estimation," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 24107–24121, Dec. 2022.

[207] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. S. Quek, and H. V. Poor, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3454–3469, 2020.

[208] O. Kotevska, J. Johnson, and A. G. Kusne, "Analyzing data privacy for edge systems," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Jun. 2022, pp. 223–228.

[209] A. N. Horvath, M. Berchier, F. Nooralahzadeh, A. Allam, and M. Krauthammer, "Exploratory analysis of federated learning methods with differential privacy on MIMIC-III," 2023, *arXiv:2302.04208*.

[210] A. Fitwi, Y. Chen, S. Zhu, E. Blasch, and G. Chen, "Privacy-preserving surveillance as an edge service based on lightweight video protection schemes using face de-identification and window masking," *Electronics*, vol. 10, no. 3, p. 236, Jan. 2021.

[211] J. Kamto, L. Qian, J. Fuller, J. Attia, and Y. Qian, "Key distribution and management for power aggregation and accountability in advance metering infrastructure," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2012, pp. 360–365.

[212] L. Jiang, Q. Song, R. Tan, and M. Li, "PriMask: Cascadable and collusion-resilient data masking for mobile cloud inference," in *Proc. 20th ACM Conf. Embedded Networked Sensor Syst.*, Nov. 2022, pp. 164–178.

[213] H. Wang, Y. Zhang, Z. Guo, T. Li, and L. Fan, "Format preserving encryption of sensitive data in database," *Proc. SPIE*, vol. 12718, pp. 206–212, Aug. 2023.

[214] Z. Hu, P. Shi, and L. Wu, "Preserving state and control privacies in networked systems with tokenized polytopic transforms," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 1, pp. 104–108, Jan. 2022.

[215] H. Kim, S.-H. Kim, J. Y. Hwang, and C. Seo, "Efficient privacy-preserving machine learning for blockchain network," *IEEE Access*, vol. 7, pp. 136481–136495, 2019.

[216] N. K. Tran and M. A. Babar, "Anatomy, concept, and design space of blockchain networks," in *Proc. IEEE Int. Conf. Softw. Archit. (ICSA)*, Mar. 2020, pp. 125–134.

[217] S. C.-K. Chau and Y. Zhou, "Blockchain-enabled decentralized privacy-preserving group purchasing for retail energy plans," in *Proc. 13th ACM Int. Conf. Future Energy Syst.*, Jun. 2022, pp. 172–187.

[218] I. Yilmaz, K. Kapoor, A. Siraj, and M. Abouyoussef, "Privacy protection of grid users data with blockchain and adversarial machine learning," in *Proc. ACM Workshop Secure Trustworthy Cyber-Phys. Syst.*, Apr. 2021, pp. 33–38.

[219] A. S. Yahaya, N. Javaid, S. Ullah, R. Khalid, M. U. Javed, R. U. Khan, Z. Wadud, and M. A. Khan, "A secure and efficient energy trading model using blockchain for a 5G-deployed smart community," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–27, Jan. 2022.

[220] M. O. Ahmad, G. Tripathi, F. Siddiqui, M. A. Alam, M. A. Ahad, M. M. Akhtar, and G. Casalino, "BAuth-ZKP—A blockchain-based multi-factor authentication mechanism for securing smart cities," *Sensors*, vol. 23, no. 5, p. 2757, Mar. 2023.

[221] M. Zahid, I. Ali, R. J. u. H. Khan, Z. Noshad, A. Javaid, and N. Javaid, "Blockchain based balancing of electricity demand and supply," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.*, Oct. 2020, pp. 185–198.

[222] J. Park and S. Chang, "Secure device control scheme with blockchain in a smart home," *Meas. Control*, vol. 56, nos. 3–4, pp. 546–557, Mar. 2023.

[223] R. Khan, A. Mehmood, Z. Iqbal, C. Maple, and G. Epiphaniou, "Security and privacy in connected vehicle cyber physical system using zero knowledge succinct non interactive argument of knowledge over blockchain," *Appl. Sci.*, vol. 13, no. 3, p. 1959, Feb. 2023.

