# Characterization and Quantification of User Privacy: Key Challenges, Regulations, and Future Directions

Razi Arshad and Muhammad Rizwan Asghar

***Abstract*—The protection of user privacy in the digital age has become an important concern with the increase in data-driven technologies. These technologies generate large amounts of user data that provide opportunities for organisations to improve the quality of their user services. The publication of user-generated data creates risks for exposing an individual's privacy. In the literature, identity theft and attribute disclosure are the two most common attacks on user-generated data. These privacy issues require data publishing organisations to protect user privacy. International regulatory standards provide consistent frameworks and guidelines that data publishing organisations can use to secure user-sensitive data. This survey discusses the characterisation and quantification of user privacy in compliance with international regulatory standards. We provide an overview of existing regulations and frameworks related to user privacy, highlighting their strengths, limitations, and implications for individuals and businesses. We discuss the steps involved in characterising and quantifying user privacy within the framework of international regulatory standards, privacy tools, and real-world case studies. Furthermore, we share promising directions for future research and development, including advancements in privacy techniques, interdisciplinary collaborations, and the role of emerging technologies. By addressing these challenges and creating a way forward, this work aims to contribute to the ongoing research on user privacy and promote the development of effective strategies for safeguarding user personal data in an increasingly interconnected world.**

***Index Terms*—Privacy-preserving techniques, privacy-enhancing techniques, trust models, privacy measures, privacy quantification, privacy loss.**

## I. Introduction

IN 1890, Warren and Brandeis [1] introduced the notation of modern privacy while in computing, the right to privacy became a matter of debate since the 1960s [2]. In 1995, the European Council passed legislation for data protection that allows for the processing of user personal data among member states [3]. Over time, the volume of user data gathered and exchanged reached incredible levels, making information easier to access and utilise [4]. By 2025, the United States (US) International Data Corporation (IDC) predicts that the total amount of user data generated globally will reach as high as 163 zettabytes, (ZB) [5]. The user data contains records of information about users or entities that are necessary for tasks requiring analysis and mining in data-driven projects [6]. In addition, user data is essential for research and strategy development as it allows the extraction of deep and insightful knowledge from various sources. However, despite the enormous benefits of user data sharing, the confidentiality of user data has been under persistent threat due to the unprecedented amount of user data reuse and analysis [7], [8], [9].

User privacy raised several legal issues both regional and global level, highlighting the individuals' concerns about how organisations manage and use their sensitive data and private information. In 2014, the White House discussed the challenges faced by businesses in protecting user privacy in its study on big data and its impact on privacy. To standardise data privacy regulations throughout Europe, the General Data Protection Regulation (GDPR) was proposed in 2017 [10]. Following GDPR, several privacy legislation [11], [12], [13] have been proposed to protect the user privacy; for instance, the California Consumer Privacy Act of 2018 (CCPA) [12] and the General Personal Data Protection Law (GPDPL) [13] are used to protect the privacy of California and Brazilian citizens respectively. These laws generally require that organisations set up the proper organisational and technical protections to ensure that user data is handled under these rules and regulations.

A person to whom data relates is known as a *data subject*. The bodies that decide when and how user data is processed are known as *data controllers*. Some entities that manage user data on behalf of data controllers are called *data processors*. To illustrate the difference between data subject, data controller, and data processor in GDPR, let us assume that Alice is a European Union (EU) resident who uses an online shopping website to purchase clothes. In this scenario, Alice is a data subject because her data, such as name, address, and payment information, is being collected by the online shopping website "FashionStore". Here, "FashionStore" is the data controller because it determines the purposes and means of processing Alice's data. More specifically, FashionStore decides why and how her data is collected, stored, and used, say to process her orders, manage her account, and send promotional offers. FashionStore decided to use a third-party payment processing service called "SecurePayment Ltd." to handle the financial transactions. In this case, SecurePayment Ltd. becomes the data processor. They process Alice's payment information on behalf of FashionStore, following Fashionstore's instructions and ensuring compliance with GDPR. SecurePayment Ltd. does not independently determine how Alice's data will be used; they act on behalf of and under the authority of Fashionstore.

Received 13 February 2024; revised 20 July 2024, 9 September 2024, and 16 October 2024; accepted 14 December 2024. Date of publication 18 December 2024; date of current version 20 October 2025. *(Corresponding author: Muhammad Rizwan Asghar.)*

The authors are with the Surrey Centre for Cyber Security, University of Surrey, GU2 7XH Guildford, U.K. (e-mail: r.arshad@surrey.ac.uk; r.asghar@surrey.ac.uk).

Digital Object Identifier 10.1109/COMST.2024.3519861

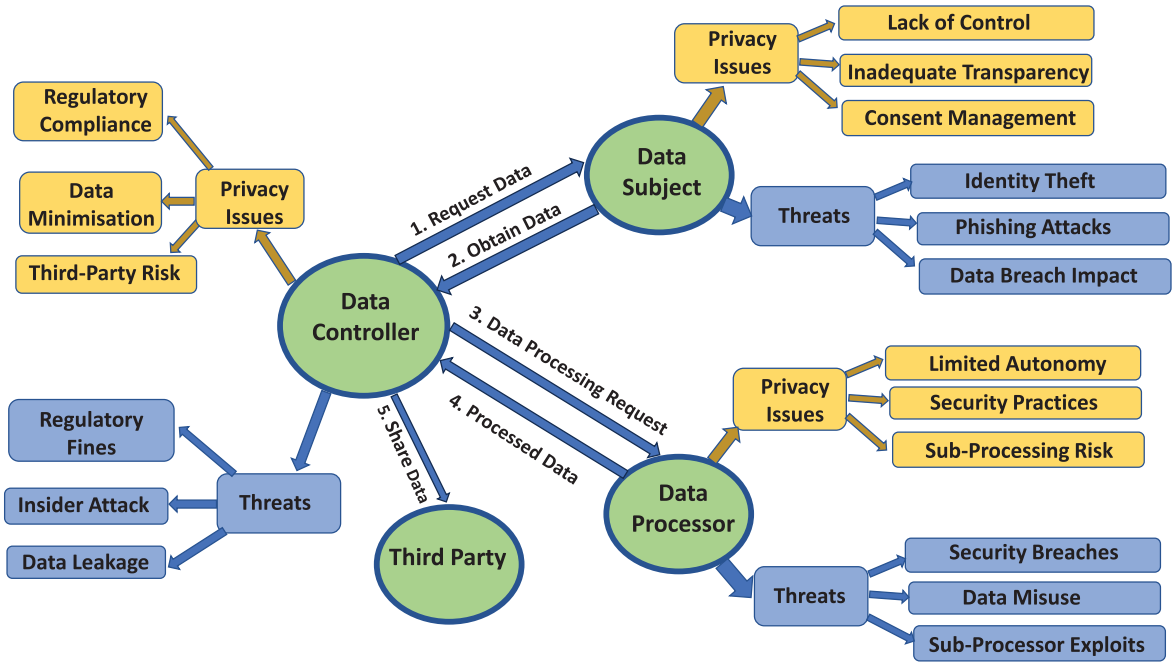


Fig. 1. The system model for user privacy in terms of data subjects, data controllers, and data processors along with potential privacy issues and threats.

Developing a comprehensive system model for user privacy that considers the responsibilities of data subjects, data processors, and data controllers is necessary for managing data flows, assigning responsibilities, and identifying potential privacy threats. Fig. 1 illustrates the comprehensive model for user privacy in terms of data subjects, data controllers, and data processors. To ensure privacy throughout data storage, sharing, and disposal, this model provides a flow in which the data controller obtains data from the data subjects, processes it through the data processor, and may share it with third parties. Several privacy issues arise when data owners lack control, transparency, and effective consent mechanisms, while data controllers face challenges in maintaining regulatory compliance, minimising data collection, and managing third party risks. Data processors, limited by their role, may suffer from limited autonomy, weak security practices, and risks associated with sub-processing. Certain threats are associated with data subjects, data controllers, and data processors. The most common threats include: identity theft, phishing, and breach impacts for data owners; regulatory fines, reputation damage, insider threats, and data leakage for data controllers; and security breaches, data misuse, and vulnerabilities in sub-processors for data processors. Addressing these issues within the user privacy model is important for protecting user privacy across all stages of data handling.

The data controller and data processor must preserve confidentiality, notify individuals in the case of a data breach, and carry out risk assessments. Data subjects have rights to their data, such as viewing and erasing it. Preventing any unauthorised disclosure of user data is the main goal of data confidentiality. This can be achieved by restricting authorised entities' access or user data de-identification. It means a particular person's information in a record or dataset is altered or deleted. The de-identification process reduces the amount

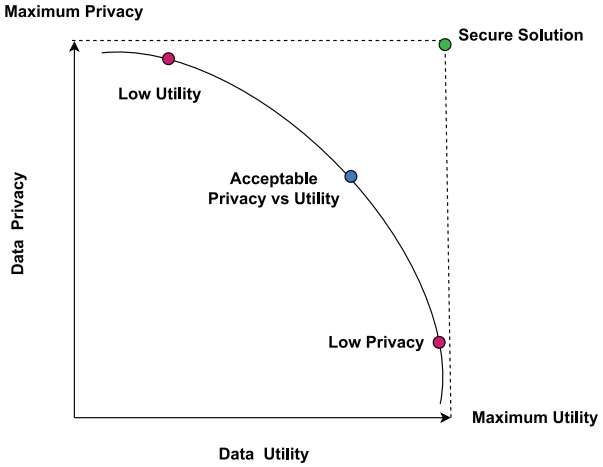


Fig. 2. Trade-off between privacy level and data utility.

of information and data detail, which usually results in losses in data interpretation and/or predictive performance [14], [15]. A trade-off between privacy and predictive accuracy can be observed in Machine Learning (ML) tasks (*i.e.,* knowledge extraction by pattern-finding algorithms) [16].

It is important to design privacy techniques which can maximise user privacy protection without minimising predictive performance but it is still a challenging issue as illustrated in Fig. 2. We observe that low-quality data with a high level of privacy level limits the effectiveness of knowledge extraction and result interpretation [14]. On the other hand, an inadequate level of privacy could lead to inverse data transformation that results in user information leakage. Privacy techniques play an important role in maintaining user privacy during communication of user-sensitive information. There are two types of

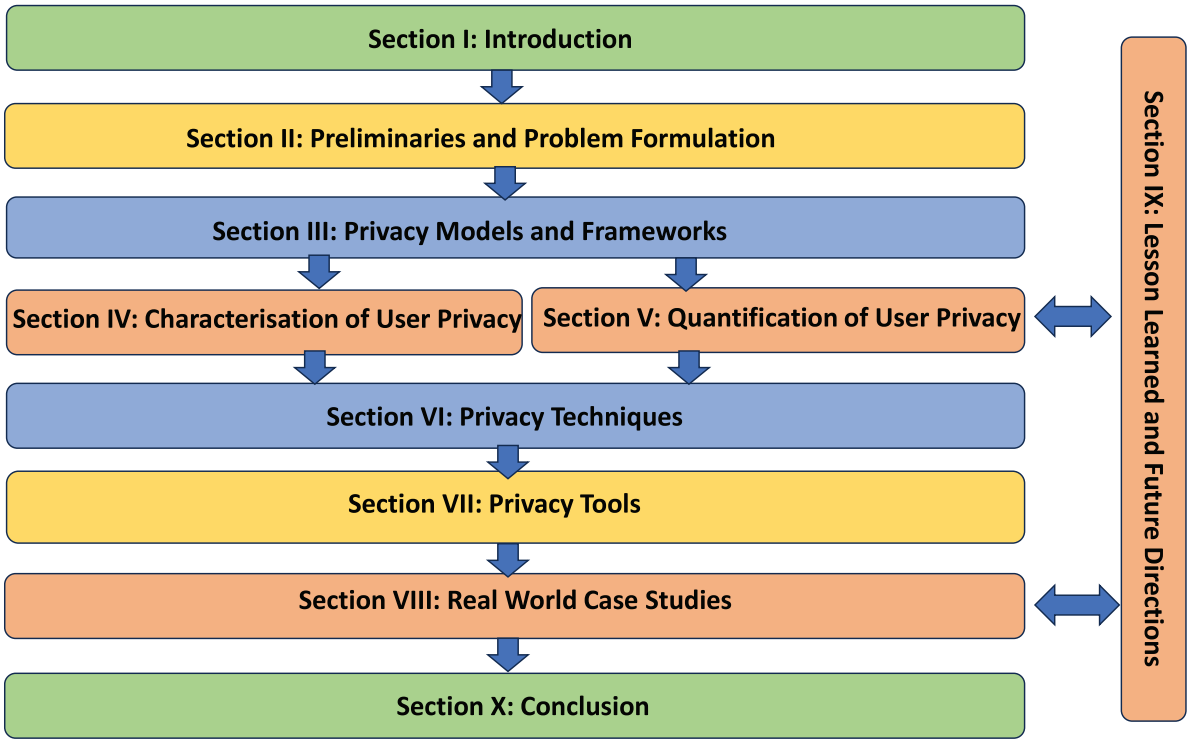


Fig. 3. Layout and structure of the survey.

privacy techniques: privacy-preserving techniques and privacy-enhancing techniques as discussed in Section VII. Despite the importance of privacy techniques, their effectiveness in terms of implementation by international standards has not recently been reviewed or discussed.

In this survey, we characterise and quantify user privacy using privacy techniques in compliance with international security standards including ISO/IEC (International Organisation for Standardisation/International Electrotechnical Commission) [17], IEEE (Institute of Electrical and Electronics Engineers) [18], and NIST (National Institute of Standards and Technology) [19]. We have noticed that the most recent surveys cover only well-known privacy techniques, and measure privacy risk for specific types of disclosure, such as identity disclosure [20], [21], [22], [23], but they did not discuss the compliance of privacy techniques by international security standards. Our survey uses previous works [24], [25], [26] by discussing privacy techniques in compliance with international security standards. Then, we thoroughly discuss the characterisation and quantification of user privacy. Finally, we provide a comprehensive analysis of privacy techniques in providing privacy protection along with the main conclusions of existing privacy studies. The significant contributions of this work can be summarised as follows.

- We present a general privacy taxonomy, models, and frameworks.
- We provide the characterisation and quantification of user privacy risks.
- We propose a mapping of privacy techniques to international security standards.
- We discuss the well-known use cases for privacy techniques in real-world scenarios.
- We share challenges, current solutions, and future directions.

A list of acronyms that are used throughout our survey paper is presented in Table X.

The rest of the article is organised as follows. Section II gives some background and context about user privacy. Section III reviews related survey articles. Section IV identifies privacy issues, requirements and defines three main trust models. Section V gives a characterisation of user privacy risks and discusses the concept of data sensitivity and its implication for privacy. The quantitative methods for measuring and assessing user privacy that include different privacy metrics and tools are covered in Section VI. Section VII introduces and reviews privacy techniques. Section VIII provides a detailed comparison of privacy challenges in various domains such as healthcare, finance, social media, and the Internet of Things (IoT). Section IX explains well-known privacy tools. Open research challenges and future directions are given in Section X. Section XI concludes this work. The layout of this survey is presented in Fig. 3.

## II. Preliminaries and Problem Formulation

Inference control is a set of principles that aim to provide statistically transformed data to the public while preserving the privacy of user data. In the data de-identification process, the user's unique identifiers are removed from the data by applying privacy techniques such that it is a very challenging task for an attacker to obtain the user-sensitive

information and still have valuable data for future analysis [38], [39], [40], [41].

To decide which privacy technique is useful for data protection and prevention of potential attacks, it is necessary to differentiate among different formats in which one can store user data. Each data storage format presents a different challenge. The most popular data formats are tabular data, microdata, and query-based databases [42]. Tabular data is an aggregated set of information, which can contain numbers or values about particular user groups. Microdata is a collection of records that are unique to a particular user or thing. Finally, iterative databases, also known as query-based databases, allow users to run statistical queries including sums, averages, max, and min. It is noted that the building blocks for query-based databases and tabular data are microdata sets. Moreover, microdata disclosure risk is typically thought to be higher than tabular data risk.

We consider an example of an electronic voting system [43] to explain the concept of these data formats in more detail. In electronic voting systems, tabular data, microdata, and query-based databases are used to manage voter information and ensure election security. Tabular data organises voter details and election results in tables that make it easier to access and update. Microdata includes detailed individual voter information, such as voting history and demographics. This information requires strong privacy protections to keep voter identities safe. Query-based databases allow authorised users to retrieve specific information through complex queries without exposing the entire dataset. A technique like Differential Privacy (DP) is used to prevent revealing individual voter details. These data types help to maintain the integrity and privacy in the voting process.

Several researchers [23], [44], [45] have investigated the basics of tabular data security. Willenborg and De Waal [23] provided a wide range of tabular data types and included several disclosure-prevention techniques in addition to privacy and information loss protections. Duncan et al. [45] focused only on tabular data and discussed different techniques for limiting the disclosure from a broad viewpoint. Several other researchers [46], [47] have presented comparative studies on the protection of query-based databases. In this survey, we classify the user data based on the following attributes:

- *Identifiers (IDs):* IDs are the attributes that directly identify an individual, such as name and social security number.
- *Quasi-Identifiers (QIDs):* QIDs are individual attributes, such as date of birth, gender, place of residence, occupation, and ethnic group that when combined to a certain extent generate unique IDs that could result in re-identification.
- *Sensitive:* This attribute is usually protected by laws and regulations that uniquely identify individual important characteristics, such as political stance, religion, and illness.
- *Non-sensitive:* All other individual attributes are expected to carry no personal information at all.

Nowadays, identity theft is one of the major privacy problems with user data [7], [48]. An attacker or adversary may guess data subject information from the de-identified datasets. For instance, assume that a hospital releases a de-identified dataset containing information about patients' medical conditions, treatments, and demographics. Even though the dataset does not contain explicit identifiers such as names and social security numbers, an attacker with access to external datasets or additional knowledge could potentially infer new information about individual patients. Assuming the attacker knows that a particular individual was hospitalised for a rare condition in a specific period and then accesses the de-identified dataset, she might be able to correlate certain patterns or combinations of medical procedures, medications, and demographics to identify that individual within the dataset. This could lead to privacy breaches and expose sensitive information about the patient's health without their consent.

Several studies show the possibility of linking personal data to a person [7], [48], [49], [50]. It was discovered in a study by Sweeney [51] that 87% of Americans can probably be identified by using just the set of QIDs (5-digit ZIP, gender, and date of birth). This study inspired researchers to investigate re-identification attacks [52] and develop new data protection methods to reduce disclosure risk [53]. The implementation of robust privacy techniques in compliance with international security standards requires an impact assessment of these techniques on user data privacy and utility. The implementation of privacy techniques must guarantee user data protection level without its usefulness.

**Summary.** Recent advancements in modern technology have completely changed how user data is gathered, processed, and utilised. The goal of privacy techniques is to process and transform user data. It might not be sufficient to prevent attackers from linking personal information to a specific person or from singling out particular individuals who have similar data if privacy techniques are not implemented following international security standards. This happens due to the gap between academic research, which is focused on theoretical advancements in the privacy-related domain and industry that is looking at the practical implementation of privacy measures.

In this survey, we bridge the gap between academics and industry by performing characterisation and quantification of user privacy risks. This survey provides the industry with actionable insights to effectively comply with international standards while enhancing user privacy in real-world applications. The implementation of international standards for privacy techniques creates a balance between technological adoption and the safeguarding of individual privacy [54].

## III. Review of Related Survey Articles

Our survey article on the characterisation and quantification of user privacy differs from all previous studies, as we widely cover the area of user privacy in the context of international security standards. There is a comprehensive literature of survey articles focusing on user privacy in different domains such as cyber security systems and blockchain. However, to the best of our knowledge, no survey article thoroughly addresses the characterisation and quantification of user privacy in the

TABLE I
DETAILED COMPARISON OF PREVIOUS SURVEYS ON PRIVACY, (✔) DENOTES THAT THE TOPIC IS COVERED, (✱) SUGGESTS THAT THE TOPIC IS PARTIALLY COVERED, AND (✘) REPRESENTS THAT THE TOPIC IS NOT COVERED

| Surveys | Year | Application | Key Contribution | Privacy Related Factors | International Standards Mapping |
|---|---|---|---|---|---|
| Toch *et al.* [27] | 2018 | Cybersecurity systems | A comprehensive survey on the cybersecurity technologies with privacy invasion analysis | Data Exposure, User identification, Data sensitivity, User control | ✘ |
| Zhang, Xue and Li [28] | 2019 | Blockchain | A detailed survey on security and privacy on blockchain | Online Transaction, Consensus Algorithms, Hash Chained Storage, Anonymous Signatures, Noninteractive Zero Knowledge Proof | ✘ |
| Humbert, Trubert, and Huguenin [29] | 2019 | Interdependent Privacy | A comprehensive survey on interdependent privacy risks and interconnected solutions | Cooperative Solution, Non-cooperative solution, Demographics, Genomics, Location, Aggregate Data | ✘ |
| Royal Society [26] | 2019 | Protecting privacy in practice | A high-level overview of five current and promising Privacy Enhancing Technologies | Privacy Enhancing Technologies | ✱ |
| Hassan, Rehmani, and Chen [30] | 2020 | Cyber-Physical Systems | An in-depth survey on DP techniques for cyber-physical systems | Privacy preservation, Privacy attacks, Design Mechanism, Technical Challenges | ✘ |
| Beigi and Liu [31] | 2020 | Social Media | A review of key achievements in protecting user privacy on social media | Identity Attack, Attribute Disclosure Attacks, Vulnerabilities and Mitigation Strategies | ✘ |
| Liu *et al.* [32] | 2020 | Online Social Networks | A thorough analysis of image privacy in online social networks | User-centric Framework, Intelligent Privacy Protection Mechanism | ✘ |
| Due, Such, and Suarez-Tangil [33] | 2020 | Smart home personal assistants | A comprehensive review of smart home personal assistant's security issues, attack vectors and countermeasures | Identity Theft, Cyberstalking, Information Leakage | ✘ |
| Pattnaik, Li, and Nurse [34] | 2023 | home networking environment | A user perspectives survey on security and privacy in a home networking environment | Multiple Home Users, Complicated Data Flow, Security and Privacy | ✘ |
| Royal Society [26] | 2023 | From privacy to partnership | A detailed report on the role of Privacy Enhancing Technologies in data governance and collaborative analysis | Privacy Enhancing Technologies | ✱ |
| Rigaki, and Garcia [35] | 2023 | Machine Learning | A survey of privacy attacks in machine learning | Attack Taxonomy, Threat Model, User Privacy Leakage | ✘ |
| Rodrigues, Villela, and Feitosa [36] | 2024 | Social Networks Privacy | A systematic mapping of social network privacy Threats and their solutions | Identity Theft, Cyberstalking, Information Leakage | ✘ |
| Zhang *et al.* [37] | 2024 | Privacy assistance Tool | A first privacy-preserving framework for LLM | Homomorphic Encryption, Computational Security, Shuffling-based Solution | ✘ |
| This Work | 2024 | User Privacy | A detailed survey on characterisation and quantification of user privacy in compliance with international regulatory standards | Privacy Risk, Privacy Threats, Privacy Metric, Privacy Attacks, International Regulatory Standards | ✔ |

context of international security standards. We categorise the previous survey work on user privacy into several categories such as cyber security systems and blockchain. The timeline, applications, key contributions, privacy-related factors, and mapping to international security standards of these survey articles are presented in Table I.

Cyber security systems are used to protect networks and computers against cyber attacks. Toch et al. [27] discussed both common and novel cyber security technologies with privacy analysis. They proposed a taxonomy for privacy risk assessment based on data exposure, user identification, data sensitivity, and user control. To process user financial information in an open environment, blockchain offers an innovative approach to storing user-sensitive information, executing transactions, performing functions, and establishing trust among users. Zhang et al. [28] analysed the blockchain security and user privacy that is crucial for its deployment in various applications including cryptocurrency systems and smart contracts. In energy systems, transportation, and healthcare applications, DP techniques for cyber-physical systems have been considered by Hassan et al. [30]. They provided research directions for enhancing user data privacy in cyber-physical systems to guide the development of modern DP solutions. The individuals' privacy not only depends on their actions and data but may also be affected by the privacy decisions and data sharing by other individuals. The interdependent privacy risks and associated solutions are discussed in [29].

The widespread use of social media has attracted several people to participate in numerous activities daily. Beigi and Liu [31] review key achievements in protecting user privacy on social media with a main focus on vulnerabilities and mitigation strategies against identity and attribute disclosure

attacks. The sharing of images on online social networks has become an important part of our everyday social interactions leading to the possibility of privacy breaches. Online images can disclose sensitive information, which makes people reconsider their priorities for personal privacy while posting images on social media. The privacy risks of sharing images on online social networks by highlighting the inadequacy of current privacy management solutions were discussed by Liu et al. [32]. They proposed a user-centric framework for intelligent privacy protection throughout the image-sharing process. The privacy threats in online social networks, such as identity theft and cyberstalking, are examined by Rodrigues et al. [36]. They provide insights into specific privacy threats and existing prevention methods that serve as a guide for future research and solutions in online social networks.

A new technology called smart home personal assistants is transforming the way home users interact with technology but there are certain security and privacy risks due to the voice channel, architecture complexity, AI features, and diverse underlying technologies. Edu et al. [33] provide a comprehensive review of smart home personal assistant's security issues, categorise attack vectors and countermeasures, and highlight the need for broader research beyond user-device interaction. Later, Pattnaik et al. [34] identify key areas for further research that include holistic methods for diverse devices, multi-user interactions, complex data flows, demographic factors, and advanced conceptual frameworks. Although location-based services make ubiquitous computing such as smart home personal assistants more convenient and useful, they also create new security gaps that could be used to violate user privacy. Jiang et al. [55] categorised and reviewed existing privacy-preserving techniques in location-based services and discussed new research opportunities to address emerging challenges in the field.

The Royal Society [26] has published a report on privacy-enhancing technologies that can help to maximise data usage by reducing its inherent risks. It provides a high-level summary of five promising and active privacy-enhancing technologies from various industries along with information on each one's readiness level and relevant case studies. Later, the Royal Society published another report [26] that examines how privacy-enhancing technologies might transform the secure and efficient use of sensitive data for wider public benefit. It takes into account how these technologies could be used to address data governance problems other than privacy. Large data sets and technological advancements have contributed to the rapid development of ML in both academic research and practical applications. At the same time, there is an increasing emphasis on how ML impacts user security, privacy, and fairness. Typically, online services collect our personal information, which is then used to train ML models that are later used by ML applications. It is unclear how these models disclose details about the training data. Rigaki and Garcia [35] analysed privacy attacks against ML and proposed an attack taxonomy and threat model that causes user privacy leakage.

The rapid development in Large Language Model (LLM) technology that is built on ML models has prompted a lot of study and practical applications, especially when it comes to the integration of LLMs with auxiliary tools, or tools using LLM agents. However, there are major privacy risks in the communication of sensitive information among LLMs and tools. Zhang et al. [37] have introduced PrivacyAsst, which is the first privacy-preserving framework for such agents. It utilises Homomorphic Encryption (HE) for computational security and a shuffling-based solution to handle unrestricted tasks that ensure compliance with privacy requirements and demonstrate effectiveness through several case studies. The Royal Society reports partially covered the topic of user privacy in compliance with international security standards but the focus of their reports is privacy enhancing technologies. However, privacy topics of existing user privacy surveys do not address the characterisation and quantification of user privacy in compliance with international security standards.


Fig. 4. Structural components of international standards.

## IV. Privacy Models and Frameworks

Three major organisations develop and publish security standards that include ISO/IEC [17], IEEE [18], and NIST [19]. In this section, first we discuss privacy risks, privacy requirements, privacy models and privacy attacks. Then, we describe the ISO/IEC, NIST, and IEEE privacy frameworks and explain their principles for privacy protection.

### A. Components of International Standards

International standards play an important role in the establishment of security and privacy best practices by providing common security guidelines. It includes technical specification, risk assessment, certification, interoperability, consistency, and resource allocation as listed in Fig. 4.

