cryptography

MDPI

Review

Pervasive User Data Collection from Cyberspace: Privacy Concerns and Countermeasures

Yinhao Jiang [1,2,*], Mir Ali Rezazadeh Baee [2,3], Leonie Ruth Simpson [2,3], Praveen Gauravaram [4], Josef Pieprzyk [3,5,6], Tanveer Zia [1,2,7], Zhen Zhao [8] and Zung Le [1,2]

1 School of Computing, Mathematics and Engineering, Charles Sturt University, Port Macquarie, NSW 2444, Australia; tzia@csu.edu.au (T.Z.); zung.le@lesofttech.com.au (Z.L.)
2 Cyber Security Cooperative Research Centre, Joondalup, WA 6027, Australia; mirali.rezazadeh@qut.edu.au (M.A.R.B.); lr.simpson@qut.edu.au (L.R.S.)
3 School of Computer Science, Queensland University of Technology, Brisbane, QLD 4001, Australia; josef.pieprzyk@gmail.com
4 Research & Innovation, Tata Consultancy Services Limited, North Sydney, NSW 2060, Australia; p.gauravaram@tcs.com
5 Data61, The Commonwealth Scientific and Industrial Research Organisation, Sydney, NSW 2000, Australia
6 Institute of Computer Science, Polish Academy of Sciences, 01-248 Warsaw, Poland
7 School of Arts and Sciences, The University of Notre Dame Australia, Sydney, NSW 2007, Australia
8 The State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China; zzhen@xidian.edu.cn
* Correspondence: yjiang@csu.edu.au; Tel.: +61-2-6933-2931

Abstract: The increasing use of technologies, particularly computing and communication paradigms, has significantly influenced our daily lives. Interconnecting devices and networks provides convenient platforms for information exchange and facilitates pervasive user data collection. This new environment presents serious privacy challenges. User activities can be continuously monitored in both digital and physical realms. Gathered data can be aggregated and analysed, revealing aspects of user behaviour that may not be apparent from a single data point. The very items that facilitate connectivity simultaneously increase the risk of privacy breaches. The data gathered to provide services can also be used for monitoring and surveillance. This paper discerns three novel categories of privacy concerns relating to pervasive user data collection: privacy and user activity in cyberspace, privacy in personal cyber–physical systems, and privacy in proactive user-driven data collection. We emphasise the primary challenges, ranging from identity tracking in browsing histories to intricate issues in opportunistic networks, situating each within practical, real-world scenarios. Furthermore, we assess the effectiveness of current countermeasures, investigating their strengths and limitations. This paper explores the challenges in preserving privacy in user interactions with dynamic interconnected systems and suggests countermeasures to mitigate identified privacy risks.

Keywords: user privacy; web privacy protection; local differential privacy; wearable device access control; lightweight encryption; location privacy; opportunistic network privacy

Citation: Jiang, Y.; Rezazadeh Baee, M.A.; Simpson, L.R.; Gauravaram, P.; Pieprzyk, J.; Zia, T.; Zhao, Z.; Le, Z. Pervasive User Data Collection from Cyberspace: Privacy Concerns and Countermeasures. *Cryptography* **2024**, *8*, 5. https://doi.org/10.3390/cryptography8010005

Academic Editor: Carlo Blundo

Received: 14 December 2023
Revised: 21 January 2024
Accepted: 24 January 2024
Published: 31 January 2024

1. Introduction

The increasing use of technologies, particularly computing and communication paradigms, has significantly influenced our daily lives. The integration of digital technologies into many aspects of our physical lives has generated a virtual dimension known as "cyberspace". For example, the use of embedded sensors, electronic tags, smart phones, vehicles, and an array of daily-use items generates massive amounts of data. Much of this is linkable to the actions of individuals and, if aggregated, provides a profile of the individual.

Interconnecting devices and networks provides convenient platforms for information exchange. The Internet of Things (IoT) is a well-known example. As the number of

interconnected 'Things' increases and computing environments improve, data monitoring and analysis becomes increasingly sophisticated. This trajectory toward a "hyper-connected world" [1] promises seamless interactions between the physical world and cyberspace, potentially enriching user experiences. Technological advances, for instance, now allow residents to see who is at their front door through a modern IoT-enabled doorbell, even when they are not at home. Additionally, they can remotely unlock the door, letting guests in.

Technological advancements have improved data-collection methodologies. Interconnected software and hardware facilitate pervasive user data collection; user activities can be continuously monitored in both digital and physical realms. For instance, in cyberspace, tools such as cookies and hyperlinked images enable data gathering, tracing user actions and revealing user preferences and online behaviours. This action may not be apparent to the user. Wearable gadgets such as smartwatches and fitness trackers capture a spectrum of data from health metrics to daily routines. Ubiquitous devices such as mobile phones capture and transmit real-world data including user location, which reveals patterns of user behaviour.

This new environment presents serious privacy challenges. The very items that facilitate connectivity simultaneously increase the risk of privacy breaches. The data gathered to provide services can also be used for monitoring and surveillance. For example, the video transmissions used to allow residents to see who is at the front door could potentially be viewed by others. As this reveals the identity and location of the visitor at a point in time, unauthorised access to this information is a privacy breach. Gathering such video data across time reveals patterns of attendance at this location. Collecting such data from multiple door bells permits mass surveillance. Sometimes, these data-gathering methods occur without explicit user consent, leading to unauthorised access to stored or transmitted data.

Westin [2] explains *"privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"*. Schoeman [3] explains privacy as *"control we have over information about ourselves"*.

Information privacy refers to the control of personal information. For systems containing private information, it is important to assess the risks associated with the collection, use, and disclosure of that information. Personal information refers to information which is directly linked to an identifiable individual.

Pervasive user data collection raises new privacy challenges. This paper aims to address the following research questions:

- How do evolving technological paradigms impact privacy, considering both cyberspace and the physical realm?
- What are the challenges associated with privacy preservation associated with various data-collection scenarios, from web browsing activities to advanced participatory sensing in real-world environments? What are the risks to user privacy?
- What countermeasures can be employed to mitigate our identified privacy risks? How effective are existing privacy-protection mechanisms?

To address these three questions, this paper focuses on user privacy in three emerging scenarios.

1.1. Privacy and User Activity in Cyberspace

In the realm of cyberspace, web browsing emerges as a significant activity that generates points that can be analysed to reveal information about the user, commonly referred to as "data exhaust". These data, collected through technologies like cookies, browser fingerprinting, and flash objects, enable detailed user tracking. Employing advanced techniques such as machine learning and big data analytics, particularly within the advertising industry, these tools facilitate the reconstruction of individual browsing histories and behaviours (Figure 1).

This analysis is critical for advertisers to implement strategies like behavioural targeting, frequency capping, retargeting, and conversion tracking, leading to highly personalised advertising experiences [4–6]. Additionally, publishers leverage these data for content customisation, significantly boosting their revenues, with reports indicating up to a 52% increase due to third-party cookie usage [7].

While these practices offer enhanced user experiences and economic benefits for publishers, they also bring forth significant privacy challenges. The core issue centres on the implicit nature of user consent in the data-collection process and the resultant lack of user control over their personal information.

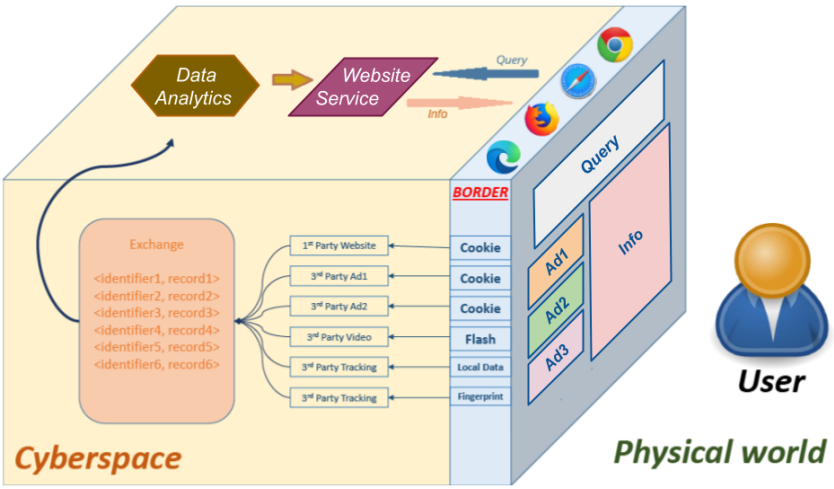

Figure 1. Analysing and tracking activities at the border. User preference information gets collected, exchanged, and analysed from browsers.

1.2. Privacy in Personal Cyber–Physical Systems

The burgeoning industry of smart devices and wearable gadgets, which collect and transmit private user data for advanced services, has brought forth significant privacy concerns. These devices, acting as personal data hubs, are at the forefront of collecting sensitive information such as activity, location, and health data, as illustrated in Figure 2. The repercussions of privacy breaches here extend beyond data loss to potentially include disinformation campaigns, behavioural manipulation, and financial exploitation. The emotional impact of feeling constantly monitored, or having intimate details exposed, can undermine public trust in technology.

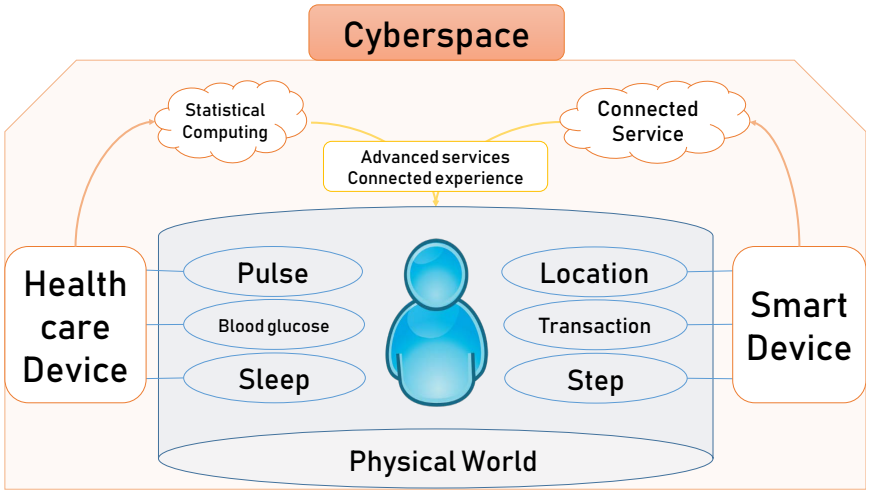

Figure 2. Personal data hub paradigm. Smart devices and healthcare devices collect personal data for cyberspace entities to provide advanced services and connected experiences.