[224] A. M. Almuhaideb and S. S. Algothami, "Efficient privacy-preserving and secure authentication for electric-vehicle-to-electric-vehicle-charging system based on ECQV," *J. Sensor Actuator Netw.*, vol. 11, no. 2, p. 28, Jun. 2022.

[225] S. Liu and Q. Zheng, ''A study of a blockchain-based judicial evidence preservation scheme,'' *Blockchain: Res. Appl.*, vol. 5, no. 2, Jun. 2024, Art. no. 100192.

[226] F. Kefeng, L. Fei, Y. Haiyang, and Y. Zhen, ''A blockchain-based flexible data auditing scheme for the cloud service,'' *Chin. J. Electron.*, vol. 30, no. 6, pp. 1159–1166, Nov. 2021.

[227] Y. Alabdulkarim, A. Alameer, M. Almukaynizi, and A. Almaslukh, ''SPIN: A blockchain-based framework for sharing COVID-19 pandemic information across nations,'' *Appl. Sci.*, vol. 11, no. 18, p. 8767, Sep. 2021.

[228] M. A. Cheema, R. I. Ansari, N. Ashraf, S. A. Hassan, H. K. Qureshi, A. K. Bashir, and C. Politis, ''Blockchain-based secure delivery of medical supplies using drones,'' *Comput. Netw.*, vol. 204, Feb. 2022, Art. no. 108706.

[229] A. Gibson and G. Thamilarasu, ''Protect your pacemaker: Blockchain based authentication and consented authorization for implanted medical devices,'' *Proc. Comput. Sci.*, vol. 171, pp. 847–856, Nov. 2020.

[230] S. Thakur and J. G. Breslin, ''Decentralized content vetting in social network with blockchain,'' in *Wireless Blockchain: Principles, Technologies and Applications*. Hoboken, NJ, USA: Wiley, Oct. 2021, pp. 269–296.

[231] R. Xu, S. Y. Nikouei, D. Nagothu, A. Fitwi, and Y. Chen, ''BlendSPS: A blockchain-enabled decentralized smart public safety system,'' *Smart Cities*, vol. 3, no. 3, pp. 928–951, Sep. 2020.

[232] M. Ul Hassan, M. H. Rehmani, and J. Chen, ''Differential privacy in blockchain technology: A futuristic approach,'' *J. Parallel Distrib. Comput.*, vol. 145, pp. 50–74, Nov. 2020.

[233] S. Gupta and M. Sadoghi, ''Blockchain transaction processing,'' 2021, *arXiv:2107.11592*.

[234] W. Abramson, W. J. Buchanan, S. Sayeed, N. Pitropakis, and O. Lo, ''PAN-DOMAIN: Privacy-preserving sharing and auditing of infection identifier matching,'' in *Proc. 4th Int. Conf. Secur. Inf. Netw. (SIN)*, Jan. 2021, pp. 1–8.

[235] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, ''A survey on privacy-preserving authentication schemes in VANETs: Attacks, challenges and open issues,'' *IEEE Access*, vol. 9, pp. 153701–153726, 2021.

[236] A. Hayat, Z. Iftikhar, M. I. Khan, A. Mehbodniya, J. L. Webber, and S. Hanif, ''A novel pseudonym changing scheme for location privacy preservation in sparse traffic areas,'' *IEEE Access*, vol. 11, pp. 89974–89985, 2023.

[237] I. Agudo, M. Montenegro-Gómez, and J. Lopez, ''A blockchain approach for decentralized V2X (D-V2X),'' *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4001–4010, May 2021.

[238] A. Sangwan, A. Sangwan, and R. P. Singh, ''A classification of misbehavior detection schemes for VANETs: A survey,'' *Wireless Pers. Commun.*, vol. 129, no. 1, pp. 285–322, Mar. 2023.