- *Technical Specification:* It includes technical requirements and guidelines for the implementation of privacy controls in a common language. It facilitates the consistent and efficient implementation of privacy controls in

an organisation. The ISO/IEC 27001 standard [56], which we discuss in Section V, provides detailed technical specifications for establishing an Information Security Management System (ISMS). For instance, a multinational company follows ISO/IEC 27001 to ensure its data security measures are robust and consistently applied across all its global operations. This includes specific controls for the encryption process, access control management, and incident response process, which help protect sensitive data from unauthorised access.

- *Risk Assessment:* It is a method for identifying and controlling user privacy risks. It includes identifying possible privacy risks, assessing their significance, and choosing suitable privacy protections. For example, a hospital using electronic health records might conduct a risk assessment to identify potential privacy risks, such as an unauthorised access to patient data and data breaches. Using standards like ISO/IEC 27701 [57] for privacy management, which we discuss later in this section, the hospital can assess the risks and implement controls, such as multi-factor authentication and regular audit logs to mitigate these risks.
- *Certification:* International standards certify organisations that demonstrate their dedication to privacy and ensure compliance with legal and regulatory requirements. For instance, a cloud service provider has obtained multiple certifications, including ISO/IEC 27001 [56] and ISO/IEC 27701 [57], which demonstrate its commitment to data security and privacy. These certifications reassure customers that cloud services meet high standards for protecting personal and sensitive user information making it a trusted platform for businesses worldwide.
- *Interoperability:* In complex technological systems, interoperability between technology and privacy controls is the main challenge. International standards are revised often to take into account new privacy risks, advancements in technology, and recommended practices to make complex technological systems work with the best privacy practices. This motivates businesses to keep improving their privacy policies. The GDPR, which we discuss in Section V, has influenced the development of interoperable privacy frameworks in Europe. For example, an EU company implemented GDPR compliance measures, it ensured that its platform could integrate seamlessly with other GDPR-compliant systems, facilitating smooth data exchanges while maintaining privacy standards.
- *Consistency:* International recognition of the standards provides consistency in privacy best practices among different countries. This is particularly important for organisations that operate across numerous jurisdictions. A Web search engine company operating globally relies on international standards like ISO/IEC 27018 [58], which focuses on protecting personal data in the cloud. By adhering to these standards, the company ensures consistent privacy practices across its various data centres worldwide that help it comply with different regulatory requirements in various countries.
- *Resource Allocation:* International standards provide recommendations on how to prioritise privacy efforts based on risk assessments and compliance requirements, thus helping organisations deploy resources more effectively. A financial institution uses ISO/IEC 27001 [56], which we discuss in Section V, to conduct risk assessments and allocate resources efficiently. By identifying high-risk areas, financial institutes can prioritise investments in security measures such as advanced encryption technologies and staff training programs, ensuring that resources are used effectively to protect customer data.

ISO/IEC, IEEE, and NIST standards play an important role in shaping privacy best practices by providing a structured and internationally recognised framework for addressing privacy concerns. Now, we discuss the privacy risks in detail.

### B. Privacy Risk

The term "privacy risk" describes the possibility of harm or adverse effects resulting from improper or unauthorised handling of user-sensitive data. Privacy risks can take many different forms and impact both people and businesses. The most common privacy threats are identity theft, data loss, unauthorised access, and data disclosure. For instance, a healthcare provider experiencing a data breach that exposes patient records can lead to identity theft and unauthorised access to user-sensitive health information. This breach can harm patients by compromising their privacy and potentially leading to financial or medical identity theft. There are comprehensive privacy taxonomies that an organisation can adopt to minimise the privacy risk and reduce privacy-related harm to their employees, customers, and partners. The first privacy taxonomy named "Solove privacy taxonomy" [59] is focused on the enhancement of end-user privacy. The second privacy taxonomy named "Pfitzmann and Hansen privacy taxonomy" [60] is aimed at preserving end-user privacy. We elaborate on the Solove privacy taxonomy with the help of an electronic voting system [43] as an example to show how each taxonomy addresses different aspects of end-user privacy.

*1) Solove Privacy Taxonomy:* The Solove privacy taxonomy is divided into four groups based on privacy risk contributing factors including information collection, information processing, information dissemination, and privacy invasion discussed as follows:

- *Information Collection:* The information collection processes pose a risk of privacy violations, as end-users may not be fully aware of the privacy risks involved in data collection. Management of concerns related to privacy violations during information collection is discussed in this phase. In the voter registration process of the electronic voting system, voters provide their details such as name, address, and national identification number. This phase addresses voter concerns about data collection, storage, and usage.
- *Information Processing:* Information processing is the use, preserving, and manipulation of collected user data. Privacy concerns arising from information processing are managed in this phase. For example, in the electronic

voting system, this may involve ensuring that voter data is securely processed, safely stored, and protected from unauthorised access during voting and tallying.

- *Information Dissemination:* The privacy concern related to information dissemination is the personal data revelation or the spreading of information threat. Privacy concerns related to information dissemination are addressed during this phase. In the electronic voting system context, this might involve concerns about how voter data could be shared or disclosed, intentionally or unintentionally. Addressing these concerns involves implementing measures to prevent unauthorised sharing of personal information and ensuring that any data is disseminated in a controlled and secure manner.
- *Privacy Invasion:* Privacy invasion is related to the disclosure of personal data or information. Decisional interference and intrusion are two common types of privacy invasion. Privacy concerns stemming from privacy invasion are addressed during this phase. In the electronic voting system, this could involve issues such as unauthorised access to voting records or attempts to influence voters' decisions.

*2) Pfitzmann and Hansen Privacy Taxonomy:* The privacy taxonomy by Pfitzmann and Hansen [60] defines five privacy properties that include anonymity, undetectability, unlinkability, unobservability, and pseudonymity. These privacy properties are used to meet the end-user privacy preservation requirements. We illustrate Pfitzmann and Hansen privacy taxonomy with the help of an IDentity Management System (IDMS) [61] and show how the privacy properties defined by Pfitzmann and Hansen – anonymity, undetectability, unlinkability, unobservability, and pseudonymity – can be applied in the context of an IDMS using tokens. The details of these privacy properties are as follows.

- *Anonymity:* Anonymity is the first privacy property in which a user can utilise an asset or consume a service without disclosing his identity to third parties. That is, a user is considered anonymous if she is not recognisable within a group of users called the anonymity set. Tokens in an IDMS can be designed so that users can access services without disclosing who they are. For example, a user may submit a token that authenticates their rights without disclosing personal information when gaining access to a secure website or service. This ensures that the user remains anonymous within the system and that other users are unable to identify them.
- *Undetectability:* Undetectability is the second privacy property in which an attacker cannot sufficiently distinguish whether an item such as a user exits or not. For instance, in a system where user data is anonymised, undetectability ensures that an attacker cannot easily determine whether a specific user's information is included in the dataset or not, thus preserving the user's privacy. In IDMs, tokens can be set up such that an attacker cannot find out if the token of a certain user is in the system. For example, undetectability guarantees that an attacker cannot determine if a specific user's information is included in the user records in an information system where tokens represent voter IDs. Due to this, the attacker is unable to recognise or follow specific individuals based on their tokens.
- *Unlinkability:* The third privacy property is unlinkability, which is closely related to the anonymity property. It is necessary property to support user privacy. From an attacker's point of view, the unlinkability of two or more items such as users or messages means that the attacker is unable to properly determine if these items are related to one another within the system. The unlinkability ensures that user actions performed with tokens are not connected. Tokens used for accessing pharmacy services and medical records in a healthcare IDMS, for instance, should not be linked together. This makes it harder for an attacker to identify the same user as the one performing these operations. The privacy and isolation of users' activities are guaranteed by this separation of actions.
- *Unobservability:* Unobservability is the fourth privacy property that refers to a user's undetectability against all users who are not engaged in an operation. More specifically, a user can use a resource or a service, without being noticed by others. This feature ensures that token usage is hidden from the adversary. Unobservability in an IDMS implies that other users or possible eavesdroppers cannot tell that a user is interacting with the service when they use their token to access it.
- *Pseudonymity:* The fifth privacy property is pseudonymity, which ensures that a user may use a resource or service without disclosing its true identity but can still be accountable for that use. A pseudonym is an identifier of a user other than one of the user's real names. IDM tokens allow users to perform actions while maintaining accountability without disclosing their true identities. Employees may utilise pseudonymous tokens in an enterprise IDMS to gain access to different resources within the organisation. Although these tokens conceal their true identities, system administrators can link them to the employee if needed. This guarantees that users can still be held accountable for their acts even while their true identities are protected.

We have discussed the privacy taxonomies with examples that are either used to preserve or enhance user privacy.

In the next subsections, we discuss privacy models and privacy attacks that focus on users' privacy in connection to their relationships and interactions with other users. An organisation can use these models to establish a mutual trust relationship among different entities that are involved in various communication protocols.

### C. Privacy Models

There are three privacy models: trusted, semi-trusted, and untrusted [62]. The details of these models are as follows:

- *Trusted Model:* In the trusted model, users need to protect their sensitive data through an external organisation, commonly referred to as a Trusted Third Party (TTP). TTP is the most reliable central entity that enables the exchange of all communications among the communicating entities.
- *Semi-trusted Model:* In the semi-trusted model, users are divided into different groups. Trust is divided among

the group of users engaged in the execution of the communication protocol. The data owner in this model does not fully trust peers, such as other users, and service providers.

- *Untrusted Model:* In an untrusted model, there is no trust among users who are involved in a communication protocol. It means safeguarding their communication privacy is their responsibility.

The privacy models are used to develop trust with other users in their relationships and interactions while the privacy framework is to help organisations to manage their privacy risks. In the literature, several authors have discussed privacy frameworks [63], [64], [65], [66]. Bangerter et al. [67] described a cryptographic framework that enables data minimisation techniques. It means that for each transaction, there is a precise specification of what pieces of data get revealed to each participant. This is called "controlled release of data". The salient feature of this framework is that the data in question is certified. So, its validity can be verified by the recipient. Later, Franz et al. [68] introduced a new metric that enables one to quantify the (un)linkability of the data items. They have considered the setting of a system that protects the unlinkability of certain elements of interest, and an adversary with the goal of nevertheless linking these elements. They also found that an adversary, who breaches privacy by linking and/or by unlinking pairs of elements, can identify the target partition (*i.e.,* uniquely link all elements) after a certain number of breaches have occurred.

Now, we discuss the privacy attack methodologies that an organisation can use to identify its attack surface.

### D. Privacy Attacks

An identity linked to a record or sensitive value poses a threat to user privacy. The threats can be categorised as record linkage, attribute linkage, table linkage, and probabilistic linkage. Let us assume that we have a table of the form "T(Unique ID, QID, Sensitive_Attributes, Non-Sensitive_Attributes)". The table values Unique ID, QID, Sensitive_Attributes, and Non-Sensitive_Attributes are defined in Section II. In these attacks, we assume that an attacker knows the victim's QID. In record and attribute linkage, we further assume that an attacker knows that the victim's sensitive value is in the published table and seeks to identify the victim-sensitive information from the table. In a table linkage attack, an attacker wants to determine the presence or absence of the victim's sensitive information from the published table.

- *Record Linkage:* In a record linkage attacker, a small number of records in the table $T$ called a group, are identified by some value qid on QID. If the victim's QID matches some value qid then the victim is linked to the few records in the group. If an attacker can find more information, she can uniquely identify the victim [69].
- *Attribute Linkage:* In attribute linkage [69], [70], the attacker may not be able to find the targeted victim's record exactly, but they may be able to determine the victim's sensitive values from the published table $T$ by looking at the set of values that are sensitive to the victim's group. There are two types of attribute linkage attacks: *homogeneity* and *background knowledge* attacks.
  - *Homogeneity Attack:* In this attack, the lack of variation in the sensitive attribute of the privacy protection model may reveal sensitive information. For example, consider a dataset containing demographic information (such as age, gender, and ZIP code) and medical records. While each attribute alone may not directly identify individuals, an attacker could launch a homogeneity attack by correlating similar demographic profiles with specific medical conditions. If the dataset shows a disproportionate number of individuals with a certain medical condition within a particular demographic group (elderly females in a certain ZIP code area), the attacker could infer sensitive information about individuals within that group.
  - *Background Knowledge Attack:* In this attack, an attacker may be able to guess sensitive data with high confidence if she has some prior knowledge. The effectiveness of these attacks depends on the attacker's access to additional information.

  In general, background knowledge attacks are difficult to prevent as compared to homogeneity attacks.
- *Table Linkage:* Record linkage and attribute linkage attacks assume a prior knowledge of the victim's record in the published table $T$. In the table linkage attack, an attacker can confidently infer whether the victim's record is present in the published table or not [69].
- *Probabilistic Linkage:* In this attack, an attacker could change their probabilistic belief about victim-sensitive information after gaining access to publicly available data, rather than the exact records, attributes, and tables they can associate with particular victims [53], [69]. In a simplified scenario, imagine a dataset with anonymised health records and another dataset containing anonymised fitness tracker data. By matching individuals based on shared characteristics, such as age, gender, and activity levels, an attacker could probabilistically link records to re-identify specific individuals and potentially infer sensitive health information.

The privacy attacks and threats deal with the protection of user Personally Identifiable Information (PII), but they are different processes. Privacy attacks are actual actions that are used to exploit or steal user personal data, such as hacking into a database or phishing scams. Privacy attacks aim to compromise user privacy. On the other hand, privacy threats are potential dangers that could lead to privacy attacks, such as vulnerabilities in a system and weak user passwords. They represent the possibility that privacy might be compromised. In simple terms, privacy attacks are the harmful actions that occur, while privacy threats are the potential risks that could lead to those attacks.

Organisations may use these privacy models, frameworks and attack methodologies to identify and prioritise privacy risks associated with their day-to-day operations. By assessing privacy risks, organisations can take appropriate measures to

mitigate them and prevent data breaches or privacy violations. NIST has proposed a privacy framework that is widely used by organisations of all sizes and agnostic to any particular technology, sector, law, or jurisdiction. The NIST privacy framework [71] is as follows.

### *E. NIST Privacy Framework*

The NIST privacy framework is a method for enhancing privacy through enterprise risk management [71]. It is divided into three main sections: Core, Profiles, and Implementation. Through the relationship between organisational roles and responsibilities, each component of the NIST privacy framework strengthens organisations' management of their privacy risk. The sections of the NIST privacy framework are as follows:

- *Core:* It is a collection of privacy-protection goals and actions that enables communicative parties within an organisation to prioritise their goals and actions in order of importance.
- **Profile:** It shows the privacy-related actions or goals that an organisation is currently performing. An organisation can create a profile by looking at all of the results and actions in the Core section and deciding which are most crucial to concentrate on based on the organisation's goals or business needs, the role(s) that the data processing ecosystem plays, the kinds of data processing that are processed, and the privacy demands of individuals.
- **Implementation:** It serves as a benchmark for how an organisation perceives privacy risk and assesses whether it has the necessary procedures and assets in place to control it.

To explain the NIST privacy framework in detail, we consider an example of a healthcare provider that implements the NIST privacy framework to provide better protection for patient data. The healthcare provider starts with the core functions in which they prioritise identifying and categorising patient health data. Then, robust data handling policies and regulatory compliance are established that implement technical measures to restrict access control. In the end, clear communication channels for patients are established that ensure strong security measures to prevent breaches. In the Profile phase, they evaluate their current practices that identify the need for stronger data encryption and improved patient communication. They prioritise these areas based on international regulatory requirements and patient feedback. During the Implementation phase, they conduct a risk assessment that upgrades encryption technologies and develop a new patient communication plan including updated privacy notices and better access to data usage information. By continuously monitoring and updating its practices, the organisation systematically improves its privacy management, aligning with its international regulatory demands and patient expectations.

### *F. International Standards for Privacy*

International standards for privacy provide guidelines and regulations to ensure the protection of individuals' personal information across borders which promotes transparency, security, and accountability. Following are the international standards that are relevant to user privacy.

- *ISO 29100 (Privacy Framework):* The ISO/IEC proposed a privacy framework named ISO/IEC 29100 [72] that protects users' PII. When privacy controls are necessary for the processing of PII then this international standard applies to natural persons and organisations that specify, procure, architect, design, develop, test, maintain, administer, and operate Information and Communication Technology (ICT) systems and services. This standard describes privacy safeguarding issues, defines actors and their roles in processing PII, specifies a common vocabulary for privacy, and offers links to established privacy principles for information technology.
- *ISO 27701 (Privacy Information Management System):* The ISO/IEC proposed another privacy framework named ISO 27701 (Privacy Information Management System) [57] that is relevant to all shapes and sizes of organisations that are PII controllers and/or PII processors processing PII within ISMS. It includes all public and private businesses, governmental organisations, and not-for-profit organisations. This standard is an extension to ISO/IEC 27001 [73] and ISO/IEC 27002 [74] that are discussed in Section VI. This standard offers guidelines for creating, implementing, maintaining, and continuously improving a Privacy Information Management System (PIMS). The requirements for PIMS that are outlined in this standard offer guidance to PII controllers and processors that are responsible and accountable for processing personal information.
- *ISO/IEC 29151 Privacy Risk:* The ISO/IEC standard named ISO/IEC 29151 [75] deals with the processing of PII in an organisation. This standard provides guidelines for establishing controls about the security of PII. This international standard provides recommendations based on ISO/IEC 27002, taking into account the conditions that may apply for processing PII in the context of an organisation's information security risk environment (s).
- *IEEE P7002 (Standard for Data Privacy Process):* IEEE has proposed a privacy framework named IEEE P7002 (Standard for Data Privacy Process) [76]. This standard provides specifications for a systems/software engineering process that takes privacy-related factors into account when developing products, services, and systems. This system uses the personal information of workers, clients, and other external users. This standard [76] encompasses all stages of the product life cycle, including development, quality control, and value realisation. It applies to projects and organisations working on the creation and implementation of systems, applications, processes, and products involving personal data. Users of this standard will be able to assess the conformance of their particular privacy practices by using the specific methods, checklists, and diagrams provided.
- *IEEE P7006 (Standard for Personal Data AI Agent):* IEEE standard named IEEE P7006 (Standard for Personal Data Artificial Intelligence (AI) Agent) [77] defines assessments made with inputs and decisions that can

TABLE II
A DETAILED COMPARATIVE ANALYSIS OF INTERNATIONAL STANDARDS RELATED TO DATA PRIVACY, PRIVACY FRAMEWORKS, AND MODELS WITH COMPARISON PARAMETERS OF ORGANISATION, STANDARD NAME, IDENTIFICATION NUMBER, PUBLICATION YEAR, REVISION YEAR, CERTIFICATION, POTENTIAL INDUSTRY, COMPUTATIONAL COST, CONTINUOUS UPDATION, LIMITED SCOPE, AND THE MAIN FOCUS OF STANDARD

| Organisation | Standard Name | Identification Number | Publication Year | Revision Year | Certification | Industry | Cost | Continuous Updation | Limited Scope | Main Focus |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC | ITST-**Privacy Framework** | 29100 | 2011 | 2017 | Yes | PII Processor | High | Yes | Yes | Privacy framework for PII protection. |
| ISO/IEC | ITST-**Privacy Architecture** | 29101 | 2018 | – | No | ICT System | High | No | Yes | ICT systems designed to interact with PII. |
| ISO/IEC | ITST-**Privacy Capability Assessment Model** | 29190 | 2015 | 2021 | No | Any | High | Yes | No | Privacy-related processes capacity management |
| ISO/IEC | ITST-**Code of Practice for PII Protection** | 29151 | 2017 | 2023 | No | PII Controller | High | Yes | Yes | PII processing in an organisation's information security risk environment |
| ISO/IEC | ITST-**Requirements and guidelines** | 27701 | 2019 | – | No | PII Controller &/ Processor | High | No | Yes | Improvement of information security management system |
| ISO/IEC | Privacy Enhancing Data De-identification Techniques–**terminology and Classifications** | 20889 | 2018 | – | No | PII Processor/ Controller | High | No | Yes | Data de-identification techniques |
| ISO/IEC | Privacy Enhancing Data De-identification **Framework** | DIS 27559 | 2022 | – | No | PII Processor/ Controller | High | Yes | Yes | Identification and mitigation re-identification risks |
| BSI | Data Protection-**Specification for personal information management system** | 10012 | 2017 | 2018 | No | Any | Low | Yes | No | Compliance of personal information management system with data protection requirements and good practice |
| NIST | **Privacy Framework** | NIST | 2021 | - | No | Any | Low | No | No | Enterprise risk management privacy tool |
| NIST | **De-identification of Personal Information** | NISTIR 8053 | 2015 | - | No | Any | Low | No | No | De-identification research direction |
| IEEE | **Personal Data AI Agent** | P7006 | 2018 | - | No | Any | Low | No | No | Ethics based AI guidelines |
| IEEE | **Data Privacy Processs** | P7002 | 2022 | - | No | Any | Low | Yes | No | System/software engineering privacy guidelines |

be made without input transparency to humans. This standard provides principles, guidelines, and inputs that direct the creation of AI and personalised algorithms to enable ethics-based AI. A major objective of this standard is to train Personal AI Agents to move beyond asymmetry and harmonise future personal data usage.

In Table II, we present a comparative analysis of international standards concerning data privacy, privacy frameworks, and models, highlighting various aspects such as publication year, revision year, certification, industry applicability, cost, continuous updation, limited scope, and main focus. Among the listed standards, ISO/IEC 29100, known as the Information Technology-Security Techniques-Privacy Framework, stands out as a comprehensive framework for protecting PII. It offers high privacy standards and continuous updation, making it suitable for PII processors across various industries. It is the only standard that offers certification training. Additionally, ISO/IEC 29190, focusing on privacy capability assessment models, provides a structured approach for managing privacy-related processes' capacity effectively. However, the choice of the most appropriate standard depends on specific organisational requirements, industry regulations, and the scope of privacy protection needed.

**Summary.** Three major organisations – ISO/IEC, IEEE, and NIST – developed and published several important security standards that provide guidelines on privacy risks, their requirement and supported privacy trust models. This section discussed the significance of international standards in establishing security and privacy best practices mainly focusing on their components such as technical specification, risk assessment, certification, interoperability, consistency, and resource allocation. The ISO/IEC 27001 for ISMS and ISO/IEC 27701 for privacy management standards show their role in ensuring user data security and privacy. We discuss security vs privacy in Section VII-D. Privacy risks such as identity theft and data breaches are discussed through privacy taxonomies like Solove's and Pfitzmann and Hansen's that categorise privacy concerns into different phases including information collection, processing, dissemination, and invasion. Additionally, privacy models – trusted, semi-trusted,

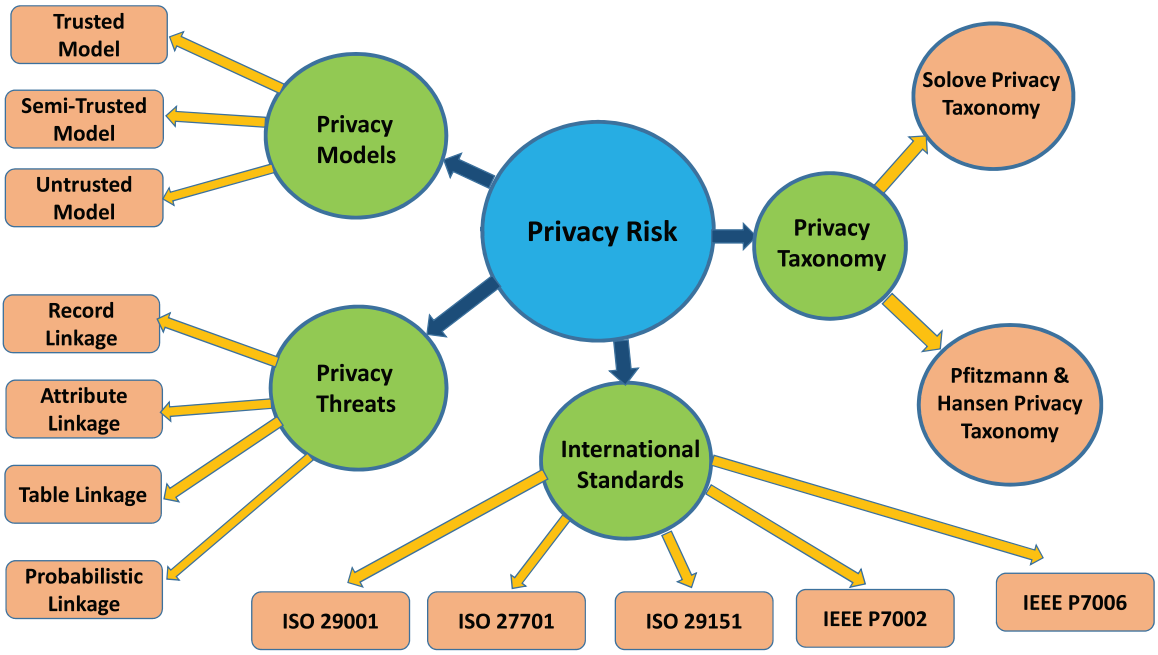


Fig. 5. The complete architecture of privacy risk with a focus on privacy models, privacy threats, and privacy taxonomy in compliance with international regulatory standards.

and untrusted – are discussed alongside privacy attacks that include record, attribute, table, and probabilistic linkage. These privacy frameworks and models help organisations manage their privacy risks with adherence to international standards and continuously updating their security practices to safeguard user-sensitive data.

## V. Characterisation of User Privacy

To understand and mitigate potential threats to user privacy, it is necessary to characterise the risks associated with user privacy [78]. The characterisation of user privacy risk prevents an organisation from the inappropriate use of user personal information and ensures that their businesses are held accountable for their data protection practices. To characterise user privacy risks, we need to discuss the sensitivity of user data and its privacy implications.

### A. Data Sensitivity

The first step in protecting user data is to conceptualise and categorise it. A study that focuses on the sensitivity of user data [79] lists the categories of information that have been legally designated as sensitive. Information being considered sensitive is based on four factors: the likelihood of harm occurring, the chance of harm occurring, the existence of a confidential relationship, and whether the risk represents the majority of concerns. A schema for evaluating data categories to determine the corresponding sensitivity of user data has been presented in [80]. This study examines several variables that affect the public's view of user data as sensitive, such as the data's accessibility, the context in which it is used, and its ability to identify specific individuals. Another component contributing to the impact of sensitivity is the possibility that certain information could be combined with other information to infer new information. Finally, decisions for data storage and sensitivity assessments are influenced by the nature of the technology. One could claim that the sensitivity assessments of user data are influenced by concerns about how the data will be used. It is critical to identify privacy attacks and vulnerabilities to explain the risks to user privacy.

We have discussed data sensitivity that an organisation can use to characterise user privacy risks. An organisation can characterise user privacy risks by first performing a threat modelling procedure. Threat modelling is used to identify potential threats and vulnerabilities such as record linkage, attribute linkage, table linkage, and probabilistic linkage. After performing threat modelling, the organisation can perform a Privacy Impact Assessment (PIA) to evaluate the impact on individual privacy rights within a specific project. The PIA is followed by the privacy risk assessment, which encompasses a broader evaluation of privacy and security risks related to data processing activities. However, organisations may change this sequence based on their specific needs and the nature of the project or system being assessed. The key is to integrate these processes coherently to ensure a comprehensive approach to characterising user privacy.

### B. Threat Modelling

Threat modelling is a systematic approach for identifying and assessing possible security flaws and privacy threats in an application or a system. It involves creating a threat model that describes potential hazards, how they affect privacy, and how to counter them. Threats can be seen and analysed with the help of tools, such as attack trees [81] and data flow diagrams [82]. Procedures for threat modelling are not covered by one international standard [83], [84].

Several organisations provide specific recommendations and effective approaches [19], [85]. The threat modelling process can be performed by an organisation by using the following known threat modelling standards.