In this context, user autonomy over personal data is crucial. The integration of smart devices into daily life mandates user control over data storage, sharing, and deletion. This requires transparent user interfaces and clear mechanisms for consent, ensuring users can make informed decisions about their data. Additionally, ensuring data security during storage and transmission, especially considering the heterogeneous nature of device capabilities, is a vital aspect of protecting user privacy in these systems.

1.3. Privacy in Proactive User-Driven Data Collection

In the digital era, the unprecedented level of proactive data collection through connected devices like smartphones and IoT gadgets has highlighted significant privacy concerns. As depicted in Figure 3, data collected from the physical world are seamlessly integrated into cyberspace, contributing to a complex privacy landscape. This paradigm shift is epitomised by participatory sensing [8,9], where individuals use their devices as sensors to collect environmental data such as noise levels, traffic conditions, and temperature. This method of data collection, utilised by billions of smartphone users, offers immense benefits but also poses serious privacy concerns, especially around identity privacy.

Moreover, the evolution of data collection has sparked interest in leveraging opportunistic networks. These networks, beneficial in both infrastructure-lacking and well-connected areas, can augment existing systems and provide localised communication. However, they introduce unique privacy challenges, particularly in terms of identity protection and data security. The balance between the convenience and innovation offered by these technologies and the need to safeguard personal privacy is a central theme in understanding and addressing the challenges of proactive user-driven data collection.

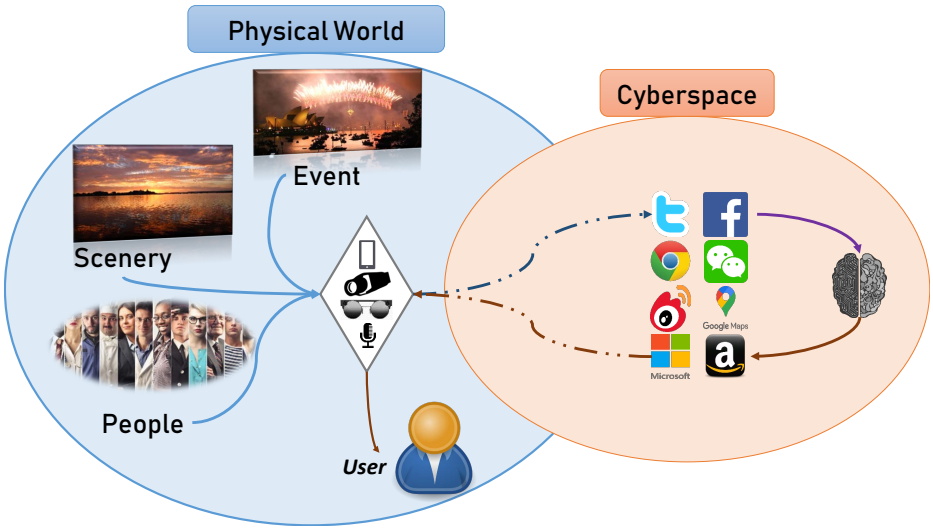

Figure 3. Information leakage during active data-collecting behaviours. People use smart devices to collect and upload different types of data that simultaneously get collected in cyberspace.

1.4. Road-Map

The rest of this paper is organised as follows. In Section 2, we discuss privacy concerns associated with user actions in cyberspace, and two featured scenarios of user activities in cyberspace are articulated: web privacy protection and user input disclosure. In Section 3, we investigate privacy concerns within the interactions of cyberspace and the physical world. We discuss scenarios regarding smart home devices and wearable gadgets. In Section 4, we explore user activities in the physical world involving pervasive computing where user privacy in participatory sensing and opportunistic networks raise user privacy concerns. Open issues are discussed in Section 5 considering privacy protection for complex applications. We conclude this paper in Section 6.

2. Privacy Concerns Raised with User Cyberspace Activities

With the boundless interactions in cyberspace come potential risks, particularly concerning user privacy. As we delve deeper into user cyberspace activities, following the trend of data exhaust collection, several privacy attack vectors surface: data exhaust tracking, the use of tracking technologies, identity tracking from browsing exhaust, and user input data disclosure.

2.1. Data Exhaust Tracing

The concept of data exhaust tracing involves the analysis of user-generated data during web browsing. These data include browsing habits, clicked links, and interactions with various web elements. When collated, these data can paint a detailed picture of a user's online behaviour [4].

2.2. Use of Tracking Technologies

The advertising industry, particularly through third-party domains connected with publishers' websites, employs technologies like cookies, flash storage, and browser fingerprinting to track users [5,6]. These tools enable the identification and tracking of users across different websites, allowing for the compilation of data to reconstruct individual browsing histories.

2.3. Identity Tracking from Browsing Exhaust

Identity tracking has emerged as a significant privacy issue, where third parties exploit browsing history, shopping behaviours, and purchase habits for targeted advertising [6]. This type of tracking often extends beyond the primary website to several other entities, leading to the creation of comprehensive user profiles.

2.4. User Input Data Disclosure

Beyond passive data collection, the recording and utilisation of user input data during web browsing poses additional privacy risks. These include the collection of personally identifiable information, potential for data leakage, and misuse of sensitive input data [10,11].

2.5. Protections and Limitations

Various measures, such as DNS Filtering, Network Proxies, VPNs, and Incognito/Private Browsing Modes, are employed to combat these privacy risks. However, they face challenges, such as difficulties against encrypted transmissions and ineffectiveness against fingerprinting tracking [12–15]. Browser extensions have proven more effective, adept at differentiating between first-party content and third-party trackers.

For user input, traditional approaches like differential privacy introduce noise into collected data but face challenges in large-scale applications [16,17]. Local differential privacy (LDP) offers a viable alternative, allowing users to perturb their data inputs, thus providing plausible deniability.

A significant limitation arises in the realm of unstructured user input, which includes free-form text, images, and videos shared or uploaded by users. Protecting the privacy of such data is challenging because it often contains nuanced and context-specific information that is difficult to anonymise without losing its inherent value or meaning [18]. Traditional privacy-preserving techniques like data masking or encryption may not be effective for unstructured data due to its variability and complexity. Furthermore, automated systems for processing unstructured data, such as natural language processing (NLP) tools, can inadvertently expose sensitive information if not designed with robust privacy safeguards.

2.6. Countermeasures

The myriad activities in cyberspace, particularly web browsing, bring forth a range of privacy concerns. Understanding these risks and adopting comprehensive solutions,

such as browser extensions and local differential privacy, can mitigate these challenges and ensure a safer, more private digital environment.

2.6.1. Web Privacy Protection: Browser Extensions

In the digital landscape, browser extensions have risen as pivotal tools for bolstering online privacy. Beyond merely blocking ads, these tools shield users' digital interactions from intrusive third-party tracking, fostering a more private browsing environment. In the following, we present our survey on several renowned browser extensions, with a summarised overview presented in Table 1.

We classify surveyed tracking protection extensions by their blocking techniques: list-based, algorithm-based, and machine-learning-based blocking. For extensions that are based on lists, a popular subcategory is crowd-sourced-list based. There are many famous and familiar names such as Ad-Blocker [19], AdBlock [20], Adblock Plus [21], and uBlock [22]. These extensions have drawn attention in the community since the early days of the battle against third-party ads. Consequently, a core blocking list *EasyList* has been contributed to and maintained by the community. At the time of writing, EasyList consists of over 17,000 third-party advertisers, 13,500 general third-party and specific URL patterns, as well as 31,000 advertisement element filters [23]. Extensions like Ad-Blocker use Easylist's filter rules to prevent ads from loading, thereby limiting user tracking. In addition to EasyList, extensions based on rules also adopt other filter lists, including anticircumvention lists or third-party tracker filter lists. The anticircumvention lists help advertisement-blocking extensions fight against the detection and circumvention of the extensions and reinsertion of ads. The third-party tracker filter lists help against tracking from companies and organisations that do not directly insert advertisements.

While crowd-sourced lists are community-driven, another approach is centralised maintenance, encompassing extensions like Ghostery [24], Disconnect [25], Blur [26], and AdGuard [27]. Owing to the centralised control, these extension companies set the blocking rules, and they typically have considerably fewer rules than crowd-sourced lists [12]. While these extensions enable rule customisation, they often define certain network requests as necessary third-party content and thus unblockable. Alongside their primary ad-blocking features, commercialised versions of these extensions offer added functionalities: Ghostery Insights [28] provides a time-lined analysis and loading performance details; Disconnect Premium [29] presents an optional VPN, full IP masking, and data encryption; Blur Premium [26] offers enhanced protection for personal information; and AdGuard Premium [30] incorporates advanced tracking and phishing protection, enhanced parental controls, and a VPN option. Regrettably, unlocking these premium features typically involves payment and occasionally granting permissions for data collection.

In addition to the conventional list-based blocking paradigm, the Firefox Multiaccount Containers extension introduces a user-curated containment strategy [31]. Instead of determining which content to block based on predefined or community-sourced lists, this extension gives users the autonomy to classify websites into isolated containers, such as 'Work', 'Shopping', and 'Social'. Each container encapsulates its associated browsing activity, ensuring that cookies, cache, and site data remain confined within its designated environment. By enabling this segregation, the extension effectively curtails the scope of third-party trackers, preventing them from correlating a user's diverse online activities across different containers. While this method requires a more hands-on approach as users must manually assign websites to the desired containers, it offers a personalised and flexible strategy to counter pervasive online tracking, emphasising user control over data compartmentalisation.

Moving beyond list-based ad-blockers, some extensions utilise algorithms to automatically decide whether a third-party's content needs to be blocked. A popular example is an extension called Privacy Badger [32], which monitors third-party organisations, counting the number of websites they use for user tracking. If an organisation's count reaches three, it blocks their content from loading. Additionally, Privacy Badger can detect canvas-based

browser fingerprinting and block tracking from third-party domains [33]. In the realm of canvas-based browser fingerprinting, another noteworthy extension is CanvasBlocker [34]. It operates by either blocking or faking the readout of the HTML5 canvas element, a prime target for fingerprinting techniques aimed at uniquely identifying and tracking users. By doing so, CanvasBlocker effectively thwarts attempts by websites to exploit this method of tracking, adding an extra layer of privacy to user browsing sessions [34,35].