[239] R. Kundu, ''Cryptographic hash functions and attacks—A detailed study,'' *Int. J. Adv. Res. Comput. Sci.*, vol. 11, no. 2, pp. 37–44, Apr. 2020.

[240] H. Takahashi, S. Nakano, and U. Lakhani, ''SHA256d hash rate enhancement by L3 cache,'' in *Proc. IEEE 7th Global Conf. Consum. Electron. (GCCE)*, Oct. 2018, pp. 849–850.

[241] C. Freitag, A. Ghoshal, and I. Komargodski, ''Optimal security for keyed hash functions: Avoiding time-space tradeoffs for finding collisions,'' in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, Jan. 2023, pp. 440–469.

[242] A. Pillai, V. Saraswat, and A. V. Ramachandran, ''Attacks on blockchain based digital identity,'' in *Proc. Int. Congr. Blockchain Appl.* Cham, Switzerland: Springer, 2022, pp. 329–338.

[243] R. Ratra, P. Gulia, and N. S. Gill, ''Performance analysis of perturbation-based privacy preserving techniques: An experimental perspective,'' *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 13, no. 5, p. 5273, Oct. 2023.

[244] G. Wang, X. Huang, Y. Li, F. Zuo, and X. He, ''A multi-blockchain based reliable noise adding method for privacy preservation in cyber-physical systems,'' in *Proc. Int. Conf. Image, Vis. Intell. Syst.* Cham, Switzerland: Springer, Jan. 2023, pp. 811–820.

[245] X. Li, Y. Cao, and M. Yoshikawa, ''Locally private streaming data release with shuffling and subsampling,'' in *Proc. IEEE 39th Int. Conf. Data Eng. Workshops (ICDEW)*, Apr. 2023, pp. 125–131.

[246] B. Ma, X. Lin, X. Wang, B. Liu, Y. He, W. Ni, and R. P. Liu, ''New cloaking region obfuscation for road network-indistinguishability and location privacy,'' in *Proc. 25th Int. Symp. Res. Attacks, Intrusions Defenses*, Oct. 2022, pp. 160–170.

[247] M. Humbert, E. Ayday, J.-P. Hubaux, and A. Telenti, ''Addressing the concerns of the lacks family: Quantification of kin genomic privacy,'' in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. - CCS*, 2013, pp. 1141–1152.

[248] S. Xie, Y. Wu, J. Li, M. Ding, and K. B. Letaief, ''Privacy for fairness: Information obfuscation for fair representation learning with local differential privacy,'' 2024, *arXiv:2402.10473*.

[249] T.-T. Kuo, J. Kim, and R. A. Gabriel, ''Privacy-preserving model learning on a blockchain network-of-networks,'' *J. Amer. Med. Inform. Assoc.*, vol. 27, no. 3, pp. 343–354, Mar. 2020.

[250] T. Nóbrega, C. E. S. Pires, and D. C. Nascimento, ''Blockchain-based privacy-preserving record linkage: Enhancing data privacy in an untrusted environment,'' *Inf. Syst.*, vol. 102, Dec. 2021, Art. no. 101826.

[251] 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.

[252] M. Byali, H. Chaudhari, A. Patra, and A. Suresh, ''FLASH: Fast and robust framework for privacy-preserving machine learning,'' *Privacy Enhancing Technol.*, vol. 2020, no. 2, pp. 459–480, Apr. 2020.

[253] W. R. Clark, L. A. Clark, D. M. Raffo, and R. I. Williams, ''Extending Fisch and Block's (2018) tips for a systematic review in management and business literature,'' *Manage. Rev. Quart.*, vol. 71, no. 1, pp. 215–231, 2021, doi: 10.1007/s11301-020-00184-8.

SIDIK PRABOWO (Student Member, IEEE) received the bachelor's and master's degrees in informatics engineering from Telkom University, Bandung, in 2011 and 2014, respectively, where he is currently pursuing the Ph.D. degree. He became a Lecturer with Telkom University. He is an Assistant Professor. He taught various courses, such as *Computer Networks*, *Internet of Things*, and *Cloud Computing*. Since 2013, he has been involved in multiple research grants from the government. His dissertation concerns the security framework for the Internet of Things in Indonesia.