- *OWASP Application Threat Modelling:* Open Web Application Security Project (OWASP) provides resources and guidelines on threat modelling of online applications [83]. OWASP's application threat modelling document provides several useful insights and techniques.
- *NIST Special Publication 800-154:* NIST's publication [86] guides integrating data-centric threat modelling into the software development lifecycle. It is not a formal standard but it is widely accepted in several organisations.
- *Microsoft Threat Modelling Tool:* Microsoft has released a threat modelling tool to assist companies in finding and solving possible vulnerabilities in their specific products [84]. It offers an organised method for threat modelling and is frequently utilised in software development processes.
- *ISO/IEC 27001:* ISO/IEC 27001 is an internationally recognised standard for ISMS [56]. It will be discussed in detail in Section VI.
- *FAIR (Factor Analysis of Information Risk):* FAIR is not a threat modelling paradigm but it offers an organised approach for understanding, evaluating, and translating information risk into financial terms [87]. It is essential for threat modelling and is frequently used in risk analysis methods.

### C. Privacy Impact Assessment (PIA)

To further characterise user privacy, a PIA, which is a methodical procedure, must be carried out to determine and evaluate any potential privacy issues related to a project, system, or operation that handles user data processing. It involves carrying out a thorough examination of data flows, processing operations, and privacy concerns. To get user data and evaluate privacy risks, PIAs frequently employ questionnaires, interviews, and checklists. An organisation can perform PIA using the following international standards.

*1) ISO 29134–PIA:* The ISO/IEC 29134 standard [88] offers recommendations for performing PIA procedures. It provides the complete format and content of a PIA report. An organisation operating user data processing systems and services that handle PII as well as those participating in project design or implementation should use this standard [88].

### D. Privacy Risk Assessments

Assessing the privacy risk is the final stage in characterising user privacy. Similar to PIAs, privacy risk assessments concentrate on assessing the degree of risk associated with identified privacy risks. It involves evaluating potential threats and vulnerabilities according to factors like impact and likelihood. It is possible to use both quantitative and qualitative risk assessment techniques. An organisation can use the following international standards to conduct privacy risk assessments.

*1) General Data Protection Regulation (GDPR):* The EU's GDPR [10] is a comprehensive privacy law that specifies the criteria for Data Protection Impact Assessments (DPIAs). DPIAs are employed to evaluate privacy risks related to data processing operations. GDPR gives persons whose personal data is being processed important rights and requires that those who process personal data comply with its regulations. Any natural or legal entity participating in the processing, including businesses and governments, must operate in compliance with the regulation. Non-compliance can result in expensive legal fees, reputational harm, and other consequences.

*2) ISO/IEC 27001:* The most well-known worldwide standard for ISMS is ISO/IEC 27001 [73]. It outlines the requirements that an ISMS needs to fulfil. When a business or organisation complies with ISO/IEC 27001, it indicates that it has implemented a risk management system for the protection of its data. The system adheres to all of the best practices and guidelines outlined in this international standard. This standard covers more than just privacy. It offers a methodical way to handle confidential business data and incorporates risk assessment and management procedures that can be used for assessing risks related to privacy.

*3) NIST Privacy Framework:* We have discussed the details of the NIST privacy framework [71] in Section IV. This framework includes risk models, risk assessment techniques, and privacy risk element identification methods. One can use this framework to conduct user privacy risk assessments.

*4) California Consumer Privacy Act (CCPA):* The CCPA of 2018 [89] offers customers greater control over the personal data that companies may gather about them. According to U.S. regulations, the companies that operate their businesses in California must evaluate the privacy risks associated with data processing activities.

*5) Personal Information Protection and Electronic Documents Act (PIPEDA):* The PIPEDA [90] is a Canadian law relating to data privacy that regulates the gathering, use, and disclosure of personal data by businesses operating in the private sector. This law provides guidelines for PIAs, which are equivalent to DPIAs that are performed in compliance with GDPR.

The PIA and risk assessment are important in evaluating potential privacy issues, but they focus on different aspects of user privacy. PIA looks at the consequences or effects of a particular event or action by asking questions like, "What will happen if this event occurs?" It aims to understand the extent and severity of the outcomes. On the other hand, privacy risk assessment identifies and evaluates potential threats or hazards by asking questions like, "What could go wrong, and how likely is it to happen?" It focuses on the probability of events and the magnitude of their possible impact. It means PIA deals with the effects, while privacy risk assessment deals with the likelihood and potential of harmful events.

In Table III, we present a comprehensive overview of various international standards and privacy laws related to the characterisation of user privacy. It includes information such as the organisation responsible for each standard, the name and ID of the standard, publication, and revision years, certification status, applicable industry, cost, continuous updation, scope limitations, and standard main focus. We have observed that the organisation investment for obtaining certification varies on

TABLE III
THE CHARACTERISATION OF USER PRIVACY IN COMPLIANCE WITH INTERNATIONAL REGULATORY STANDARDS WITH COMPARISON PARAMETERS OF ORGANISATION NAME, STANDARDS NAME, IDENTIFICATION NUMBER, PUBLICATION YEAR, REVISION YEAR, CERTIFICATION, POTENTIAL INDUSTRY, COMPUTATIONAL COST, CONTINUOUS UPDATION, LIMITED SCOPE, AND MAIN FOCUS AREAS

| Organisation | Standard Name | ID | Publication Year | Revision Year | Certification | Industry | Cost | Continuous Updation | Limited Scope | Main Focus |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC | ITST-**Information Security Management Systems-Requirements** | 27001 | 2013 | 2023 | Yes | Any | High | Yes | No | Information security management systems |
| ISO/IEC | ITST-**Information Security Management Systems-Controls** | 27002 | 2013 | 2022 | No | Any | High | Yes | No | Cyber security best practices and controls |
| ISO/IEC | ITST-**Guidelines for PIA** | 29134 | 2017 | 2023 | No | PII Processor | High | Yes | Yes | PIA |
| NIST | **Data-Centric System Threat Modelling** | SP 800-54 | 2016 | – | No | Any | Low | No | No | Data-centric system threat modelling procedure |
| OWASP | **Application Threat Modelling** | OWASP | 2020 | – | No | Website Business | Low | No | Yes | Web application threat modelling |
| Microsoft | **Threat Modelling** | Microsoft Threat Modelling Tool | 2018 | 2023 | No | Any | Low | Yes | No | Potential security issues identification and fixation |
| Privacy Act | **California Consumer Privacy Act** | CCPA | 2018 | – | No | California Business | Low | No | Yes | Privacy rights and consumer protection for California state residents in the US |
| Canadian Law | **Personal Information Protection and Electronic Documents Act** | PIPEDA | 2000 | – | No | Commercial | Low | No | Yes | User personal information management. |

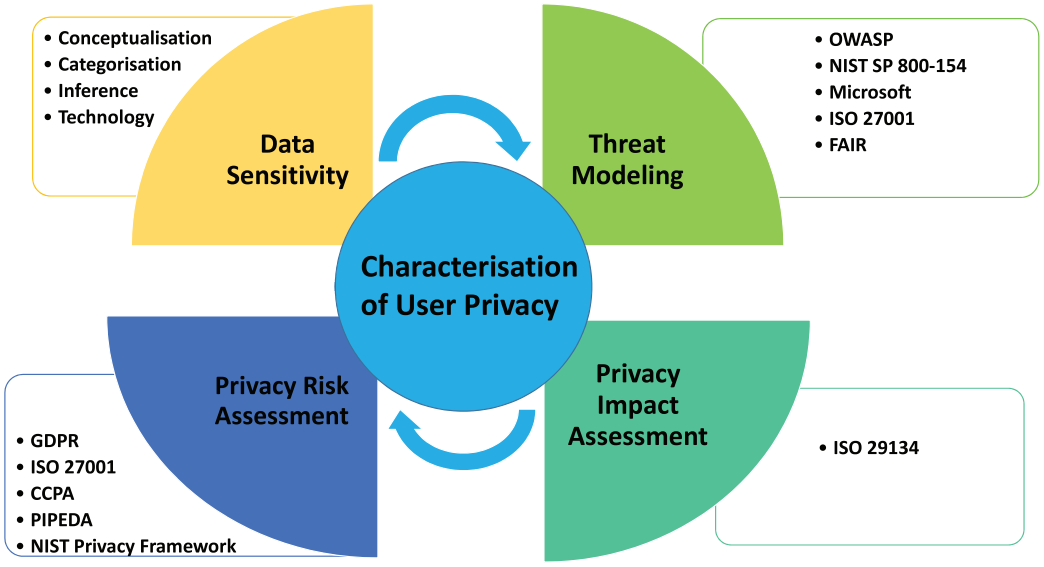


Fig. 6. The detailed process for characterisation of user privacy starts with data sensitivity measurement then thread modelling process, PIA, and privacy risk assessment.

standard complexity and organisation size. In general, ISO/IEC standards have high certification costs as compared with NIST, OWASP, and Microsoft. ISO/IEC 27001 is the only standard that is offering training for certification. We have observed that ISO/IEC standards and Microsoft threat modelling tools are continuously updated every five years, which ensures they remain relevant to technological advancements and evolving regulatory landscapes. The international standards also have some limitations such as the resource-intensive nature of compliance.

**Summary.** This section outlines the process of characterising user privacy risks with a focus on understanding and mitigating privacy risks to prevent the misuse of personal data. Characterising user privacy involves analysing data sensitivity

issues and identifying privacy attacks. Data sensitivity is determined by factors such as the likelihood and potential harm of data breaches, the existence of confidential relationships, and how easily data can identify individuals. Privacy attacks exploit vulnerabilities in data protection systems to access sensitive information. To address these risks, organisations should perform threat modelling, PIAs, and privacy risk assessments. Threat modelling identifies potential security flaws using frameworks including OWASP, NIST, and Microsoft's Threat Modelling Tool. PIAs evaluate potential privacy issues in data processing, using standards such as ISO 29134, GDPR, and PIPEDA. Privacy risk assessments measure the likelihood and impact of privacy threats with the help of standards such as GDPR and ISO/IEC 27001. This section also compares various international standards and privacy laws, highlighting their certification costs, continuous updates, and scope limitations, with a focus on maintaining relevance with technological advancements.

Now, we discuss the quantification of user privacy in the subsequent sections.

## VI. Quantification of User Privacy

The quantity used to measure how closely the privacy of a user can be estimated in digital contexts is known as "quantification of user privacy" [91]. Quantification of user privacy is essential for an organisation because it gives them a clear understanding of their data privacy policies, allowing them to recognise potential privacy hazards, guarantee regulatory compliance, and build user confidence. In general, organisations allow third parties with expertise in data analytics to access their data to extract more valuable insights from it. Additionally, these organisations are becoming more aware of the privacy of individual data. Thus, privacy controls that keep an eye on how data is used securely are highly desired for contemporary businesses, but systematically analysing and quantifying privacy risk is a challenging task [92], [93]. The quantification of user privacy is enabled by privacy metrics, which offer a systematic way of measuring, evaluating, and examining various aspects of data privacy within an organisation. These metrics work as numerical indicators that support an understanding of the degree of user data protection provided and the effectiveness of privacy measures.

### A. Privacy Metrics

The primary objective of privacy metrics is to determine how much privacy users have within a system and how much protection is provided by privacy techniques. Privacy metrics work as a quantification tool, while user privacy can be enhanced using privacy techniques. The characteristics of a system, such as how much private data is exposed or the number of users who are identical in one way or another, are input into privacy metrics. The privacy metric outputs a number that can quantify the degree of privacy in a system that is subsequently used in the comparison of different privacy techniques. The system characteristics can be used as a starting point for the selection of privacy metrics. The privacy metric output determines the suitability of privacy techniques. An ineffective selection of privacy techniques violates the privacy of the system.

*1) Conditions for Privacy Metrics:* There is not a single consensus on the requirements that privacy metrics have to fulfil. Several authors have examined privacy metrics conditions that contribute to characterising the privacy degree used in the quantification of user privacy [94], [95], [96], [97], [98], [99], [100]. For instance, Alexander and Smith [101] suggested that privacy metrics may give a bound, which is an extent to which an adversary can successfully identify people. Later, Andersson and Lundin [94] argued that privacy metrics must be based on the likelihood of an adversary identifying an individual. On the other hand, Syverson [102] explained that privacy metrics must indicate the difficulty of an adversary to succeed. Bertino et al. [95] proposed that privacy metrics specify privacy level, data quality, and the amount of sensitive data that is not concealed after applying the privacy techniques. A consideration of adversary success in terms of accuracy, uncertainty, and correctness is discussed by Shokri et al. in [103]. The condition for privacy metrics should be proportional to the increasing strength of the adversary. Now, we discuss the characteristics of privacy metrics.

*2) Characteristic of Privacy Metrics:* It can be a challenging task to choose privacy metrics for a situation due to large number and variety of available privacy measures. The choice of privacy metrics is determined by the types of adversaries we need to defend against and which features of privacy should be measured. Next, we determine the input data that is available to compute the metrics and which data sources require protection. Additionally, we discuss whether any of the chosen metrics have issues and if there are any validated implementations available. Lastly, we consider methods for determining parameter values for the chosen metrics. The main characteristics that can be used to categorise privacy metrics include adversary goals, adversary capabilities, data sources, input for privacy metrics, and output of privacy metrics. They act as a first set of guidelines that can be used to select privacy metrics for a given scenario.

- *Adversary Goals:* The purpose of privacy metrics is to measure the degree of privacy in a system provided by privacy techniques that a particular adversary frequently targets. The adversary's goal is to obtain sensitive information and threaten user privacy for fun, profit, social, political, and other reasons.
- *Adversary Capabilities:* Privacy may be more successfully attacked by a stronger adversary possessing sufficient resources or prior knowledge. For instance, an individual adversary with limited capability might exploit weak security measures to access personal email accounts that contain sensitive information, such as financial transactions. A group of hackers might collaborate to breach a large corporation's database, gaining access to millions of customer records. They could then sell or exploit this data for financial gain or other malicious purposes that compromise the privacy of countless individuals. On a larger scale, a state-sponsored adversary might conduct surveillance on its citizens through the monitoring of

telecommunications or Internet activity. By using sophisticated surveillance technologies and legal authority, they could systematically collect and analyse large amounts of personal data, violating individuals' privacy rights.

- *Data Sources:* Data is the main source of information that can be in the form of published data or observable data. Privacy techniques aim to protect the data but an adversary tries to gain sensitive information. In the case of published data, an adversary attempts to identify individuals or try to reveal the individual's sensitive information.
- *Privacy Metric Inputs:* Privacy metrics use various types of input for determining privacy values. The input includes, but is not limited to the estimate, resources, and prior knowledge of the adversary. In the case of an adversary's resources, it can cover several aspects, such as computational power, time, and bandwidth. The applicability of a measure in a given situation depends on input data availability.
- *Privacy Metric Output:* The privacy metric output is a property type that a privacy metric measures. Different types of output properties measure different aspects of privacy including uncertainty, information gain or loss, error, time, and accuracy. In the case of information gain or loss, the privacy metric measures how much information an opponent gains or how much information a user loses as a result of information disclosure.

### B. Privacy Notions

Several privacy notations are available in the literature [53], [104], [105]. In this section, we discuss the most general privacy notions that can be used for the quantification of user privacy.

- *Anonymity Set Size:* The anonymity set for an individual $u$ is the set of users in which the attacker cannot distinguish $u$ from the set of users [106], [107], [108], [109], [110]. The size of the anonymity set is mainly problematic because it only depends on the total number of users in the system [111]. It does not take into account the likelihood that any individual in the anonymity set will be attacked.
- *k-anonymity:* Conceptually, $k$-anonymity relates to the size of the anonymity set. The main idea behind $k$-anonymity is to publish statistical databases. For example, an electronic voting database *EvDb* contains a user-unique identifier (such as name) and sensitive information (such as voting candidate name). $k$-anonymity assumes that any uniquely identifying columns will be removed before the publication of the database and then divide the *EvDb* into equivalency classes containing at least $k$ rows that have the same QIDs [104], [112]. QIDs cannot directly identify users but help them identify the users when paired with other published data [104].
  Several algorithms transform *EvDb* to make it $k$ anonymous by utilising suppression or generalisation techniques [113] or random sampling techniques [114] that will be discussed in Section VII. Many studies have demonstrated that $k$-anonymity is insufficient against correlation with other datasets [53] and for high-dimensional data [52]. $k$-anonymity does not provide attribute hiding, nor does it provide security against attribute disclosure [115]. Furthermore, $k$-anonymous data releases do not protect against multiple releases of the same dataset [116], [117]. $k$-anonymity is commonly used today and applied to new privacy domains despite these shortcomings.
- *($\alpha$,k)-anonymity:* ($\alpha$,$k$)-anonymity is the extension of $k$-anonymity with addition of attribute disclosure prevention property. The frequency of a sensitive value in any equivalence class (rows with the same QID values) must be smaller than $\alpha$ [105], [118]. The research has shown that attribute linkage can happen even in cases where the sensitive value's frequency is smaller than $\alpha$ [21].
- *l-diversity:* The $k$-anonymity principle is modified by the $l$-diversity to restrict the diversity of publicly available data. It specifies that there must be at least $l$ well-represented sensitive values in each equivalency class. There are various ways to formulate this general principle. The $l$-diversity principle requires $l$ different values in each class. Nevertheless, probabilistic inference attacks are not prevented by this straightforward formulation [119]. More robust formulations depend on the idea that the $l$ most commonly used values of the sensitive property should have approximately equal frequencies in each equivalent class [53]. While $l$-diversity is an enhancement of $k$-anonymity property, it is not always enough to prevent certain types of attacks. It does not, in particular, protect privacy in the following situations: multiple statistical data releases are available [116]; sensitive values have a bias distribution; or sensitive attributes are semantically equivalent [119], such as numerical values that are close to one another [120]. Furthermore, if the adversary knows the data sanitisation process, they could be able to regenerate sensitive attributes [121].
- *m-invariance:* The $k$-anonymity principle is modified by $m$-invariance [116] to allow several releases of the same dataset, each of which may contain rows that have been added, changed, or removed. An attacker can determine the sensitive values by correlating the insertions and deletions between two releases of $k$-anonymous data. By $m$-invariance, this attack can only be prevented if each equivalency class has at least $m$ rows and different values for all sensitive attributes. Furthermore, every release must have the same set of unique sensitive values in each equivalency class.
- *t-closeness:* Let us assume that an adversary knows the global distribution of sensitive values to disclose the attribute of the user, $t$-closeness modifies the $k$-anonymity by bounding the distribution of sensitive values. It states that, in an equivalency class, sensitive values must have a distribution that is similar to the distribution of the entire table [119].
- *Stochastic t-closeness:* In the data distribution table, $t$-closeness leaves the sensitive value in its original

form. Stochastic $t$-closeness extends the definition of $t$-closeness [122]. It allows stochastic modification of data table-sensitive values.

- *(c, t)-isolation:* The purpose of $K$-anonymity is to prepare and publish statistical databases without considering the presence of an adversary. ($c$, $t$)-isolation extends $k$-anonymity notion to take into consideration for an adversary. The effectiveness of an adversary's point isolation in a database is measured by ($c$, $t$)-isolation [123]. Here, $c$ is an isolation parameter and $t$ is the privacy threshold.
- *(k, e)-anonymity:* The $k$-anonymity prepares and publishes a statistical database with categorical attributes. ($k$, $e$)-anonymity extends the notion of $k$-anonymity by taking into account numerical attributes [120]. The sensitive attributes range in any equivalency class in ($k$, $e$)-anonymity must be larger than $e$. The absence of uniform distribution of values inside the range of $e$ in ($k$, $e$)-anonymity can result in attribute disclosure through proximity attacks. Let us assume that we have the distribution of sensitive values in the range $e$. On one end, 85% of sensitive values are distributed in short intervals while on the other end, 15% of sensitive values are distributed. The adversary can guess with a confidence level of 85% that sensitive values lie in short intervals [21], [124].
- *($\epsilon$, m)-anonymity:* ($\epsilon$, m)-anonymity extends the notion of $k$-anonymity by adding the numerical attributes in the published statistical databases. It prevents the proximity attack by limiting the guessing probability of sensitive attributes to at most 1/$m$ against ($k$, $e$)-anonymity [124].

These are the few privacy notions that will be used in privacy metrics for the quantification of user privacy. Now, we discuss user privacy quantification in terms of entropy, which is used to measure how closely the original value of an attribute can be estimated. That is, how much user private information is leaked after applying privacy techniques. Following are the user privacy quantification measures in terms of entropy:

- *Entropy:* The foundation for modern information security principles is based on the concept of entropy proposed in [125]. Entropy, in general, quantifies the degree of uncertainty in estimating a random variable's value. It can be understood as the anonymity set size or extra information required by the adversary for user identification in terms of privacy [126]. Let us consider that an adversary wants to identify the member of the anonymity set that performs a specific action such as posting a special message on social media. The adversary guesses probability $p(x)$ for the anonymity set members $x$. It shows the possibility that $x$ is the suspected user such that the sum of probabilities $p(x)$ is equal to 1. The adversary can use prior knowledge and random guessing to estimate the probability. Formally, members of the anonymity set are represented by $\{x_1, \ldots, x_n\}$ of the discrete random variable $X$, and the (estimated) probability that a given member would be the target is denoted by $p(x_i)$. Then, entropy $H$ of $X$'s can be written in Equation (1) as:

$$H(x) = -\sum_{x \in X} p(x) log_2 p(x) \tag{1}$$

  Entropy is greatly influenced by outlier values, which means the likelihood of anonymity set users being the target is quite low [127], [128]. Entropy does not reveal the accuracy or precision of the adversary's estimates; rather, it only indicates their level of uncertainty [103]. Furthermore, entropy does not reveal how much bandwidth or computing power the opponent needs to succeed [100], [102].
- *Rényi Entropy:* Rényi entropy is the generalisation of Shannon entropy [98] that measures uncertainty in a random variable. It uses an extra parameter $\alpha$ and if the value of $\alpha \rightarrow 1$ then it becomes a particular case of Shannon entropy. The Rényi entropy can be calculated in Equation (2) as:

$$H_\alpha(X) = \frac{1}{1-\alpha} log_2 \sum_{x \in X} p(x)^\alpha \tag{2}$$

  Max-entropy or Hartley entropy $H_0$ is the special case of Rényi entropy with $\alpha = 0$ that represents the best case scenario where the ideal privacy of a user is achieved [98].
- *Normalised Entropy:* The range of entropy depends on the anonymity set number which means entropy values cannot be compared using absolute value. Hartley entropy is used to normalise entropy. The normalised entropy can be used to represent the amount of information leakage in the system [129].
- *Conditional Entropy:* The amount of information required to describe a random variable $X$ for a given random variable $Y$ with the assumption that $Y$ has a known value is measured by conditional entropy. The true distribution of the attribute in the databases is represented by the random variable $X$. The adversary's observations, such as probabilistic data release [52], can then be interpreted as $Y$. The conditional entropy can be computed from Equation (3). The entropy of a conditional probability distribution should not be confused with conditional entropy [111]:

$$H(x|Y) = \sum_{y \in Y} \sum_{x \in X} p(x, y) log_2 p(x|y) \tag{3}$$

- *Asymmetric Entropy:* Asymmetric entropy differs from conditional entropy in the sense that the opponent has prior information about random variable $X$ distribution, and the point $\alpha$, with the maximum value of uncertainty [130]. The adversary's chance of successfully determining the target is represented by $p(x)$ in asymmetric entropy, which ignores the anonymity set members probabilities [131] as computed in the Equation 4.

$$H_{AS} = \frac{p(x)(1-p(x))}{(-2\alpha+1)p(x)+\alpha^2} \tag{4}$$

- *Relative Entropy:* The variation between two probability distributions is measured by relative entropy. The absolute continuity criterion for the two probability distributions must be met, meaning that if $q(x) = 0$ then $p(x^*) = 0$.

TABLE IV
THE MEASUREMENT OF PRIVACY AND UTILITY LEVELS USING PRIVACY METRICS WITH PARAMETERS OF PRIVACY NOTIONS, INDENTED DOMAIN, PUBLISHED DATA, OBSERVABLE DATA, CONTEXT DEPENDENCY, LIMITED SCOPE, PRIVACY AND UTILITY LEVEL

| Privacy Notions | Domain | Published Data | Observable Data | Context Dependency | Limited Scope | Privacy Level | Utility Level | Scalability | Complexity | Ref. No |
|---|---|---|---|---|---|---|---|---|---|---|
| $k-$ anonymity | Databases | Yes | No | Yes | Yes | High | Low | High | Low | [113] |
| $(\alpha, k)$ anonymity | Databases | Yes | No | Yes | Yes | High | Low | High | Low | [105] |
| $l$-diversity | Databases | Yes | No | Yes | Yes | High | Low | High | Low | [53] |
| $m-$invariace | Databases | Yes | No | Yes | Yes | High | Low | High | Low | [116] |
| $t-$closeness | Databases | Yes | No | Yes | Yes | High | Low | High | Low | [119] |
| Stochastic $t-$closeness | Databases | Yes | No | Yes | Yes | High | Low | High | Medium | [122] |
| $(c, t)-$ isolation | Databases | Yes | No | Yes | Yes | High | Specific data and parameter choices | High | Medium | [123] |
| $(k, e)-$ anonymity | Databases | Yes | No | Yes | Yes | High | Specific data and parameter choices | High | Medium | [120] |
| $(\epsilon, m)-$ anonymity | Databases | Yes | No | Yes | Yes | High | Parameter selection and Implementation strategies | High | Medium | [124] |
| Renyi Entropy | Communication | Yes | Yes | No | No | High | Specific application and analysis | Medium | High | [98] |
| Normalised Entropy | Communication | Yes | Yes | No | No | High | Dataset for analysis | Medium | High | [131] |
| Conditional Entropy | Communication | Yes | Yes | No | No | High | Specific Application and requirements | Medium | High | [111] |
| Asymmetric Entropy | Genome Privacy | Yes | Yes | No | No | Low | High | Medium | High | [129] |
| Relative Entropy | Communication | Yes | Yes | No | No | Low | High | Medium | High | [132] |
| Mutual Information | Genome Privacy | Yes | Yes | No | No | Low | High | Medium | High | [133] |
| Conditional Mutual Information | Communication | Yes | Yes | No | No | Low | High | Medium | High | [134] |

The amount of probabilistic information revealed to the adversary is represented by relative entropy, the distributions $X^*$ represent the true distribution and $X$ is the adversary estimate [132]. The estimate of the adversary's deviation from reality is then indicated by relative entropy as in Equation (5):

$$D_{RE}(X^*||X) = \sum_{x,x^*} p(x^*) log_2 \frac{P(x^*)}{q(x)} \tag{5}$$

Moreover, some relative entropy implementations replace the adversary's observations $Y$ for the adversary's estimate $X$.

