electronics

MDPI

Review

A Narrative Review of Identity, Data and Location Privacy Techniques in Edge Computing and Mobile Crowdsourcing

Syed Raza Bashir, Shaina Raza * and Vojislav Misic

Department of Computer Science, Toronto Metropolitan University, 350 Victoria Street, Toronto, ON M5B 2K3, Canada; syedraza.bashir@torontomu.ca (S.R.B.); vmisic@torontomu.ca (V.M.)
* Correspondence: shaina.raza@torontomu.ca

Abstract: As digital technology advances, the proliferation of connected devices poses significant challenges and opportunities in mobile crowdsourcing and edge computing. This narrative review focuses on the need for privacy protection in these fields, emphasizing the increasing importance of data security in a data-driven world. Through an analysis of contemporary academic literature, this review provides an understanding of the current trends and privacy concerns in mobile crowdsourcing and edge computing. We present insights and highlight advancements in privacy-preserving techniques, addressing identity, data, and location privacy. This review also discusses the potential directions that can be useful resources for researchers, industry professionals, and policymakers.

Keywords: privacy; security; edge computing; location; mobile crowdsourcing; cloud computing

check for updates

Citation: Bashir, S.R.; Raza, S.; Misic, V. A Narrative Review of Identity, Data and Location Privacy Techniques in Edge Computing and Mobile Crowdsourcing. *Electronics* **2024**, *13*, 4228. https://doi.org/10.3390/electronics13214228

Academic Editors: Roberto Barchino, José Amelio Medina-Merodio, Salvador Otón Tortosa and José Javier Martínez-Herráiz

Received: 3 August 2024
Revised: 23 October 2024
Accepted: 26 October 2024
Published: 28 October 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The advent of the digital era and information overload has resulted in a significant increase in connected devices, generating a substantial volume of data transmitted over the Internet [1]. Managing predominantly through cloud infrastructures, the ubiquity of smart devices such as smartphones, tablets, smartwatches, and fitness trackers has made it even more complex. These devices routinely gather extensive contextual information about users, including their locations, activities, and environmental conditions—data that are vital for applications aimed at predicting user behavior and delivering personalized experiences [2,3].

In response to these developments, mobile crowdsourcing has emerged as a pivotal solution. This approach involves individuals collectively contributing data via various digital platforms [4]. Applications such as traffic monitoring systems leverage crowdsourced data to provide real-time insights. However, these methods also raise significant concerns regarding data privacy and the risks of unauthorized access to sensitive information [5,6].

The rapid increase in mobile data traffic poses substantial challenges for data management and processing. Edge computing has been identified as a promising solution to these challenges by processing data closer to its source rather than relying solely on central servers. This approach helps alleviate network congestion but also introduces new privacy and security vulnerabilities that must be addressed [7].

This paper explores the intersection of mobile crowdsourcing and edge computing with a particular emphasis on privacy preservation. It highlights the potential for integrating these technologies to enhance data processing efficiency while maintaining user privacy. We provide an overview of existing research on these technologies and their implications for privacy. Our goal is to equip researchers, practitioners, and policymakers with the necessary insights to navigate the complexities of ensuring privacy while advancing technological capabilities. Additionally, we discuss potential strategies for mitigating privacy risks associated with decentralized data processing and propose future research directions to address these challenges comprehensively.

1.1. Literature Review Strategy

Our literature review strategy involved searches in academic repositories such as ACM Digital Library, IEEE Xplore, Springer, Elsevier, Google Scholar, DBLP, CiteSeerX, Microsoft Academic Search, Web of Science, and ScienceDirect. Publications from the period 2012 to 2021 were primarily considered, with a final selection of approximately 52 peer-reviewed papers from an initial pool of 150 papers based on relevance to mobile crowdsourcing and edge computing. These papers were analyzed for trends, methodologies, findings, and gaps in research. The publication trend in the last few years is given in Figures 1–3.

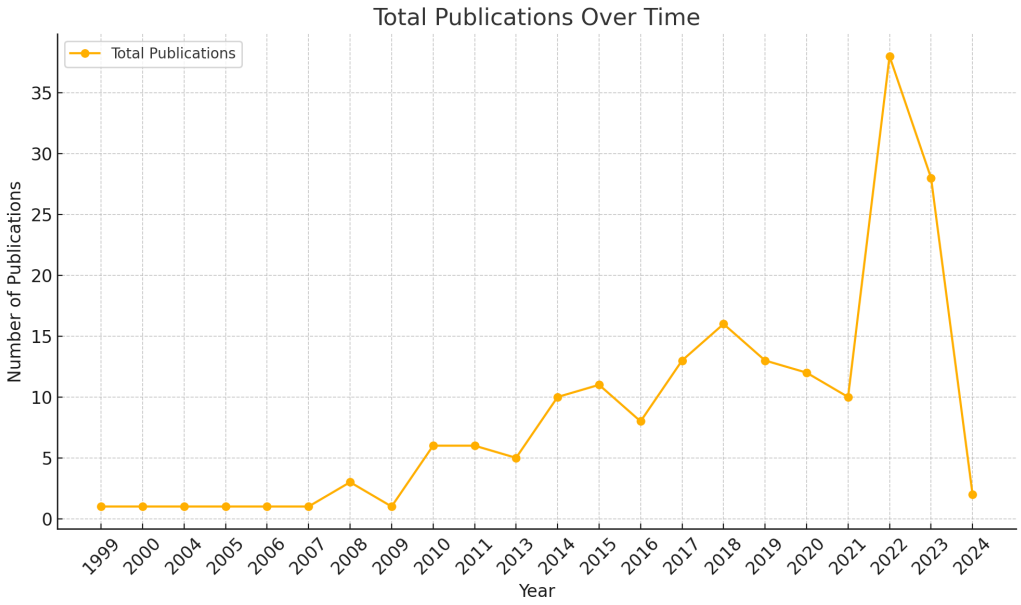


Figure 1. Publication trend on privacy in edge computing and mobile crowdsourcing in recent years. The full year 2024 is not covered, so additional publications are expected.

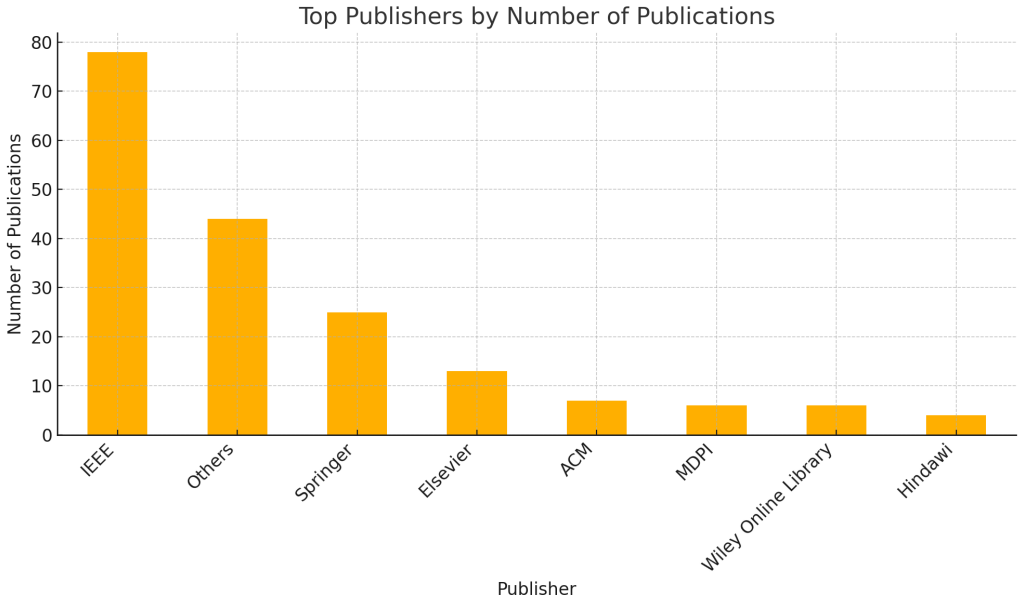


Figure 2. Top publishers by number of publications in the field.