A newly emerged ad-blocking tool adopts machine learning techniques based on a perceptual study from the ads' loading content. Existing works [36–38] have introduced a new concept of perceptual ad-blocking, which seeks to improve resilience against ad obfuscation and minimise the manual effort needed to create ad-blockers. For traditional ad-blocking relying on crowd-sourced lists or ones based on centralised maintenance, two downsides have been identified: (1) the consistency of filter lists requires constant synchronisation with the latest versions and (2) different strategies have been developed for evading crowd-sourced lists (like EasyList) such as changing domains, moving resources to the publishers, removing ad keywords from URLs, and removing image dimensions from URLs. Thus, it became an arms race between ads and tracker-blocking tools and third-party domains. Researchers claim that the novel approach of using perceptual signals effectively reduces the arms race with web publishers and ad networks [39]. Storey et al. [36] based their perceptual ad-blocking on a legal requirement for the recognisable display of ads by humans. Based on the legal requirement, Storey et al.'s Ad-Highlighter [40] focuses on learning captured visual and behavioural information that can be used to distinguish ads, e.g., the text "Sponsored", the ad's circled "i" information icon, or an ad network logo. However, this method has its challenges, as the markup information can be rendered invisible. To overcome the challenge of this specific rendering, [38] introduced the project Sentinel, a machine learning version of Adblocker Plus that uses an object-detection neural network to locate ads in raw website page screenshots [41]. To further enhance rendered web pages, ref. [37] introduced a new technique to achieve the goal. In their work, a deep-learning-based ad-blocker module is embedded into Chromium's rendering engine so that images of ads can be detected directly [37].

Besides many experimental adoptions of machine learning for perceptual ad-blocking, ref. [42] showed a different way of using machine-learning-based classification to block ads. Iqbal et al. [42] introduced AdGraph, which applies machine learning approaches to graph representations built from web pages considering aspects such as the HTML structure, network requests, and JavaScript behaviour. When AdGraph's modifications were applied to Chromium, the results showed higher accuracy and reduced computational overheads compared to traditional ad-blocking extensions.

Table 1. Surveyed web browser extensions.

Technique	Ref.	Feature
List based	[20] [19] [21] [22]	Crowd-sourced list
	[24] [25] [26] [27]	Centralised maintenance
	[31]	User-curated list based
Algorithm based	[32] [33] [34]	Detect browser fingerprinting
Machine learning	[36]	On image pattern
	[38]	On screenshot
	[37]	On rendering engine
	[42]	On behaviour pattern

2.6.2. Local Differential Privacy

Local differential privacy (LDP) is a refinement of differential privacy, aimed at ensuring that the removal of an individual entry does not significantly alter the overall data distribution [16,43]. Distinctive for its noise perturbation at the user end, LDP has been applied in notable projects like Google's RAPPOR [44] and Apple's Learning with Privacy [45].

LDP's core is based on the Random Response principle [46], ensuring a probability that collected data reflect the true value. This principle has been adapted for various applications by major tech companies, including Google, Apple, and Microsoft, spanning areas like longitudinal collections and itemsets mining.

Google's RAPPOR uses unary encoding with a permanent randomised response, integrating Bloom filters for efficient encoding in large-domain surveys [44,47]. This has led to advances in frequency estimation and heavy hitter identification under LDP [48–50]. Apple, meanwhile, employs discrete Fourier Transformation and sketching algorithms for noise addition and domain dimensionality reduction, demonstrating centralised differential privacy applications within an LDP framework [51,52].

Microsoft has further expanded LDP's scope to include telemetry collection [53], graph data analysis [54], language data analysis [55], iterative interactions [56], and incorporating prior knowledge [57]. These developments illustrate the evolving landscape of LDP, addressing the intricacies of various data types and privacy concerns.

Additionally, Federated Learning exemplifies the integration of LDP principles with decentralised data processing, emphasising privacy in training directly on source data, such as user devices. This approach is complemented by ongoing research in optimising noise injection in LDP to balance data utility and privacy [58–60].

The realm of LDP is also making strides in handling time-series data, a growing concern due to the rise of IoT devices and financial analyses. This type of data, characterised by its sequential nature, poses unique challenges in privacy protection. Techniques like adaptive noise strategies and the sliding window approach are being explored to address these challenges, providing flexibility in data collection granularity and enabling varied privacy tiers based on data sensitivity [61].

In recent developments, the application of LDP to unstructured user inputs like voiceprints, face graphs, and sensitive texts presents new challenges. These include the complexity of data types, maintaining data utility post-transformation, and ensuring computational feasibility on personal devices. Adaptations of current DP works to LDP models are underway, focusing on the localised processing of sensitive data while maintaining its semantic integrity and functional utility. This expansion of LDP into diverse domains of unstructured data marks a significant progression in the field, addressing the increasing demand for robust privacy solutions in our digital age.

Voice data, known for their variability, pose unique challenges in LDP implementation, especially in preserving essential characteristics for applications like voice recognition. Han et al. extend differential privacy to voiceprints, introducing a metric privacy model that accounts for the similarity between voiceprints [62]. Adapting this approach to LDP entails developing localised voiceprint sanitisation methods. These methods should perturb voice data at the source, balancing the privacy–utility trade-off and ensuring computational efficiency for feasible implementation on standard user devices. The goal is to protect voiceprint privacy while maintaining the utility for voice recognition and other voice-based applications.

The complexity and sensitivity of facial images require intricate processing to maintain privacy while preserving utility in applications like facial recognition. Jia-Wei Chen et al. provide a framework for facial image obfuscation based on perceptual indistinguishability [63]. Similarly, Liyue Fan proposed methods for pixelizing images to protect identifiable features [64]. For adapting these approaches to an LDP model, efficient, local obfuscation techniques are needed. This involves customising algorithms for on-device processing,

ensuring facial data are privatised before leaving the user's device and maintaining the balance between privacy protection and the utility of the obfuscated images.

Sensitive text data present complex challenges for LDP. Maintaining the semantic and contextual relevance of text after privacy transformations is a key difficulty. Current DP works, such as Natasha Fernandes et al.'s work [65], focus on text obfuscation by using 'bags-of-words' models. This approach aims to obscure authorship clues while preserving content. Feyisetan et al. demonstrate advanced text perturbation methods to balance privacy and analytical utility [66]. The potential development for LDP in this domain involves adapting these methodologies for local implementation on user devices. This adaptation would ensure privacy from the initial data-generation stage, possibly through the use of lightweight, efficient algorithms suitable for real-time processing on personal devices.

2.7. Discussion

We surveyed protections on browsing exhaust and user-response disclosure for data collection at the traditional border between the physical world and cyberspace. For browsing exhaust protection, there is an ongoing arms race between web browser extensions and exhaust-tracking techniques. Core concepts for the developing browser extensions have evolved from elementary rule-based filters to perceptual blocking involving machine learning technologies, where further research can be focused. For private user-response disclosure, LDP has shown its promising applications from *Google and Apple's* implementation. Despite the current research streams on LDP data utilisation, the realisation of LDP on special survey domains and approaches requires more research.

3. Privacy Concerns in Personal Cyber–Physical Systems

Recent incidents, such as the unintentional revelation of secret military bases by a fitness tracking app in 2018 [67] and a substantial data breach at a smart toy manufacturer in 2015 [68], have brought to light significant privacy concerns within personal cyber–physical systems. These events highlight the criticality of addressing two primary privacy concerns, which also represent key attack vectors: unauthorised data access in smart devices and vulnerabilities in the secure transmission of data.

3.1. Unauthorised Data Access in Smart Devices

Smart devices and wearable gadgets, which play a pivotal role in health monitoring, are increasingly vulnerable to unauthorised data access. These devices, diverse in their computing and communication capabilities, are prime targets for cyberattacks. The most prevalent attack vectors involve exploiting software vulnerabilities through sophisticated hacking methods and gaining unauthorised access via deceptive phishing attacks. The data at stake, encompassing sensitive health records and precise location information, are at risk of being misused, resulting in substantial privacy violations.

3.2. Vulnerabilities in Data Transmission

A significant concern in the realm of personal cyber–physical systems, especially in healthcare, is the secure transmission of sensitive patient data, including medical histories and physiological metrics. This data transmission necessitates robust encryption to ensure privacy and maintain data integrity. Nevertheless, the challenge arises with healthcare devices constrained by limited resources, where traditional encryption methods like the Advanced Encryption Standard (AES) encounter operational difficulties. These limitations make the devices susceptible to sophisticated cyber threats, such as man-in-the-middle attacks, during the data-transmission process.

3.3. Protections and Limitations

To address privacy concerns in personal cyber–physical systems, several protective measures have been developed, though they come with inherent limitations.

Rigorous data-access controls are implemented to prevent unauthorised access to sensitive data on smart devices. However, these controls often falter when users inadvertently grant permissions to third-party applications, leading to potential security loopholes. Developing user-friendly yet secure access-control mechanisms remains a critical challenge.

In terms of data transmission, AES is a widely adopted method in well-resourced devices [69]. However, AES is less feasible for resource-limited healthcare devices due to its high computational demand. As a result, there is an increasing need for adaptable encryption solutions that balance security with the operational capabilities of these devices.

The overarching challenge is striking a balance between efficiency and security. While lightweight encryption techniques offer promise, there is still a pressing need for innovations in encryption technology that can provide robust security without compromising the operational efficiency of various devices in these systems.

3.4. Countermeasures

With rising privacy concerns as many devices become connected and transform into personal physical cyber systems, several countermeasures have been developed to protect users. In our survey, we focus on the emerging technology of access-control enforcement for wearable equipment and lightweight encryption in healthcare devices.

3.4.1. Access-Control Enforcement for the Wearable Equipment

The technology of access-control enforcement plays a core protection role in many IoT network systems since it directly answers the privacy issue of accessibility mentioned above. It applies a range of selective policies, setting the criteria of who can access the data. The main purpose of an access-control-enforcement mechanism is to block unauthorised and random queries towards a protected data repository. Besides the passive protection, rather than blocking arbitrary connections, it sets up a bottom line against insider attacks or general platform sharing with an efficient privilege update and revocation mechanism. Access-control mechanisms for IoT systems have drawn much research attention, and several works have been proposed as effective and practical solutions for wearable technology in different scenarios. Since access-control enforcement has a wide research scope, in the following section we survey a few typical works and focus on wearable gadgets and connected healthcare devices.

One research focus required for wearable gadgets is to develop context-aware access control with a more expressive policy. In 2010, Garcia-Morchon and Wehrle [70] proposed a modular context-aware access-control mechanism that allows a system administrator to compose each module with a well-defined goal so that access policies for different required functionalities can be assigned to different modules. Ray et al. [71] tried to improve the expressiveness by using attribute-based access control from the NIST NGAC framework and achieved the first conceptual prototype for an IoT infrastructure. Later in the same year, Salama et al. [72] successfully combined public key infrastructure and attribute-based access control for a multilevel access control on patient healthcare monitoring.