- *Mutual Information:* The amount of information communicated between two random variables is measured by mutual information. Mutual information estimates the amount of information leaked from a privacy mechanism and is computed among data true distribution $X^*$ and the adversary's observations $Y$ as in Equation (6), which has foundations in [133].

$$\begin{aligned} I(X^*; Y) &= H(X^*) - H(X^*|Y) \\ &= \sum_{x^* \in X^*} \sum_{y \in Y} p(x^*, y) log_2 \frac{p(x^*, y)}{p(x^*)p(y)} \end{aligned} \tag{6}$$

The entropy of $X^*$ can be used to normalise the mutual information between $X^*$ and $Y$ such that comparisons between scenarios are possible. In this instance, the average number of bits leaked from each entry is measured by normalised mutual information [134]. The entropy of $X^*$ can be used to normalise the mutual information between $X^*$ and $Y$ such that comparisons between scenarios are possible. In this case, the average number of bits leaked from each entry is measured by normalised mutual information as in Equation (7), and is based on [134].

$$I(X^*; Y|Z) = H(X^*|Z) - H(X^*|Y, Z) \tag{7}$$

Privacy metrics serve as quantifiable measures to assess the level of privacy and utility inherent in data processing activities. In Table IV, we have discussed the measurement of privacy and utility level using privacy metrics in terms of privacy notions, data source, context dependency, and scope. Context dependency acknowledges that privacy concerns and utility expectations may vary across different domains. Table IV presents various privacy notions and their associated metrics across different domains, such as databases, communication, and genome privacy. Notions like $k$-anonymity, $(\alpha, k)$-anonymity, and $l$-diversity are commonly applied in databases, offering high privacy levels but low

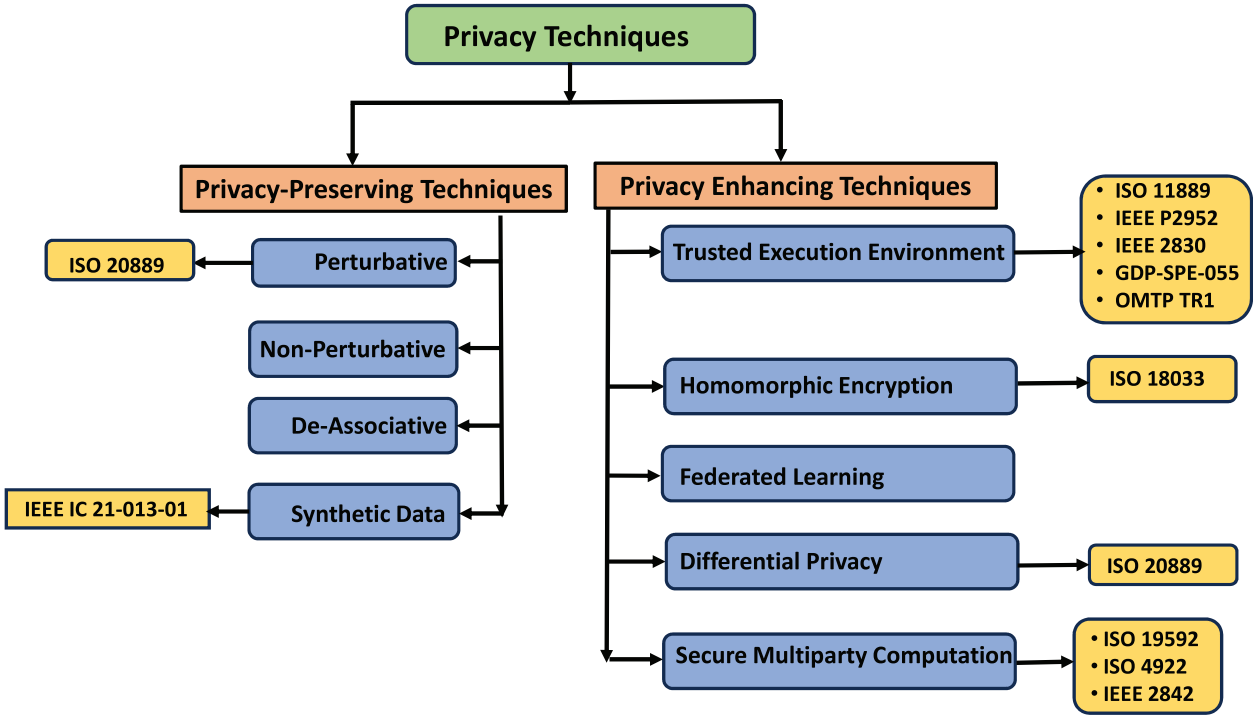


Fig. 7. The complete classification of privacy techniques that include privacy-preserving techniques and privacy-enhancing techniques in compliance with international regulatory standards.

utility. These metrics generally rely on published data, exhibit context dependency, and have a limited scope. Certain metrics, such as Renyi Entropy and Normalised Entropy, applied in communication, offer high utility levels but may provide lower privacy levels. They deal with observable data and are less context-dependent. Genome privacy metrics, such as Asymmetric Entropy and Mutual Information, offer high utility but lower privacy levels, often dealing with observable data. Table IV also lists the trade-offs between privacy and utility and emphasises the need for careful consideration of these factors when selecting and implementing privacy metrics in various domains. We have also observed that maintaining a balance between privacy and utility levels is essential for developing trust, enhancing user satisfaction, and ensuring ethical data practices in diverse socio-technical environments.

**Summary.** Quantification of user privacy in digital contexts is important for organisations to understand and enforce their data privacy policies, and identify potential privacy risks that ensure regulatory compliance, which increases user trust level. The privacy metrics enable the quantification of the user privacy process by systematically measuring and evaluating various aspects of user data privacy. It gave several numerical indicators that are used to quantify the degree of user data protection and the effectiveness of user privacy measures. Privacy metrics also consider system characteristics such as data exposure and user similarity that help organisations select suitable privacy techniques. These metrics must fulfil certain conditions that include bounds on adversary success, the likelihood of identification, and difficulty for adversaries. Characteristics of privacy metrics include adversary goals, capabilities, data sources, inputs, and outputs, guiding the selection of metrics for specific scenarios. Various privacy notions like $k$-anonymity, $l$-diversity, and $t$-closeness, along with entropy measures such as Shannon entropy, Renyi entropy, and mutual information, are used to quantify user privacy. These notions and measures highlight the trade-offs between privacy and utility. It emphasises the need for a balanced approach to ensure trust, user satisfaction, and ethical data practices across different domains like databases, communication, and genome privacy.

## VII. Privacy Techniques

Privacy techniques are methods and strategies used to protect individuals' sensitive information and data from unauthorised access, use, or disclosure while still allowing the collection and analysis of valuable information. Privacy techniques can be classified into Privacy-Preserving Techniques (PPTs) and Privacy-Enhancing Techniques (PETs), which are discussed in Sections VII-A and VII-B, respectively. Fig. 7 illustrates the complete classification among PPTs and PETs. Pinkas [135] has defined PPTs used to preserve privacy in the presence of adversarial participants who attempt to gather valuable information about their peers. In [136], Heurix et al. defined PETs as a subset of technological solutions that aim to protect an individual's or a group's privacy. PPTs are mainly concerned with safeguarding data from unauthorised access and ensuring confidentiality, while PETs focus on empowering individuals with control and transparency over their personal information.

We have discussed characterisation and quantification of user privacy in Sections V and VI, respectively. PPTs and PETs are used in the characterisation and quantification of user privacy. These techniques are used as a foundation

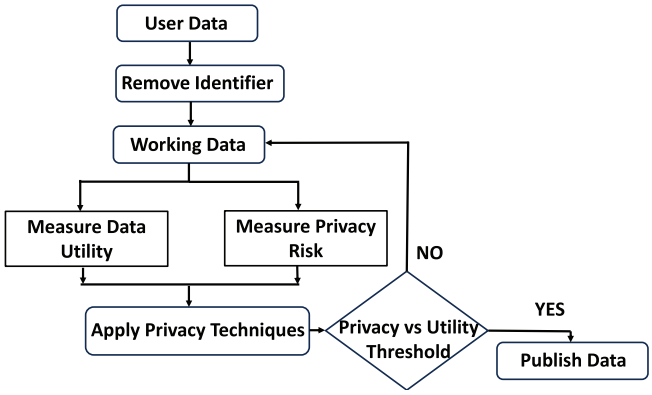


Fig. 8. The complete process of data de-identification.

for threat modelling, PIA, and privacy risk assessment. In threat modelling, they help to identify and mitigate potential vulnerabilities and attack vectors. In PIAs, they provide the mechanisms to evaluate and minimise the risks associated with data processing and storage. In PIAs, PETs help to determine the potential consequences of data handling practices on individual privacy. Privacy metrics are used to quantify the effectiveness of these techniques in protecting user-sensitive data by providing measurable benchmarks for privacy protection. Lastly, privacy notions such as anonymity, confidentiality, and data minimisation are used by these techniques to ensure that these notions are practically achievable and enforceable within a given system.

### A. Privacy-Preserving Techniques (PPTs)

To preserve data confidentiality, user-sensitive information must either be de-identified, *i.e.,* PII about an individual in a record, or the dataset is transformed or removed and data access must be restricted to approved organisations. Fig. 8 illustrates the complete process of data de-identification.

PPTs generate de-identified data in such a way that makes it difficult, if not impossible, for an adversary to learn user-sensitive information while maintaining useful data for further investigation [39]. De-identification process results in a reduced set of information bits and more data granularity, which generally leads to losses in data interpretability or predictive performance [7], [14], [15], [16]. It is inevitable to develop PPTs that minimise data compromise and provide a higher level of privacy protection. A major challenge associated with de-identification is figuring out how to distribute data that helps businesses, governments, and organisations to make decisions without revealing private information about particular data subjects. The balance between utility and data privacy has driven research toward creating new PPTs or reusing traditional privacy techniques.

The concepts of protecting sensitive user data were first introduced by [137] and later investigated, *e.g.,* by [23]. They proposed the classification of PPTs based on the characteristics of the user data based on perturbative and non-perturbative approaches. The perturbative approach relates to the deletion of information or the reduction of detail; whereas, the non-perturbative approach deals with information distortion. De-associative techniques are another category of PPTs that removes the connection between QID and sensitive attributes. Synthetic data is a de-identification technique whose objective is to publish artificial data using original data by maintaining the characteristics and features of the original data. The transformation from original data to artificial data is achieved through privacy techniques [46], [138], [139]. PPTs are classified into four major categories: Non-perturbative technique, Perturbative technique, De-associative technique, and Synthetic data. The non-perturbative technique is divided into five main categories which are Global Recoding, Local Recoding, Top-Bottom Coding, Sampling and Suppression. The perturbative technique is classified into seven types which are Rounding, Noise, Shuffling, Re-sampling, PRAM and Microaggregation. Recoding, Local Recoding, Top-Bottom Coding, Sampling and Suppression. The de-associate technique has four types which are Slicing, Bucketisation, Angelisation and Anatomisation. The synthetic data has three main categories that include partially synthetic, hybrid synthetic and fully synthetic data. Now, we discuss the categories of PPTs in detail in the subsequent sections along with international standards.

*1) Non-Perturbative:* The non-perturbative techniques aim at minimising the quantity of information in the data by either lowering the level of information or partially hiding information while maintaining the accuracy of the original data. Non-perturbative techniques do not completely change the original data. They can be divided into five categories including global and local recoding, top-and-bottom coding, suppression, and sampling.

- *Global Recoding:* This method is referred to as a full-domain generalisation. Global recoding involves merging many categories to form new, more inclusive categories [23], [137], [140].
- *Local Recoding:* The user data is recoded locally into broader intervals or categories when required [141]. Generally, global recoding differs from local recoding in that all attribute values belong to equal domain levels while local recoding; on the other hand, it generalises the values to other domain levels [142].
- *Top-and-Bottom Coding:* One particular instance of recoding is top-and-bottom coding. This method is used for numerical qualities that are continuous or discrete. The top recoding covers values above a specific threshold level where the attribute frequencies range tends to become smaller while the bottom recoding covers values under another threshold level. The determination of the appropriate threshold level is not an easy task [23].
- *Suppression:* In suppression, data can be suppressed from the original data so that they are not released or replaced with a special character or a missing value. Cell, tuple, and attribute suppression are the three common suppression levels [23], [112], [143].
- *Sampling:* Sampling is a technique for protecting user data. When the original set of census data represents the complete population then rather than being made public, a sample S set is released [144].

*2) Perturbative:* The perturbative technique is used to modify the user data before its release. These must be applied to ensure that perturbed user data sets and original dataset statistics do not differ significantly. DP, which we discuss in Section VII-B5, is also the subtype of the perturbative techniques. The perturbative techniques include swapping, re-sampling, noise, micro aggregation, rounding, the Post-RAndomisation Method (PRAM), and shuffling.

- *Swapping:* The basic idea of the data swapping technique [145] is to swap the values of specific attributes between records. This approach involves swapping entries that belong to different sub-domains but are similar on a set of attributes. The swapping can be divided into two subdomains: data swapping and rank swapping.
- *Re-sampling:* Re-sampling is a technique that uses the replacement bootstrap method. The re-sampling method consists of taking multiple small samples and averaging them together. Re-sampling was initially used for tabular protection [146], but user data sets may additionally benefit from this technique [140].
- *Noise:* Noise is known as randomisation and is used to protect user data. Noise can be added or multiplied with the user's data to enhance the randomness in it. Additive noise has been studied extensively since 1980 [147], [148], [149], [150], [151]. Additive noise can be categorised into four types that include uncorrelated noise addition, correlated noise addition, noise addition with linear transformation, and noise addition with non-linear transformation. In some cases, constant variance is a part of additive noise so it is better to use multiplicative noise [152].
- *Microaggregation:* Microaggregation is a technique that is used to partition a dataset into groups using the maximal similarity criterion. Microaggregation was initially proposed for continuous variables [153], [154], but later it has been expanded to include categorical data [155]. Three criteria are used in microaggregation, including the definition of group homogeneity, the clustering techniques employed to identify homogeneous groups, and the calculation of the aggregated function. It is typically performs better in situations where the groupings' attribute values are more homogeneous [153], [154], [155], [156], [157], [158], [159], [160].
- *Rounding:* Rounding is a technique that has been used for a very long time [161]. Its goal is to substitute rounded values for the original values of the attributes. In multi-valued attribute data, rounding is performed on one attribute, but multivariate rounding is possible [23]. This technique is suitable for data that has continuous attributes.
- *Post RAndomisation Method (PRAM):* This method uses a probability mechanism in such a way that an intruder cannot be confident that a given match corresponds to the right person or not. It is proposed by [162] and is used for categorical data (unique attribute data). In PRAM, a specific probability is applied to the recoding of one or more category attribute values, and this recoding is carried out independently for every record. PRAM is particularly useful in those cases where a user data collection has multiple characteristics and using other de-identification techniques, such as global recoding, top-and-bottom coding, and local suppression that would result in an excessive amount of information loss [140].
- *Shuffling:* Shuffling is a technique that is used to replace data-sensitive attributes with new data that has similar distributional attributes. Shuffling is a variant of swapping that was proposed by [163], [164], [165]. Data shuffling provides a lower level of disclosure risk with a higher level of utility as compared with swapping techniques but shuffled data carries a similar risk of attribute exposure as data swapping and rank switching [140].

*3) De-Associative:* The main purpose of this technique is to create buckets that separate the relationship between sensitive properties and QID. Techniques like bucketisation, atomisation, angelisation, and slicing are part of de-associative techniques.

- *Bucketisation:* Partitions are the foundation of bucketisation. In a bucket, several values are sensitive for every record. These records are permuted to protect sensitive values. As a result, the bucketised data is made up of a collection of buckets with sensitive values permutation that make it difficult for an adversary to identify which tuples are in which bucket. A permutation-based approach was proposed by [120] to reduce the correlation between QID and sensitive characteristics that are appropriate for user data and query-based databases.
- *Anatomisation:* Anatomisation is a technique proposed by [166] that is based on the bucketisation principle. In this technique, it publishes two distinct tables: a QID and a Sensitive table instead of publishing permuting sensitive values. Anatomisation has gained popularity in the field of data privacy, but its use is limited and it is susceptible to background knowledge attacks [167]. It is recommended to use other privacy techniques.
- *Angelisation:* Angelisation is a method similar to anatomisation and is proposed by [168]. The user data is separated into buckets and batches in this method and any pair of buckets and batch publication corresponds to the angelisation.
- *Slicing:* The slicing approach is proposed by [169] that preserves attribute correlations by grouping many QIDs with the sensitive values. The division of a user data set into vertical and horizontal portions is the idea of slicing.

*4) Synthetic Data:* Synthetic data is the artificial data that is obtained from original data through some transformation that maintains the characteristics and features of the original data. Rather than publishing original data, [139] proposed generating synthetic user data. Synthetic data is becoming more and more popular [170] due to its lack of privacy concerns that are present in other privacy techniques. In general, deep learning models or data mining techniques are used to create synthetic data whose statistical characteristics are comparable to those of the original data. As a result, after analysing a particular set of synthetic data, data analysts would be able to derive the same statistical findings as they would find from the original user data. There are types of synthetic

TABLE V
COMPARISON OF PPTS IN COMPLIANCE WITH INTERNATIONAL REGULATORY STANDARDS WITH PARAMETERS OF PPTS, BRIEF DESCRIPTION, TYPES, PRIVACY RISKS RELATED TO PPTS, ADVANTAGES, LIMITATIONS, AND STANDARDS

| Techniques | Description | Types | Privacy Risk | Advantages | Limitations | Standards |
|---|---|---|---|---|---|---|
| **Non-Perturbative** | Reduces information before data release | - Global Recoding<br>- Local Recoding<br>- Top-Bottom Coding<br>- Sampling<br>- Suppression | Reveal the presence of dataset sensitive attributes | - Data structure unchanged<br>- No unique combinations | - Reduce information details<br>- High generalisation level<br>- Low data utility | No Standard |
| **Perturbative** | Distort the data before its release | - Rounding<br>- Noise<br>- Shuffling<br>- Re-sampling<br>- Swapping<br>- PRAM<br>- Microaggregation | Reveal the presence of dataset-sensitive attributes | - Uncertain values<br>- New combinations may appear | - Inconsistent values<br>- Great quantity of distortion required in extreme values | ISO/IEC 20889 |
| **De-Associative** | Break the correlation between quasi and sensitive attribute before data release | - Slicing<br>- Bucketisation<br>- Angelisation<br>- Anatomisation | Expose correlation between Quasi and sensitive attributes | - Publishes original quasi identifier<br>- No relationship between QID and sensitive attributes | - High disclosure risk because of original QID<br>- Sensitive values swapping leads to inaccurate results | No Standard |
| **Synthetic Data** | Prevents individual's disclosure when releasing statistics or derived information | - Partially Synthetic<br>- Hybrid Synthetic<br>- Fully Synthetic | Reveal the presence of sensitive attributes in synthetic dataset | - Quantifiable privacy protection<br>- Low disclosure risk | - Attribute relationship analysis requires large datasets<br>- Costly in Computation | IEEE IC-21-013-01 |

data that have been identified by [138]: fully, partially, and hybrid synthetic data.

- *Fully Synthetic:* In fully synthetic data, there is no release of the actual data since all values on the user data are replaced with the simulated values [139]. As a result, the disclosure risk is typically very low [138]. Synthetic data provides only the information combined with the statistical model about the original data, which is typically limited to certain statistical features and requires less time and energy [171].
- *Partially Synthetic:* The basic idea of partially synthetic data is to select a subset of rows and columns of user data for synthesis [172], [173]. It is also named selective synthesis. Partially synthetic data is typically helpful when applied to attribute values that carry a high risk of disclosure. As a result, when unreal values are used in place of real data values at a higher disclosure risk, the disclosure risk is reduced. Partial synthetic data often has the same amount of records as real data.
- *Hybrid:* The process of combining synthetic and original data generates hybrid data. Integration of synthetic data with the most effective attributes of other privacy techniques is the fundamental idea [174]. The combination of microaggregation and synthetic data is demonstrated by [175]. In comparison to other synthetic data techniques, the security level in hybrid datasets is the lowest, and record numbers do not need to match the original data record numbers.
- *IEEE IC-21-013-01:* IEEE IC-21-013-01 [176] is the only standard available for the PPTs. It is a partnership between academia and industry focused on accuracy and privacy in synthetic data. In addition to enabling privacy-preserving data utilisation, synthetic data may improve algorithmic fairness. The objective of this standard is to provide terminology guidelines and best practices for the privacy and accuracy of synthetic data.

**Summary.** In this section, we have explained the PPTs that any organisation may use to preserve user privacy. We have compared various PPTs in compliance with international regulatory standards, providing insights into their descriptions, types, associated privacy risks, advantages, limitations, and adherence to standards as illustrated in Table V. Non-perturbative techniques, such as global recoding and sampling, maintain the data structure but reduce information details, resulting in a high level of generalisation and low data utility. Perturbative techniques, including rounding and noise, distort data before release, offering uncertain values and potentially introducing new combinations but requiring a significant amount of distortion, particularly for extreme values. De-associative techniques, such as slicing and bucketisation, aim to break correlations between quasi and sensitive attributes but may pose high disclosure risks due to original quasi-identifiers. Synthetic data techniques, such as partially and fully synthetic, offer quantifiable privacy protection and low disclosure risk but require large datasets for attribute relationship analysis and are computationally costly. Notably, only synthetic data techniques adhere to the IEEE IC-21-013-01 standard, underlining the importance of standardised approaches in privacy-preserving practices.

### B. Privacy Enhancing Techniques (PETs)

The PETs are categorised into five main categories that include Trusted Execution Environment (TEE), HE, Secure Multiparty Computation (SMPC), Federated Learning (FL), and DP. The details about each category of PETs are discussed

in subsequent sections. An organisation can use PETS to enhance user privacy.

*1) Homomorphic Encryption (HE):* Using HE, one can perform operations on encrypted data. Upon decryption, the operations performed on the encrypted data match the result of operations performed on plain data. There are different types of HE schemes including Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SWHE), and Fully Homomorphic Encryption (FHE). PHE [177] supports an unlimited number of one type of operations (*i.e.,* addition or multiplication) on the encrypted data. PHE can be further divided into two types: multiplicative and additive PHE. RSA (Rivest, Shamir, and Adleman) is an example of multiplicative PHE [178] while Paillier cryptosystem [179] is an example of additive PHE. PHE schemes have relatively low computation and storage overheads. They are used in many practical applications, although they support only one type of operation. The Polly Cracker scheme [180] and Boneh-Goh-Nissim (BGN) [181] are SWHE schemes. They support an arbitrary number of additions and one multiplication operation or vice versa.

A Fully Homomorphic Encryption (FHE) scheme allows an unlimited number of operations on the encrypted data and the resulting output lies within the encrypted data limit. In 2009, Gentry [182] presented the first feasible lattice-based FHE scheme in his seminal PhD thesis. Gentry's proposed scheme gives not only an FHE scheme but also a general framework to obtain an FHE scheme. HE is particularly useful in situations when the user data is outsourced to third-party storage for computation and privacy is a major concern. HE can be used to enable novel solutions in highly controlled areas, such as healthcare, where data challenges can be eliminated by preventing data sharing. The following are the international standards that an organisation can use for the implementation of HE.

- *ISO/IEC 18033-6:2019:* It is an IT security standard that describes the generation of suitable security parameters of two partially homomorphic algorithms called Paillier and Exponential ElGamal encryption, and the method of homomorphically processing the encrypted data [183].
- *ISO/IEC AWI 18033-8:* The continuation of ISO/IEC 18033-6:2019 for FHE is ISO/IEC AWI 18033-8 [184]. The proposed international standard outlines cryptographic techniques that use FHE to compute a function on encrypted data while maintaining the confidentiality of the computation's input, intermediate, and output data. This standard has been deleted by ISO/IEC.
- *Open Homomorphic Encryption Standard:* In 2018, the Homomorphic Encryption.org community accepted the first Homomorphic Encryption Standard (HES) created by an open consortium of government, academics, and industry. It outlines the schemes, explains the collection of information regarding their security, and suggests a broad range of parameters to be used for HE at different security levels. It provides these security parameter recommendations by outlining known attacks and their approximate execution times.

*2) Secure Multi-Party Computation (SMPC):* In addition to HE techniques, another method for doing computations on encrypted data is SMPC. By using the SMPC technique, parties with sensitive inputs wishing to compute a joint function together without disclosing their inputs to one another can perform computation on it. At the end of the protocol's execution, the parties have learned nothing more than what the output itself has disclosed. The SMPC approach eliminates the requirement for a reliable third party. There are two general protocols for SMPC. Yao's garbled circuits were invented by Yao in 1986 [185] and Goldreich et al. (GMW) protocol [186]. Yao's garbled circuit is a secure two-party computation protocol. In this protocol, the sender builds a circuit for the function that has to be calculated, then chooses two symmetric keys at random for each wire in the circuit, giving rise to two possible values: '0' and '1'. The truth table for each gate in the circuit is then sent, in a random order, along with the keys that correspond to each gate's inputs. By executing an Oblivious Transfer (OT) protocol [187] with the sender party, the receiver obtains the matching keys for its input bits obliviously. Subsequently, the circuit is evaluated by deciphering the garbled truth table for each gate.

Another SMPC protocol is GMW protocol. In this protocol, the function that needs to be calculated is represented as a circuit of XOR and AND gates, similar to Yao's circuit. Parties send their shares to each other after dividing their inputs into shares. As the XOR operation is linear, each party can compute the XOR of the shares they hold without any communication. The result of an XOR gate is simply the XOR of the corresponding shares from each party. This step does not require communication because no further interaction is required.

The OT protocol must be executed by the parties to calculate the AND gate output. The computation cost of secure two-party and multi-party computation protocols is significantly decreased by the OT extension algorithm [188]. It is preferable to build function-specific SMPC protocols by taking into account the computation and communication costs of the generic protocols, even though the GMW protocol and Yao's garbled circuit protocol can compute any function. These particular functions include secure logical operations, such as private set intersection protocols , equality and comparison functions. The following are the international standards that an organisation can use for the implementation of SMPC protocols.

- *ISO/IEC 19592-1-2:2016-2017:* This standard describes cryptographic secret-sharing methods and their characteristics. The update to ISO/IEC 19592-1:2016 [189] is ISO/IEC 19592-2:2017 [190], which discusses five secret sharing algorithms that fulfil recoverability and message confidentiality requirements.
- *ISO/IEC 4922-1:2013:* This standard [191] describes SMPC techniques based on the secret sharing methods outlined in ISO/IEC 19592-2. This standard describes the addition, subtraction, shared random number generation, and multiplication methods.
- *IEEE 2842-2021:* The recommended IEEE practice for SMPC is IEEE 2842-2021 [18]. This standard gives an

overview, technical specification, and security levels of SMPC.

*3) Trusted Execution Environment (TEE):* A secure portion of a computer device's Central Processing Unit (CPU) is called a TEE. TEE makes it possible to access and run code that is separate from the rest of the system. TEEs consist of both hardware and software components. As TEEs are segregated from the remaining system, the code within TEEs cannot be read by the Operating System (OS) or hypervisor – a procedure that divides an OS and its applications from the physical hardware of a computer. Using memory encryption enclave technology, TEE offers hardware-enforced isolation. This technology is available by several names and is mostly supplied by hardware manufacturers, such as AMD, ARM, and Intel.

In virtualised cloud environments, protection against malicious insider actors, such as malicious hypervisors, is guaranteed by the trust model for secure enclave solutions. However, side-channel attacks on the processors that provide security functionalities are still feasible [192]. Some producers provide patches or solutions to TEEs but they cannot guarantee that CPUs are immune to side-channel attacks. It is up to the solution provider to mitigate the security risk.

There are many applications for TEEs [193], [194], [195]. It is used with biometric authentication techniques (*i.e.,* voice authentication, fingerprint sensors, and facial recognition). TEE runs the matching engine and related processing needed for user authentication. TEE also guarantees that the computing is "securely" outsourced in the context of a cloud. This implies that the provider is unable to obtain any knowledge about the relevant data. Furthermore, it makes multi-party computation on untrusted platforms secure. It offers privacy for IoT devices, large-scale data analytics, and more privacy-conscious ML "as a service". Due to memory constraints, scalability can be problematic for large-scale processing because only a certain amount of data may be processed simultaneously. Following are the international standards that an organisation can use to employ TEE in their operations.

- *ISO/IEC 11889-1:2015:* It is a four-part standard on Trusted Platform Module (TPM) that was developed through industrial partnership and later adopted by ISO/IEC [196]. It outlines the TPM's architectural components, a tool that promotes trust across computing systems as a whole. In the context of how a TPM contributes to building trust in a computing platform, several TPM ideas were explained. Platform requirements are guided by ISO/IEC 11889-1:2015, which describes how a TPM contributes to building trust in a computer platform. ISO/IEC 11889's scope is restricted to TPM standards alone.
- *IEEE 2830-2021:* It is a standard for the requirements and technological foundation of shared ML based on TEE [197]. This standard specifies the architecture for ML, wherein a TTP processes encrypted data that has been gathered from several sources to build a model. The functional components, workflows, security specifications, technological specifications, and protocols are also specified in this standard.
- *OMTP TR1 Standard:* The Trusted Environment of Open Mobile Terminal Platform (OMTP TR0) has been replaced by the Advanced Trusted Environment (OMTP TR1) [198]. OMTP presents several practical recommendations, which can be implemented in silicon platforms that are currently in use. The same practical methodology was used during TR1's development to produce a more thorough security road map. Such a strategy is in line with the industry's overarching goals of establishing hardware-backed security, as well as existing threats and potential profits.
- *GlobalPlatform GPD_SPE_055 Standard:* The global platform [199] provides an organisation with technical standards that manage cutting-edge digital services and products that are secure by design. It offers consumers end-to-end protection, privacy, ease of use, and simplicity.
- *Platform Security Architecture (PSA) Standard:* A solution for connecting device security is provided by the PSA Certified IoT platform [200], which covers everything from analysis to certification and security evaluation. To ensure that security is no longer a barrier to product development, this framework offers standardised tools to help address the increasingly heterogeneous requirements for IoT [200].
- *IEEE P2952:* It is a standard for secure computing based on TEE [201]. It offers a foundation for a secure computing system based on TEE and provides technical specifications for isolation, secrecy, compatibility, performance, usability, and security that are necessary for an extensive secure computing platform.