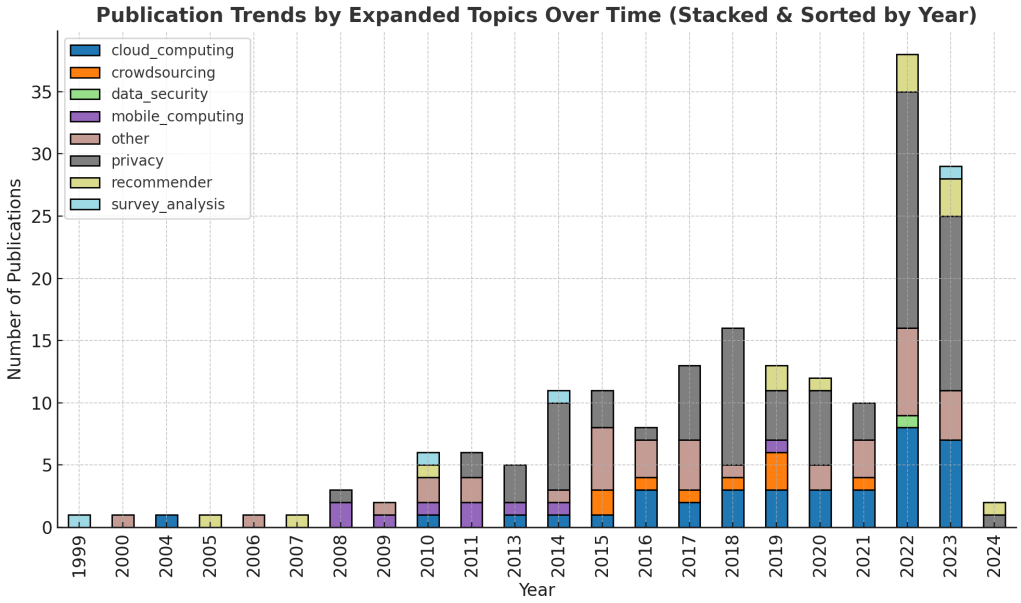


Figure 3. Publication trends over time by topic.

We used queries to search for relevant literature, shown in Listing 1:

Listing 1. Search Query Strings for Mobile Crowdsourcing and Edge Computing Studies.

```
1. ("Mobile Crowdsourcing" AND "Edge Computing" AND "Privacy Preservation
    ↪ ") AND ("Data Security" OR "Real-Time Data Processing") AND
    ↪ (2012-2023)

2. ("Mobile Crowdsourcing" AND "Edge Computing") AND ("User Context" OR "
    ↪ Personalized Services") AND ("IoT" OR "Cloud Computing") AND (peer-
    ↪ reviewed)

3. ("Mobile Crowdsourcing" AND "Edge Computing") AND ("Privacy" AND "
    ↪ Information Overload") AND ("Smart Devices" OR "User Behavior
    ↪ Prediction") AND (2012-2023)
```

1.2. Contributions

This work contributes the following to the field:

1. This review offers an overview of mobile crowdsourcing and edge computing, with an emphasis on the importance of privacy preservation.
2. We synthesize both contemporary and foundational literature to provide an understanding of identity privacy, data privacy, and location privacy (based on their relevance to importance) and identify current research trends.

A meta-review of previous surveys is presented in Table 1, and the main keywords used in this work are given in Table A1.

Table 1. Related surveys.

Domain	Focus	Key Contributions and Privacy Aspects
Edge Computing	Real-time and local data processing, IoT integration, Edge AI, Security	Studies highlighted capabilities for local processing, integration with AI, and identified gaps in privacy protection specific to edge computing environments. Key studies include [7–14].
Mobile Computing	Security Trends, Healthcare, Cloud Integration, AR Applications	Focused on evolving security challenges, particularly in mobile cloud contexts and healthcare applications during the COVID-19 pandemic, and AR enhancements. Relevant studies include [15–19].

1.3. Necessity of This Review

This review addresses a literature gap that surrounds the rapidly evolving fields of mobile crowdsourcing and edge computing. As our reliance on data-driven systems continues to grow, this review provides a timely analysis of current trends, privacy concerns, and research gaps in these interconnected domains. We also shed some light on key privacy issues, including those related to identity, data, and location, and offer some information to researchers, industry professionals, and policymakers. The flow of this review is shown in Figure 4.

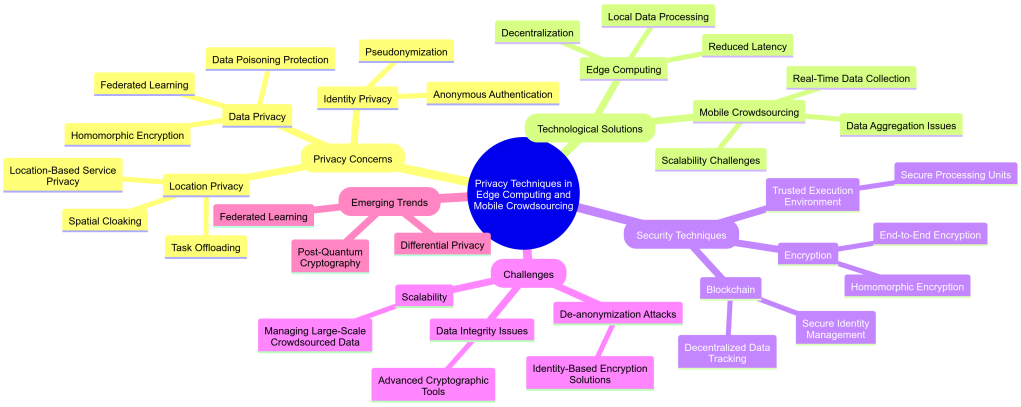


Figure 4. Flow of the privacy-preserving methods covered in this work.

2. Privacy Concerns in Mobile Crowdsourcing and Edge Computing

We discuss mobile crowdsourcing and edge computing and examine privacy challenges in these domains, focusing on identity privacy, data privacy, and location privacy due to their significant impact on protecting users in these interconnected systems.

2.1. Identity Privacy

Identity privacy is crucial in protecting individual personal information from being exposed or inferred during mobile crowdsourcing or edge computing activities [20]. This protection encompasses safeguarding personal details such as names, social security numbers, and other identifiers that could link activities to a specific individual.

In mobile crowdsourcing, data are often collected from numerous participants, making it essential to ensure their anonymity or pseudonymity. This is critical to prevent the misuse of personal information [21]. If personal identifiers are exposed, it can lead to identity theft, where malicious actors might use stolen identities to commit fraud or other illegal activities [22]. Thus, safeguarding identity privacy is fundamental for establishing and maintaining user trust.

The complexity of data collection processes in mobile crowdsourcing also raises concerns about implied consent and the need for more transparent consent management. Often, users agree to data collection practices without fully understanding the implications,

inadvertently compromising their privacy. Therefore, it is vital to develop clearer consent mechanisms that ensure users are informed and their privacy is respected throughout the data collection process.

2.2. Data Privacy

Data privacy in the context of mobile crowdsourcing and edge computing involves protecting the data collected, processed, and stored from unauthorized access, alteration, or disclosure [23]. This protection is crucial, as crowdsourced data often include sensitive information such as health records, financial transactions, and personal communications. Ensuring the confidentiality and integrity of such data is vital to prevent unauthorized access and maintain user trust [23].

Various regulations, such as the General Data Protection Regulation (GDPR) (https://gdpr-info.eu/) (accessed on 22 October 2024) and the Health Insurance Portability and Accountability Act (HIPAA) (https://www.hhs.gov/hipaa/) (accessed on 22 October 2024), mandate strict measures to safeguard data privacy. Breaches can lead to severe consequences, including financial losses, reputational damage, and erosion of user trust. A significant concern in this domain is the risk associated with third-party data sharing. Once data enter the crowdsourcing ecosystem, users often lose control over their personal information as it flows through multiple parties in edge computing environments. This lack of control raises privacy risks that need to be addressed.