Another research focus for wearable gadgets and connected healthcare devices is usability. This feature is neglected by most of the existing access-control works since an administrative model is generally assumed for access-control scenarios. However, especially for wearable gadgets, there is no administrative staff for these private devices, and the users are the ones who configure, manage, and protect the devices and resources. Thus, for the users who often lack the necessary security knowledge, an easy-to-use interface and enhanced presentation need to be provided for policy configuration [73]. In 2011, Kim et al. [74] proposed the first access-control mechanism that provides a full solution to usability. Their newly introduced automated Clairvoyant access right assignment mechanism can suggest suitable access-control policies. Unfortunately, their work is designed for smart home scenarios where its inherent *overprivilege* property can be tolerated [73]. To address this issue of overprivilege, Tian et al. [75] proposed an automated access policy generation based on checking the functionality and behaviour of the entity that asks for

access. Their access-control mechanism was oriented towards smartphone applications accessing local resources, which can be extended to other IoT systems like accessing data in wearable gadgets. After an appropriate access policy is generated, it is then provided to the user for review.

Other research focuses include distributed environments [76,77], dynamic access control [78], scalability [79], and multilateral security [80]. These works will be compared with aforementioned works with other focuses in Table 2.

Table 2. Comparative analysis of access-control mechanisms for wearable equipment.

Ref.	Primary Focus	Strengths	Limitations/Applications
[70]	Modular Context-Aware Access Control	Flexibility in module composition for diverse functionalities	Complex administration
[71]	NIST NGAC Framework Application	Enhanced expressiveness with attribute-based control	Conceptual prototype
[72]	Multilevel access control with PKI	Combination of PKI and attribute-based control for layered security	Focused on patient monitoring
[74]	Usability in Access Control	Automated Clairvoyant access right assignment for user convenience	Overprivilege issues
[75]	Automated Policy Generation for Smartphones	Functionality and behavior-based policy suggestion	Oriented towards smartphone apps
[76]	BiLayer Access Control Model	Secure and scalable model for IoT environments	Additional infrastructure support
[77]	Virtual Patient Record Security	Protects patient data in distributed environments	Specific to healthcare data management
[78]	Indeterminacy-Tolerant Access Control	Robust in dynamic and uncertain environments	Complexity in implementation and management
[79]	RFID Tag Access Control in Healthcare	Scalable solution for RFID systems in healthcare	Specific to RFID technology and healthcare context
[80]	Multilevel and Multilateral Security	Lightweight approach suitable for IoT devices	Multilateral security requirements

3.4.2. Lightweight Encryption in Healthcare Devices

Lightweight symmetric encryption can provide encryption requirements from connected healthcare devices, especially implantable medical devices like pacemakers where other protections are difficult to implement. Connected healthcare devices are usually computationally weak and restrained by battery life, and implantable medical devices often are additionally restricted with a minimal physical size that leads to implementation constraints in hardware [81–83].

With these limitations, some features/properties in lightweight encryption become rather more acceptable and welcome. These features include implementation flexibility, a smaller block size, encryption rounds saving, and restricted versatility.

- *Implementation Flexibility*—For the implementation of encryption on resource-restrained devices, the trade-off is only determined when applied to a specific scenario [84]. Thus, when a feature is specifically needed for a deployment scenario, the encryption algorithm should be optimised with acceptable sacrifice to other aspects.
- *Lower Size*—For healthcare devices that have a small physical size and need to run for an extended period with limited battery, the design of an encryption algorithm may

need to prioritise resource limitations. In this case, a smaller block size or internal state becomes acceptable.

- *Less Rounds*—For healthcare devices, a particular nature is that its total amount of output messages is considered relatively fewer. For example, a pacemaker working for ten years outputs less than 2^{30} pairs of plaintext and ciphertext, which may lead to the relaxation of the total number of primitive rounds while retaining approximately the same security level [85].
- *Limited Versatility*—The healthcare device where the encryption algorithm is to be implemented is usually function- and operation-focused, which makes encryption algorithms that have limited versatility rather welcome.

Considering the above implementation difficulties, security requirements, and feature preferences, our survey on lightweight symmetric encryption focuses on the algorithms that have a small block size or internal state and can manage short keys. Most of the candidate algorithms lie in block ciphers and stream ciphers due to the restrained resource. For hash function-based algorithms, only PHOTON [86] and Spongent [87] have ideally a small internal state size. A summary of the surveyed algorithms is shown in Table 3.

Table 3. Comparison among suitable lightweight encryption schemes.

Block Ciphers				
Name	**Ref.**	**Key**	**Block**	**Rounds**
Joltik	[88]	64/80/96/128	64	24/32
Mantis	[89]	128	64	14
Skinny	[89]	64–384	64/128	32–56
Qarma	[90]	128/256	64/128	16/24
T-TWINE	[91]	80/128	64	36
GIFT-64	[92]	128	65	28
SPARX-64/128	[93]	64	64	32
Stream Ciphers				
Name	Ref.	Key	IV	IS
A2U2	[94]	61	64	95
Sprout	[95]	80	70	89
Plantlet	[96]	80	90	110
Hash				
Name	Ref.	Digest	Block	IS
PHOTON	[86]	80–256	16/32/64	100–288
Spongent	[87]	80–256	8/16	88–272
ISAPv1-A-128a	[97]	64	128	320
Saturnin	[98]	192	256	256

While lightweight encryption offers optimised solutions tailored for resource-constrained devices, it is pivotal to be cognisant of potential trade-offs. Balancing efficiency with robust security is a delicate act. In some instances, the efficiency of lightweight encryption might come at the cost of reduced security when compared to their heavyweight counterparts. Such trade-offs necessitate meticulous evaluation, especially when patient health and data are at stake.

3.5. Discussion

For private data stored in many smart devices including wearable equipment that builds a personal data hub, we explored how the data collected by these devices can be accessed and the challenges associated with transmitting sensitive data from resource-constrained devices. Existing access-control approaches help with the general purpose of controlling accessibility. However, most research works have not considered the usability that presents an essential requirement for personal scenarios. Another field in access control

for future research is how to delicately assign accessibility according to the sensitivity of the collected data. An example would be that location information in residential areas, compared to public places, should be considered highly private and not suitable to be accessed by most applications. In terms of protection during transmission, lightweight encryption has shown practical promise in many IoT devices. For healthcare devices, which could benefit from the seamless 5G network in the near future, characterised lightweight encryption schemes are expected to fit the challenging privacy scenarios.

4. Privacy Concerns during User-Driven Data Collection

With the rise of user-driven data collection through connected devices and participatory sensing platforms, privacy risks have become increasingly prevalent. This section delves into the specific attack vectors in these scenarios, focusing on the inadvertent leakage of personal information and the vulnerabilities in decentralised networks, particularly opportunistic networks (OppNets).

As participatory sensing becomes more integrated into our daily lives through the proliferation of smart devices, users frequently encounter decentralised network structures, including OppNets. This trend of leveraging sensors in devices for data collection exposes users to notable privacy risks. Often, media containing sensitive information like location, time, and identity is uploaded unknowingly by users, leading to inadvertent data exposure [99].

OppNets, serving as a common alternative to traditional network infrastructures, are increasingly relevant in a variety of contexts, not just in remote or poorly connected areas. These networks are characterised by their decentralised and dynamic nature, which presents unique privacy challenges. Understanding these challenges is essential for addressing the specific attack vectors that arise within these networks, which are becoming more commonplace as participatory sensing grows.

4.1. Inadvertent Data Leakage

A major attack vector in user-driven data collection is the inadvertent leakage of personal information. Users often share media files embedded with sensitive data such as geolocation and timestamps without realising the potential privacy implications. This type of accidental exposure underlines the need for increased awareness and more stringent control over data-sharing practices in the era of widespread participatory sensing.

4.2. Residual Data Traces

Residual data traces in digital content pose another significant privacy concern. Attempts to remove personal data from uploads often leave behind remnants vulnerable to exploitation. Addressing this risk requires effective data-sanitation methods capable of thoroughly eliminating personal traces and protecting user privacy in the digital space.

4.3. Collector Vulnerability

In the realm of participatory sensing, the entities collecting data—whether individuals or applications—face distinct vulnerabilities. As aggregators of sensitive user information, these collectors can become targets for cyberattacks. Ensuring their security is crucial and necessitates robust protective measures for both the data and the collectors.

4.4. OppNets Network Node Vulnerability

The decentralised structure of OppNets inherently makes intermediate nodes susceptible to compromise or malicious activities. These nodes, critical for ensuring seamless data transmission in the absence of stable, centralised networks, can become potential targets for various cyber threats. Security breaches in these nodes, ranging from data interception to unauthorised access, can have far-reaching consequences, jeopardising the safety and privacy of transmitted information. The studies by Kumar et al. [100], Tsai et al. [101], and

Irshad et al. [102] highlight the vulnerabilities and potential security breaches that can occur in these scenarios.

OppNets Network Authentication Risks

The decentralised framework of OppNets introduces complexities in authentication processes, representing significant privacy risks. Ensuring the secure transmission of sensitive personal information in OppNets requires robust, adaptable authentication mechanisms [103,104]. Developing these mechanisms is essential for safeguarding data against unauthorised access and maintaining the integrity of information within these versatile networks.

4.5. Countermeasures

Addressing privacy concerns in user-driven data collection, particularly in participatory sensing and OppNets, involves diverse countermeasures including access control, advanced encryption, location privacy protection, and robust authentication. While the ample computational power of modern smartphones enables the use of sophisticated encryption methods without significant limitations, our research primarily focuses on enhancing location privacy in participatory sensing and ensuring anonymous authentication within OppNets. This targeted approach allows us to concentrate on specific challenges and vulnerabilities inherent in these systems, such as protecting sensitive location data and securing decentralised network interactions, which are crucial in the dynamics of pervasive user data collection.

4.5.1. Location Privacy in Participatory Sensing

The issue of location privacy sits at the forefront of concerns in participatory sensing. The very act of sharing location details within the sensing communication network or with third-party entities can jeopardise an individual's privacy. However, the dichotomy arises when considering the utility of location data. Low-quality or imprecise location data could diminish the overall value of participatory sensing. Consequently, there is an ongoing struggle to strike a balance between preserving location quality and ensuring location privacy, a topic of much interest to researchers. Over the years, various methodologies have been explored to address this challenge. The most impact among these can be distilled into three primary techniques:

- *Dummy locations*—Initially introduced by Kido et al. [105], the concept of dummy locations involves sending queries with the user's actual location and several fake locations. This technique effectively confounds service providers, making it difficult to pinpoint the user's true location. Further advancements in this area include the work of Liu et al. [106], who developed a spatiotemporal correlation-aware dummy-based privacy-protection scheme, and Hara et al. [107], who focused on dummy-based user location unionisation under real-world constraints. These developments enhance the method's effectiveness, particularly in scenarios where individual location information is crucial.
- *Obfuscation*—Duckham and Kulik's novel approach [108] involves negotiating the degradation of location information. This technique allows for a tailored balance between privacy protection and service quality. Through negotiation algorithms, users can dynamically adjust the level of obfuscation applied to their location data, ensuring adequate privacy while maintaining the efficacy of the service. The method has evolved to include various forms of perturbation [109] and generalisation [110], making it adaptable to a wide range of participatory sensing applications.
- *k-anonymity*—Stemming from the foundational concept of k-anonymity [111], Gruteser and Grunwald [112] developed a method that conceals a user's location within a group of $k-1$ other users. This approach has been further refined in studies like Niu et al. [113], offering enhanced anonymity in privacy-aware location-based services.