*4) Federated Learning (FL):* FL is an ML method that enables data owners to collaborate on training ML models [202]. It keeps the data hidden from the server and other data owners. FL can be implemented using a decentralised and a centralised approach. In a centralised FL approach, data owners receive the first training model from the trusted server, which also starts the training process. Using their locally stored sensitive data, the data owners locally trained the model. The server receives the updated parameters to perform global model aggregation. Only the global model aggregation parameters may be updated by the server. These procedures are repeated until the model is completely trained. In a decentralised FL approach, there is no centralised trusted server. Every data owner can directly edit the global model and communicate with each other. The decentralised design has certain advantages as there is no single point of failure but processing on a single server may cause security problems or unfairness.

The data distribution across a sample is used to divide FL into three types including Federated Transfer Learning (FTL), Vertical FL (VFL), and Horizontal FL (HFL) [202]. In HFL, every data owner with a different sample shares the same feature sample. In this scenario, data can be gathered by a server from various data owners. In VFL, the feature spaces may vary, but the sample space is primarily shared by several customers. Several secure VFL models, such as decision trees, association rule mining, and Naive Bayes classifiers, are proposed in the literature [203]. FTL is a recently developed

framework that allows for some data overlapping in both the sample and feature spaces. Complementary knowledge can be moved between domains in a federation using FTL and by combining data from many sources, an adaptable and powerful model may be created for the target area. In summary, FL reduces the chance of data breaches because no data is stored in one place that could be more valuable to an attacker.

*5) Differential Privacy (DP):* DP [204] is a method of data anonymisation that measures privacy using mathematical definitions. It measures how much personal information, a computation's output reveals about an individual. It is frequently used to protect an individual's privacy whose data is included in a dataset for statistical analysis [30], [205], [206]. DP is a novel method of protecting privacy that can be measured more precisely than the methods found in many privacy laws and policies.

Formally, two datasets, $D_1$ and $D_2$, which differ by no more than one record each, are used to define DP [204]. For each subset of the output $S$ within the range of $M$, and for all datasets $D_1$ and $D_2$ differing by no more than one record, a randomised algorithm $M$ is $\epsilon$ differentially private that defines

$$Prob[M(D_1) \in S] \leq exp(\epsilon) prob[M(D_2) \in S] + \delta \quad (8)$$

($\epsilon$, $\delta$)-DP is the name assigned to this formulation as listed in Equation 8, in which $\delta$ is the relaxation parameter. $\epsilon$-DP offers higher privacy guarantees if $\delta$ is ignored. The privacy level control parameter is $\epsilon$. It establishes the amount of additional noise added to the dataset, changing its properties and making values more difficult to reveal, such as direct or indirect identities of certain individuals.

Another method is Rènyi DP (RDP) [207]. An algorithm is ($\alpha$, $\epsilon$)-RDP if there is a Rènyi divergence of order $\alpha$ between any two neighbouring databases, and this divergence is less than or equal to $\epsilon$. RDP's straightforward privacy budget accounting makes it a practical choice as explained in [207]. In a scenario, where entities are distributed to provide data to a central point for data aggregator [208], distributed DP extends the definition of ($\epsilon$, $\delta$)-DP. It is possible that the data aggregator is dishonest and engages in collusion with some of the participants. With computational DP, an opponent that is computationally bounded takes the place of the unrestricted adversary that is employed in DP. Computationally DP techniques can provide more accurate query results by utilising a weaker adversary model [209]. Central (Global) DP (CDP) and Local DP (LDP) are the two different forms of DP. In the CDP, user data is accessible to the aggregator. The user data is first processed through noise by the aggregator before being shared with a third party for processing. The primary disadvantage of this approach is that user-sensitive data is accessible to the central aggregator. Users must all have trust in the aggregator to protect individuals' privacy and act honestly. In the CDP, noise addition proceeds through three different mechanisms: Gaussian [210], Laplace [211], and exponential [204]. The most popular mechanism in CDP is Gaussian, which is described in Equation (9). For a query function $f : D \longrightarrow R$ a randomised algorithm $M$ satisfies ($\epsilon$, $\delta$)-DP if

$$M(D) = f(D) + N\left(0, \sigma^2\right) \quad (9)$$

In the CDP, there is a special case in which noise can be added to the client side to ensure that clients do not depend on the server. This paradigm is referred to as the "LDP model" and was initially formalised by [212] and [213] first presented the LDP to the database community and it gained popularity with the work of [214]. Due to its successful implementation in end-user device apps, LDP has become increasingly popular. LDP is used by Google's Rappor [215] framework to protect users' browsing patterns by identifying frequently visited locations and configurations. To enhance user experience, Microsoft [216] further uses LDP to gather telemetry data. The deployments' trust model determines whether to use CDP or LDP.

A malicious server model prevents CDP from offering privacy protection. LDP lowers the accuracy of the model even while it shields the clients from rogue servers. Furthermore, the DP itself does not account for the malicious colliding client model. An approach would be to combine a hybrid solution with additional privacy-enhancing measures. Using SMPC and HE, it is still possible to protect against malicious server models in the solution without sacrificing accuracy. However, there is a cost associated with these methods, which involves extra computation and communication costs.

DP enables organisations to adjust their privacy level so that attackers are unable to access the correct user data. It prevents attackers from accessing perfect user data by applying differentially private computation for each query separately which leads to different answers for the same query by other researchers. These different approximate answers are still meaningful for performing statistical aggregations. DP aims to guarantee that a querier cannot reveal information specific to individual participants. Additionally, random noise addition ensures that any individual in the dataset can deny their specific information or even participation in the dataset. This deniability aspect of DP is important in the case of linkage attacks where attackers combine multiple sources to identify the personal information of a target individual. DP provides a quantifiable measure of privacy guarantees through the parameter $\epsilon$. By adjusting the value of $\epsilon$, data aggregators can control the level of privacy according to the sensitivity of the dataset.

There are several challenges and limitations of DP. The first challenge is that DP does not apply to individual-level analysis. Such analysis is not possible with DP-applied data. It prevents an analyst from learning information particular to specific individuals. For example, DP is not suitable for a bank that wants to determine instances of fraudulent activity. The second challenge is that DP does not support small data. Similar to sampling errors, the inaccuracy introduced by DP can be ignored for large datasets but it is not the case for small ones. For a small dataset, the noise added by DP can seriously impact any analysis based on it. The third challenge is that there is no consensus over the optimal value of $\epsilon$, *i.e.,* the level of distortion for the data to be both private and useful.

$\epsilon = 0$ is the perfect privacy case but it completely changes the original data and makes it useless. However, if the applications of DP become prevalent, guidelines to reach this optimality for various cases may be established in the future. The fourth challenge is that there is no simple answer for sharing personal data with DP without the consent of GDPR or CCPA compliance. It depends on the dataset, applied DP algorithm, and the parameter $\epsilon$. To be on the safe side, companies can list all processors of DP-applied data as data processors if data processing involves personal data usage. DP provides a way to manage the level of privacy vs utility. However, as already discussed, there is no agreement on the optimal level for this tradeoff yet. A white paper by Vitaly et al. [217] states that DP offers a powerful alternative to overcome the limitations of traditional anonymisation approaches and policymakers should work closely with researchers to formulate recommendations for it.

In summary, DP is more helpful when used for statistical analysis and general trends rather than identifying specific patterns or abnormalities in data. The following are the international standards that an organisation can use for the implementation of PETs.

- *ISO/IEC 20889:2018:* In compliance with the privacy principles outlined in ISO/IEC 29100, de-identification procedures are described and designed using the privacy-enhancing data de-identification approaches [218]. This standard outlines vocabulary, classifies de-identification techniques based on their attributes, and explains how to apply every approach to lower the likelihood of re-identification.
- *$\epsilon$-KTELO:* It is a framework for defining differentially-private computations [219]. It is a system and programming framework for implementing new and existing privacy algorithms into practice. New methods were implemented by $\epsilon$-KTELO to support the scalability and generality of $\epsilon$-KTELO operators. These are the techniques for computing lossless reductions of the data representation.

The following are the related projects and guidance that an organisation can incorporate to perform privacy-enhancing computations on user data.

- *ISO/IEC 29100:2011:* ISO/IEC 29100:2011 [72] is an international standard that provides a high-level framework for the protection of PII within ICT systems. It is general and places organisational, technical, and procedural aspects in an overall privacy framework.

### C. Privacy vs Utility

In the data de-identification process, it is possible that a significant amount of valuable information may be lost and the de-identified data thereafter have no use. The de-identified data is released to the public for usage in diverse applications. We need to consider the interpretation of data in terms of information loss when it is released for general purposes and the predictive performance of data in terms of data mining/ML tasks. The multiple privacy techniques enhance the privacy of user data; on the other hand, they could increase information loss. The information loss is measured by comparing the statistics between the original and de-identified datasets [220], [221]. The information loss measures the usefulness of the dataset after applying the particular privacy technique. The loss in information can be measured through the statistics changes that include means, variances, and correlations computation in the datasets.

Several researchers [14], [222], [223] have suggested assessing the de-identified data usefulness concerning data mining tasks. Predictive models are constructed using de-identified datasets and the usefulness of the de-identified dataset is determined by the models' prediction accuracy. The goal of de-identified data should be to be comparable to the original data as closely as possible to maximise data utility. The maximal utility may lead to a lower level of data protection, which may have an impact on businesses as well as data subjects. The trade-off between these measures is an interesting topic of research and achieving the balance between data privacy and utility usually requires substantial effort in applications of privacy techniques [14], [224], [225].

### D. Privacy vs Security

In the digital world, user privacy and security are interrelated terms but they are two different concepts. User privacy deals with user personal information and how it can be viewed and accessed. Security, on the other hand, is the protection of user personal data and information. For instance, when a user downloads an application on a smartphone, it asks the user to accept a privacy policy. This policy will specify the user data that the application will collect and how it will be utilised. Security aims to protect user personal information and data using cyber security tools and techniques.

Implementing strong security requirements might require a large amount of user data collection and monitoring, which could compromise user privacy. For instance, Khan, Ghanem, and Coffele [226] have discussed several methods with compartmentalisation techniques to improve user data protection through integrated and multi-layered techniques. Askin, Kutta, and Dette [227] examine statistical techniques for ensuring DP protects individual data within large data sets. These techniques are important in the healthcare domain, where the discrete measurement of user medical conditions in terms of mm-wave sensing [228] is required. With the increased use of user surveillance and large data analytics, Prince et al. [229] discussed the importance of user privacy awareness and how users are becoming more concerned about privacy.

Emerging technologies, say AI and Mobile Edge Computing (MEC), present new security and privacy challenges. Wang et al. [230] use the AI perspective on the security and privacy of MEC that uses advanced algorithms and protocols to protect data processing at the edge of networks. Similarly, Iwaya et al. [231] conducted a systematic mapping study on the security and privacy of mobile and ubiquitous health systems by defining the need for comprehensive security measures that do not compromise patient privacy. Furthermore, Yang et al. [232] showed that privacy can be maintained

TABLE VI
DETAILED COMPARISON OF PETS IN COMPLIANCE WITH INTERNATIONAL REGULATORY STANDARDS WITH COMPARISON PARAMETERS OF ORGANISATION, STANDARD NAME, IDENTIFICATION NUMBER, PUBLICATION YEAR, REVISION YEAR, CONTINUOUS UPDATION, PRIVACY TECHNIQUES, ADVANTAGES, LIMITATIONS, AND THE MAIN FOCUS OF STANDARDS

| Organisation | Standard Name | Identification Number | Publication Year | Revision Year | Continuous Updation | Privacy Techniques | Technique Advantages | Technique Limitations | Main Focus |
|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC | ITST-**Encryption Algorithms** | 18033 | 2015 | 2021 | Yes | HE | Encrypted computation | Computational overhead | Homomorphic encryption algorithms, parameters and operations. |
| ISO/IEC | Information Technology-**Trusted platform module library** | 11889 | 2009 | 2015 | No | TEE | High security | Limited support | Trusted platform module architectural. |
| ISO/IEC | Privacy Enhancing Data De-identification Techniques–**Terminology and Classifications** | 20889 | 2018 | – | No | DP | High privacy | Low utility | Data de-identification techniques |
| ISO/IEC | ITST-**Secret Sharing** | 19592 | 2017 | – | No | SMPC | – | – | Cryptographic secret sharing scheme specifications |
| ISO/IEC | Information Security **Secure Multiparty Computation-Part 1** | 4922-1 | 2023 | – | Yes | SMPC | – | – | SMPC terminology and specification |
| ISO/IEC | Information Security **Secure Multiparty Computation- Part 2** | 4922-2 | – | – | No | SMPC | Privacy preservation | Computational complexity | Secure multiparty computation and secret sharing |
| IEEE | **Framework for Trusted Execution Environment** | 2830 | 2021 | – | Yes | TEE | High security | Limited support | Trusted execution environment in privacy-preserving ML |
| IEEE | **Secure Computing based on TEE** | P2952 | 2022 | - | Yes | TEE | High security | Limited support | Cyber security applications of TEE applications |
| IEEE | **Recomended practices for SMPC** | 2842 | 2021 | - | Yes | SMPC | – | – | SMPC framework with security levels and use cases. |
| OMTP TR1 | **Advanced Trusted Environment** | OMTP | 2009 | - | No | TEE | – | – | Mobile phone TEEs requirments and examples. |
| GlobalPlatform | **TEE Low-level API** | GPD-SPE-55 | 2018 | - | No | TEE | – | – | Highly technical details for TEEs industrial products. |

without sacrificing the utility of data analytics by using privacy-preserving data analysis methods, such as K-Means clustering with local DP. In domains such as IoT and smart cities, these techniques are important for providing secure, privacy-preserving insights from large datasets.

In communication networks, Qin et al. [233] discussed enhancing primary user security in cognitive radio networks through secondary user selection, which defines the complex combination between user privacy and network security that ensures the security and privacy of user data transmission. Similarly, Khan and Asif [234] examine secure 5G network communications using reflective in-band full duplex Non-Orthogonal Multiple Access (NOMA), which uses advanced techniques to provide secure, high-efficiency data transmission. As new technologies and threats arise, the complex relationship between security and privacy requires constant monitoring. For example, ML and AI improve security and privacy but also create issues with bias and data privacy. Organisations may develop systems that are secure and supportive of user privacy by using a comprehensive strategy that takes into account user demands and rights. This will promote confidence and trust in the digital ecosystem.

**Summary.** In this section, we present a comprehensive overview of international standards for PETs, highlighting key insights into their standardisation, techniques, advantages, limitations, and main focuses as illustrated in Table VI. ISO/IEC standards cover various aspects such as encryption algorithms for encrypted computation with homomorphic encryption, trusted platform module library for high-security architectural support, and privacy-enhancing data de-identification techniques focusing on high privacy but low utility in data de-identification. The main disadvantage of HE and SMPC is high computational complexity while a TEE has limited operational support. Additionally, IEEE standards contribute to the field with frameworks and recommended practices for TEE ensuring high security. Furthermore, standards from OMTP TR1 and GlobalPlatform use specifics of TEEs, detailing requirements, and low-level APIs for mobile phone TEEs, showcasing a specialised focus on industrial products and technical implementations. Similarly, Table VII highlights the importance of standardisation efforts across different PETs to ensure interoperability, security, and effectiveness in PETs. It summarises international standards for PETs that an organisation can use to enhance user privacy. In this table, we present a comparative analysis of various PETs with their descriptions, privacy risks, protection mechanisms, advantages, limitations, and associated standards. The TEE standards, such as those from OMTP TR1, IEEE, and ISO/IEC, emphasise the secure outsourcing of sensitive data for computations that ensure efficient computation without information loss. TEEs face challenges such as side-channel attacks and computational complexities. The HE standards focus on secure operations on sensitive data in compliance with ISO/IEC standards that have benefits including information loss prevention but need to address issues involving high bandwidth and latency. The SMPC standards, including ISO/IEC and IEEE, enable

TABLE VII
COMPARISON OF VARIOUS ASPECTS OF PETS IN COMPLIANCE WITH INTERNATIONAL REGULATORY STANDARDS WITH PARAMETERS OF TECHNIQUE, THEIR DESCRIPTION, PRIVACY RISK, PROTECTION AREA, ADVANTAGES, LIMITATIONS, AND CORRESPONDING STANDARDS

| Techniques | Description | Privacy Risk | Protection | Advantages | Limitations | Standards |
|---|---|---|---|---|---|---|
| **Trusted Execution Environment** | Securely outsource sensitive data for computations | Reveals Sensitive Attributes | Computation and storage | Efficient computation and zero loss of information | Side-channel attacks and distributed big datasets' computational complexity | - OMTP TR1<br>- GPD-SPE-055<br>- IEEE 2830-2021<br>- IEEE P2952<br>- ISO/IEC 11889 |
| **Homomorphic Encryption** | Secure operations on sensitive data | Reveals Sensitive Attributes | Computation and storage | Information loss and operation computation | High bandwidth and Latency Issues | - ISO/IEC 18033 |
| **Secure Multi-party Computation** | Provides joint analysis of sensitive data | Reveals Sensitive Attributes | Computation | No TTP | High computational complexity | - ISO/IEC 19592-1<br>- ISO/IEC 19592-2<br>- ISO/IEC 4922<br>- IEEE 2842 |
| **Federated Learning** | Provides remote decentralised data for training algorithms | Reveals sensitive individual's information and presence | Computation | Very little loss of information | Model inversion and Membership inference attacks | No Standard |
| **Differential Privacy** | Prevent individuals disclosure during information release | Reveals individual's sensitive information | Computation and storage | Formal Mathematical Proof and Quantifiable Privacy Protection Levels | Random Noise and Information Loss | - ISO/IEC 20889<br>- NIST |

joint analysis of sensitive data without a TTP, yet face high computational complexity. Additionally, DP standards from ISO/IEC and NIST, prevent individual disclosure during information release through formal mathematical proofs. It provides quantifiable privacy protection levels but needs to address challenges like random noise and information loss. Notably, FL lacks a standardised approach that presents a challenge regarding individual privacy and susceptibility to attacks including model inversion and membership inference. This detailed comparison explains the diverse strategies and considerations in privacy protection and the ongoing efforts to standardise and mitigate associated risks.

## VIII. REAL WORLD CASE STUDIES

In this section, we discuss several use cases that illustrate the many roles that privacy plays in real-world scenarios. These scenarios aim to demonstrate situations in which privacy techniques may help to achieve a more comprehensive data goal. We choose these use cases based on their applicability to important data-driven real-world problems.

### A. Health Care Research

Recent developments in Artificial Intelligence (AI) provide unprecedented opportunities in healthcare research that involves audio, and medical imaging. An estimated 50 petabytes of data are produced by hospitals worldwide each year [235]. Patient health data is essentially private, and if it is exploited or privacy is violated, there may be consequences for public mistrust.

*1) Privacy in Medical Imaging:* In healthcare research, medical imaging is a vital tool that provides researchers and doctors with precise pictures of the inside of the human body. These pictures help in disease diagnosis, tracking the progress of the disease, and assessing the effectiveness of treatment. Medical imaging methods include Magnetic Resonance Imaging (MRI), Computed Tomography (CT) scans, ultrasounds, and X-rays. Each type of imaging technology offers a unique set of data about the organs and tissues of the body. One of the most traditional and widely used types of medical imaging is X-rays. They are especially helpful for examining bones and identifying breaks or fractures. CT scans often combine with X-ray images taken from various perspectives to produce a more in-depth image of the body. tumours, internal bleeding, and other diseases that might not be evident on regular X-rays are often identified with this technique. Ultrasound is a common diagnostic tool for diseases of the liver, kidneys, and heart. It creates images of soft tissues by using sound waves.

Magnetic fields and radio waves are used in MRI, a form of scan that creates detailed images of the interior organs and tissues of the body. The pictures generated by MRI provide important information regarding the diagnosis and staging of disease growth. ML algorithms can be trained on sets of MRI data to identify certain features or anomalies in pictures. With this technology, researchers may analyse a vast number of images to find patterns that connect elements such as genetics, patient behaviour, and environmental factors to brain function.

- *Privacy Challenge:* Sensitive health information about patients may be revealed by big data analytics and MRI imaging. A person's presence in a dataset may contain sensitive information. Neuroimages can occasionally be re-identified, even though names, addresses, and scan dates can be removed from the images to de-identify them.
- *FL based Solution:* In FL, training models are "sent" to remote data-holding devices (say servers) for local training. It is a sort of remote execution that makes it

possible for researchers to train models using data from other sites without having to access those data sets. For instance, a FL approach would enable researchers at several universities with access to neuroimaging data to train their models on imaging data from all participant data that would otherwise be "invisible" to analysts.

- *DP based Solution:* Neuroimage re-identification can also be avoided by using the DP technique. To achieve DP, a random noise must be added to the outputs. As a result, cross-referencing with publicly available data becomes more challenging. By referring to a predetermined privacy budget or the amount of data that is considered acceptable to be leaked from the site, the controller can adjust performance-privacy trade-offs. DP also makes it possible to quantify privacy risk as the probability of re-identification.

*2) Privacy in Audio Data:* Audio data is an important tool in healthcare research because it can provide valuable insights into various health conditions that help improve patient care. Researchers and healthcare providers can diagnose diseases, monitor patient progress, and enhance treatment plans by analysing the patterns and characteristics of speech and other sounds. Diagnosing diseases is one of the most significant parts of audio data in healthcare research. For instance, a person's voice alterations can provide important indications about their health. Speech abnormalities, such as a weaker voice, a slower speech tempo, or vocal tremors, are common in people with Parkinson's disease. Through the process of capturing and analysing these speech patterns, doctors can accurately diagnose and monitor the advancement of Parkinson's disease. Similarly, mental health issues can be determined from audio data. Anxiety or sadness can cause audible vocal changes in people, such as a flat tone, slurred speech, or extended pauses. Healthcare professionals can determine warning indications of mental health problems and track patients' treatment responses over time by analysing these voice traits.

One kind of dementia that impairs a person's memory, motor abilities, and cognition is Alzheimer's disease. Researchers studying Alzheimer's disease look for non-invasive methods to identify and screen Alzheimer's disease that are increasingly turning to speech and audio data [236]. Speech content, such as vocabulary range, and speech rhythm, such as hesitation owing to word-finding difficulties, can both be impacted by Alzheimer's disease. ML models can be trained with audio data that includes both verbal and nonverbal vocalisations, such as breathing, coughing, and speech pauses to forecast illness. Therefore, vocal biomarkers offer a promising direction for diagnosing Alzheimer's disease and related studies when combined with AI.

- *Privacy Challenge:* Vocal data is susceptible to re-identification due to the large number of publicly accessible, recognisable audio files (such as those on YouTube), which facilitate easy re-identification. Sensitive information is revealed by an individual's presence in a dataset, in addition to the content of the data.
- *Anonymisation based Solution:* One solution is to combine privacy techniques with audio-specific anonymisation techniques for securing audio biometric data. To change a patient's vocal quality, for instance, voice transformation procedures can be applied that include AI-based tools, such as Google Cloud's Speech API, that may automate the transcription of audio data. After that, an ML algorithm can scan the audio data and identify key elements, such as names, dates, ages, and locations. The identifiers can be quickly modified by emphasising distinguishable elements.

### B. IoT

The net zero carbon emissions are part of a collective effort to mitigate climate change. In climate technologies, digital twins are an emerging area of research that is a virtual counterpart of a physical object such as a wind turbine or process such as economic transaction patterns. It works as a decision-support tool after integrating sensors with other models and physical-virtual systems. The establishment of best practices and privacy solutions is the key to digital twins adoption.

The development and evaluation of digital twins have several important phases. First, it needs to build a virtual model that precisely copies the real-world object or process that it simulates such as a product production line or a wind turbine. It involves integrating historical data, real-time sensor data, and other appropriate data that ensure the twin's precision and reliability during the simulation of real-world conditions. To guarantee accuracy and efficacy, the digital twin must then be verified and calibrated against its physical counterpart. The performance and behaviour of the digital twin are compared to actual data obtained from the physical asset as part of this validation procedure. It assists in discovering any variations or potential areas for improvement in the twin. After validation, the digital twin provides insights into operational efficiencies, predictive maintenance, and performance optimisation that make it a useful tool in the decision-making process. It gathers and processes data from sensors and other sources continually to refine its predictions and recommendations over time. Other aspects of assessing digital twin's evaluation are to test its scalability, compatibility with other systems, and resistance to different operating scenarios and conditions. Security and privacy considerations of digital twins are critical throughout the development and deployment process to protect sensitive data and ensure compliance with regulations.

- *Privacy Challenge:* Digital twin development and evaluation require energy data for potential research and innovation. The energy data is communicated between digital twins and physical assets. Data sharing in this case raises privacy concerns among many stakeholders including people, businesses, the government, and regulators.
- *Privacy Solution:* Privacy solutions should be implemented in the coupled digital twin-asset ecosystem at several key points.
  - *Individual Privacy Solutions:* The smart meters are used to measure the end-user's real-time energy consumption. The roll-out of smart meters in Europe and the United Kingdom (UK) raises privacy concerns for the collection of energy consumption data [237].

TABLE VIII
THE PRIVACY CHALLENGES AND THEIR SOLUTIONS IN REAL-WORLD CASES

| Domain | Sub Domain | Limitations | Privacy Challenge | Privacy Solution |
|---|---|---|---|---|
| **Health care** | Medical Imaging | Data minimisation and Re-identification | Revelation of patient-sensitive health information | Use FL Technique or DP |
| | Medical Audio Data | | Re-identification of audio data | Use audio-specific anonymisation techniques |
| **IoT** | – | Few privacy solutions and best practices | Data sharing among stakeholders | Use Synthetic Data or DP techniques |
| **Social Media Data** | – | Public mistrust and lack of technology | Revelation of personal sensitive information | Use FHE technique |

Despite this privacy concern, smart meter data offers tremendous potential for renewable energy integration. The most efficient way to address the privacy limitations of smart meters is to use non-cryptographic techniques such as adding random "noise" to the smart meter energy consumption dataset using DP. The other approach is to include spatial aggregation, which enables load balancing without gathering data at the home level by arranging smart meters in a geographical cluster.

– *Government Privacy Solutions:* Optimising the advantages of an energy digital twin will require combining summary statistics from several energy consumption data sets. Relevant aspects of user data could be shared via synthetic data that allow government and regulatory authorities to decide without accessing entire datasets. The data comes from physical assets used to monitor and control the grid and national power distribution system. The TEE combined with HE provides security to collaborative cloud computing from attacks.

### C. Social Media Data

Social media, including gaming platforms, budgeting tools, wellness apps, and networking sites, is used by more than 4 billion people worldwide to create and share content, track their actions, and get satisfaction [238]. The degree to which users engage and produce material on these platforms has increased the value of social media services as a source of research data. Users frequently offer their personal information, such as a self-described location or an uploaded profile photo. The majority of metadata, such as the timestamp on a message or the geotag on an image, is automatically recorded. Social media data usage can be resource-intensive and invasive, despite its beneficial value. Public mistrust and technological limitations make it difficult to access and use social media data.

The social media data is diverse and broad, which can offer researchers several possibilities by providing them insights into communication patterns, societal trends, and human behaviour. To ensure user privacy and trust, the collection and usage of social media data for research purposes must follow ethical considerations and transparency guidelines. Social media platforms such as Facebook, Twitter, and Instagram offer Application Programming Interfaces (APIs) through which researchers can routinely access social media data. These APIs enable regulated access to data such as posts, comments, likes, and user profiles based on platform restrictions and user permissions. Transparency requires clear communication about the data sources, data collection techniques, and study goals. Researchers need to be transparent about how they manage and examine data, including any processing methods or algorithms used to extract insights. This transparency brings credibility and makes it possible for more researchers to verify or reproduce findings. When using data from social media, ethical considerations are also very important. For sensitive or identifiable data, researchers must obtain informed consent and, whenever feasible, anonymise data to protect user privacy and anonymity. Compliance with legal requirements and platform terms of service is necessary for data usage and protection.