Furthermore, mobile crowdsourcing systems are vulnerable to specific attacks like Sybil attacks and data poisoning [24]. These attacks can manipulate the crowdsourcing process and potentially expose sensitive user information. Addressing these vulnerabilities requires robust security measures to protect against unauthorized data access and ensure data integrity throughout the crowdsourcing lifecycle.

2.3. Location Privacy

Location privacy is the protection of information regarding an individual geographical location, particularly as it is obtained through mobile crowdsourcing and edge computing. This involves ensuring that location data cannot be used to track or monitor an individual's movements without their explicit consent. Unauthorized access to location data poses significant risks, including stalking, harassment, and other malicious activities where an individual's movements might be tracked without their knowledge or consent [25]. The disclosure of sensitive locations, such as homes, workplaces, or places of interest, can lead to security risks and privacy violations [26]. Therefore, it is crucial for users to have control over who can access their location data and for what purposes. Ensuring location privacy is fundamental to preserving users' autonomy and their right to control their personal information [27].

The risks associated with sharing location data are many, for example, malicious actors can use precise location information to deduce behavioral patterns and predict where someone might be at any given time, potentially facilitating physical tracking or blackmail [25]. Additionally, unauthorized sharing or breaches of location data can lead to unintended surveillance and discrimination by authorities or third parties [28].

To mitigate these risks, it is essential for organizations to implement robust privacy measures. These include obtaining explicit user consent before enabling location-tracking features and ensuring transparency about how location data are used and shared. Techniques such as spatial cloaking and cryptographic methods can also enhance location privacy by anonymizing data and securing communication channels [29].

Adhoc Solutions

To address privacy concerns in mobile crowdsourcing and edge computing, researchers and practitioners are developing several innovative solutions.

One approach is the implementation of decentralized systems [30], which enhance user control over data and minimize the risks associated with centralized data repositories.

This helps prevent vulnerabilities that arise from having a single point of failure or attack. Organizations are also shifting towards using advanced encryption techniques [31] to protect data both when it is stored and during transfer. The goal is to ensure that even if someone intercepts the data, it remains unintelligible without proper authorization, thereby safeguarding sensitive information. Technologies like differential privacy [32] help in protecting sensitive information while still allowing for meaningful data analysis. By adding noise to datasets, these techniques make it difficult to identify individual users, thus preserving privacy while enabling valuable insights.

There is an increasing focus on creating clear and easy-to-use systems for managing consent [33]. These frameworks ensure that users are fully informed about data-sharing practices and can easily control their preferences. This empowers users to have more say over their personal information and its handling, especially on crowdsourcing platforms. Also, leveraging blockchain technology [24] provides traceability and immutability in data handling practices. Blockchain enhances security and transparency, allowing users to verify how their data are used and shared. This not only improves security but also builds trust by providing a transparent record of transactions and data usage.

3. Mobile Crowdsourcing

Mobile crowdsourcing represents a field where collective user contributions, primarily via mobile devices, drive data collection and service provision [34,35]. Mobile crowdsourcing leverages the ubiquitous nature of mobile devices into a vast pool of user-submitted data, encompassing geospatial and behavioral data as well as environmental and health metrics. Its applications are vast, covering environmental monitoring, disaster response, urban planning, healthcare, and transportation, and highlight the versatility and impact of mobile crowdsourcing [36].

A quintessential example of the potential of mobile crowdsourcing is seen in Waze [37], a navigation app that integrates user-generated traffic data to provide real-time routing advice and traffic condition updates. This not only showcases the practical implementation of mobile crowdsourcing but also demonstrates how user participation can significantly enhance service quality and responsiveness.

We show the key stages in mobile crowdsourcing in Figure 5.

1. Tasking Stage: This initial phase involves defining clear and actionable data collection objectives that align with the overarching goals of crowdsourcing.
2. Collecting Stage: At this point, the data are actively acquired from users through their mobile devices. The data can range from environmental readings to user-generated content and location data, providing a rich dataset for analysis.
3. Storing Stage: The collected data are centralized on cloud or edge servers for processing. This stage is crucial for managing the volume of data and ensuring it is accessible for analysis.
4. Mining Stage: Advanced analytics, machine learning (ML), and data mining techniques are applied to the aggregated data to extract meaningful insights, patterns, and trends.
5. Publishing Stage: The final stage involves disseminating the findings and insights to end-users or stakeholders, often through the same mobile platforms used for data collection.

The technological infrastructure supporting mobile crowdsourcing includes a range of components from mobile devices and network communication protocols to cloud and edge computing platforms. These technologies facilitate the efficient collection, transmission, and processing of crowdsourced data. However, this complex ecosystem also introduces challenges related to scalability, data quality control, and the integration of heterogeneous data sources. The transmission of sensitive personal information, such as location data and personal identifiers, to centralized servers poses risks related to data security and user privacy [38,39].

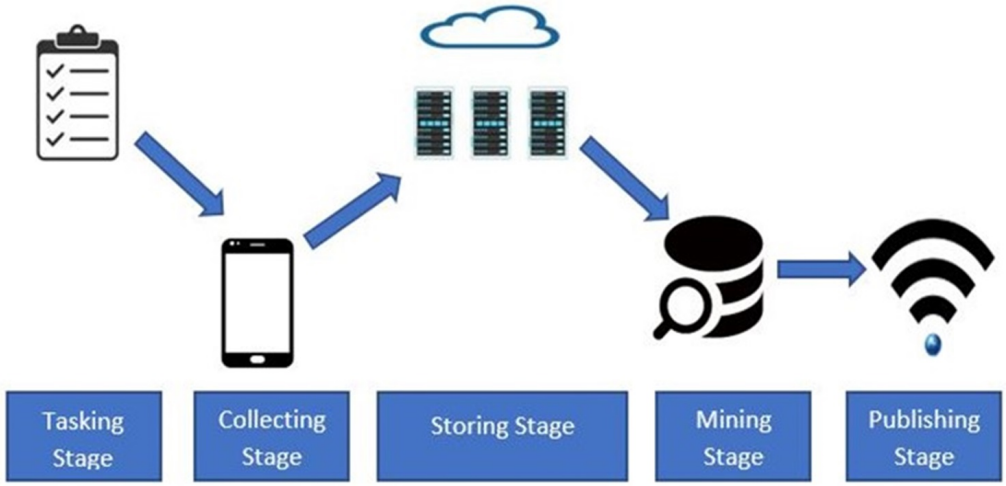


Figure 5. Anatomy of a mobile crowdsourcing campaign.

Literature: In mobile computing, recent surveys have focused on security trends, healthcare applications during the COVID-19 pandemic, and the integration with cloud computing. One study [15] explored evolving security challenges in mobile cloud computing and strategies for safeguarding these environments. The significant role of mobile computing in healthcare, especially during the pandemic, was highlighted in a survey [16], addressing both challenges and potential solutions. Additionally, the integration of mobile computing with edge computing is examined in [17], where the authors discuss the benefits of leveraging edge computing for reducing latency and improving processing capabilities in mobile applications. The survey [18] delves into the advancements in mobile augmented reality (AR), focusing on the integration of mobile computing with AR to enhance user experiences and application performance. Further research [19] reviews the application of mobile computing in smart cities.

3.1. Privacy Concerns in Mobile Crowdsourcing

3.1.1. Identity Privacy in Mobile Crowdsourcing

Identity privacy in mobile crowdsourcing is an important aspect of safeguarding user data, which includes sensitive information like names, addresses, and contact details. Discussions on identity privacy focus on the implementation of robust forward security measures to protect cloud data [21,40]. Identity-based encryption methods are highlighted as a means to secure cloud data, which shows the multifaceted approach required to enhance privacy protection in cloud computing contexts [22]. Consolidated Identity Management Systems (CIDM) are proposed to safeguard user identity by separating authorization credentials, adding an extra authentication layer, and securing communication links with cloud service providers [41]. Further discussions emphasize blockchain-based trust models and strategies for identity management that negate the need for trusted third parties [42,43].