While effective in specific scenarios, it is less robust for continuous location tracking and can suffer from reduced accuracy [114], potentially affecting service reliability.

4.5.2. Anonymous Authentication for OppNets

In OppNets, ensuring both authentication and anonymity is crucial. While authentication validates nodes and secures the network, anonymity protects users' identities, a critical aspect in today's privacy-conscious digital landscape.

The authentication procedure in OppNets serves a dual purpose: verifying a node's credentials and shielding the network from unauthorised intrusion. It also maintains the integrity of the packets received by nodes. The absence of direct paths between distant nodes in OppNets intensifies the challenge of constructing efficient authentication algorithms. Add to this the pursuit of preserving anonymity in these dynamic settings and we are faced with an intricate problem. A few novel algorithms that have navigated this complex maze are discussed in the literature and encapsulated in Table 4.

Carver and Lin's 2012 proposition represents one of the earlier forays into this domain. They advocated an authentication scheme for OppNets that capitalised on group-oriented broadcast encryption, deeply rooted in pairing [115,116] and identity-based signatures. Optimised for Bluetooth and 3G communications [117], their methodology ensured packet forwarding without necessitating recipient knowledge, thereby preserving user privacy to an extent. However, this method unveiled the sender's details after authentication. An inherent limitation was the dependency on a trusted third-party entity for key generation and group taxonomy, a potential Achilles' heel if this third party were ever compromised [118].

Exploring complete user privacy, Guo et al.'s 2015 framework set a new benchmark [119]. Designed for constrained wireless network environments with short-lived connectivity, their strategy assigned a super node for node registration. Their security approach blended both symmetric and asymmetric encryption techniques, buttressed by the use of hash functions to cloak user identities. Kumar et al. in 2017 built upon this foundation, emphasizing dynamic user identities for key exchanges and integrating RSA encryption to safeguard data during transmission.

Taking a divergence from conventional encryption methodologies, Kuo et al. charted fresh waters with their authentication scheme, deeply entrenched in hash functions and point operations [120]. Though not originally crafted for OppNets, its roaming authentication capability indicated potential compatibility, promising enhanced performance and bolstered security.

Table 4. Comparison among anonymous authentication for OppNets.

Ref.	Technique	Feature
[117]	Broadcast encryption	Partial privacy
[119]	Symmetric and asymmetric encryption	Hashed user ID
[100]	RSA encryption	Dynamic user ID
[120]	Hash functionality Point operation	Encryption free

4.6. Discussion

The existence of users and data generated by users raise concerns about protecting user privacy during active data-collecting activities. From these concerns, we survey the problems of location privacy in participatory sensing and anonymous authentication in OppNets. To protect a participant's location data, a compromise in the quality of the location data is usually the trade-off, although many efforts have been made to mitigate the effect. Concerning identity privacy in OppNets, existing solutions heavily rely on encryption techniques, which can be expensive considering heterogeneous devices. Encryption-free anonymous authentication requires more research as it potentially has more application scenarios.

5. Future Vision on Complex Privacy Problems

There are many complex privacy problems already identified that soon could have a considerable impact on industry as well as our daily lives. We deliver our future vision on three of these privacy concerns, i.e., trajectory privacy, privacy in smart metering, and involuntary information leakage with ambient intelligence.

5.1. Trajectory Privacy

When we apply the traditional scenario of cookie privacy concerns to mobile applications, users' trajectories become at risk due to location information embedded in cookie logs. Cookie logs in cyberspace may contain high-quality user location information, which can be collected directly by using GPS coordinates with a user's fast consent to an unexplained location service permission requirement or indirectly collected with location tags from a local network or service provider in the physical world. This potential privacy breach should be categorised to a more dangerous level than web browsing history or personal preference logs. More detailed physical activities, routine habits, or even mental status can be inferred by analytical work on user trajectories. The infamous Uber travel history leakage lawsuit in 2017 [121] is a relevant example. Ref. [122] developed a privacy analysis system on user login records and physical context information and deepened the understanding of user physical-world privacy leakage via cyberspace privacy leakage. It becomes clear that user trajectories can be discovered and confirmed when third parties analyse their cookie logs as users move and browse in their daily lives let alone potential exogenous records of GPS coordinates. These cookie logs may further be exchanged with other analytics companies for centralised analysis connecting with other web activities, exposing the private physical trajectory to more entities. Compared with other private data, physical trajectory is more effective for reidentification by auditing relevant activity logs at locations and comparing differential timelines. The balance between utility and privacy with location data has drawn much research attention. However, for this physical-world trajectory leakage via user cyberspace data, further research efforts are required.

5.2. Privacy in Smart Metering

As part of the pervasive data collection in cyberspace, smart metering in smart energy supply networks represents a critical evolution in data interaction between consumers and service providers. This evolution aligns with the broader theme of our paper, which examines how technological advancements in data collection impact user privacy [123].

For smart energy supply, smart metering collects detailed consumption data and helps evaluate the status of a smart energy grid for more efficient resource distribution. This data transmission, often in plaintext, raises significant privacy concerns, especially when linked with the personal activities of consumers [124–126].

Consumption data, inherently tied to the private activities of consumers, form the core of sensitive information valuable to service providers [127]. Alongside these data, location tags and physical address information significantly contribute to the risk profile. While location tags provide a dynamic geospatial context, physical addresses link the consumption data directly to a fixed, real-world location. This amalgamation of consumption patterns, location's context, and identifiable addresses creates a substantial attack surface, attracting the attention of potential adversaries.

To mitigate these risks, the application of cryptography is vital. By employing advanced cryptographic techniques, the sensitive attributes of the data—including consumption patterns, location tags, and physical addresses—can be securely encrypted. This ensures that even if data are intercepted or accessed by unauthorised entities, the critical components remain unintelligible and protected. Moreover, cryptographic solutions can be tailored to safeguard the integrity and confidentiality of this information, both during transmission and storage, thereby significantly reducing the attractiveness of the data to potential attackers and minimising the risks associated with data breaches.

However, a key obstacle is the limited resources that the smart meters have to perform strong cryptography [127]. Therefore, it remains a challenge for future research focusing on cryptography-based mechanisms that must provide confidentiality while minimising resource consumption.

5.3. Privacy Challenges in Vehicular Ad Hoc Networks

The evolution of transportation systems, driven by the integration of vehicles and infrastructure, has given rise to Vehicular Ad Hoc Networks (VANETs) [128]. VANETs represent another aspect of the pervasive data-collection paradigm discussed in this paper. The integration of these networks in transportation systems, especially in autonomous vehicles, brings forth unique privacy and cybersecurity challenges.

One of the primary vulnerabilities in VANETs is the potential for data breaches. In autonomous vehicles, vast amounts of data are collected and transmitted, including sensitive personal information such as location, travel patterns, and in some cases, user identity [129]. The interception of these data by unauthorized entities can lead to privacy violations and identity theft. Additionally, the high mobility of vehicles complicates the network's security, making it challenging to establish stable and secure communication channels.

In response to these challenges, VANETs require robust authentication protocols to ensure that only legitimate vehicles and infrastructure components participate in the network [130]. Advanced cryptographic techniques and secure communication protocols are essential to protect data transmission from eavesdropping and tampering. The scalability of these security measures is crucial due to the high number of vehicles and the dynamic nature of VANETs [131,132].

Anonymity in VANETs is another critical countermeasure to safeguard user privacy. While ensuring the authenticity of messages and the reliability of data sources, it is vital to anonymize data to prevent the tracking and profiling of individual vehicles or drivers [133,134]. Techniques like pseudonymization, where vehicles periodically change their identifiers to prevent long-term tracking, are employed to strike a balance between security and privacy [135–142].

Moreover, data-minimisation strategies are essential in autonomous vehicles to collect only the data necessary for the intended purpose, reducing the volume of sensitive information that could be compromised.

As we envision a future marked by interconnected vehicular systems, understanding and mitigating these cybersecurity vulnerabilities becomes paramount. Dedicated research and the development of innovative solutions are required to address these intricate privacy issues effectively, ensuring that VANETs can realise their transformative potential for the transportation sector in a secure and privacy-preserving manner.

5.4. Involuntary Privacy Leakage with Ambient Intelligence

Ambient intelligence renders environments more perceptive to users. Sensors detect environmental state changes, which accelerates computing services tailored to user needs [143]. As smart devices become integral in daily routines, a mobile ambient intelligence ecosystem, replete with diverse functionalities, gradually emerges. The enhanced user experiences from smartphones and wearable gadgets have led users to permit data collection. However, this inadvertently paves the way for potential private information leaks.

These devices, connected to the internet, bridge the real world and cyberspace, rendering them susceptible to threats from both domains. An instance of cyber threat is outlined in [144], detailing smartwatches unintentionally revealing users' real-time location data. Such vulnerabilities, as Manuel puts it, are "pretty common". Though software-centric cyberattacks can be rectified promptly, breaches might still happen due to subpar testing, even with robust security mechanisms [144].

On the other end, threats emanating from the physical realm can be either inadvertent or deliberate. An inadvertent breach could be an unknown individual's image being unintentionally captured and uploaded on social media. While the uploader remains unaware

of the individual's identity, sophisticated algorithms might recognize them, revealing when and where the image was captured.

The onset of advanced smartphone capabilities has amplified our ability to chronicle every intricate detail of daily life. Consequently, the destiny of information about those inadvertently captured is vested in the hands of device users. The digital doorbell serves as another poignant example in this context. With an increasing number of households installing them, these devices constantly monitor front-door activities, often recording passersby or neighbours without their consent. Such recordings might get stored, shared, or even analysed without the knowledge of those captured.

In the face of these challenges, it becomes imperative for smart devices to evolve in their capacity to discern environments and adopt suitable privacy measures while also equipping users with the awareness and tools to navigate their surroundings with due diligence.

6. Conclusions

Emerging technologies continually change the ways user data are gathered and processed, and the scale at which this can be performed. This presents an evolving challenge to user privacy. In this paper, we explored multifaceted privacy concerns arising from the integration of cyberspace and the physical world.

From our examination, we identify three central themes: data exhaust tracing, personal data hub, and active data collection. These categories aptly represent the diverse privacy challenges currently prevalent. Within these, we further detailed six primary concerns, from identity tracking in browsing exhaust to data-transmission security and privacy implications in opportunistic networks. We situated these concerns in practical application scenarios, elucidating their distinct characteristics and their departures from traditionally understood problems.