- *Privacy Challenge:* Social media data include personal information such as an individual's age, gender, political preference, and photos that can reveal a location, place of residence, and romantic status. Technical difficulties arise when it comes to gathering and utilising social media data in a way that protects privacy. Cross-platform studies at the user level may be difficult or nearly impossible if social media users post anonymously or under pseudonyms that do not match across platforms.
- *DP based Solution:* DP is used to hide information about individual users within a dataset before it is released for research purposes but there are restrictions on the inclusion of noise and the integration of data from various sources. Researchers can use FHE or other cryptographic techniques to query data holders without actually asking for data on social media networks.

**Summary:** We have discussed real-world privacy challenges and their corresponding solutions across different domains as listed in Table VIII. In the healthcare sector, challenges including the revelation of patient-sensitive health information in medical imaging and the re-identification of audio data in medical audio data are addressed through techniques such as FL or DP, and audio-specific anonymisation techniques, respectively. These techniques focus on data minimisation and privacy-preserving measures. In the IoT domain, where few privacy solutions and best practices exist, challenges

related to data sharing among stakeholders can be mitigated using synthetic data or DP techniques that offer robust privacy protection. Furthermore, in the social media domain, challenges arise from public mistrust and technological limitations leading to the revelation of sensitive information. These challenges are handled with FHE techniques that emphasise enhanced privacy measures to regain public trust and safeguard personal data. This comparative analysis highlights the domain-specific nature of privacy challenges and defines the importance of privacy solutions to address them effectively in diverse contexts.

## IX. Privacy Tools

In this section, we discuss several privacy tools, their purposes, and implementation details that help in the characterisation and quantification of user privacy. Certain tools make it possible to evaluate various privacy mechanism configurations, which in turn makes it possible to evaluate the degree of privacy that has been achieved.

### A. $\mu$-ARGUS

$\mu$-ARGUS [239] is the first tool that provides privacy in published data. This tool uses several privacy techniques, such as noise addition, $k$-Anonymity, and microaggregation, to create de-identified data that will be used in scientific research.

### B. ARX Data Anonymisation Tool

Sensitive personal data can be anonymised with this open-source tool [240]. Users can import, configure, examine, analyse, and export data with this tool. The user can also specify a privacy model at each stage. Several privacy methods, including $k$-anonymity, $l$-diversity, $t$-closeness, and DP, have already been implemented using this tool. This tool does not use any attack or adversary models.

### C. Amnesia

This tool's primary goal is to use generalisation and suppression procedures to turn relational and transactional databases into anonymised data [241]. This tool supports k-anonymity mechanisms. Amnesia aims to exclude from public data any sensitive information that could be used as identifying information. Furthermore, this tool enables the removal of QIDs in addition to direct identifiers.

### D. SdcTools

SdcTool provides free statistical disclosure control capability in the form of open-source software [242]. Sdcmicro is a tool that is created to anonymise user data. It uses anonymisation techniques such as suppression, $k$-anonymity, microaggregation, and several other techniques. In terms of implementation, sdcMicro comes in the form of an R-package and is freely available for research purposes.

### E. Anonimatron

This is an open-source data anonymisation for structured databases and files [243]. Its primary objective is to de-identify or anonymise user-specific data. This tool saves that relation in a synonym and changes an attribute's value in the database to achieve it. All of the database's tables use these synonyms, keeping the database similar while remaining anonymous. The synonyms are kept in a file that can be downloaded and used at a later time.

### F. Aircloak

This tool protects privacy and makes use of a patented technique for data anonymisation [244]. Aircloak supports all types of data that include unstructured text. Several techniques such as $k$-anonymity, and DP noise served as the foundation for Aircloak's anonymisation process. Aircloak offers a dynamic addition of noise in the anonymisation process based on these principles.

### G. UTD Anonymisation ToolBox

UTD anonymisation toolbox [245] implements Datafly [246], $k$-Anonymity, incognito, $l$-diversity, $t$-closeness, and Anatomy [166]. UTD toolbox is available for free download and public use by researchers. This toolbox has scalability issues when handling larger datasets.

### H. Cornell Anonymisation Toolkit

This toolkit [247] uses a generalisation technique for data transformation. In addition, this tool is a research prototype and has problems with scalability when dealing with big data sets.

### I. OpenAnonymiser

This tool was developed by computer science researchers from the University of Vienna, Austria in 2008 [248]. It can automatically anonymise data according to user-selected privacy models and risk thresholds, which can be controlled through a Web-based graphical user interface. The anonymisation algorithm implemented by OpenAnonymiser is quite simple with limited scalability and flexibility. Data and configuration settings need to be provided in an application-specific XML format. The tool is published as open-source software running on all major operating systems (Windows, Linux, and MacOS).

### J. TIAMAT

It stands for 'Tool for Interactive Analysis of Microdata Anonymisation Techniques' and was developed by Dai et al. [249]. This tool supports different anonymisation algorithms, such as Mondrian [250] and k-Member [251]. It also supports three different privacy and risk models for analysing and optimising the utility of output data. The processes supported by TIAMAT are made available through a cross-platform graphical user interface that runs on all major operating systems, with a focus on comparing the properties

TABLE IX
COMPARISON OF VARIOUS ASPECTS OF PRIVACY TOOLS WITH COMPARISON PARAMETERS OF TOOL NAME, OPEN-SOURCE, SOFTWARE-BASED, WEB-BASED, RELEASE YEAR, PRIVACY MECHANISM, COST, PRIVACY EVALUATION, AND UTILITY EVALUATION

| Tool | Open-source | Software-based | Web-based | Release Year | Privacy Mechanism | Cost | Privacy Evaluation | Utility Evaluation |
|---|---|---|---|---|---|---|---|---|
| **$\mu$-ARGUS** | Yes | Yes | No | 2014 | Non-perturbative & Perturbative | No | Yes | No |
| **ARX** | Yes | Yes | No | 2020 | Non-perturbative & Perturbative | No | Yes | Yes |
| **Amnesia** | Yes | Yes | Yes | 2019 | Non-perturbative | No | Yes | Yes |
| **SdcMicro** | Yes | Yes | No | 2017 | Non-perturbative & Perturbative | No | Yes | Yes |
| **Anonimatron** | Yes | Yes | No | 2020 | Anonymisation | No | No | No |
| **Aircloak** | No | Yes | No | 2014 | Non-perturbative & Perturbative | Yes | Yes | Yes |
| **UTD** | Yes | Yes | No | 2014 | Non-perturbative & Perturbative & De-associative | No | Yes | Yes |
| **Cornell** | Yes | Yes | No | 2009 | Non-perturbative | No | Yes | Yes |
| **Open Anonymiser** | Yes | No | Yes | 2008 | k-anonymity | No | Yes | No |
| **TIAMAT** | No | Yes | No | 2009 | k-anonymisation, Mondrian, k-member | - | Yes | Yes |
| **SECRETA** | No | Yes | Yes | 2014 | Perturbative | - | Yes | Yes |
| **PrioPrivacy** | Yes | Yes | No | 2019 | Non-perturbative & Perturbative | No | Yes | Yes |
| **Probabilistic anonymisation** | Yes | Yes | No | 2018 | Non-perturbative & Perturbative | No | Yes | Yes |

of different anonymisation techniques. However, this tool is not available for download and its source is not open.

### *K. SECRETA*

This tool is developed by Poulis et al. [252]. The main focus of this tool is on analysing the effectiveness and efficiency of anonymisation algorithms for tabular as well as set-valued data. It features a cross-platform graphical user interface that operates in two modes: evaluation and comparison. Input data have to be provided as CSV files. However, analogously to TIAMAT, this tool and its source code are unfortunately not available to the community [253].

### *L. PrioPrivacy*

The Research Studio Data Science developed the PrioPrivacy tool that was first released in 2019 [254]. This tool anonymises tabular data and provides a high degree of flexibility in the selection of the variables that must be kept private for the use of anonymised data. It is an extension of the ARX Data Anonymisation Tool with additional features. As PrioPrivacy is built on ARX, it is also implemented in Java, which makes it interoperable with all major platforms. It is under active development.

### *M. Probabilistic Anonymisation*

It was developed by Avraam et al. in 2018 [255]. This tool adds random noise to data to perturbate it instead of directly basing its approach on privacy and utility models. To be more precise, to avoid correlation with other data, normally distributed random noise with user-specified variances is added. Similar to sdcMicro, the tool can be used with data that is provided in a variety of forms because it is offered as a package for the R statistics programming environment.

**Summary.** We provide a comparative analysis of various privacy tools based on several key aspects as illustrated in Table IX. Each tool's open-source availability, software-based nature, and Web-based accessibility are discussed, alongside their release years. Privacy-preserving mechanisms employed by these tools, including both non-perturbative and perturbative techniques, are specified that offer insights into their operational approaches. Additionally, the table highlights the cost implications of these tools and their evaluations regarding privacy and utility, which is crucial for assessing their effectiveness and practicality in real-world applications. We have observed that the ARX is an open-source and software-based tool that offers both non-perturbative and perturbative privacy-preserving mechanisms. It is particularly suitable for scenarios where a balance between privacy protection and utility preservation is essential. Its recent release indicates ongoing development and potential adaptation to evolving privacy challenges. However, the choice of the best tool ultimately depends on specific use-case requirements and preferences regarding factors such as cost, evaluation methodologies, and the nature of the data being handled.

## X. Lesson Learned and Future Research Directions

In this section, we discuss the lesson learned from existing research on the characterisation and quantification of user privacy and elaborate further on open problems present in the adoption of international standards for the preservation of user privacy which was discussed in Sections V,VI, and VII. The following are the main challenges in the privacy domain:

- *New International Standards:* A new international standard for user privacy is important to establish unified guidelines, ensuring consistent protection of personal data across borders and enhancing trust in digital services worldwide. For instance, in FL, as discussed in Section VII, a new international standard for user privacy is crucial to establish clear guidelines and protocols that ensure robust protection of personal data while facilitating collaborative ML across distributed networks.
- *New Privacy Metric and Notions:* The fundamental challenge for an organisation is to apply privacy techniques having minimal information disclosure and loss. Currently, there is no one-size-fits-all solution for data privacy and the standard privacy techniques do not provide a one-size-fits-all solution for data privacy in the modern data-rich world. It means how data can be gathered, exchanged, and analysed has become more sophisticated with the advancement of technology decreasing the efficacy of existing privacy techniques. The design of new privacy metrics and concepts helps in addressing these issues.
- *Efficient Privacy Techniques:* These are used to provide privacy solutions that can effectively produce optimal privacy vs utility data for public health, finance, and other sectors. It involves the implementation of several key techniques into practice such as personal identifiers can be removed from data by data anonymisation and de-identification, which ensures that no one can be directly linked to the data. DP hides specific entries in the data while maintaining general trends for precise analysis through the addition of noise. Strong access controls and encryption protect data against unauthorised access and security breaches. Data minimisation makes sure that information is only used for the intended reasons and it aims at minimising the amount of unnecessary information that is collected. Regular PIAs ensure that privacy security measures remain up to date with changing data practices by supporting the identification and mitigation of any potential risks. User data is further protected by multi-layered safety measures, which strengthen the defence against possible threats.

### A. Open Problems in International Standards

The preservation of user privacy is a complex issue, and implementation of international standards to address user privacy challenges is important for ensuring consistency, interoperability, and protection of individuals' rights across borders.

*1) Jurisdictional Variability:* Privacy laws and regulations vary significantly between different countries, which creates challenges for multinational organisations to comply with multiple sets of requirements. Harmonising these regulations while respecting cultural differences and legal traditions poses a significant challenge. One example of jurisdictional variability in privacy challenges is the difference between the EU's GDPR and the privacy landscape in the U.S. The GDPR applies to all organisations processing the personal data of individuals in the EU, regardless of where the organisation is located. It imposes strict requirements on data controllers and processors, including obtaining explicit consent for data processing, implementing data protection measures, and notifying authorities of data breaches. In the U.S., privacy laws are fragmented, with sector-specific regulations (*e.g.,* HIPAA [256] for healthcare, COPPA [257] for children's data) and state-level laws (*e.g.,* California Consumer Privacy Act, or CCPA [12]). There is no comprehensive federal privacy law similar to the GDPR, leading to a patchwork of regulations that vary across states and industries.

**Lesson Learned.** Countries have very different privacy laws, so it is very challenging for multinational corporations to comply with them all. For instance, the U.S. needs one federal law similar to the GDPR rather than a collection of rules governing various industries and states, which could be difficult for multinational organisations to manage and enforce these regulations worldwide.

**Future Directions.** There is a need for continuous efforts to harmonise privacy regulations globally, such as the GDPR in Europe and the APEC Privacy Framework [258] in the Asia-Pacific region. Harmonisation aims to create consistent standards for data protection across jurisdictions that increase the cooperation between regulatory authorities.

*2) Cross-Border Data Transfers:* With the increase in the globalisation of data flows, the privacy and security of personal data transferred across borders pose a significant challenge. Data localisation requirements and restrictions on international data transfers can create problems for data-driven innovation and economic growth. For example, in the case of Personal Data transfer from the EU to the U.S., the GDPR imposes strict requirements on the transfer of personal data outside the European Economic Area (EEA). It prohibits transfers to countries without an "adequate" level of data protection unless specific safeguards are in place.

To facilitate data transfers between the EU and the U.S., the Privacy Shield Framework [259] was established in 2016. It allowed certified U.S. companies to receive personal data from the EU in compliance with GDPR requirements. However, the Privacy Shield was invalidated by the European Court of Justice in the "Schrems II" ruling [260] in July 2020. The court cited concerns over U.S. surveillance practices and the lack of effective remedies for EU citizens. In the absence of the Privacy Shield, organisations rely on Standard Contractual Clauses (SCCs) [261], which are approved by the European Commission, to legitimise data transfers to countries without adequacy decisions. While SCCs remain a valid mechanism for cross-border data transfers, the "Schrems II" ruling highlighted the need for organisations to conduct

assessments of the destination country's legal regime and provide additional safeguards if necessary.

**Lesson Learned.** The international exchange of personal data increases threats to security and privacy. Restrictions on international data transfers and domestic data retention laws may discourage innovation and economic expansion. For instance, there are strict rules for moving data outside of the European Economic Area under the EU's GDPR. The Privacy Shield, which facilitated data movement from the EU to the U.S., was declared invalid. Standard Contractual Clauses (SCCs) are now used by organisations to organise lawful data transfers; however, they still need to evaluate and protect against legal risks in the country of destination.

**Future Direction.** Organisations need unified rules that facilitate cross-border data transfers for performing innovation in their products, which leads to economic growth. They are exploring alternative mechanisms for cross-border data transfers, such as Binding Corporate Rules (BCRs) [262], which are internal data transfer policies approved by EU data protection authorities. Some organisations are considering implementing technical measures, such as encryption and pseudonymisation, to enhance data protection during transfers and reduce the risk of unauthorised access. The use of encryption technology comes under the encryption export control laws that prevent the unauthorised transfer of cryptographic technology to individuals, organisations, and countries deemed as adversaries. The Wassenaar arrangement [263] harmonises encryption export control policies among participating countries. It promotes consistent standards for regulating the export of encryption technology while balancing the need for security, privacy, and innovation.

*3) Emerging Technologies:* The rapid advancements in technologies such as AI/ML, biometrics, and IoT bring new privacy challenges. These technologies often involve the collection and processing of large amounts of personal data, raising concerns about surveillance, discrimination, and unauthorised access. For example, an IT company specialising in healthcare devices released a new wearable fitness tracker device. The wearable device collects sensitive health data, including heart rate and sleep patterns, which can reveal intimate details about users' lifestyles and health conditions. The storage of health data on wearable devices or associated mobile apps poses security risks, such as data breaches or unauthorised access by malicious actors. In addition, the long-term retention of user data by wearable device manufacturers may pose risks to privacy, as outdated or unnecessary data could be exploited if accessed by unauthorised parties. To mitigate these risks, wearable device manufacturers providing users with options to delete or anonymise their data can mitigate these risks.

**Lesson Learned.** The rapid development of technologies such as AI, biometrics, and IoT presents novel privacy challenges since they collect and manage massive amounts of personal data. It raises concerns about monitoring, bias, and unapproved data access. For instance, the fitness tracker of a healthcare organisation collects sensitive health information that raises concerns about data breaches and improper use of out-of-date information. The manufacturers need to enable users to remove or conceal their data in order to reduce these risks.

**Future Direction.** The integration of privacy considerations into the design and development of products and services is known as privacy by design and default. It provides a framework for integrating privacy protections into the design and operation of systems, products, and services which enhance user privacy and ensure compliance with international standards and regulations. As we discussed in Section VII, international standards can promote the adoption of PETs and practices across industries that promote a culture of privacy protection and accountability, ultimately benefiting users and organisations.

### *B. Open Problems in Privacy Metrics*

A privacy metric is a quantification tool that is used to measure how much privacy a user has in the system. We have discussed privacy metrics in Section VI that still have some open problems.

*1) Privacy Linkage:* Privacy linkage refers to the case when one user's actions affect multiple users' privacy such as in social networks [264] or location privacy [265]. The privacy linkage measures how an existing privacy metrics value varies with increasing dependency. It is computed using a difference [266] or comparing absolute values [267]. The main problem with privacy linkage is that it is difficult to quantify the impact of an increase in user dependence on privacy. Achieving this requires the use of time-consuming and complex methods.

**Lesson Learned.** In privacy linkage, measuring the extent to which dependencies affect overall privacy is a difficult task because the actions of one user can impact the privacy of other users, *e.g.,* in social networks or location services. This measurement is quite challenging to quantify and requires time-consuming, advanced techniques.

**Future Direction.** One possible future direction is to develop new metrics that specifically take linkage into account. In this situation, the metrics that quantify the effects that one user's actions on the privacy of other users may be advantageous.

*2) Aggregation of Privacy Metrics:* It can be useful to aggregate (or compose) metrics in scenarios that involve a large number of users, such as in the case of the communication system. Aggregating privacy metrics relies on the quality and reliability of the underlying data sources. Inaccurate or incomplete data can lead to biased or misleading aggregated metrics, undermining their usefulness and trustworthiness. Privacy metrics may need to be aggregated from diverse sources, such as different organisations or systems, each with its own data formats, standards, and quality. Integrating heterogeneous data sources while maintaining privacy and consistency presents a significant challenge.

**Lesson Learned.** In aggregating privacy metrics for several users, it is mainly dependent on the accuracy and consistency of the data like in communication systems. Metrics that are biased or misleading might be produced from incomplete or inaccurate data, which reduces their significance. It can be difficult to aggregate data from several sources, each of which

has unique formats and standards. It is important to manage data carefully to ensure consistency and user privacy.

**Future Direction.** One possible direction is to develop context-aware aggregation approaches that consider the specific context in which data is aggregated and used. This involves incorporating contextual factors, such as user profiles, data sources, and application domains to tailor aggregation methods and privacy protections accordingly. The other possible direction is to investigate multi-level aggregation techniques that enable hierarchical aggregation of privacy metrics at different levels of granularity. This allows for balancing between preserving individual privacy and deriving useful insights at various aggregation levels. Developing privacy metrics and aggregation methods tailored to emerging technologies, such as IoT, AI, and blockchain, poses unique privacy challenges that require specialised approaches for aggregating and analysing privacy metrics [268]. In blockchain, privacy metrics evaluate how well the system protects user identities and transaction information. Important metrics are secrecy (the degree to which transaction data, such as amounts, are kept private), anonymity (the degree to which transactions are difficult to associate with an individual), and unlinkability (the degree to which it is challenging to associate various transactions with the same user). Even though blockchain data are publicly accessible, these metrics help to maintain the privacy and security of users' activity.

*3) Privacy Metric Quality:* There are few studies in the literature [269], [270] that investigate the quality of the privacy metric. It is recommended that high-quality metrics should be used for the quantification of user privacy, but there is no mutual consensus on what is high quality and how it should be quantified.

**Lesson Learned.** It is important to use high-quality privacy metrics to determine user privacy accurately but there is limited consensus on what makes a metric high-quality or how to measure it. This lack of consensus makes it more challenging to ensure reliable and effective privacy quantification.

**Future Direction.** It is widely believed that the privacy metric value is greatly varied with consistency and uniformity. The quantity of privacy metrics, quality indicators, and relevant scenarios all affect the usefulness of privacy metrics. Thus, more investigation is required to assess the value and significance of privacy measurements.

### C. Open Problems in Privacy Techniques

Privacy techniques encompass a broad array of issues spanning from technological advancements to legal and ethical considerations.

*1) Management of Dynamic Data:* Dynamic data management is one of the main challenges to the wider adoption of preserving techniques. A set of privacy techniques applied to dynamic data would not successfully solve the privacy preservation problem because data is dynamically modified with time. In particular, when certain records are added, removed, or modified, sensitive data would not be properly secured. The current solutions are based on the static publication of the user data which supports one-time publication.

TABLE X
LIST OF ACRONYMS AND CORRESPONDING DEFINITIONS

| Acronyms | Definitions |
|---|---|
| AI | Artificial Intelligence |
| APIs | Application Programming Interfaces |
| BCRs | Binding Corporate Rules |
| BGN | Boneh-Goh-Nissim |
| CCPA | California Consumer Privacy Act |
| CDP | Central Differential Privacy |
| CPU | Central Processing Unit |
| CT | Computed Tomography |
| DP | Differential Privacy |
| EU | European Union |
| EEA | European Economic Area |
| FAIR | Factor Analysis of Information Risk |
| FHE | Fully Homomorphic Encryption |
| FL | Federated Learning |
| FTL | Federated Transfer Learning |
| GDP | Global Differential Privacy |
| GDPR | General Data Protection Regulation |
| GMW | Goldreich, Micali and Wigderson |
| GPDPL | General Personal Data Protection Law |
| HE | Homomorphic Encryption |
| HES | Homomorphic Encryption Standard |
| HFL | Horizontal Federated Learning |
| IDMS | IDentity Management System |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| ISMS | Information Security Management System |
| ISO | International Organisation for Standardisation |
| IDC | International Data Corporation |
| IDs | Identifiers |
| IoT | Internet of Things |
| ITST | Information Technology Security Technique |
| LDP | Local Differential Privacy |
| LLM | Large Language Model |
| MEC | Mobile Edge Computing |
| ML | Machine Learning |
| MRI | Magnetic Resonance Imaging |
| NIST | National Institute of Standards and Technology |
| NOMA | Non-Orthogonal Multiple Access |
| OMTP | Open Mobile Terminal Platform |
| OS | Operating System |
| OT | Oblivious Transfer |
| OWASP | Open Web Application Security Project |
| PETs | Privacy-Enhancing Techniques |
| PHE | Partially Homomorphic Encryption |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PIMS | Privacy Information Management System |
| PIPEDA | Personal Information Protection and Electronic Documents Act |
| PPTs | Privacy-Preserving Techniques |
| PRAM | Post-RAndomisation Method |
| QIDs | Quasi-Identifiers |
| RDP | Renyi Differential Privacy |
| RSA | Rivest, Shamir, and Adleman |
| SCCs | Standard Contractual Clauses |
| SMPC | Secure Multi-Party Computation |
| SWHE | Somewhat Homomorphic Encryption |
| TEE | Trusted Execution Environment |
| TPM | Trusted Platform Module |
| TTP | Trusted Third Party |
| VFL | Vertical Federated Learning |
| ZB | Zeeta Bytes |

**Lesson Learned.** Management of dynamic data poses a significant challenge to the adoption of effective privacy techniques. Techniques designed for static data may not

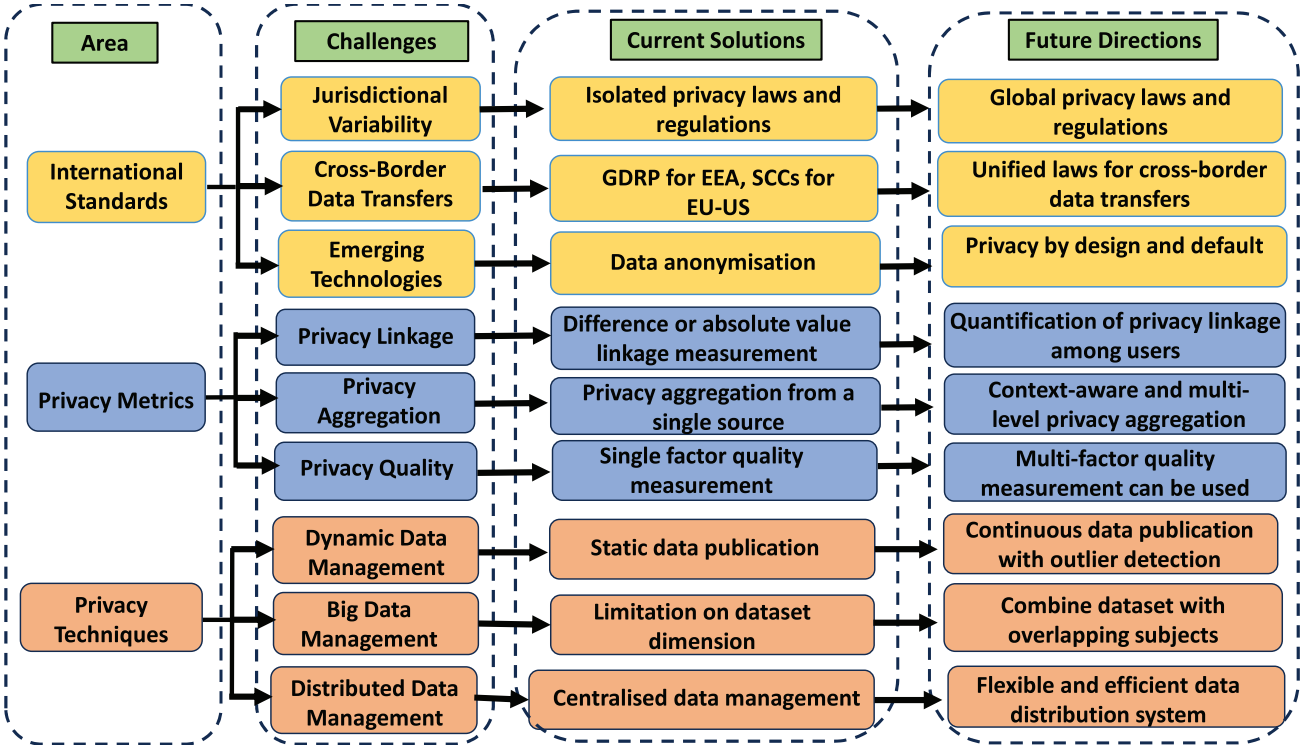


Fig. 9. Lesson learned and future research direction in characterisation and quantification of user privacy.

sufficiently protect user privacy when data is constantly changing over time, such as when records are added, removed, or modified. Current solutions often rely on publishing data in a static form, which limits their effectiveness in dynamically changing environments.

**Future Direction.** To address the management of dynamic data, we need to develop flexible, interactive, and adaptable privacy techniques that publish continuous data with the integration of outliers detection techniques.

*2) Management of Big Data:* Management of big data is another challenge to the wider adoption of privacy techniques. A growing number of attributes are caused by the enormous increase in digital data that is currently being gathered and shared. In some situations, the so-called "curse of dimensionality" may apply, potentially leading to information loss in de-identified datasets.

In literature, some approaches [250], [271] are presented that address the limitation of the dimensionality. Furthermore, since global recoding and other approaches rely heavily on data variances, big data variety may impose additional limitations [272].

**Lesson Learned.** The major challenge in the implementation of efficient privacy measures is to manage large user data sets. The quantity of digital data being gathered and exchanged is huge, and there are more and more user attributes to manage. Big data comes in a wide range of formats and sources, which makes privacy initiatives much more difficult and presents new issues that must be resolved for efficient data security.

**Future Direction.** One possible future direction is to construct big data by combining datasets having overlapping subjects. The second possible direction is to develop efficient cryptographic methods that enhance data utility and reduce computational overhead.