3.1.2. Data Privacy in Mobile Crowdsourcing

Data privacy in mobile crowdsourcing involves developing methods and techniques focused on enhancing data security and privacy within cloud environments. Research efforts include sophisticated methods for conducting spatial data queries that prioritize user privacy without compromising data utility [44]. Techniques leveraging advanced cryptographic tools such as homomorphic encryption show the potential for employing encryption to fortify privacy measures in cloud computing [23].

3.1.3. Location Privacy in Mobile Crowdsourcing

Ensuring the privacy of location data in mobile cloud computing involves various innovative methods such as cipher-text retrieval techniques for location privacy protec-

tion [26]. Other approaches include the use of spatial cloaking to anonymize location data for queries in cloud environments [45]. Advanced cryptographic techniques, such as SHA-2 for robust mutual authentication and location privacy, are employed to ensure secure communication and privacy preservation in mobile cloud computing settings [46].

Collectively, these research efforts illustrate the diverse strategies being explored to protect identity, data, and location privacy in cloud computing. These methods are summarized in Table 2.

Table 2. Privacy concerns and solutions in mobile cloud computing.

Privacy Concern	Research Focus	Key Solutions
Identity Privacy in Cloud Computing	Safeguarding sensitive user data such as names, addresses, and contact details	• Robust forward security measures [21,40] • Identity-based encryption methods [22] • Consolidated Identity Management Systems (CIDM) [41] • Blockchain-based trust models and identity management [42,43]
Data Privacy in Cloud Computing	Enhancing data security and privacy within cloud environments	• Spatial data query methods prioritizing user privacy [44] • Advanced cryptographic tools such as homomorphic encryption [23]
Location Privacy in Cloud Computing	Ensuring privacy of location data	• Cipher-text retrieval techniques for location privacy protection [26] • Spatial cloaking to anonymize location data [45] • SHA-2 for robust mutual authentication and location privacy [46]

4. Edge Computing and Privacy Concerns

Edge computing represents a paradigm shift in data processing and management. It emphasizes the decentralization of computational resources to bring data storage and processing closer to the sources of data [7]. This approach is particularly beneficial for real-time and latency-sensitive applications across diverse domains such as autonomous vehicles, smart homes, emergency response systems, smart agriculture, and modernized power grids.

Conceptual Framework: Edge computing seeks to address the inherent limitations of centralized cloud computing models by distributing computational tasks to the edge of the network [47]. This strategic distribution significantly reduces latency by minimizing the distance between the data source and the processing unit and alleviates bandwidth constraints on the network. Such enhancements boost overall system responsiveness and reliability.

Technological Advancements and Architectural Design: The architectural design of edge computing is inherently modular and scalable. As depicted in Figure 6, the typical architecture comprises three primary layers: the user layer, edge layer, and cloud layer. Each layer plays a distinct role in the ecosystem, with smart devices at the user layer generating data, edge servers at the edge layer processing this data in real time, and cloud servers at the cloud layer providing long-term storage and further analytics capabilities.

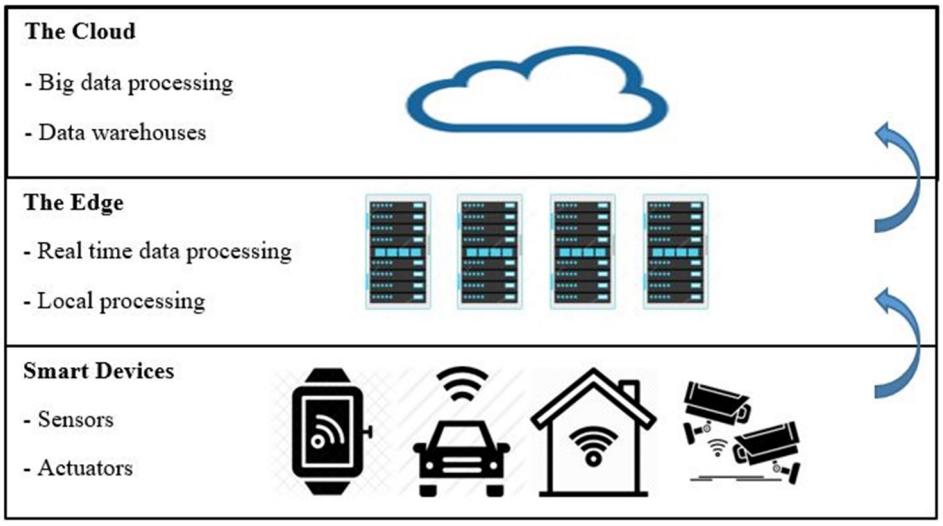


Figure 6. Edge computing architecture illustrating the interplay between user, edge, and cloud layers.

Benefits of Edge Computing: The decentralization inherent in edge computing brings several benefits. By processing data closer to its source, it significantly reduces latency, which is crucial for applications that require real-time feedback, such as autonomous driving and emergency response systems [48]. Furthermore, edge computing contributes to bandwidth efficiency by minimizing the volume of data that needs to be transmitted to the cloud, thereby reducing network congestion and associated costs.

Integration with Smart Technologies: Edge computing is integral to the evolution of smart technologies [19]. It enables the seamless integration of IoT devices, smart sensors, and other data sources, facilitating the development of intelligent applications that can operate autonomously and interact with their environment in real time. This integration is crucial for the advancement of smart cities, industrial automation, and personalized healthcare, among other applications.

Literature: Recent studies, such as those by [8,9], distinguish edge computing from cloud computing by detailing its capabilities for real-time and local data processing, highlighting emerging research, and practical applications. Research in [10] explores 'Edge AI', examining how edge computing and AI are integrated, their applications, and the impact of AI algorithms on decision-making and data processing at the network edge. Issues of security and privacy specific to edge computing are addressed in [11], where it is noted that conventional cloud computing privacy methods are inadequate. Ref. [12] highlights concerns about location privacy in edge computing environments, while [7] reviews security and privacy preservation methods, noting a predominant focus on cloud computing over edge-specific strategies. Additionally, a survey [13] discusses edge computing's influence on IoT development, advocating for its suitability over other computing paradigms for IoT scenarios. Furthermore, Ref. [14] presents a comprehensive review of current research on security in edge computing, pinpointing challenges in new models, application scenarios, and technological environments, with specific attention to access control, key management, privacy protection, attack mitigation, and anomaly detection.

4.1. Privacy Concerns in Edge Computing

Edge computing, despite its benefits, introduces complex privacy issues due to its decentralized nature. This subsection delves into identity, data, and location privacy, highlighting ongoing research and emerging solutions aimed at enhancing security and privacy in edge environments.

4.1.1. Identity Privacy in Edge Computing

Several studies have explored pseudonym technology, cryptographic methods, and data aggregation schemes in edge computing environments to preserve identity privacy [49–51]. However, these methods are challenged by de-anonymization attacks [29,52,53] and limited data integrity [50]. Notably, research efforts are being made to enhance security and privacy through various methods focused on maintaining anonymity, preventing unauthorized access, and ensuring user data integrity. Innovations include anonymous authentication mechanisms leveraging identity-based cryptography for secure device-to-edge server communications [54], and the combination of secret sharing with homomorphic encryption to bolster data privacy [55]. Another approach involves using fully homomorphic encryption with multikey capabilities to secure data processing [56], and optimizing federated learning to enhance privacy and efficiency in edge environments [57].

4.1.2. Data Privacy in Edge Computing

In edge computing, ensuring data privacy is crucial due to decentralized processing and storage. Innovative approaches include partitioning deep neural networks to balance privacy with energy consumption [58] and integrating federated learning with hybrid differential privacy and adaptive compression to protect data in industrial settings [32]. Challenges in location-based services are addressed by crafting specific privacy protection strategies [25], and a novel framework for secure data sharing emphasizes privacy-preserving computations across the computing landscape [59]. Additionally, Local Differential Privacy (LDP) techniques process data while preserving personal information, though they can reduce data utility due to noise addition [60].