In addition to highlighting these concerns, we assessed existing technological countermeasures. Through a comparative analysis, we identified both the strengths and weaknesses of current solutions, thereby pinpointing existing research gaps and potential obstacles to their practical implementation.

Moreover, the evolving technological landscape brings forth complex privacy challenges. We extend our analysis to the realms of user trajectories, smart metering, and ambient intelligence. These scenarios, encompassing elements from various domains, underline the growing intricacy of privacy-related challenges.

To conclude, as the boundary between the digital and physical blurs further, the imperative for robust privacy safeguards amplifies. While we have delineated possible research avenues and directions in this survey, the overarching takeaway remains: the quest for privacy in a hyperconnected era is dynamic, demanding constant vigilance, innovation, and adaptation.

Author Contributions: Y.J. is the main author of the current paper. He contributed to the development of the ideas, design of the study, theory, analysis, and article writing. M.A.R.B. contributed to the development of the ideas and article writing. L.R.S. conceptualised the ideas and contributed to the writing. P.G. contributed to the development of the ideas and its design. J.P. contributed to the development of the ideas and participated in its design. T.Z. contributed to the development of ideas and supervisory oversight throughout the research. Z.Z. contributed to the development of ideas. Z.L. contributed to the structuring of the survey and provided editorial assistance. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Cyber Security Research Centre Limited, whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
DP	Differential privacy
LDP	Local differential privacy
NLP	Natural language processing
AES	Advanced Encryption Standard
CGMs	Continuous Glucose Monitors
OppNets	Opportunistic networks
VANETs	Vehicular Ad Hoc Networks

References and Notes

1. Conti, M.; Passarella, A.; Das, S.K. The Internet of People (IoP): A new wave in pervasive mobile computing. *Pervasive Mob. Comput.* **2017**, *41*, 1–27. [CrossRef]
2. Fraenkel, O.K. ALAN F. WESTIN. Privacy and Freedom. Pp. xvi. New York: Atheneum, 1967. $10.00. *Ann. Am. Acad. Political Soc. Sci.* **1968**, *377*, 196–197. [CrossRef]
3. Schoeman, F. Privacy: Philosophical Dimensions. *Am. Philos. Q.* **1984**, *21*, 199–213.
4. Zawadziński, M.; Sweeney, M. *Identity in AdTech: Unravelling the ID Problem*; Clearcode: New York, NY, USA, 2019.
5. Soltani, A.; Canty, S.; Mayo, Q.; Thomas, L.; Hoofnagle, C.J. Flash cookies and privacy. In Proceedings of the 2010 AAAI Spring Symposium Series, Palo Alto, CA, USA, 22–24 March 2010.
6. Eckersley, P. How unique is your web browser? In Proceedings of the International Symposium on Privacy Enhancing Technologies Symposium, Berlin, Germany, 21–23 July 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 1–18.
7. Ravichandran, D.; Korula, N. Effect of disabling third-party cookies on publisher revenue. 2019.
8. Burke, J.A.; Estrin, D.; Hansen, M.; Parker, A.; Ramanathan, N.; Reddy, S.; Srivastava, M.B. *Participatory Sensing*; UCLA: Los Angeles, CA, USA, 2006.
9. Campbell, A.T.; Eisenman, S.B.; Lane, N.D.; Miluzzo, E.; Peterson, R.A. People-centric urban sensing. In Proceedings of the 2nd Annual International Workshop on Wireless Internet, Boston, MA, USA, 2–5 August 2006; p. 18-es.
10. Hamilton, I.A. The Whistleblower Who Exposed Cambridge Analytica's Facebook Data Abuse is Testifying before the Senate. 2019.
11. Perlroth, N. Yahoo Says Hackers Stole Data on 500 Million Users in 2014. *The New York Times*, 22 September 2016.
12. Merzdovnik, G.; Huber, M.; Buhov, D.; Nikiforakis, N.; Neuner, S.; Schmiedecker, M.; Weippl, E. Block me if you can: A large-scale study of tracker-blocking tools. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, France, 26–28 April 2017; pp. 319–333.
13. Perta, V.C.; Barbera, M.; Tyson, G.; Haddadi, H.; Mei, A. A glance through the VPN looking glass: IPv6 leakage and DNS hijacking in commercial VPN clients. *Proc. Priv. Enhancing Technol.* **2015**, *2015*, 77–91. [CrossRef]
14. Cover Your Tracks. 2023. Available online: https://coveryourtracks.eff.org/ (accessed on 10 October 2023).
15. Englehardt, S.; Narayanan, A. Online tracking: A 1-million-site measurement and analysis. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1388–1401.
16. Dwork, C.; McSherry, F.; Nissim, K.; Smith, A. Calibrating noise to sensitivity in private data analysis. In Proceedings of the Theory of Cryptography Conference, New York, NY, USA, 4–7 March 2006; Springer: Berlin/Heidelberg, Germany, 2006; pp. 265–284.
17. Yang, Y.; Zhang, Z.; Miklau, G.; Winslett, M.; Xiao, X. Differential privacy in data publication and analysis. In Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data, Scottsdale, AZ, USA, 20–24 May 2012; pp. 601–606.
18. Zhao, Y.; Chen, J. A survey on differential privacy for unstructured data content. *ACM Comput. Surv. (CSUR)* **2022**, *54*, 1–28. [CrossRef]
19. Ad-Blocker. Block Annoying Ads to Surf Web Faster.
20. AdBlock. Surf the web without annoying pop ups and ads!
21. Adblock Plus. Adblock Plus: The world's No. 1 free ad blocker.
22. Hill, R. gorhill/uBlock. 2020.
23. EasyList. Overview. Available online: https://easylist.to (accessed on 10 October 2023).
24. Ghostery. Ghostery Makes the Web Cleaner, Faster and Safer! Available online: https://www.doobybrain.com/blog/2017/11/20/ghostery-makes-the-web-cleaner-faster-and-safer (accessed on 10 October 2023).
25. Disconnect. Take back your privacy.
26. Abine, I. Keep your web activity and personal info private.
27. AdGuard. AdGuard Knowledgebase. 2023. Available online: https://adguard.com/kb (accessed on 10 October 2023).
28. Ghostery. Insights.
29. Disconnect. FAQ.
30. AdGuard. Flash Sale. 2023.

31. Mozilla. Multi-Account Containers. GitHub Repository. 2023. Available online: https://github.com/mozilla/multi-account-containers (accessed on 10 October 2023).
32. EFF. Privacy Badger. 2018.
33. EFF. Privacy Badger. 2019.
34. Developer, E. Canvas Fingerprint Blocker. 2023.
35. Salomatin, A.A.; Iskhakov, A.Y.; Meshcheryakov, R.V. Comparison of the Effectiveness of Countermeasures Against Tracking User Browser Fingerprints. *IFAC-PapersOnLine* **2022**, *55*, 244–249. [CrossRef]
36. Storey, G.; Reisman, D.; Mayer, J.; Narayanan, A. The future of ad blocking: An analytical framework and new techniques. *arXiv* **2017**, arXiv:1705.08568.
37. Abi Din, Z.; Tigas, P.; King, S.T.; Livshits, B. Percival: Making In-Browser Perceptual Ad Blocking Practical With Deep Learning. *arXiv* **2019**, arXiv:1905.07444.
38. Paraska, O. Towards more intelligent ad blocking on the web. *Medium*, 24 June 2018.
39. Tramèr, F.; Dupré, P.; Rusak, G.; Pellegrino, G.; Boneh, D. AdVersarial: Perceptual Ad Blocking meets Adversarial Machine Learning. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 2005–2021.
40. Storey, G.; Reisman, D.; Mayer, J.; Narayanan, A. Perceptual Ad Highlighter.
41. AdblockPlus. Developed by AdblockPlus.
42. Iqbal, U.; Snyder, P.; Zhu, S.; Livshits, B.; Qian, Z.; Shafiq, Z. Adgraph: A graph-based approach to ad and tracker blocking. In Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 18–21 May 2020.
43. Dwork, C. Differential privacy. In *Encyclopedia of Cryptography and Security*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 338–340.
44. Erlingsson, Ú.; Pihur, V.; Korolova, A. Rappor: Randomized aggregatable privacy-preserving ordinal response. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 1054–1067.
45. Apple Inc. *Learning with Privacy at Scale*; Apple Inc.: Cupertino, CA, USA, 2017.
46. Warner, S.L. Randomized response: A survey technique for eliminating evasive answer bias. *J. Am. Stat. Assoc.* **1965**, *60*, 63–69. [CrossRef] [PubMed]
47. Bloom, B.H. Space/Time Trade-offs in Hash Coding with Allowable Errors. *Commun. ACM* **1970**, *13*, 422–426. [CrossRef]
48. Hsu, J.; Khanna, S.; Roth, A. Distributed private heavy hitters. In Proceedings of the International Colloquium on Automata, Languages, and Programming, Warwick, UK, 9–13 July 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 461–472.
49. Bassily, R.; Nissim, K.; Stemmer, U.; Thakurta, A.G. Practical locally private heavy hitters. In Proceedings of the Advances in Neural Information Processing Systems, Long Beach, CA, USA, 4–9 December 2017; pp. 2288–2296.
50. Wang, T.; Li, N.; Jha, S. Locally differentially private heavy hitter identification. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 982–993. [CrossRef]
51. Wang, T.; Li, N.; Jha, S. Locally differentially private frequent itemset mining. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–24 May 2018; pp. 127–143.
52. Cormode, G.; Kulkarni, T.; Srivastava, D. Marginal release under local differential privacy. In Proceedings of the 2018 International Conference on Management of Data, Houston, TX, USA, 10–15 June 2018; pp. 131–146.
53. Ding, B.; Kulkarni, J.; Yekhanin, S. Collecting telemetry data privately. In Proceedings of the Advances in Neural Information Processing Systems, Long Beach, CA, USA, 4–9 December 2017; pp. 3571–3580.
54. Qin, Z.; Yu, T.; Yang, Y.; Khalil, I.; Xiao, X.; Ren, K. Generating synthetic decentralized social graphs with local differential privacy. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 425–438.
55. McMahan, H.B.; Ramage, D.; Talwar, K.; Zhang, L. Learning differentially private language models without losing accuracy. *arXiv* **2017**, arXiv:1710.06963.
56. Nguyên, T.T.; Xiao, X.; Yang, Y.; Hui, S.C.; Shin, H.; Shin, J. Collecting and analyzing data from smart device users with local differential privacy. *arXiv* **2016**, arXiv:1606.05053.
57. Jia, J.; Gong, N.Z. Calibrate: Frequency estimation and heavy hitter identification with local differential privacy via incorporating prior knowledge. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 2008–2016.
58. Joseph, M.; Roth, A.; Ullman, J.; Waggoner, B. Local differential privacy for evolving data. In Proceedings of the Advances in Neural Information Processing Systems, Montréal, QC, Canada, 3–8 December 2018; Volume 31.
59. Erlingsson, Ú.; Feldman, V.; Mironov, I.; Raghunathan, A.; Talwar, K.; Thakurta, A. Amplification by shuffling: From local to central differential privacy via anonymity. In Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms, San Diego, CA, USA, 6–9 January 2019; pp. 2468–2479.
60. Xue, Q.; Ye, Q.; Hu, H.; Zhu, Y.; Wang, J. DDRM: A continual frequency estimation mechanism with local differential privacy. *IEEE Trans. Knowl. Data Eng.* **2022**, *35*, 6784–6797. [CrossRef]