*3) Management of Distributed Data:* Management of distributed data is the third main challenge to the wider adoption of privacy techniques. The requirement for the massive amount of real-time data for different types of analysis allows organisations to move from a centralised data storage solution to a decentralised one. When data is stored by different parties, collaborative data publishing in which multiple data providers release data for general use or data mining tasks is frequently used as a solution to this problem but the rapidly growing volume of data requires the exploration of new security measures. Some solutions allow multiple collaborations of different parties using secure cryptographic mechanisms [273].

**Lesson Learned.** The adoption of efficient privacy techniques is affected by the management of distributed data. Organisations are shifting from centralised to decentralised data storage solutions as they depend more and more on real-time data for a variety of analyses. This problem is usually addressed with the help of collaborative data publishing, in which several parties release data for public consumption or mining activities. Secure cryptographic techniques are one type of solution that allows collaboration among several parties while maintaining data confidentiality and privacy. These developments are important for preserving confidence and protecting sensitive data in remote data environments.

**Future Direction.** The possible future work is to develop a flexible and efficient distributed system for handling distributed data that balances computational and disclosure costs. The lesson learned and future research directions are listed in Fig. 9.

## XI. Conclusion

The exponential growth of data-driven technologies has not only drastically changed the way people conduct activities and acquire information but also has raised security and privacy issues for them. Users are increasingly sharing their personal information on the online platforms of various organisations. These organisations publish and share user-generated data with third parties which risks exposing individuals' privacy. Detecting privacy issues and proposing techniques to protect users' privacy is a challenging issue. Most of the existing works focus on introducing new attacks and thus the gap between protection and detection becomes larger for an organisation. In this survey, we discuss the important issues in the characterisation and quantification of user privacy in compliance with international regulatory standards. Then, we provide an overview of existing regulations and frameworks related to user privacy, highlighting their strengths, limitations, and implications for businesses and individuals. In the end, we discuss promising directions for future research and development, including advancements in privacy techniques, interdisciplinary collaborations, and the role of emerging technologies. This work aims to contribute to the ongoing research on user privacy in compliance with international standards and promote the development of effective strategies for safeguarding user personal data in an increasingly interconnected world.

## References


[1] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard Law Rev.*, vol. 4, no. 5, pp. 193–220, 1890. [Online]. Available: http://www.jstor.org/stable/1321160

[2] L. J. Hoffman, "Computers and privacy: A survey," *ACM Comput. Surv.*, vol. 1, no. 2, pp. 85–103, Jun. 1969. [Online]. Available: https://doi.org/10.1145/356546.356548

[3] P. O. P. DATA, "Directive 95/46/EC of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Off. J. L*, vol. 281, pp. 31–50, Nov. 1995.

[4] N. Crato and P. Paruolo, "The power of microdata: An introduction," *Data-Driven Policy Impact Evaluation: How Access to Microdata is Transforming Policy Design*. Cham, Switzerland: Springer, 2019, pp. 1–14.

[5] D. R.-J. G.-J. Rydning, J. Reinsel, and J. Gantz, "The digitization of the world from edge to core," Framingham: Int. Data Co., Framingham, MA, USA, White Paper, 2018.

[6] P. Radanliev, D. De Roure, and R. Walton, "Data mining and analysis of scientific research data records on COVID-19 mortality, immunity, and vaccine development-in the first wave of the COVID-19 pandemic," *Diabetes Metab. Synd., Clin. Res. Rev.*, vol. 14, no. 5, pp. 1121–1132, 2020.

[7] T. Carvalho, P. Faria, L. Antunes, and N. Moniz, "Fundamental privacy rights in a pandemic state," *Plos One*, vol. 16, no. 6, 2021, Art. no. e0252169.

[8] G. Jung, H. Lee, A. Kim, and U. Lee, "Too much information: Assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea," *Front. Public Health*, vol. 8, p. 305, Jun. 2020.

[9] N. Peiffer-Smadja, R. Maatoug, F.-X. Lescure, E. D'Ortenzio, J. Pineau, and J.-R. King, "Machine learning for COVID-19 needs global collaboration and data-sharing," *Nature Mach. Intell.*, vol. 2, no. 6, pp. 293–294, 2020.

[10] P. Voigt and A. Von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, vol. 10, 1st Ed. Cham, Switzerland: Springer, 2017.

[11] M. L. Rustad and T. H. Koenig, "Towards a global data privacy standard," *Florida Law Rev.*, vol. 71, pp. 18–16, Sep. 2018.

[12] "California Consumer Privacy act (CCPa)." Oag.ca.gov. Accessed: Jan. 31, 2024. [Online]. Available: https://oag.ca.gov/privacy/ccpa

[13] "Brazilian general data protection law (LGPD, English translation)," Iapp.org. Accessed: Feb. 1, 2024. [Online]. Available: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

[14] J. Brickell and V. Shmatikov, "The cost of privacy: Destruction of data-mining utility in anonymized data publishing," in *Proc. 14th ACM SIGKDD Int. Conf. Knowl. Discovery Data Min.*, 2008, pp. 70–78.

[15] T. Li and N. Li, "On the tradeoff between privacy and utility in data publishing," in *Proc. 15th ACM SIGKDD Int. Conf. Knowl. Discovery Data Min.*, 2009, pp. 517–526.

[16] T. Carvalho, N. Moniz, P. Faria, and L. Antunes, "Towards a data privacy-predictive performance trade-off," *Expert Syst. Appl.*, vol. 223, Aug. 2023, Art. no. 119785.

[17] "ISO-international organization for standardization." iso.org. Accessed: Jan. 26, 2024. [Online]. Available: https://www.iso.org/home.html

[18] *IEEE Recommended Practice for Secure Multi-Party Computation*, IEEE Standard 2842-2021, 2021, Accessed: Jan. 22, 2024. [Online]. Available: https://standards.ieee.org/ieee/2842/7675/

[19] "National institute of standards and technology." Nist.gov. Accessed: Feb. 1, 2024. [Online]. Available: https://www.nist.gov/

[20] J. Domingo-Ferrer, "A survey of inference control methods for privacy-preserving data mining," in *Privacy-Preserving Data Mining: Models Algorithms*. Boston, MA, USA: Springer, 2008, pp. 53–80.

[21] B. C. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," *ACM Comput. Surv.*, vol. 42, no. 4, pp. 1–53, 2010.

[22] G. J. Matthews and O. Harel, "Data confidentiality: A review of methods for statistical disclosure limitation and methods for assessing privacy," *Statist. Surv.*, vol. 5, pp. 1–29, Feb. 2011. [Online]. Available: https://doi.org/10.1214/11-SS074

[23] L. Willenborg and T. De Waal, *Elements of Statistical Disclosure Control*, vol. 155. New York, NY, USA: Springer, 2012.

[24] T. Carvalho, N. Moniz, P. Faria, and L. Antunes, "Survey on privacy-preserving techniques for microdata publication," *ACM Comput. Surv.*, vol. 55, no. 14, pp. 1–42, Mar. 2023. [Online]. Available: https://doi.org/10.1145/3588765

[25] I. Wagner and D. Eckhoff, "Technical privacy metrics: A systematic survey," *ACM Comput. Surv.*, vol. 51, no. 3, pp. 1–38, Jun. 2018. [Online]. Available: https://doi.org/10.1145/3168389

[26] "Royalsociety." Accessed: Jan. 16, 2024. [Online]. Available: https://royalsociety.org/news-resources/projects/privacy-enhancing-technologies

[27] E. Toch et al., "The privacy implications of cyber security systems: A technological survey," *ACM Comput. Surv.*, vol. 51, no. 2, pp. 1–27, 2018.

[28] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–34, 2019.

[29] M. Humbert, B. Trubert, and K. Huguenin, "A survey on interdependent privacy," *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–40, 2019.

[30] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 746–789, 1st Quart., 2020.

[31] G. Beigi and H. Liu, "A survey on privacy in social media: Identification, mitigation, and applications," *ACM Trans. Data Sci.*, vol. 1, no. 1, pp. 1–38, 2020.

[32] C. Liu, T. Zhu, J. Zhang, and W. Zhou, "Privacy intelligence: A survey on image privacy in online social networks," *ACM Comput. Surv.*, vol. 55, no. 8, pp. 1–35, 2022.

[33] J. S. Edu, J. M. Such, and G. Suarez-Tangil, "Smart home personal assistants: A security and privacy review," *ACM Comput. Surv.*, vol. 53, no. 6, pp. 1–36, 2020.

[34] N. Pattnaik, S. Li, and J. R. Nurse, "A survey of user perspectives on security and privacy in a home networking environment," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–38, 2023.

[35] M. Rigaki and S. Garcia, "A survey of privacy attacks in machine learning," *ACM Comput. Surv.*, vol. 56, no. 4, pp. 1–34, Nov. 2023. [Online]. Available: https://doi.org/10.1145/3624010

[36] A. Rodrigues, M. L. Villela, and E. Feitosa, "A systematic mapping study on social network privacy: Threats and solutions," *ACM Comput. Surv.*, vol. 56, no. 7, pp. 1–29, 2024.

[37] X. Zhang et al., "Privacyasst: Safeguarding user privacy in tool-using large language model agents," *IEEE Trans. Depend. Secure Comput.*, vol. 21, no. 6, pp. 5242–5258, Nov./Dec. 2024.

[38] M. Elliot, E. Mackey, K. O'Hara, and C. Tudor, *The Anonymisation Decision-Making Framework*, Manchester, U.K.: UKAN, 2016.
[39] P. Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," *UCLA Law Rev.*, vol. 57, p. 1701, Aug. 2011.
[40] L. Caruccio, D. Desiato, G. Polese, G. Tortora, and N. Zannone, "A decision-support framework for data anonymization with application to machine learning processes," *Inf. Sci.*, vol. 613, pp. 1–32, Oct. 2022.
[41] L. Ohno-Machado, S. Vinterbo, and S. Dreiseitl, "Effects of data anonymization by cell suppression on descriptive statistics and predictive modeling performance," *J. Am. Med. Inform. Assoc.*, vol. 9, no. 6, pp. S115–S119, 2002.
[42] G. Danezis et al., "Privacy and data protection by design-from policy to engineering," 2015, *arXiv:1501.03726*.
[43] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, "A review of e-voting: The past, present and future," *Ann. Telecommun.*, vol. 71, pp. 279–286, Aug. 2016.
[44] L. Willenborg and T. De Waal, *Statistical Disclosure Control in Practice*, vol. 111. New York, NY, USA: Springer, 1996.
[45] G. T. Duncan, S. E. Fienberg, R. Krishnan, R. Padman, S. F. Roehrig, "Disclosure limitation methods and information loss for tabular data," *Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for Statistical Agencies*. Amsterdam, The Netherlands: Elsevier, 2001, pp. 135–166.
[46] V. Torra, *Guide to Data Privacy: Models, Technologies, Solutions*. Cham, Switzerland: Springer, 2022.
[47] C. C. Aggarwal and P. S. Yu, "A general survey of privacy-preserving data mining models and algorithms," *Privacy-Preserving Data Mining: Models Algorithms*, Boston, MA, USA: Springer, 2008, pp. 11–52.
[48] L. Rocher, J. M. Hendrickx, and Y.-A. De Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models," *Nat. Commun.*, vol. 10, no. 1, pp. 1–9, 2019.
[49] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *Proc. IEEE Symp. Security Privacy (SP)*, 2008, pp. 111–125.
[50] S. Ochoa, J. Rasmussen, C. Robson, and M. Salib, *Reidentification of Individuals in Chicago's Homicide Database: A Technical and Legal Study*, Massachusetts Inst. Technol., Cambridge, MA, USA, 2001.
[51] L. Sweeney, "Simple demographics often identify people uniquely," Carnegie Mellon Univ., San Francisco, CA, USA, Working Paper, 2000.
[52] C. C. Aggarwal, "On *k*-anonymity and the curse of dimensionality," in *Proc. VLDB*, 2005, pp. 901–909.
[53] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," in *Proc. 22nd Int. Conf. Data Eng. (ICDE)*, 2006, p. 24.
[54] N. Notario et al., "PRIPARE: Integrating privacy best practices into a privacy engineering methodology," in *Proc. IEEE Security Privacy Workshops*, 2015, pp. 151–158.
[55] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, "Location privacy-preserving mechanisms in location-based services: A comprehensive survey," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–36, 2021.
[56] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for information security management," *J. Inf. Secur.*, vol. 4, no. 2, pp. 92–100, 2013.
[57] *Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines*, ISO/IEC Standard 27701:2019, 2019, Accessed: Feb. 1, 2024. [Online]. Available: https://www.iso.org/standard/71670.html
[58] *Information Technology—Security Techniques—Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors*, ISO/IEC Standard 27018:2019, 2019, Accessed: May 28, 2024. [Online]. Available: https://www.iso.org/standard/76559.html
[59] D. J. Solove, "A taxonomy of privacy," *U. Pa. L. Rev.*, vol. 154, no. 3, p. 477, 2005.
[60] A. Pfitzmann and M. Hansen, *A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, Technische Universität Dresden, Dresden, Germany, 2010.
[61] E. Paintsil and L. Fritsch, "A taxonomy of privacy and security risks contributing factors," in *Proc. IFIP PrimeLife Int. Summer School Privacy Identity Manag. Life*, Helsingborg, Sweden, 2011, pp. 52–63.
[62] Z. Wang et al., "Privacy-preserving crowd-sourced statistical data publishing with an untrusted server," *IEEE Trans. Mobile Comput.*, vol. 18, no. 6, pp. 1356–1367, 2019.
[63] Y. Zhang, X. Ye, X. Xiao, T. Xiang, H. Li, and X. Cao, "A reversible framework for efficient and secure visual privacy protection," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 3334–3349, 2023.
[64] B. Sedlak, I. Murturi, P. K. Donta, and S. Dustdar, "A privacy enforcing framework for data streams on the edge," *IEEE Trans. Emerg. Topics Comput.*, vol. 12, no. 3, pp. 852–863, Jul.–Sep. 2024.
[65] W. Wang, X. Li, X. Qiu, X. Zhang, V. Brusic, and J. Zhao, "A privacy preserving framework for federated learning in smart healthcare systems," *Inf. Process. Manag.*, vol. 60, no. 1, 2023, Art. no. 103167.
[66] L. Ouyang, F.-Y. Wang, Y. Tian, X. Jia, H. Qi, and G. Wang, "Artificial identification: A novel privacy framework for federated learning based on blockchain," *IEEE Trans. Comput. Social Syst.*, vol. 10, no. 6, pp. 3576–3585, Dec. 2023.
[67] E. Bangerter, J. Camenisch, and A. Lysyanskaya, "A cryptographic framework for the controlled release of certified data," in *Proc. Int. Workshop Secur. Protocols*, 2006, pp. 20–42.
[68] M. Franz, B. Meyer, and A. Pashalidis, "Attacking unlinkability: The importance of context," in *Proc. Int. Workshop Privacy Enhancing Technol.*, 2007, pp. 1–16.
[69] B. C. M. Fung, K. Wang, and P. S. Yu, "Anonymizing classification data for privacy preservation," *IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 5, pp. 711–725, May 2007.
[70] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu, "Tools for privacy preserving distributed data mining," *SIGKDD Explor. Newslett.*, vol. 4, no. 2, pp. 28–34, Dec. 2002. [Online]. Available: https://doi.org/10.1145/772862.772867
[71] N. Lefkovitz and K. Boeckl, *NIST Privacy Framework: An Overview*, Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, 2020.
[72] *Information Technology—Security Techniques—Privacy Framework*, ISO/IEC Standard 29100:2011, 2011, Accessed: Jan. 23, 2024. [Online]. Available: https://www.iso.org/standard/45123.html
[73] E. Humphreys, *Implementing the ISO/IEC 27001: 2013 ISMS Standard*. Boston , MA, USA: Artech House, 2016.
[74] *Information Security, Cybersecurity and Privacy Protection—Information Security Controls*, ISO/IEC 27002:2022, 2022, Accessed: Feb. 1, 2024. [Online]. Available: https://www.iso.org/standard/75652.html
[75] *Information Technology—Security Techniques—Code of Practice for Personally Identifiable Information Protection*, ISO/IEC 29151:2017, 2017, Accessed: Feb. 5, 2024. [Online]. Available: https://www.iso.org/standard/62726.html
[76] *IEEE Standard for Data Privacy Process*, IEEE Standard 7002-2022, 2022, Accessed: Feb. 1, 2024. [Online]. Available: https://sagroups.ieee.org/7002/
[77] *IEEE P7006 Working Group Draft Meeting Agenda Teleconference*, IEEE Standard P7006, 2024, Accessed: Feb. 1, 2024. [Online]. Available: https://sagroups.ieee.org/7006/
[78] T. Dalenius, "Towards a methodology for statistical disclosure control," *Statistik Tidskrift*, vol. 15, pp. 429–444, 1977.
[79] P. Ohm, "Sensitive information," *S. Cal. L. Rev.*, vol. 88, p. 1125, Sep. 2014.
[80] J. M. Rumbold and B. K. Pierscionek, "What are data? A categorization of the data sensitivity spectrum," *Big data Res.*, vol. 12, pp. 49–59, Jul. 2018.
[81] S. Mauw and M. Oostdijk, "Foundations of attack trees," in *Proc. 8th Int. Conf. Inf. Security Cryptol. (ICISC)*, Seoul, South Korea, 2006, pp. 186–198.
[82] P. Torr, "Demystifying the threat modeling process," *IEEE Security Privacy*, vol. 3, no. 5, pp. 66–70, Sep./Oct. 2005.
[83] M. Aydos, Ç. Aldan, E. Coşkun, and A. Soydan, "Security testing of Web applications: A systematic mapping of the literature," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6775–6792, 2022.
[84] B. Potter, "Microsoft SDL threat modelling tool," *Netw. Secur.*, vol. 1, no. 1, pp. 15–18, 2009.
[85] "IEEE-the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity." IEEE.org. Accessed: Feb. 1, 2024. [Online]. Available: https://www.ieee.org/
[86] M. Souppaya and K. Scarfone, "Guide to data-centric system threat modeling," Nat. Inst. Stand. Technol., Boston, MA, USA, document NIST SP 800-154, 2016.
[87] J. Freund and J. Jones, *Measuring and Managing Information Risk: A FAIR Approach*. Oxford, U.K.: Butterworth-Heinemann, 2014.
[88] *Information Technology—Security Techniques—Guidelines for Privacy Impact Assessment*, ISO/IEC Standard 29134:2023, May 2023. [Online]. Available: https://www.iso.org/standard/86012.html
[89] E. Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)*, Santa Clara Univ., Santa Clara, CA, USA, 2020.

[90] Department of Justice Canada, "Personal information protection and electronic documents act," 2000. [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/

[91] D. Agrawal and C. C. Aggarwal, "On the design and quantification of privacy preserving data mining algorithms," in *Proc. 20th ACM SIGMOD-SIGACT-SIGART Symp. Princ. Database Syst.*, New York, NY, USA, 2001, pp. 247–255. [Online]. Available: https://doi.org/10.1145/375551.375602

[92] J. L. Becker, *Measuring Privacy Risk in Online Social Networks*, Univ. California, Davis, CA, USA, 2009.

[93] I. Wagner and E. Boiten, "Privacy risk assessment: From art to science, by metrics," in *Proc. Int. Workshops Data Privacy Manag. (DPM)*, Barcelona, Spain, 2018, pp. 225–241.

[94] C. Andersson and R. Lundin, "On the fundamentals of anonymity metrics," in *The Future of Identity Information Society*, S. Fischer-Hübner, P. Duquenoy, A. Zuccato, and L. Martucci, Eds. Boston, MA, USA: Springer, 2008, pp. 325–341.

[95] E. Bertino, D. Lin, and W. Jiang, "A survey of quantification of privacy preserving data mining algorithms," in *Privacy-Preserving Data Mining: Models Algorithms*. Boston, MA, USA: Springer, 2008, pp. 183–205.

[96] M. Bezzi, "An information theoretic approach for privacy metrics," *Trans. Data Privacy*, vol. 3, no. 3, pp. 199–215, Dec. 2010.

[97] K. Chatzikokolakis, C. Palamidessi, and M. Stronati, "Constructing elastic distinguishability metrics for location privacy," 2015, *arXiv:1503.00756*.

[98] S. Clauß and S. Schiffner, "Structuring anonymity metrics," in *Proc. 2nd ACM Workshop Digit. Identity Manag.*, New York, NY, USA, 2006, pp. 55–62. [Online]. Available: https://doi.org/10.1145/1179529.1179539

[99] D. J. Kelly, R. A. Raines, M. R. Grimaila, R. O. Baldwin, and B. E. Mullins, "A survey of state-of-the-art in anonymity metrics," in *Proc. 1st ACM Workshop Netw. Data Anonymization*, New York, NY, USA, 2008, pp. 31–40. [Online]. Available: https://doi.org/10.1145/1456441.1456453

[100] S. J. Murdoch and R. N. M. Watson, "Metrics for security and performance in low-latency anonymity systems," in *Proc. Int. Symp. Privacy Enhancing Technol.*, Berlin, Germany, 2008, pp. 115–132.

[101] J. Alexander and J. Smith, "Engineering privacy in public: Confounding face recognition," in *Proc. Int. Workshop Privacy Enhancing Technol.*, Berlin, Germany, 2003, pp. 88–106.

[102] P. Syverson, "Why i'm not an entropist," in *Proc. 17th Int. Workshop*, Berlin, Germany, 2013, pp. 213–230.

[103] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Proc. IEEE Symp. Security Privacy*, 2011, pp. 247–262.

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

[105] R. C.-W. Wong, J. Li, A. W.-C. Fu, and K. Wang, "($\alpha$, k)-anonymity: An enhanced k-anonymity model for privacy preserving data publishing," in *Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discovery Data Min.*, New York, NY, USA, 2006, pp. 754–759. [Online]. Available: https://doi.org/10.1145/1150402.1150499

[106] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *J. Cryptol.*, vol. 1, pp. 65–75, Jan. 1988.

[107] D. Kesdogan, J. Egner, and R. Büschkes, "Stop-and-go-MIXes providing probabilistic anonymity in an open system," in *Proc. Int. Workshop Inf. Hiding*, Berlin, Germany, 1998, pp. 83–98.

[108] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *Proc. Int. Conf. Pervasive Comput.*, Berlin, Germany, 2005, pp. 152–170.

[109] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Proc. Int. Conf. Pervasive Comput.*, Berlin, Germany, 2009, pp. 390–397.

[110] T. S. Heydt-Benjamin, H.-J. Chae, B. Defend, and K. Fu, "Privacy for public transportation," in *Proc. Int. Conf. Workshop Privacy Enhancing Technol.*, Berlin, Germany, 2006, pp. 1–19.

[111] C. Diaz, C. Troncoso, and G. Danezis, "Does additional information always reduce anonymity?" in *Proc. ACM Workshop Privacy Electron. Soc.*, New York, NY, USA, 2007, pp. 72–75. [Online]. Available: https://doi.org/10.1145/1314333.1314347

[112] P. Samarati, "Protecting respondents identities in microdata release," *IEEE Trans. Knowl. Data Eng.*, vol. 13, no. 6, pp. 1010–1027, Nov./Dec. 2001. [Online]. Available: https://doi.org/10.1109/69.971193

[113] P. Samarati and L. Sweeney, "Generalizing data to provide anonymity when disclosing information (abstract)," in *Proc. 17th ACM SIGACT-SIGMOD-SIGART Symp. Princ. Database Syst.*, New York, NY, USA, 1998, p. 188. [Online]. Available: https://doi.org/10.1145/275487.275508

[114] N. Li, W. Qardaji, and D. Su, "On sampling, anonymization, and differential privacy or, *k*-anonymization meets differential privacy," in *Proc. 7th ACM Symp. Inf., Comput. Commun. Secur.*, New York, NY, USA, 2012, pp. 32–33. [Online]. Available: https://doi.org/10.1145/2414456.2414474

[115] X. Xiao and Y. Tao, "Personalized privacy preservation," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, New York, NY, USA, 2006, pp. 229–240. [Online]. Available: https://doi.org/10.1145/1142473.1142500

[116] X. Xiao and Y. Tao, "M-invariance: Towards privacy preserving re-publication of dynamic datasets," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, New York, NY, USA, 2007, pp. 689–700. [Online]. Available: https://doi.org/10.1145/1247480.1247556

[117] R. Shokri, C. Troncoso, C. Diaz, J. Freudiger, and J.-P. Hubaux, "Unraveling an old cloak: K-anonymity for location privacy," in *Proc. 9th Annu. ACM Workshop Privacy Electron. Soc.*, New York, NY, USA, 2010, pp. 115–118. [Online]. Available: https://doi.org/10.1145/1866919.1866936

[118] K. Wang, B. C. M. Fung, and P. S. Yu, "Handicapping attacker's confidence: An alternative to *k*-anonymization," *Knowl. Inf. Syst.*, vol. 11, no. 3, pp. 345–368, 2007. [Online]. Available: https://doi.org/10.1007/s10115-006-0035-5

[119] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond *k*-anonymity and *l*-diversity," in *Proc. IEEE 23rd Int. Conf. Data Eng.*, 2007, pp. 106–115.

[120] Q. Zhang, N. Koudas, D. Srivastava, and T. Yu, "Aggregate query answering on anonymized tables," in *Proc. IEEE 23rd Int. Conf. Data Eng.*, 2007, pp. 116–125.

[121] L. Zhang, S. Jajodia, and A. Brodsky, "Information disclosure under realistic assumptions: Privacy versus optimality," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 573–583.

[122] J. Domingo-Ferrer and J. Soria-Comas, "From *t*-closeness to differential privacy and vice versa in data anonymization," *Knowl.-Based Syst.*, vol. 74, pp. 151–158, Jan. 2015.

[123] S. Chawla, C. Dwork, F. McSherry, A. Smith, and H. Wee, "Toward privacy in public databases," in *Proc. 2nd Int. Conf. Theory Cryptogr.*, Berlin, Germany, 2005, pp. 363–385. [Online]. Available: https://doi.org/10.1007/978-3-540-30576-7_20

[124] J. Li, Y. Tao, and X. Xiao, "Preservation of proximity privacy in publishing numerical sensitive data," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, New York, NY, USA, 2008, pp. 473–486. [Online]. Available: https://doi.org/10.1145/1376616.1376666

[125] C. E. Shannon, "Communication theory of secrecy systems," *Bell system Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[126] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Proc. Int. Workshop Privacy Enhancing Technol.*, Berlin, Germany, 2003, pp. 41–53.

[127] Z. Ma, F. Kargl, and M. Weber, "Measuring long-term location privacy in vehicular communication systems," *Comput. Commun.*, vol. 33, no. 12, pp. 1414–1427, 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366410001076

[128] G. Tóth, Z. Hornák, and F. Vajda, "Measuring anonymity revisited," in *Proc. 9th Nordic Workshop Secure IT Syst.*, Jan. 2004, pp. 1–6.

[129] C. Díaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Proc. Int. Conf. Privacy Enhancing Technol.*, Berlin, Germany, 2003, pp. 54–68.

[130] S. Marcellin, D. A. Zighed, and G. Ritschard, "An asymmetric entropy measure for decision trees," in *Proc. 11th Inf. Process. Manag. Uncertainty Knowl.-Based Syst. (IPMU)*, Paris, France, 2006, pp. 1292–1299.

[131] E. Ayday, J. L. Raisaro, J.-P. Hubaux, and J. Rougemont, "Protecting and evaluating genomic privacy in medical tests and personalized medicine," in *Proc. 12th ACM Workshop Privacy Electron. Soc.*, 2013, pp. 95–106.

[132] Y. Deng, J. Pang, and P. Wu, "Measuring anonymity with relative entropy," in *Proc. Int. Workshop Formal Aspects Secur. Trust*, Berlin, Germany, 2007, pp. 65–79.

[133] Z. Lin, M. Hewett, and R. B. Altman, "Using binning to maintain confidentiality of medical data," in *Proc. AMIA Symp.*, 2002, p. 454.

[134] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Trans. Inf. Forensics Security*, vol. 8, pp. 838–852, 2013.