4.1.3. Location Privacy in Edge Computing

Ensuring location privacy within edge computing is paramount due to the proliferation of location-based services. Techniques include task offloading with reinforcement learning to protect privacy in autonomous transport systems [47], and dual K-anonymous caching strategies within edge environments to safeguard location data [61]. Dynamic strategies to protect location privacy in multi-user mobile edge systems highlight the need for agile response mechanisms in privacy protection [62]. Additional efforts focus on balancing service efficiency with privacy in location-based services [25] and task offloading frameworks that consider location privacy [62]. Vehicular crowdsourcing applications also reflect a focus on driver privacy, combining pseudonym and mix-zone techniques [63,64].

This literature review is summarized in Table 3.

Challenges: Despite its numerous advantages, edge computing faces several challenges, including security concerns, data privacy issues, and management complexities [17]. The distributed nature of edge computing introduces multiple points of vulnerability that must be secured against potential threats. Managing data privacy also becomes more complex as data are processed across numerous edge devices and locations. Solutions to these challenges include implementing advanced encryption techniques, establishing robust access control measures, and developing standardized protocols for data management and security.

The increasing need to embed AI capabilities at the edge allows devices to perform sophisticated data analysis and decision-making processes locally. This enhances the autonomy of smart applications and reduces dependency on central servers. Furthermore, the ongoing development of 5G networks is expected to significantly bolster the capabilities of edge computing, enabling faster data processing and exchange rates.

Mobile crowdsourcing and edge computing have revolutionized data processing and service delivery by bringing computation closer to the data source. However, these technologies pose significant privacy challenges, particularly when handling sensitive user information such as personal identity and location data. This case study examines a smart city project that integrates edge computing and mobile crowdsourcing to improve public services like traffic management, waste disposal, and public safety. Residents contribute

data via mobile applications, which are processed at distributed edge devices throughout the city. This initiative faces several privacy challenges, including identity privacy, data privacy, and location privacy.

Table 3. Privacy concerns and solutions in edge computing.

Privacy Concern	Research Focus	Challenges and Solutions
Identity Privacy	Pseudonym technology, cryptographic methods, data aggregation schemes [49–51]	• De-anonymization attacks [29,52,53] • Limited data integrity [50] • Anonymous authentication using identity-based cryptography [54] • Secret sharing with homomorphic encryption [55] • Fully homomorphic encryption with multikey capabilities [56] • Optimized federated learning [57]
Data Privacy	Ensuring data privacy due to decentralized processing and storage	• Partitioning deep neural networks for privacy and energy balance [58] • Federated learning with hybrid differential privacy and adaptive compression [32] • Location-based service privacy strategies [25] • Secure data sharing frameworks [59] • Local Differential Privacy (LDP) techniques [60]
Location Privacy	Protecting privacy in location-based services	• Task offloading with reinforcement learning in autonomous transport systems [47] • Dual K-anonymous caching strategies [61] • Dynamic multi-user privacy protection [62] • Balancing service efficiency with location privacy [25] • Task offloading frameworks for location privacy [62] • Pseudonym and mix-zone techniques in vehicular crowdsourcing [63,64]

5. Enhancing Privacy in Mobile Crowdsourcing and Edge Computing: A Case Study

Mobile crowdsourcing and edge computing have transformed data processing and service delivery by making computation closer to the data source. However, these technologies also present privacy concerns, especially when handling sensitive user information like personal identity and location data. We consider a smart city project that integrates edge computing and mobile crowdsourcing to enhance public services such as traffic management, waste disposal, and public safety. Residents participate by sharing data via mobile applications, which are processed at edge devices distributed across the city. Traffic patterns are monitored using mobile data collected from citizens' smartphones, while waste management facilities use data from smart bins. As residents contribute sensitive information, this project faces the following privacy challenges: identity privacy (protecting citizens' identities), data privacy (secure processing of shared data), and location privacy (protecting individuals' exact whereabouts).

5.1. Identity Privacy in Edge Computing

To protect identity privacy, the project implemented identity-based encryption [20] and forward security [40]. Forward security ensures that even if an encryption key is compromised, previously encrypted data remain secure. Additionally, decentralized identity management using blockchain-based [24] trust models was introduced to reduce reliance on centralized authorities. Each participant had a digital identity verified by decentralized nodes, mitigating risks of identity theft and unauthorized access.

5.2. Data Privacy with Federated Learning

For safeguarding data privacy, the project employed federated learning [33] with hybrid differential privacy. ML models are trained on data collected from citizens without centralizing their data. Instead, model updates are shared from edge devices back to a central server. This reduces the risk of data exposure while still leveraging crowdsourced data for model improvements.

5.3. Location Privacy with K-Anonymous Caching

To protect location privacy, K-anonymous caching [61] was used to obfuscate user's exact locations by combining location data with that of other users in a given area. For instance, when a user reports parking availability, the system aggregates reports from multiple users in the vicinity to ensure individual anonymity.

5.4. Recommendations

The following recommendations are made to enhance the project's effectiveness:

- Establish clear guidelines for data collection, storage, and usage. Implement anonymization techniques and conduct regular audits to enhance transparency and accountability.
- Integrate post-quantum cryptography [65] to future-proof encryption systems against quantum computing threats. Utilize privacy-preserving authentication (PPA) [66] for efficient and secure data handling.
- Leverage blockchain for decentralized identity management to enhance trust models and improve data security with tamper-resistant record-keeping.
- Incorporate privacy considerations from the outset of projects through thorough privacy impact assessments and embrace principles like data minimization.
- Encourage public participation in decision-making processes related to data usage and enforce regulatory oversight to ensure compliance with evolving privacy standards.
- Focus on scalability by integrating AI and machine learning for dynamic risk detection in real time. Implement trusted execution environments for secure processing of sensitive data.
- Balance energy consumption with privacy needs using energy-efficient cryptographic methods that maintain security without compromising performance.

6. Discussion

This paper has explored the critical privacy concerns associated with mobile crowdsourcing and edge computing. As these technologies continue to evolve and become integral to modern data processing and storage solutions, addressing privacy concerns becomes paramount.

Identity privacy in cloud and edge computing is a multifaceted challenge. Research emphasizes robust forward security measures and identity-based encryption to protect sensitive user information [21,22,40]. Proposals such as CIDM aim to enhance security by separating authorization credentials and securing communication links [41]. Additionally, blockchain-based trust models and decentralized identity management systems offer promising approaches to reduce the need for trusted third parties, mitigating the risks of identity theft and unauthorized access [42,43]. However, significant challenges remain, particularly in countering de-anonymization attacks and ensuring the integrity of anonymized data [29]. Ongoing research into advanced cryptographic methods and innovative authentication mechanisms, including those leveraging identity-based cryptography, is needed for addressing these vulnerabilities.

Ensuring data privacy in cloud and edge computing environments is critical due to the decentralized nature of these technologies. Innovative approaches such as partitioning deep neural networks to balance privacy with energy consumption and employing federated learning with hybrid differential privacy are making significant strides in this area [32,58]. Techniques like homomorphic encryption and LDP have shown potential in protecting data privacy by enabling secure data processing and analysis [23,60]. Despite their promise,

these techniques often introduce challenges such as increased computational overhead and reduced data utility due to noise addition.

The protection of location privacy is particularly crucial in mobile computing due to the pervasive use of location-based services. Research has proposed several methods to address this issue, including cipher-text retrieval techniques, spatial cloaking, and SHA-2 for robust mutual authentication [26,45,46]. Strategies such as task offloading with reinforcement learning and dual K-anonymous caching have been explored to enhance location privacy in edge computing environments [47,61]. These techniques offer dynamic and scalable solutions to protect location data while maintaining the efficiency of edge services.

The implications of these privacy concerns are vast and multifaceted. As mobile computing becomes more ubiquitous, ensuring robust privacy protection mechanisms is not only a technical challenge but also a societal imperative. The interplay between user trust and technology adoption cannot be overlooked. Compliance with the regulations such as data protection laws requires the development of sophisticated privacy-preserving technologies that can adapt to diverse legal requirements and protect user data across different jurisdictions.