61. He, Y.; Wang, F.; Deng, X.; Ni, J.; Feng, J.; Liu, S. Ordinal Data Stream Collection with Condensed Local Differential Privacy. In Proceedings of the 2022 IEEE 24th International Conference on High Performance Computing & Communications; 8th International Conference on Data Science & Systems; 20th International Conference on Smart City; 8th International Conference on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), Hainan, China, 18–20 December 2022; pp. 562–569.
62. Han, Y.; Li, S.; Cao, Y.; Ma, Q.; Yoshikawa, M. Voice-indistinguishability: Protecting voiceprint in privacy-preserving speech data release. In Proceedings of the 2020 IEEE International Conference on Multimedia and Expo (ICME), London, UK, 6–10 July 2020; pp. 1–6.
63. Chen, J.W.; Chen, L.J.; Yu, C.M.; Lu, C.S. Perceptual indistinguishability-net (pi-net): Facial image obfuscation with manipulable semantics. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Nashville, TN, USA, 20–25 June 2021; pp. 6478–6487.
64. Fan, L. Image pixelization with differential privacy. In Proceedings of the Data and Applications Security and Privacy XXXII: 32nd Annual IFIP WG 11.3 Conference, DBSec 2018, Bergamo, Italy, 16–18 July 2018; Proceedings 32; Springer: Berlin/Heidelberg, Germany, 2018; pp. 148–162.
65. Fernandes, N.; Dras, M.; McIver, A. Generalised differential privacy for text document processing. In Proceedings of the Principles of Security and Trust: 8th International Conference, POST 2019, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2019, Prague, Czech Republic, 6–11 April 2019; Proceedings 8; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; pp. 123–148.
66. Feyisetan, O.; Balle, B.; Drake, T.; Diethe, T. Privacy-and utility-preserving textual analysis via calibrated multivariate perturbations. In Proceedings of the 13th International Conference on Web Search and Data Mining, Houston, TX, USA, 3–7 February 2020; pp. 178–186.
67. Lamothe, D.; Gibbons-Neff, T.; Sonne, P. A map showing the users of fitness devices lets the world see where U.S. soldiers are and what they are doing. *The Washington Post*, 29 January 2018 .
68. Gibbs, S. VTech hack: Four crucial takeaways from the breach of 6.4 m children's details. *The Guardian*, 30 November 2015 .
69. Centeno, J.K.M.; Chhabra, P.S.; Fianza, C.L.; Montes-Austria, I.; Ocampo, R. Performance Analysis of Encryption Algorithms on Smartwatches. In Proceedings of the TENCON 2018—2018 IEEE Region 10 Conference, Jeju Island, Republic of Korea, 28–31 October 2018; pp. 0162–0166.
70. Garcia-Morchon, O.; Wehrle, K. Modular context-aware access control for medical sensor networks. In Proceedings of the 15th ACM Symposium on Access Control Models and Technologies, Pittsburgh, PA, USA, 9–11 June 2010; pp. 129–138.
71. Ray, I.; Alangot, B.; Nair, S.; Achuthan, K. Using attribute-based access control for remote healthcare monitoring. In Proceedings of the 2017 Fourth International Conference on Software Defined Systems (SDS), Valencia, Spain, 8–11 May 2017; pp. 137–142.
72. Salama, U.; Yao, L.; Wang, X.; Paik, H.; Beheshti, A. Multi-Level Privacy-Preserving Access Control as a Service for Personal Healthcare Monitoring. In Proceedings of the 2017 IEEE International Conference on Web Services, ICWS 2017, Honolulu, HI, USA, 25–30 June 2017; Altintas, I., Chen, S., Eds.; IEEE: Piscataway, NJ, USA, 2017; pp. 878–881. [CrossRef]
73. Ravidas, S.; Lekidis, A.; Paci, F.; Zannone, N. Access control in Internet-of-Things: A survey. *J. Netw. Comput. Appl.* **2019**, *144*, 79–101. [CrossRef]
74. Kim, T.H.J.; Bauer, L.; Newsome, J.; Perrig, A.; Walker, J. Access right assignment mechanisms for secure home networks. *J. Commun. Netw.* **2011**, *13*, 175–186. [CrossRef]
75. Tian, Y.; Zhang, N.; Lin, Y.H.; Wang, X.; Ur, B.; Guo, X.; Tague, P. Smartauth: User-centered authorization for the internet of things. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, 16–18 August 2017; pp. 361–378.
76. Alshehri, S.; Raj, R.K. Secure access control for health information sharing systems. In Proceedings of the 2013 IEEE International Conference on Healthcare Informatics, Philadelphia, PA, USA, 9–11 September 2013; pp. 277–286.
77. Burnap, P.R.; Spasić, I.; Gray, W.A.; Hilton, J.C.; Rana, O.F.; Elwyn, G. Protecting patient privacy in distributed collaborative healthcare environments by retaining access control of shared information. In Proceedings of the 2012 International Conference on Collaboration Technologies and Systems (CTS), Denver, CO, USA, 21–25 May 2012; pp. 490–497.
78. Heydari, M.; Mylonas, A.; Katos, V.; Gritzalis, D. Towards indeterminacy-tolerant access control in iot. In *Handbook of Big Data and IoT Security*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 53–71.
79. Rahman, F.; Bhuiyan, M.Z.A.; Ahamed, S.I. A privacy preserving framework for RFID based healthcare systems. *Future Gener. Comput. Syst.* **2017**, *72*, 339–352. [CrossRef]
80. Diez, F.P.; Touceda, D.S.; Cámara, J.M.S.; Zeadally, S. Lightweight Access Control System for Wearable Devices. *IT Prof.* **2019**, *21*, 50–58. [CrossRef]
81. Biryukov, A.; Perrin, L.P. State of the Art in Lightweight Symmetric Cryptography. 2017. Available online: https://eprint.iacr.org/2017/511 (accessed on 10 October 2023).
82. Masoud, M.; Jannoud, I.; Ahmad, A.; Al-Shobaky, H. The power consumption cost of data encryption in smartphones. In Proceedings of the 2015 International Conference on Open Source Software Computing (OSSCOM), Amman, Jordan, 10–13 September 2015; pp. 1–6.
83. Ronen, E.; Shamir, A.; Weingarten, A.O.; O'Flynn, C. IoT goes nuclear: Creating a ZigBee chain reaction. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 195–212.

84. Robshaw, M. Lightweight cryptography and RAIN RFID. In Proceedings of the Lightweight Cryptography Workshop, Gaithersburg, MD, USA, 17–18 October 2016.
85. Leander, G.; Nikov, V.; Rechberger, C.; Rijmen, V. The Prince Challenge.
86. Guo, J.; Peyrin, T.; Poschmann, A. The PHOTON family of lightweight hash functions. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 222–239.
87. Bogdanov, A.; Knežević, M.; Leander, G.; Toz, D.; Varıcı, K.; Verbauwhede, I. SPONGENT: A lightweight hash function. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Nara, Japan, 28 September–1 October 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 312–325.
88. Jean, J.; Nikolić, I.; Peyrin, T. Joltik v1. 3. *CAESAR Round* **2015**, *2*.
89. Beierle, C.; Jean, J.; Kölbl, S.; Leander, G.; Moradi, A.; Peyrin, T.; Sasaki, Y.; Sasdrich, P.; Sim, S.M. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 123–153.
90. Avanzi, R. The QARMA block cipher family. Almost MDS matrices over rings with zero divisors, nearly symmetric even-mansour constructions with non-involutory central rounds, and search heuristics for low-latency s-boxes. *IACR Trans. Symmetric Cryptol.* **2017**, 4–44. [CrossRef]
91. Kubo, H.; Funabiki, Y.; Bogdanov, A.; Morioka, S.; Isobe, T. Tweakable TWINE: Building a Tweakable Block Cipher on Generalized Feistel Structure. In Proceedings of the Advances in Information and Computer Security: 14th International Workshop on Security, IWSEC 2019, Tokyo, Japan, 28–30 August 2019; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11689, p. 129.
92. Banik, S.; Bogdanov, A.; Peyrin, T.; Sasaki, Y.; Sim, S.M.; Tischhauser, E.; Todo, Y. Sundae-gift. *Submiss. Round* **2019**, *1*, 157–161.
93. Dinu, D.; Perrin, L.; Udovenko, A.; Velichkov, V.; Großschädl, J.; Biryukov, A. Design strategies for ARX with provable bounds: Sparx and LAX. In Proceedings of the Advances in Cryptology—ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 4–8 December 2016; Proceedings, Part I 22; Springer: Berlin/Heidelberg, Germany, 2016; pp. 484–513.
94. David, M.; Ranasinghe, D.C.; Larsen, T. A2U2: A stream cipher for printed electronics RFID tags. In Proceedings of the 2011 IEEE International Conference on RFID, Orlando, FL, USA, 12–14 April 2011; pp. 176–183.
95. Armknecht, F.; Mikhalev, V. On lightweight stream ciphers with shorter internal states. In Proceedings of the International Workshop on Fast Software Encryption, Istanbul, Turkey, 8–11 March 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 451–470.
96. Mikhalev, V.; Armknecht, F.; Müller, C. On ciphers that continuously access the non-volatile key. *IACR Trans. Symmetric Cryptol.* **2016**, 52–79. [CrossRef]
97. Dobraunig, C.; Eichlseder, M.; Mangard, S.; Mendel, F.; Unterluggauer, T. ISAP—Towards side-channel secure authenticated encryption. *IACR Trans. Symmetric Cryptol.* **2017**, 80–105. [CrossRef]
98. Canteaut, A.; Duval, S.; Leurent, G.; Naya-Plasencia, M.; Perrin, L.; Pornin, T.; Schrottenloher, A. Saturnin: A Suite of Lightweight Symmetric Algorithms for Post-Quantum Security. 2019. Available online: https://inria.hal.science/hal-02436763 (accessed on 10 October 2023).
99. Timberg, C. Austrian student challenges Facebook's use of personal data. *Indenpendent*, 20 October 2012.
100. Kumar, P.; Chauhan, N.; Chand, N. Authentication with privacy preservation in opportunistic networks. In Proceedings of the 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 10–11 March 2017; pp. 183–188.
101. Tsai, J.L.; Lo, N.W. Provably secure anonymous authentication with batch verification for mobile roaming services. *Ad Hoc Netw.* **2016**, *44*, 19–31. [CrossRef]
102. Irshad, A.; Sher, M.; Alzahrani, B.A.; Albeshri, A.; Chaudhry, S.A.; Kumari, S. Cryptanalysis and improvement of a Multi-server Authentication protocol by Lu et al. *KSII Trans. Internet Inf. Syst.* **2018**, *12*, 523–549.
103. Alajeely, M.; Doss, R.; Ahmad, A. Routing protocols in opportunistic networks—A survey. *IETE Tech. Rev.* **2018**, *35*, 369–387. [CrossRef]
104. Abouarork, M.; Ahmad, K. Authentication in opportunistic networks: State and art. *J. Discret. Math. Sci. Cryptogr.* **2021**, *24*, 1689–1700. [CrossRef]
105. Kido, H.; Yanagisawa, Y.; Satoh, T. An anonymous communication technique using dummies for location-based services. In Proceedings of the ICPS'05, Proceedings, International Conference on Pervasive Services, 2005, Santorini, Greece, 11–14 July 2005; pp. 88–97.
106. Liu, H.; Li, X.; Li, H.; Ma, J.; Ma, X. Spatiotemporal correlation-aware dummy-based privacy protection scheme for location-based services. In Proceedings of the IEEE INFOCOM 2017—IEEE Conference on Computer Communications, Atlanta, GA, USA, 1–4 May 2017; pp. 1–9.
107. Hara, T.; Suzuki, A.; Iwata, M.; Arase, Y.; Xie, X. Dummy-based user location anonymization under real-world constraints. *IEEE Access* **2016**, *4*, 673–687. [CrossRef]
108. Duckham, M.; Kulik, L. A formal model of obfuscation and negotiation for location privacy. In Proceedings of the International Conference on Pervasive Computing, Munich, Germany, 8–13 May 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 152–170.