[135] B. Pinkas, "Cryptographic techniques for privacy-preserving data mining," *SIGKDD Explor. Newslett.*, vol. 4, no. 2, pp. 12–19, Dec. 2002. [Online]. Available: https://doi.org/10.1145/772862.772865

[136] J. Heurix, P. Zimmermann, T. Neubauer, and S. Fenz, "A taxonomy for privacy enhancing technologies," *Comput. Secur.*, vol. 53, pp. 1–17, Sep. 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404815000668

[137] T. De Waal and L. C. R. J. Willenborg, "A view on statistical disclosure control for microdata," *Surv. Methodol.*, vol. 22, no. 1, pp. 95–103, 1996.

[138] J. Domingo-Ferrer, D. Sánchez, and J. Soria-Comas, *Database Anonymization: Privacy Models, Data Utility, and Microaggregation-Based Inter-Model Connections*. Cham, Switzerland: Springer, 2022.

[139] D. B. Rubin, "Statistical disclosure limitation," *J. Off. Statist.*, vol. 9, no. 2, pp. 461–468, 1993.

[140] A. Hundepool et al., *Handbook on Statistical Disclosure Control*, ESSnet, Stockholm, Sweden, 2010.

[141] A. Takemura, "Local recoding and record swapping by maximum weight matching for disclosure control of microdata sets," *J. Off. Statist.*, vol. 18, no. 2, p. 275, 2002.

[142] J. Xu, W. Wang, J. Pei, X. Wang, B. Shi, and A. W.-C. Fu, "Utility-based anonymization using local recoding," in *Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discovery Data Min.*, 2006, pp. 785–790.

[143] C. Hurkens and S. Tiourine, "Models and algorithms for the microdata protection problem," *J. Off. Statist.*, vol. 14, no. 4, pp. 437–447, 1998.

[144] C. Skinner, C. Marsh, S. Openshaw, and C. Wymer, "Disclosure control for census microdata," *J. Off. Statist.*, vol. 10, p. 31, Mar. 1994.

[145] T. Dalenius and S. P. Reiss, "Data-swapping: A technique for disclosure control," *J. Statist. Plan. Inference*, vol. 6, no. 1, pp. 73–85, 1982. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0378375882900581

[146] G. Heer, "A bootstrap procedure to preserve statistical confidentiality in contingency tables," in *Proc. Int. Seminar Statist. Confidential.*, Luxembourg City, Luxembourg, 1993, pp. 261–271.

[147] J. J. Kim, "A method for limiting disclosure in microdata based on random noise and transformation," in *Proc. Sect. Surv. Res. Methods*, Alexandria, VA, USA, 1986, pp. 303–308.

[148] N. L. Spruill, "The confidentiality and analytic usefulness of masked business microdata," *Rev. Public Data Use*, vol. 12, no. 4, pp. 1–6, 1984.

[149] P. Tendick, "Optimal noise addition for preserving confidentiality in multivariate data," *J. Statist. Plan. Inference*, vol. 27, no. 3, pp. 341–353, 1991.

[150] R. Brand, "Microdata protection through noise addition," in *Inference Control Statistical Databases: From Theory to Practice*, Berlin, Germany: Springer, 2002, pp. 97–116.

[151] G. R. Sullivan, *The Use of Added Error to Avoid Disclosure in Microdata Releases*. Ames, IA, USA: Iowa State Univ., 1989.

[152] T. K. Nayak, B. Sinha, and L. Zayatz, "Statistical properties of multiplicative noise masking for confidentiality protection," *J. Off. Statist.*, vol. 27, no. 3, p. 527, 2011.

[153] J. Domingo-Ferrer and J. M. Mateo-Sanz, "Practical data-oriented microaggregation for statistical disclosure control," *IEEE Trans. Knowl. Data Eng.*, vol. 14, no. 1, pp. 189–201, Jan./Feb. 2002.

[154] J. Domingo-Ferrer, A. Oganian, À. Torres, and J. M. Mateo-Sanz, "On the security of microaggregation with individual ranking: Analytical attacks," *Int. J. Uncertain., Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 477–491, 2002.

[155] V. Torra, "Microaggregation for categorical variables: A median based approach," in *Proc. Int. Conf. Privacy Statist. Databases*, Barcelona, Spain, 2004, pp. 162–174.

[156] D. Defays and P. Nanopoulos, "Panels of enterprises and confidentiality: The small aggregates method," in *Proc. Symp. Design Anal. Longitudinal Surv.*, 1993, pp. 195–204.

[157] J. Domingo-Ferrer, A. Martínez-Ballesté, J. M. Mateo-Sanz, and F. Sebé, "Efficient multivariate data-oriented microaggregation," *VLDB J.*, vol. 15, pp. 355–369, Nov. 2006.

[158] M. Laszlo and S. Mukherjee, "Minimum spanning tree partitioning algorithm for microaggregation," *IEEE Trans. Knowl. Data Eng.*, vol. 17, no. 7, pp. 902–911, Jul. 2005.

[159] S. Martínez, D. Sánchez, and A. Valls, "Semantic adaptive microaggregation of categorical microdata," *Comput. Secur.*, vol. 31, no. 5, pp. 653–672, 2012.

[160] S. L. Hansen and S. Mukherjee, "A polynomial algorithm for optimal univariate microaggregation," *IEEE Trans. Knowl. Data Eng.*, vol. 15, no. 4, pp. 1043–1044, Jul./Aug. 2003.

[161] T. Dalenius, "A simple procedure for controlled rounding," *Statistik Tidskrift*, vol. 3, pp. 202–208, 1981.

[162] J. M. Gouweleeuw, P. Kooiman, and P. De Wolf, "Post randomisation for statistical disclosure control: Theory and implementation," *J. Off. Statist.*, vol. 14, no. 4, p. 463, 1998.

[163] S. E. Fienberg and J. McIntyre, "Data swapping: Variations on a theme by Dalenius and Reiss," in *Proc. Int. Conf. Privacy Statist. Databases*, Barcelona, Spain, 2004, pp. 14–29.

[164] K. Muralidhar and R. Sarathy, "A theoretical basis for perturbation methods," *Statist. Comput.*, vol. 13, pp. 329–335, Oct. 2003.

[165] K. Muralidhar and R. Sarathy, "A rejoinder to the comments by Polettini and Stander," *Statist. Comput.*, vol. 13, pp. 339–342, Oct. 2003.

[166] X. Xiao and Y. Tao, "Anatomy: Simple and effective privacy preservation," in *Proc. 32nd Int. Conf. Very Large Data Bases*, 2006, pp. 139–150.

[167] Y. Ye, L. Wang, J. Han, S. Qiu, and F. Luo, "An anonymization method combining anatomy and permutation for protecting privacy in microdata with multiple sensitive attributes," in *Proc. Int. Conf. Mach. Learn. Cybern. (ICMLC)*, 2017, pp. 404–411.

[168] Y. Tao, H. Chen, X. Xiao, S. Zhou, and D. Zhang, "ANGEL: Enhancing the utility of generalization for privacy preserving publication," *IEEE Trans. Knowl. Data Eng.*, vol. 21, no. 7, pp. 1073–1087, Jul. 2009.

[169] T. Li, N. Li, J. Zhang, and I. Molloy, "Slicing: A new approach for privacy preserving data publishing," *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 3, pp. 561–574, Mar. 2012.

[170] A. Machanavajjhala, D. Kifer, J. Abowd, J. Gehrke, and L. Vilhuber, "Privacy: Theory meets practice on the map," in *Proc. IEEE 24th Int. Conf. Data Eng.*, 2008, pp. 277–286.

[171] T. Carvalho, N. Moniz, P. Faria, L. Antunes, and N. Chawla, "Privacy-preserving data synthetisation for secure information sharing," 2022, *arXiv:2212.00484*.

[172] R. J. Little et al., "Statistical analysis of masked data," *J. Off. Statist.*, vol. 9, p. 407, Jun. 1993.

[173] R. J. Little, F. Liu, and T. E. Raghunathan, "Statistical disclosure techniques based on multiple imputation," in *Applied Bayesian Modeling Causal Inference from Incomplete-Data Perspectives: An Essential Journey Donald Rubin's Statistical Family*. Hoboken, NJ, USA: Wiley, 2004, pp. 141–152.

[174] R. A. Dandekar, J. Domingo-Ferrer, and F. Sebé, "LHS-based hybrid microdata vs rank swapping and microaggregation for numeric microdata protection," in *Inference Control Statistical Databases: From Theory to Practice*. Berlin, Germany: Springer, 2002, pp. 153–162.

[175] J. Domingo-Ferrer and Ú. González-Nicolás, "Hybrid microdata using microaggregation," *Inf. Sci.*, vol. 180, no. 15, pp. 2834–2844, 2010.

[176] (Inst. Elect. Electron. Eng., Piscataway, NJ, USA). *Synthetic Data Industry Connections Activity Initiation Document (ICAID)*. Accessed: Jan. 22, 2024. [Online]. Available: https://standards.ieee.org/wp-content/uploads/import/governance/iccom/IC21-013_Synthetic_Data.pdf

[177] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–35, Jul. 2018. [Online]. Available: https://doi.org/10.1145/3214303

[178] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978. [Online]. Available: https://doi.org/10.1145/359340.359342

[179] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn.*, Berlin, Germany, 1999, pp. 223–238.

[180] M. Fellows and N. Koblitz, "Combinatorial cryptosystems galore!" in *Finite Fields: Theory, Applications, and Algorithms* (Contemporary Mathematics), vol. 168. Providence, RI, USA: Am. Math. Soc., 1994, pp. 51–61. [Online]. Available: https://doi.org/10.1090/conm/168/01688

[181] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Proc. Theory Cryptogr. Conf.* , Berlin, Germany, 2005, pp. 325–341.

[182] C. Gentry, *A Fully Homomorphic Encryption Scheme*. Stanford, CA, USA: Stanford Univ. Press, 2009.

[183] *IT Security Techniques—Encryption Algorithms*, ISO/IEC sTANDARD 18033-6:2019, 2019, Accessed: Jan. 22, 2024. [Online]. Available: https://www.iso.org/standard/67740.html

[184] *Information Security—Encryption Algorithms*, ISO/iEC Standard WD 18033-8," Accessed: Jan. 22, 2024. [Online]. Available: https://www.iso.org/standard/83139.html

[185] A. C.-C. Yao, "How to generate and exchange secrets," in *Proc. 27th Annu. Symp. Found. Comput. Sci. (SFCS)*, 1986, pp. 162–167.

[186] O. Goldreich, S. Micali, and A. Wigderson, "How to play ANY mental game," in *Proc. 19th Annu. ACM Symp. Theory Comput.*, New York, NY, USA, 1987, pp. 218–229. [Online]. Available: https://doi.org/10.1145/28395.28420

[187] M. O. Rabin, "How to exchange secrets with oblivious transfer," Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Rep. 2005/187, 2005. [Online]. Available: http://eprint.iacr.org/2005/187

[188] Y. Ishai, J. Kilian, K. Nissim, and E. Petrank, "Extending oblivious transfers efficiently," in *Proc. Annu. Int. Cryptol. Conf.*, Berlin, Germany, 2003, pp. 145–161.

[189] *Information Technology—Security Techniques—Secret Sharing*, ISO/IEC Standard 19592-1:2016, Accessed: Jan. 22, 2024. [Online]. Available: https://www.iso.org/standard/65422.html

[190] *Information Technology—Security Techniques—Secret Sharing*, ISO/IEC Standard 19592-2:2017, Accessed: Jan. 22, 2024. [Online]. Available: https://www.iso.org/standard/65425.html

[191] *Information Security—Secure Multiparty Computation*, ISO/IEC Standard 4922-2, Accessed: Jan. 22, 2024. [Online]. Available: https://www.iso.org/standard/80514.html

[192] A. Nilsson, P. N. Bideh, and J. Brorsson, "A survey of published attacks on Intel SGX," 2020, *arXiv:2006.13598*.

[193] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, 2015, pp. 57–64.

[194] Y. Cao, J. Zhang, Y. Zhao, P. Su, and H. Huang, "SRFL: A secure & robust federated learning framework for IoT with trusted execution environments," *Expert Syst. Appl.*, vol. 239, Apr. 2024, Art. no. 122410.

[195] P. Musale and A. J. Lee, "Trust TEE?: Exploring the impact of trusted execution environments on smart home privacy norms," in *Proc. Privacy Enhancing Technol.*, pp. 5–23, 2023.

[196] *Information Technology—Trusted Platform Module Library*, ISO/IEC 11889-1:2015, 2015, Accessed: Jan. 22, 2024. [Online]. Available: https://www.iso.org/standard/66510.html

[197] *IEEE Standard for Technical Framework and Requirements of Trusted Execution Environment based Shared Machine Learning*, IEEE Standard 2830-2021, Accessed: Jan. 22, 2024. [Online]. Available: https://standards.ieee.org/ieee/2830/10231/

[198] (Open Mobile Terminal Platform, London, U.K.). *Advanced Trusted Environment: OMTP TR1*. Accessed: Jan. 22, 2024. [Online]. Available: http://www.omtp.org/OMTP_Advanced_Trusted_Environment_OMTP_TR1_v1_1.pdf

[199] "Specifications archive." GlobalPlatform.org. Accessed: Feb. 2, 2024. [Online]. Available: https://globalplatform.org/specs-library/

[200] "PSA certified: IoT security framework and certification." Psacertified.org. Accessed: Feb. 1, 2024. [Online]. Available: https://www.psacertified.org/

[201] "P2952 standard for secure computing based on trusted execution environment." Sagroups.ieee.org. Accessed: Jan. 22, 2024. [Online]. Available: https://sagroups.ieee.org/2952/

[202] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowl.-Based Syst.*, vol. 216, Mar. 2021, Art. no. 106775.

[203] Q. Li et al., "A survey on federated learning systems: Vision, hype and reality for data privacy and protection," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 4, pp. 3347–3366, Apr. 2023.

[204] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, Aug. 2014. [Online]. Available: https://doi.org/10.1561/0400000042

[205] Y. Zhao and J. Chen, "A survey on differential privacy for unstructured data content," *ACM Comput. Surv.*, vol. 54, no. 10, pp. 1–28, Sep. 2022. [Online]. Available: https://doi.org/10.1145/3490237

[206] A. Ünsal and M. Önen, "Information-theoretic approaches to differential privacy," *ACM Comput. Surv.*, vol. 56, no. 3, pp. 1–18, Oct. 2023. [Online]. Available: https://doi.org/10.1145/3604904

[207] I. Mironov, "Renyi differential privacy," in *Proc. IEEE 30th Comput. Security Found. Symp. (CSF)*, 2017, pp. 263–275.

[208] E. Shi, H. Chan, E. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Proc. Annu. Netw. Distrib. System Secur. Symp. (NDSS)*, 2011, pp. 1–17.

[209] M. Gong, Y. Xie, K. Pan, K. Feng, and A. K. Qin, "A survey on differentially private machine learning," *IEEE Comput. Intell. Mag.*, vol. 15, no. 2, pp. 49–64, May 2020.

[210] J. Dong, A. Roth, and W. J. Su, "Gaussian differential privacy," *J. Roy. Statist. Soc. Ser. B, Statist. Methodol.*, vol. 84, no. 1, pp. 3–37, 2022.

[211] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. Theory Cryptogr. Conf.*, Berlin, Germany, 2006, pp. 265–284.

[212] H. B. McMahan, D. Ramage, K. Talwar, and L. Zhang, "Learning differentially private recurrent language models," in *Proc. Int. Conf. Learn. Represent.*, 2017, pp. 1–14. [Online]. Available: https://api.semanticscholar.org/CorpusID:3461939

[213] J. Hsu, S. Khanna, and A. Roth, "Distributed private heavy hitters," in *Proc. Int. Colloq. Automata, Lang., Program.*, Berlin, Germany:, 2012, pp. 461–472.

[214] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *Proc. IEEE 54th Annu. Symp. Found. Comput. Sci.*, 2013, pp. 429–438.

[215] U. Erlingsson, V. Pihur, and A. Korolova, "RAPPOR: Randomized aggregatable privacy-preserving ordinal response," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, 2014, pp. 1054–1067. [Online]. Available: https://doi.org/10.1145/2660267.2660348

[216] B. Ding, J. Kulkarni, and S. Yekhanin, "Collecting telemetry data privately," in *Proc. 31st Int. Conf. Neural Inf. Process. Syst.*, 2017, pp. 3574–3583.

[217] V. Feldman, K. Kakaes, K. Ligett, K. Nissim, A. Slavkovic, and A. Smith, *Differential Privacy: Issues for Policymakers*, Simons Inst. Theory Comput., Berkeley, CA, USA, 2020.

[218] *Privacy Enhancing Data De-Identification Terminology and Classification of Techniques*, ISO/IEC Standard 20889:2018, 2018, Accessed: Jan. 23, 2024. [Online]. Available: https://www.iso.org/standard/69373.html

[219] D. Zhang et al., "$\epsilon$ KTELO: A framework for defining differentially private computations," *ACM Trans. Database Syst.*, vol. 45, no. 1, pp. 1–44, Feb. 2020. [Online]. Available: https://doi.org/10.1145/3362032

[220] J. Domingo-Ferrer and V. Torra, "Distance-based and probabilistic record linkage for re-identification of records with categorical variables," in *Proc. Butlletí de lACIA, Associació Catalana dIntelligència Artif.*, 2002, pp. 243–250.

[221] S. Fletcher and M. Z. Islam, "Measuring information quality for privacy preserving data mining," *Int. J. Comput. Theory Eng.*, vol. 7, no. 1, pp. 21–28, 2015.

[222] T. Carvalho and N. Moniz, "The compromise of data privacy in predictive performance," in *Proc. 19th Int. Symp. Intell. Data Anal. (IDA)*, Porto, Portugal, 2021, pp. 426–438.

[223] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, "Workload-aware anonymization," in *Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discovery Data Min.*, 2006, pp. 277–286.

[224] J. Domingo-Ferrer, J. M. Mateo-Sanz, and V. Torra, "Comparing SDC methods for microdata on the basis of information loss and disclosure risk," in *Proc. ETK-NTTS*, 2001, pp. 807–826.

[225] V. S. Iyengar, "Transforming data to satisfy privacy constraints," in *Proc. 8th ACM SIGKDD Int. Conf. Knowl. Discovery Data Min.*, 2002, pp. 279–288.

[226] R. Khan, K. Ghanem, and F. Coffele, "Digital security by design: A review of combined hardware-software-based cybersecurity with Compartmentalization," in *Proc. IEEE Int. Workshop Technol. Defense Security (TechDefense)*, 2023, pp. 181–186.

[227] Ö. Askin, T. Kutta, and H. Dette, "Statistical quantification of differential privacy: A local approach," in *Proc. IEEE Symp. Security Privacy (SP)*, 2022, pp. 402–421.

[228] N. Gillani, T. Arslan, and G. Mead, "An unobtrusive method for remote quantification of parkinson's and essential tremor using mm-wave sensing," *IEEE Sensors J.*, vol. 23, no. 9, pp. 10118–10131, May 2023.

[229] C. Prince, N. Omrani, A. Maalaoui, M. Dabic, and S. Kraus, "Are we living in surveillance societies and is privacy an illusion? An empirical study on privacy literacy and privacy concerns," *IEEE Trans. Eng. Manag.*, vol. 70, no. 10, pp. 3553–3570, Oct. 2023.

[230] C. Wang, Z. Yuan, P. Zhou, Z. Xu, R. Li, and D. O. Wu, "The security and privacy of mobile edge computing: An artificial intelligence perspective," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 22008–22032, Dec. 2023.

[231] L. H. Iwaya, A. Ahmad, and M. A. Babar, "Security and privacy for mHealth and uHealth systems: A systematic mapping study," *IEEE Access*, vol. 8, pp. 150081–150112, 2020.

[232] M. Yang, I. Tjuawinata, and K.-Y. Lam, "$K$-means clustering with local $d_x$-privacy for privacy-preserving data analysis," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 2524–2537, 2022.

[233] M. Qin, S. Yang, H. Deng, and M. H. Lee, "Enhancing security of primary user in underlay cognitive radio networks with secondary user selection," *IEEE Access*, vol. 6, pp. 32624–32636, 2018.
[234] R. Khan and R. Asif, "Reflective in-band full duplex NOMA communications for secure 5G networks," in *Proc. Int. Conf. Smart Appl., Commun. Netw. (SmartNets)*, 2021, pp. 1–6.
[235] G. Price. "How large is the digital universe? How fast is it growing? 2014 EMC digital universe study now available:" Apr. 2014. [Online]. Available: https://www.infodocket.com/2014/04/16/how-large-is-the-digital-universe-how-fast-is-it-growing-2014-emc-digital-universe-study-now-available/
[236] K. L. Viola et al., "Towards non-invasive diagnostic imaging of early-stage alzheimer's disease," *Nature Nanotechnol.*, vol. 10, no. 1, pp. 91–98, 2015.
[237] D. Eckhoff and I. Wagner, "Privacy in the smart city—Applications, technologies, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 489–516, 1st Quart., 2017.
[238] P. Ani Petrosyan (Statista, Hamburg, Germany). *Internet and Social Media Users in the World 2023*. Oct. 2023. [Online]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/
[239] A. De Waal, A. Hundepool, and L. Willenborg, "ARGUS, Software for statistical disclosure," in *Proc. Annu. Res. Conf.*, 1996, p. 45.
[240] F. Prasser and F. Kohlmayer, *Putting Statistical Disclosure Control into Practice: The ARX Data Anonymization Tool*. Cham, Switzerland: Springer, 2015, pp. 111–148. [Online]. Available: https://doi.org/10.1007/978-3-319-23633-9_6
[241] D. T. M. Terrovitis and N. Dimakopoulos. "Amnesia anonymization tool-data anonymization made easy." Amnesia.openaire.eu. Accessed: Jan. 10, 2024. [Online]. Available: https://amnesia.openaire.eu/
[242] M. Templ, A. Kowarik, and B. Meindl, "Statistical disclosure control for micro-data using the R package sdcMicro," *J. Statist. Softw.*, vol. 67, no. 4, pp. 1–36, 2015.
[243] "GDPR compliant testing." Realrolfje.github.io. Accessed: Jan. 23, 2024. [Online]. Available: https://realrolfje.github.io/anonimatron/
[244] "Peace of mind–immediate insights." Aircloak.com. Accessed: Jan. 10, 2024. [Online]. Available: https://aircloak.com/
[245] "Anonymization toolBox; data security and privacy lab." Labs.utdallas.edu. Accessed: Jan. 10, 2024. [Online]. Available: https://labs.utdallas.edu/dspl/software/anonymization-toolbox/
[246] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *Int. J. Uncertain., Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 571–588, 2002.
[247] "Cornell anonymization toolkit." SourceForge.net. Accessed 10-01-2024. [Online]. Available: https://sourceforge.net/projects/anony-toolkit/,
[248] "Open anonymizer." SourceForge.net. Accessed: Jun. 25, 2024. [Online]. Available: https://sourceforge.net/projects/openanonymizer/
[249] C. Dai, G. Ghinita, E. Bertino, J.-W. Byun, and N. Li, "TIAMAT: A tool for interactive analysis of microdata anonymization techniques," *Proc. VLDB Endowment*, vol. 2, no. 2, pp. 1618–1621, 2009.
[250] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, "Mondrian multidimensional K-anonymity," in *Proc. 22nd Int. Conf. Data Eng. (ICDE)*, 2006, p. 25.
[251] J.-W. Byun, A. Kamra, E. Bertino, and N. Li, "Efficient *k*-anonymization using clustering techniques," in *Proc. Int. Conf. Database Syst. Adv. Appl.*, 2007, pp. 188–200.
[252] G. Poulis, A. Gkoulalas-Divanis, G. Loukides, S. Skiadopoulos, and C. Tryfonopoulos, *SECRETA: A System for Evaluating and Comparing Relational and Transaction Anonymization Algorithms*, Univ. Konstanz, Konstanz, Germany, 2014.
[253] "The SECRETa system." Users.uop.gr. Accessed: Jun. 25, 2024. [Online]. Available: https://users.uop.gr/~poulis/SECRETA/
[254] A. Bampoulidis, I. Markopoulos, and M. Lupu, "PrioPrivacy: A local recoding k-anonymity tool for prioritised quasi-identifiers," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell.-Compan. Volume*, 2019, pp. 314–317.
[255] D. Avraam, A. Boyd, H. Goldstein, and P. Burton, "A software package for the application of probabilistic anonymisation to sensitive individual-level data: A proof of principle with an example from the ALSPAC birth cohort study," *Longitudinal Life Course Stud.*, vol. 9, no. 4, pp. 433–446, 2018.
[256] "HiPaa home." HHS.gov. Accessed: Jan. 31, 2024. [Online]. Available: https://www.hhs.gov/hipaa/index.html
[257] "Children's online privacy protection rule ('COPPa')." FTC.gov. Accessed: Jan. 31, 2024. [Online]. Available: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
[258] "APEC privacy framework." APEC.org. Accessed: Jan. 31, 2024. [Online]. Available: https://www.apec.org/publications/2005/12/apec-privacy-framework
[259] "EU-U.S. privacy shield." ICO.org.uk. Accessed: Jan. 1, 2024. [Online]. Available: https://ico.org.uk/make-a-complaint/eu-us-privacy-shield/
[260] "CURIA-documents." Curia.europa.eu. Accessed: Jan. 31, 2024. [Online]. Available: https://curia.europa.eu/juris/document/document.jsf;jsessionid=CF8C3306269B9356ADF861B57785FDEE?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=9812784
[261] "Standard contractual clauses (SCC)." Commission.europa.eu. Accessed: Jan. 31, 2024. [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
[262] "Guide to binding corporate rules." ICO.org.uk. Accessed: Jan. 31, 2024. [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/guide-to-binding-corporate-rules/
[263] "Home-the Wassenaar arrangement." Wassenaar.org. Accessed: Feb. 8, 2024. [Online]. Available: https://www.wassenaar.org/
[264] K. Thomas, C. Grier, and D. M. Nicol, "unfriendly: Multi-party privacy risks in social networks," in *Proc. 10th Int. Symp. Privacy Enhancing Technol. (PETS)*, Berlin, Germany, 2010, pp. 236–252.
[265] N. Vratonjic, K. Huguenin, V. Bindschaedler, and J.-P. Hubaux, "How others compromise your location privacy: The case of shared public IPs at hotspots," in *Proc. 13th Int. Symp. Privacy Enhancing Technol. (PETS)*, Bloomington, IN, USA, 2013, pp. 123–142.
[266] A.-M. Olteanu, K. Huguenin, R. Shokri, and J.-P. Hubaux, "Quantifying the effect of co-location information on location privacy," in *Proc. 14th Int. Symp. Privacy Enhancing Technol. (PETS)*, Amsterdam, The Netherlands, 2014, pp. 184–203.
[267] B. Bloessl, C. Sommer, F. Dressler, and D. Eckhoff, "The scrambler attack: A robust physical layer attack on location privacy in vehicular networks," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, 2015, pp. 395–400.
[268] J. Wang, L. Wu, S. Zeadally, M. K. Khan, and D. He, "Privacy-preserving data aggregation against malicious data mining attack for IoT-enabled smart grid," *ACM Trans. Sen. Netw.*, vol. 17, no. 3, pp. 1–25, Jun. 2021. [Online]. Available: https://doi.org/10.1145/\penalty-\@M3440249
[269] I. Wagner, "Genomic privacy metrics: A systematic comparison," in *Proc. IEEE Security Privacy Workshops*, 2015, pp. 50–59.
[270] I. Wagner, "Evaluating the strength of genomic privacy metrics," *ACM Trans. Privacy Secur.*, vol. 20, no. 1, pp. 1–34, Jan. 2017. [Online]. Available: https://doi.org/10.1145/3020003
[271] D. Kifer and J. Gehrke, "Injecting utility into anonymized datasets," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, 2006, pp. 217–228.
[272] A. Zigomitros, F. Casino, A. Solanas, and C. Patsakis, "A survey on privacy properties for data publishing of relational data," *IEEE Access*, vol. 8, pp. 51071–51099, 2020.
[273] L. Lyu et al., "Towards distributed privacy-preserving prediction," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, 2020, pp. 4179–4184.