Future research should focus on enhancing the scalability and efficiency of privacy-preserving methods [57,67], addressing the challenges of de-anonymization and data utility, and exploring new cryptographic techniques to ensure robust privacy protection. The integration of artificial intelligence and machine learning into privacy protection strategies offers promising avenues for innovation. These technologies can help identify and mitigate privacy risks in real time, providing an additional layer of security in dynamic and complex computing environments. Additionally, interdisciplinary collaboration among researchers, industry practitioners, and policymakers is essential to create standardized guidelines and frameworks for privacy protection in mobile computing.

6.1. Emerging Trends in Privacy Preservation

Some key trends and emerging technologies to enhance privacy while enabling valuable insights and innovations are the following:

1. Artificial Intelligence (AI) and ML are increasingly being used to enhance privacy protection. These methods and technologies are already being used for anomaly detection, breach prediction, and automation of privacy-preserving processes [28].
2. Federated Learning is also a promising approach to privacy-preserving machine learning [68]. This technique allows models to be trained on different distributed datasets without centralizing the data and addresses privacy concerns in sectors such as healthcare and finance. The process involves the following: (1) initial model training on a central server; (2) distribution of the model to individual devices; (3) local training on each device; (4) transmission of model updates back to the central server; (5) aggregation of updates to improve the global model.
3. Encryption remains a main method of data protection, with many methods for enhancing its capabilities and applications. For example, homomorphic encryption [23] allows computations to be performed on encrypted data without decryption. This method allows secure data processing in untrusted environments, such as public clouds.
4. Post-Quantum Cryptography [65] is used for encrypting algorithms that are resistant to attacks by both classical and quantum computers. Key developments include the following: (1) NIST standardization process for post-quantum cryptographic algorithms [69]. (2) Integration of post-quantum algorithms into existing protocols [69]. (3) Hybrid approaches combining classical and post-quantum methods.
5. Privacy-Enhancing Computation (PEC) [70] covers a range of technologies that enable data to be processed or analyzed while keeping it encrypted or otherwise protected.
6. Trusted Execution Environments (TEEs) [71] provide isolated execution environments within processors and allow sensitive computations to be performed securely even on

untrusted systems. This allows hardware-level isolation of sensitive code and data and protection against privileged software attacks.

7. Secure Multi-Party Computation (SMPC) [72] allows multiple parties to compute a function together over their inputs while keeping these inputs private. Some use cases include privacy-preserving benchmarking, secure auctions and voting systems, and machine learning in a collaborative environment across multiple data owners.

6.2. Interdisciplinary Efforts

In the domains of mobile crowdsourcing and edge computing, fostering interdisciplinary collaboration is essential to create comprehensive frameworks that balance technological advancement with user privacy. Research is also directed towards decentralized systems, which enhance user control over data and mitigate risks associated with centralized data repositories by processing data closer to its source. Blockchain technology can be integrated for traceability and immutability in data handling practices and can enhance security and transparency, allowing users to verify how their data are used and shared.

Incorporating energy efficiency into mobile crowdsourcing and edge computing is crucial for sustainable technology development [73]. One effective strategy is the use of edge computing, which enhances energy efficiency by processing data closer to where it is generated. These methods can help in reducing the need for extensive data transmission and lowering overall energy consumption. This approach can help minimize latency and improve data processing speeds and can also significantly reduce the carbon footprint associated with centralized data centers.

7. Conclusions

This paper has examined the critical privacy concerns inherent in mobile crowdsourcing and edge computing, focusing on identity, data, and location privacy. Despite significant advancements, robust and scalable privacy-preserving methods are still required to address challenges such as de-anonymization attacks and data integrity issues. Ensuring user trust, complying with regulatory standards, and promoting the broader adoption of mobile computing technologies depend on effectively addressing these privacy concerns. Future research should prioritize developing scalable and efficient privacy-preserving techniques and integrating artificial intelligence and machine learning for real-time privacy risk mitigation. Additionally, interdisciplinary collaboration among researchers, industry practitioners, and policymakers is essential to create standardized guidelines and frameworks for privacy protection.

Author Contributions: Conceptualization, S.R.B. and V.M.; Methodology, S.R.B.; Validation, S.R.B, S.R. and V.M.; Formal Analysis, S.R.B. and S.R.; Investigation, S.R.B.; Resources, S.R.B. and V.M.; Writing—Original Draft Preparation, S.R.B.; Writing—Review & Editing, S.R. and V.M.; Visualization, S.R.B. and S.R.; Supervision, V.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Important Definitions.

Keyword	Definition
Privacy	The protection of sensitive information from unauthorized access, ensuring personal data such as identity, location, and activities are secure.

Table A1. *Cont.*

Keyword	Definition
Security	Measures taken to protect systems and data from cyber-attacks, unauthorized access, and breaches in both mobile crowdsourcing and edge computing.
Edge Computing	A decentralized approach where data processing occurs closer to the data source (e.g., IoT devices) rather than relying on centralized cloud servers, enhancing performance and reducing latency.
Mobile Crowdsourcing	A method where data are collected from a large number of individuals through mobile devices, often for real-time applications such as traffic monitoring or environmental sensing.
Location Privacy	The protection of an individual's geographical location information to prevent unauthorized tracking or misuse.
Data Privacy	Ensuring that the collected data remain confidential and are not accessed or altered without permission, with special attention to sensitive information like health or financial data.
Identity Privacy	The safeguarding of personal identifiers such as names or social security numbers to prevent identity theft or unauthorized linking of activities to an individual.
Cloud Computing	The use of remote servers to store, manage, and process data, as opposed to local servers or personal devices, often integrated with edge computing for enhanced scalability.
IoT (Internet of Things)	The network of connected devices, such as smartphones and smart home appliances, that collect and exchange data through the internet.
Differential Privacy	A privacy technique that adds random noise to data sets, preventing the identification of individual data points while allowing analysis of aggregate trends.
Pseudonymization	The process of replacing private identifiers (like names) with pseudonyms to ensure anonymity while still allowing the data to be useful.
Homomorphic Encryption	A type of encryption that allows computations to be performed on encrypted data without needing to decrypt it, ensuring data privacy even during analysis.
Federated Learning	A machine learning technique that allows multiple devices to collaboratively train a model without sharing raw data, preserving data privacy.
Sybil Attack	A type of security attack where a single adversary creates multiple fake identities in a network to manipulate the system, commonly discussed in crowdsourcing security.
Data Poisoning	A malicious attack where false or misleading data are introduced into a dataset to corrupt the outcome of a crowdsourced or machine learning model.
Spatial Cloaking	A privacy technique used to blur or generalize location data to protect an individual's exact location; commonly used in location-based services.
Blockchain	A decentralized digital ledger technology that securely records transactions across multiple systems, enhancing transparency and security, especially for data privacy.

Table A1. *Cont.*

Keyword	Definition
Encryption	A method of converting readable data into an encoded format that can only be read by someone who has the correct decryption key, protecting data during storage and transmission.
Task Offloading	The process of transferring computational tasks from resource-limited devices (e.g., mobile devices) to more powerful edge servers, improving efficiency and performance.
Trusted Execution Environment (TEE)	A secure area of a device processor that ensures code and data loaded inside are protected from being tampered with the goal to provide a safe execution space for sensitive operations.