AJI GAUTAMA PUTRADA (Member, IEEE) received the bachelor's degree in electrical engineering and the master's in microelectronics from ITB, in 2003 and 2009, respectively. He is currently pursuing the Ph.D. degree in computer science with the Doctoral Program, Telkom University. He was the Research and Development Director of PT. Cetta Nusantara Technology, where he developed low-level broadband wireless access (BWA) solutions, such as WiMAX and LTE. He became a Lecturer with Telkom University, Bandung, where he is an Assistant Professor. He taught various courses, such as computer architecture, microcontroller systems, and operating systems. Since 2015, he has been involved in multiple research grants from the government on smart lighting. From 2020 to 2022, he was entrusted to become the Vice Director of the Advanced and Creative Networks Research Center (AdCNet RC), Telkom University. His dissertation topic concerns user comfort in smart lighting with machine learning.

IKKE DIAN OKTAVIANI (Graduate Student Member, IEEE) was born in Cirebon, in October 1995. She received the bachelor's and master's degrees in informatics from Telkom University, Bandung, Indonesia, in 2016 and 2020, respectively, where she is currently pursuing the Ph.D. degree. She became a Lecturer in technology information with Telkom University. Her research interest includes data imputation in the Internet of Things data.

MAMAN ABDUROHMAN (Member, IEEE) received the master's and Ph.D. degrees from ITB, in 2004 and 2010, respectively. He is currently a Professor of information technology with Telkom University (formerly STT Telkom), where he has been a full-time Lecturer and a Researcher, since 2000. Previously, he was the Director of Bandung Techno Park (BTP), Telkom University, focusing on research commercialization and business incubation. In the last three years, he has received institutional and national research grants from Telkom University and the Ministry of Higher Education Board. He has authored more than 60 articles published in international and national journals, such as *International Journal of Electrical Engineering and Informatics* and *International Journal of Informational and Education Technology*, and conferences, such as the International Conference of ICT and the International Conference on Computer Engineering and Technology. His current research interests include the IoT, smart card technology, and smart lighting.

MARIJN JANSSEN is currently a Full Professor of ICT and governance with the Section of Information and Communication Technology, Faculty of Technology, Policy and Management, Delft University of Technology. He has published more than 600 refereed publications, and his Google H-score is 85, having more than 27K citations. He was nominated in 2018 and 2019 by Apolitical as one of the 100 most influential people in the Digital Government worldwide. He is the Co-Editor-in-Chief of the Government Information Quarterly and an Associate Editor of the Decision Support Systems and Information Systems Frontiers.

HILAL HUDAN NUHA (Senior Member, IEEE) received the bachelor's degree in telecommunication engineering from the Telkom Institute of Technology (IT Telkom), Bandung, Indonesia, in 2009, the master's degree in informatics from Telkom University, Bandung, in 2011, and the Ph.D. degree from the King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, in 2019. In 2019, he was trusted as the Chair of the Telematics Research Group, Telkom University. He is currently an Associate Professor with Telkom University and the Head of the Communication and Information Technology Infrastructure Research Group. His research interests include machine learning for networked sensors and information theory.

SARWONO SUTIKNO (Member, IEEE) received the bachelor's degree in electronics from Bandung Institute of Technology, Bandung, Indonesia, in 1984, and the M.E. and Dr.Eng. degrees in integrated systems from Tokyo Institute of Technology, Tokyo, Japan, in 1990 and 1994, respectively. His security engineering focus includes information security management systems. He holds several professional certifications, including Indonesia Internal Auditor Professional (IIAP) from IIA, Certified in Cybersecurity (CC) from (ISC)2, ISMS Provisional Auditor Certificate, CISA, CISSP, CISM, and CSX-F. He is also appointed as an ISACA Academic Advocate. His research interests include implementing cryptographic algorithms in integrated circuits and hardware security, including embedded system security.