109. Ganti, R.K.; Pham, N.; Tsai, Y.E.; Abdelzaher, T.F. PoolView: Stream privacy for grassroots participatory sensing. In Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems, Sydney, Australia, 6–9 November 2008; pp. 281–294.
110. Ardagna, C.A.; Cremonini, M.; Damiani, E.; Di Vimercati, S.D.C.; Samarati, P. Location privacy protection through obfuscation-based techniques. In Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy, Redondo Beach, CA, USA, 8–11 July 2007; Springer: Berlin/Heidelberg, Germany, 2007; pp. 47–60.
111. Samarati, P. Protecting respondents identities in microdata release. *IEEE Trans. Knowl. Data Eng.* **2001**, *13*, 1010–1027. [CrossRef]
112. Gruteser, M.; Grunwald, D. Anonymous usage of location-based services through spatial and temporal cloaking. In Proceedings of the 1st International Conference on Mobile Systems, Applications and Services, San Francisco, CA, USA, 5–8 May 2003; pp. 31–42.
113. Niu, B.; Li, Q.; Zhu, X.; Cao, G.; Li, H. Achieving k-anonymity in privacy-aware location-based services. In Proceedings of the IEEE INFOCOM 2014—IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 754–762.
114. Mokbel, M.F.; Chow, C.Y.; Aref, W.G. The new casper: Query processing for location services without compromising privacy. In Proceedings of the 32nd International Conference on Very Large Data Bases, Seoul, Republic of Korea, 12–15 September 2006; pp. 763–774.
115. Baee, M.A.R. Implementation and Performance Analysis of Identity-Based Authentication in Wireless Sensor Networks. Master's Thesis, Universiti Teknologi Malaysia, Skudai, Malaysia, 2014.
116. Baee, M.A.R.; Simpson, L.; Boyen, X.; Foo, E.; Pieprzyk, J. On the Efficiency of Pairing-Based Authentication for Connected Vehicles: Time Is Not on Our Side! *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3678–3693. [CrossRef]
117. Carver, C.; Lin, X. A privacy-preserving proximity friend notification scheme with opportunistic networking. In Proceedings of the 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 10–15 June 2012; pp. 5387–5392.
118. Avoussoukpo, C.B.; Xu, C.; Tchenagnon, M. Ensuring Users Privacy and Mutual Authentication in Opportunistic Networks: A Survey. *Int. J. Netw. Secur.* **2020**, *22*, 118–125.
119. Guo, M.-H.; Liaw, H.-T.; Chiu, M.-Y.; Tsai, L.-P. Authenticating with privacy protection in opportunistic networks. In Proceedings of the 2015 11th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE), Taipei, Taiwan, 19–20 August 2015; pp. 375–380.
120. Kuo, W.C.; Wei, H.J.; Cheng, J.C. An efficient and secure anonymous mobility network authentication scheme. *J. Inf. Secur. Appl.* **2014**, *19*, 18–24. [CrossRef]
121. Braun, E. Un Français demande 45 millions d'euros à Uber pour avoir précipité son divorce. *Le Figaro*, 2 August 2017.
122. Wang, H.; Gao, C.; Li, Y.; Zhang, Z.L.; Jin, D. From fingerprint to footprint: Revealing physical world privacy leakage by cyberspace cookie logs. In Proceedings of the 2017 ACM on Conference on Information and Knowledge Management, Singapore, 6–10 November 2017; pp. 1209–1218.
123. Saxena, N.; Choi, B.J. State of the art authentication, access control, and secure integration in smart grid. *Energies* **2015**, *8*, 11883–11915. [CrossRef]
124. Wu, J.; Guo, S.; Li, J.; Zeng, D. Big data meet green challenges: Big data toward green applications. *IEEE Syst. J.* **2016**, *10*, 888–900. [CrossRef]
125. Wu, J.; Guo, S.; Li, J.; Zeng, D. Big data meet green challenges: Greening big data. *IEEE Syst. J.* **2016**, *10*, 873–887. [CrossRef]
126. Uribe-Pérez, N.; Hernández, L.; De la Vega, D.; Angulo, I. State of the art and trends review of smart metering in electricity grids. *Appl. Sci.* **2016**, *6*, 68. [CrossRef]
127. Kumar, P.; Lin, Y.; Bai, G.; Paverd, A.; Dong, J.S.; Martin, A. Smart grid metering networks: A survey on security, privacy and open research issues. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 2886–2927. [CrossRef]
128. Saeed, Y.; Lodhi, S.A.; Ahmed, K. Obstacle management in vanet using game theory and fuzzy logic control. *ACEEE Int. J. Commun.* **2013**, *4*.
129. Akalu, R. Privacy, consent and vehicular ad hoc networks (VANETs). *Comput. Law Secur. Rev.* **2018**, *34*, 37–46. [CrossRef]
130. Azam, F.; Yadav, S.K.; Priyadarshi, N.; Padmanaban, S.; Bansal, R.C. A comprehensive review of authentication schemes in vehicular ad-hoc network. *IEEE Access* **2021**, *9*, 31309–31321. [CrossRef]
131. Goudarzi, S.; Abdullah, A.H.; Mandala, S.; Soleymani, S.A.; Baee, M.A.R.; Anisi, M.H.; Aliyu, M.S. A systematic review of security in vehicular Ad Hoc network. In Proceedings of the Second Symposium on Wireless Sensor and Cellular Networks (WSCN'13), Jeddah, Saudi Arabia, 13–16 December 2013; pp. 1–10.
132. Soleymani, S.A.; Abdullah, A.H.; Hassan, W.H.; Anisi, M.H.; Goudarzi, S.; Rezazadeh Baee, M.A.; Mandala, S. Trust management in vehicular ad hoc network: A systematic review. *EURASIP J. Wirel. Commun. Netw.* **2015**, *2015*, 146. [CrossRef]
133. Lagana, M.; Feiri, M.; Sall, M.; Lange, M.; Tomatis, A.; Papadimitratos, P. Secure communication in vehicular networks—PRESERVE DEMO. In Proceedings of the IEEE Vehicular Networking Conference, VNC 2012, IEEE Communications Society, Seoul, Republic of Korea, 14–16 November 2012; pp. 11–12.
134. Feiri, M.; Petit, J.; Schmidt, R.K.; Kargl, F. The impact of security on cooperative awareness in VANET. In Proceedings of the 2013 IEEE Vehicular Networking Conference, Boston, MA, USA, 16–18 December 2013; pp. 127–134.
135. Baee, M.A.R.; Simpson, L.; Foo, E.; Pieprzyk, J. Broadcast Authentication in Latency-Critical Applications: On the Efficiency of IEEE 1609.2. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11577–11587. [CrossRef]

136. Palaniswamy, B.; Camtepe, S.; Foo, E.; Simpson, L.; Rezazadeh Baee, M.A.; Pieprzyk, J. Continuous authentication for VANET. *Veh. Commun.* **2020**, *25*, 100255. [CrossRef]
137. Baee, M.A.R.; Simpson, L.; Boyen, X.; Foo, E.; Pieprzyk, J. A Model to Evaluate Reliability of Authentication Protocols in C-ITS Safety-Critical Applications. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9306–9319.
138. Baee, M.A.R.; Simpson, L.; Boyen, X.; Foo, E.; Pieprzyk, J. Authentication strategies in vehicular communications: A taxonomy and framework. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 1–50. [CrossRef]
139. Baee, M.A.R. Privacy-Preserving Authentication and Key Management for Cooperative Intelligent Transportation Systems. Ph.D. Thesis, Queensland University of Technology, Brisbane City, Australia, 2021. [CrossRef]
140. Rezazadeh Baee, M.A.; Simpson, L.; Boyen, X.; Foo, E.; Pieprzyk, J. ALI: Anonymous Lightweight Inter-Vehicle Broadcast Authentication with Encryption. *IEEE Trans. Dependable Secur. Comput.* **2023**, *20*, 1799–1817. [CrossRef]
141. Baee, M.A.R.; Simpson, L.; Foo, E.; Pieprzyk, J. The Security of "2FLIP" Authentication Scheme for VANETs: Attacks and Rectifications. *IEEE Open J. Veh. Technol.* **2023**, *4*, 101–113. [CrossRef]
142. Baee, M.A.R.; Simpson, L.; Boyen, X.; Foo, E.; Pieprzyk, J. A Provably Secure and Efficient Cryptographic-Key Update Protocol for Connected Vehicles. *IEEE Trans. Dependable Secur. Comput.* **2023**, 1–18. [CrossRef]
143. Cook, D.J.; Augusto, J.C.; Jakkula, V.R. Ambient intelligence: Technologies, applications, and opportunities. *Pervasive Mob. Comput.* **2009**, *5*, 277–298. [CrossRef]
144. Judd, B. Smartwatch apps let parents keep track of their kids but data breaches mean strangers can watch them too. *ABC News*, 10 February 2020.