References

1. Bashir, S.R.; Raza, S.; Misic, V.B. BERT4Loc: BERT for Location—POI Recommender System. *Future Internet* **2023**, *15*, 213. [CrossRef]
2. Adomavicius, G.; Tuzhilin, A. Context-aware recommender systems. In *Recommender Systems Handbook*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 217–253.
3. Raza, S.; Ding, C. Progress in context-aware recommender systems—An overview. *Comput. Sci. Rev.* **2019**, *31*, 84–97. [CrossRef]
4. Liu, Z.; Li, Z.; Wu, K. UniTask: A unified task assignment design for mobile crowdsourcing-based urban sensing. *IEEE Internet Things J.* **2019**, *6*, 6629–6641. [CrossRef]
5. Bashir, S.R.; Mišić, V.B. Improving Rating and Relevance with Point-of-Interest Recommender System. In Proceedings of the ICC 2022-IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 1734–1739.
6. Hu, L.; Shahabi, C. Privacy assurance in mobile sensing networks: Go beyond trusted servers. In Proceedings of the 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Mannheim, Germany, 29 March–2 April 2010; pp. 613–619.
7. Zhang, J.; Chen, B.; Zhao, Y.; Cheng, X.; Hu, F. Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *IEEE Access* **2018**, *6*, 18209–18237. [CrossRef]
8. Barakat, M.; Saeed, R.A.; Edam, S. A Comparative Study on Cloud and Edgeb Computing: A Survey on Current Research Activities and Applications. In Proceedings of the 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Benghazi, Libya, 21–23 May 2023; pp. 679–684. [CrossRef]
9. Lu, S.; Lu, J.; An, K.; Wang, X.; He, Q. Edge Computing on IoT for Machine Signal Processing and Fault Diagnosis: A Review. *IEEE Internet Things J.* **2023**, *10*, 11093–11116. [CrossRef]
10. Singh, R.; Gill, S.S. Edge AI: A survey. *Internet Things-Cyber-Phys. Syst.* **2023**, *3*, 71–92. [CrossRef]
11. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and privacy in fog computing: Challenges. *IEEE Access* **2017**, *5*, 19293–19304. [CrossRef]
12. Guan, Y.; Shao, J.; Wei, G.; Xie, M. Data security and privacy in fog computing. *IEEE Netw.* **2018**, *32*, 106–111. [CrossRef]
13. Yousefpour, A.; Fung, C.; Nguyen, T.; Kadiyala, K.; Jalali, F.; Niakanlahiji, A.; Kong, J.; Jue, J.P. All one needs to know about fog computing and related edge computing paradigms: A complete survey. *J. Syst. Archit.* **2019**, *98*, 289–330. [CrossRef]
14. Zeyu, H.; Geming, X.; Zhaohang, W.; Sen, Y. Survey on edge computing security. In Proceedings of the 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), Fuzhou, China, 12–14 June 2020; pp. 96–105.
15. Sheikh, B.; Butt, A.; Hanif, J. Mobile Cloud Computing: A Survey on Current Security Trends and Future Directions. *Eng. Proc.* **2023**, *32*, 22. [CrossRef]
16. Ali, Y.; Khan, H.U. A Survey on harnessing the Applications of Mobile Computing in Healthcare during the COVID-19 Pandemic: Challenges and Solutions. *Comput. Netw.* **2023**, *224*, 109605. [CrossRef] [PubMed]
17. Jararweh, Y.; Doulat, A.; AlQudah, O.; Ahmed, E.; Al-Ayyoub, M.; Benkhelifa, E. The future of mobile cloud computing: Integrating cloudlets and mobile edge computing. In Proceedings of the 2016 23rd International conference on telecommunications (ICT), Thessaloniki, Greece, 16–18 May 2016; pp. 1–5.
18. Irshad, S.; Rambli, D.R.A. Advances in mobile augmented reality from user experience perspective: A review of studies. In Proceedings of the Advances in Visual Informatics: 5th International Visual Informatics Conference, IVIC 2017, Bangi, Malaysia, 28–30 November 2017; Proceedings 5; Springer: Berlin/Heidelberg, Germany, 2017; pp. 466–477.
19. Liu, Q.; Gu, J.; Yang, J.; Li, Y.; Sha, D.; Xu, M.; Shams, I.; Yu, M.; Yang, C. Cloud, edge, and mobile computing for smart cities. In *Urban Informatics*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 757–795.

20. Yu, Y.; Mu, Y.; Ni, J.; Deng, J.; Huang, K. Identity privacy-preserving public auditing with dynamic group for secure mobile cloud storage. In Proceedings of the Network and System Security: 8th International Conference, NSS 2014, Xi'an, China, 15–17 October 2014; Proceedings 8; Springer: Berlin/Heidelberg, Germany, 2014; pp. 28–40.
21. Veeresh, V.; Parvathy, L.R. Identity-based Encryption to Implement Anti-Collusion Information Sharing Schemes in Cloud Computing. In Proceedings of the 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 4–6 May 2023; pp. 1177–1182.
22. Suresha, D.; Karibasappa, K.; Shivamurthy. Ensuring Privacy Preservation Access Control Mechanism in Cloud based on Identity based Derived Key. *Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 630–636.
23. Wang, J.; Wu, F.; Zhang, T.; Wu, X. DPP: Data Privacy-Preserving for Cloud Computing based on Homomorphic Encryption. In Proceedings of the 2022 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Suzhou, China, 17–18 November 2022; pp. 29–32.
24. Kumar, N.; Aggarwal, S.; Raj, P. *The Blockchain Technology for Secure and Smart Applications Across Industry Verticals*; Academic Press: New York, NY, USA, 2021.
25. Liu, S. Privacy protection and service evaluation methods for location-based services in edge computing environments. *arXiv* **2022**, arXiv:2212.03417.
26. Zhang, Y.; Zhang, Q.; Jiang, Y.; Yan, Y. A location privacy protection method based on cipher-text retrieval in cloud environment. *Secur. Priv.* **2022**, *5*, e250. [CrossRef]
27. Ko, H.; Lee, H.; Kim, T.; Pack, S. LPGA: Location privacy-guaranteed offloading algorithm in cache-enabled edge clouds. *IEEE Trans. Cloud Comput.* **2020**, *10*, 2729–2738. [CrossRef]
28. Yang, L.; Tian, M.; Xin, D.; Cheng, Q.; Zheng, J. AI-Driven Anonymization: Protecting Personal Data Privacy While Leveraging Machine Learning. *arXiv* **2024**, arXiv:2402.17191.
29. Gambs, S.; Killijian, M.O.; del Prado Cortez, M.N. De-anonymization attack on geolocated data. *J. Comput. Syst. Sci.* **2014**, *80*, 1597–1614. [CrossRef]
30. Cutillo, L.A.; Molva, R.; Strufe, T. Privacy preserving social networking through decentralization. In Proceedings of the 2009 Sixth International Conference on Wireless On-Demand Network Systems and Services, Wengen, Switzerland, 22–24 January 2009; pp. 145–152.
31. Brakerski, Z.; Vaikuntanathan, V. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In Proceedings of the Annual Cryptology Conference, Virtual Event, 16–20 August 2021; Springer: Berlin/Heidelberg, Germany, 2011; pp. 505–524.
32. Jiang, B.; Li, J.; Wang, H.; Song, H. Privacy-preserving federated learning for industrial edge computing via hybrid differential privacy and adaptive compression. *IEEE Trans. Ind. Inform.* **2021**, *19*, 1136–1144. [CrossRef]
33. Zhao, B.; Liu, X.; Chen, W.N.; Deng, R. CrowdFL: Privacy-preserving mobile crowdsensing system via federated learning. *IEEE Trans. Mob. Comput.* **2022**, *22*, 4607–4619. [CrossRef]
34. Guo, B.; Wang, Z.; Yu, Z.; Wang, Y.; Yen, N.Y.; Huang, R.; Zhou, X. Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm. *ACM Comput. Surv. (CSUR)* **2015**, *48*, 1–31. [CrossRef]
35. Ren, J.; Zhang, Y.; Zhang, K.; Shen, X. Exploiting mobile crowdsourcing for pervasive cloud services: Challenges and solutions. *IEEE Commun. Mag.* **2015**, *53*, 98–105. [CrossRef]
36. Kong, X.; Liu, X.; Jedari, B.; Li, M.; Wan, L.; Xia, F. Mobile crowdsourcing in smart cities: Technologies, applications, and future challenges. *IEEE Internet Things J.* **2019**, *6*, 8095–8113. [CrossRef]
37. Driving Directions, Live Traffic & Road Conditions Updates—Waze. 2024. Available online: https://www.waze.com/live-map/ (accessed on 20 January 2024).
38. A. Almusaylim, Z.; Jhanjhi, N. Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing. *Wirel. Pers. Commun.* **2020**, *111*, 541–564. [CrossRef]
39. Abbas, N.; Zhang, Y.; Taherkordi, A.; Skeie, T. Mobile edge computing: A survey. *IEEE Internet Things J.* **2017**, *5*, 450–465. [CrossRef]
40. Li, F.; Wang, J.; Song, Z. Privacy Protection of Cloud Computing Based on Strong Forward Security. *Int. J. Cloud Appl. Comput. (IJCAC)* **2023**, *13*, 1–9. [CrossRef]
41. Khalil, I.; Khreishah, A.; Azeem, M. Consolidated Identity Management System for secure mobile cloud computing. *Comput. Networks* **2014**, *65*, 99–110. [CrossRef]
42. Khajehei, K. Preserving Privacy in Cloud Identity Management Systems Using DCM (Dual Certificate Management). *Int. J. Wirel. Microw. Technol* **2018**, *8*, 54–65. [CrossRef]
43. Bendiab, K.; Kolokotronis, N.; Shiaeles, S.; Boucherkha, S. WiP: A novel blockchain-based trust model for cloud identity management. In Proceedings of the 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Athens, Greece, 12–15 August 2018; pp. 724–729.
44. Miao, Y.; Yang, Y.; Li, X.; Wei, L.; Liu, Z.; Deng, R.H. Efficient Privacy-Preserving Spatial Data Query in Cloud Computing. *IEEE Trans. Knowl. Data Eng.* **2023**, *36*, 122–136. [CrossRef]
45. Jadallah, H.; Al Aghbari, Z. Spatial cloaking for location-based queries in the cloud. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 3339–3347. [CrossRef]

46. Rana, K.; Yadav, H.; Agrawal, C. Mutual Authentication and Location Privacy using HECC and SHA 2 in Mobile Cloud Computing Environment. In Proceedings of the 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 6–7 March 2020; pp. 362–369.
47. Gao, H.; Huang, W.; Liu, T.; Yin, Y.; Li, Y. Ppo2: Location privacy-oriented task offloading to edge computing using reinforcement learning for intelligent autonomous transport systems. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 7599–7612. [CrossRef]
48. Luo, Q.; Hu, S.; Li, C.; Li, G.; Shi, W. Resource scheduling in edge computing: A survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2131–2165. [CrossRef]
49. Lysyanskaya, A.; Rivest, R.L.; Sahai, A.; Wolf, S. Pseudonym systems. In Proceedings of the Selected Areas in Cryptography: 6th Annual International Workshop, SAC'99, Kingston, ON, Canada, 9–10 August 1999; Proceedings 6; Springer: Berlin/Heidelberg, Germany, 2000; pp. 184–199.
50. Wang, L.; Liu, G.; Sun, L. A secure and privacy-preserving navigation scheme using spatial crowdsourcing in fog-based VANETs. *Sensors* **2017**, *17*, 668. [CrossRef] [PubMed]
51. Lu, R.; Lin, X.; Luan, T.H.; Liang, X.; Shen, X. Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE Trans. Veh. Technol.* **2011**, *61*, 86–96. [CrossRef]
52. Narayanan, A.; Shmatikov, V. Robust de-anonymization of large sparse datasets. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, USA, 18–21 May 2008; pp. 111–125.
53. Nilizadeh, S.; Kapadia, A.; Ahn, Y.Y. Community-enhanced de-anonymization of online social networks. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 537–548.
54. Kang, N.; Ning, Z.; Zhang, S.; Waqas, M. *Identity-Based Edge Computing Anonymous Authentication Protocol*; Tech Science Press: Nanjing, China, 2023.
55. Xie, H.; Guo, Y.; Wang, H.; Chen, Q.; Fang, C.; Zhu, N. Privacy-preserving method of edge computing based on secret sharing and homomorphic encryption. In Proceedings of the International Conference on Cloud Computing, Internet of Things, and Computer Applications (CICA 2022), Kaifeng, China, 19–21 May 2022; SPIE: New York, NY, USA, 2022; Volume 12303, pp. 79–85.
56. Liao, J.; Wang, H.; Wu, J. A multikey fully homomorphic encryption privacy protection protocol based on blockchain for edge computing system. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7539. [CrossRef]
57. He, C.; Liu, G.; Guo, S.; Yang, Y. Privacy-preserving and low-latency federated learning in edge computing. *IEEE Internet Things J.* **2022**, *9*, 20149–20159. [CrossRef]
58. Chaopeng, G.; Zhengqing, L.; Jie, S. A privacy protection approach in edge-computing based on maximized dnn partition strategy with energy saving. *J. Cloud Comput.* **2023**, *12*, 29. [CrossRef]
59. Zheng, K.; Ding, C.; Wang, J. A Secure Data-Sharing Scheme for Privacy-Preserving Supporting Node–Edge–Cloud Collaborative Computation. *Electronics* **2023**, *12*, 2737. [CrossRef]
60. Shin, H.; Kim, S.; Shin, J.; Xiao, X. Privacy enhanced matrix factorization for recommendation with local differential privacy. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1770–1782. [CrossRef]
61. Zhang, S.; Hu, B.; Liang, W.; Li, K.C.; Gupta, B.B. A caching-based dual k-anonymous location privacy-preserving scheme for edge computing. *IEEE Internet Things J.* **2023**, *10*, 9768–9781. [CrossRef]
62. Wang, W.; Zhou, X.; Qiu, T.; He, X.; Ge, S. Location Privacy-aware Service Migration against Inference Attacks in Multi-user MEC Systems. *IEEE Internet Things J.* **2023**, *11*, 1413–1426. [CrossRef]
63. Ni, J.; Zhang, K.; Lin, X.; Xia, Q.; Shen, X.S. Privacy-preserving mobile crowdsensing for located-based applications. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.
64. Basudan, S.; Lin, X.; Sankaranarayanan, K. A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing. *IEEE Internet Things J.* **2017**, *4*, 772–782. [CrossRef]
65. Zanetti, M.; Würth, I. Post Quantum Cryptography. Ph.D. Thesis, OST Ostschweizer Fachhochschule, St. Gallen, Switzerland, 2022.
66. Liu, H.; Ning, H.; Xiong, Q.; Yang, L.T. Shared authority based privacy-preserving authentication protocol in cloud computing. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *26*, 241–251. [CrossRef]
67. Wang, H.; Yang, Y.; Wang, E.; Liu, X.; Wei, J.; Wu, J. Bilateral privacy-preserving worker selection in spatial crowdsourcing. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 2533–2546. [CrossRef]
68. Kairouz, P.; McMahan, H.B.; Avent, B.; Bellet, A.; Bennis, M.; Bhagoji, A.N.; Bonawitz, K.; Charles, Z.; Cormode, G.; Cummings, R.; et al. Advances and open problems in federated learning. *Found. Trends Mach. Learn.* **2021**, *14*, 1–210. [CrossRef]
69. The National Institute of Standards and Technology (NIST). Post-Quantum Cryptography. 2024. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography (accessed on 30 September 2024).
70. The National Institute of Standards and Technology (NIST). Privacy-Enhancing Cryptography (PEC). 2024. Available online: https://csrc.nist.gov/projects/pec (accessed on 30 September 2024).
71. Trustonic. What Is a Trusted Execution Environment (TEE)? 2024. Available online: https://www.trustonic.com/technical-articles/what-is-a-trusted-execution-environment-tee/ (accessed on 30 September 2024).

72. Zhao, C.; Zhao, S.; Zhao, M.; Chen, Z.; Gao, C.Z.; Li, H.; Tan, Y.a. Secure multi-party computation: Theory, practice and applications. *Inf. Sci.* **2019**, *476*, 357–372. [CrossRef]
73. Zhu, S.; Ota, K.; Dong, M. Green AI for IIoT: Energy efficient intelligent edge computing for industrial internet of things. *IEEE Trans. Green Commun. Netw.* **2021**, *6*, 79–88. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.