sustainability

Review

Big Data Privacy in Smart Farming: A Review

Mohammad Amiri-Zarandi [1], Rozita A. Dara [1,*], Emily Duncan [2] and Evan D. G. Fraser [2]

[1] Data Management and Privacy Governance Lab, School of Computer Science, University of Guelph, Guelph, ON N1G 2W1, Canada; mamiriza@uoguelph.ca
[2] Geography, Environment and Geomatics, University of Guelph, Guelph, ON N1G 2W1, Canada; edunca01@uoguelph.ca (E.D.); frasere@uoguelph.ca (E.D.G.F.)
* Correspondence: drozita@uoguelph.ca

Abstract: Smart farming aims to improve farming using modern technologies and smart devices. Smart devices help farmers to collect and analyze data regarding different aspects of their business. These data are utilized by various stakeholders, including farmers, technology providers, supply chain investigators, and agricultural service providers. These data sources can be considered big data due to their volume, velocity, and variety. The wide use of data collection and communication technologies has increased concerns about the privacy of farmers and their data. Although some previous studies have reviewed the security aspects of smart farming, the privacy challenges and solutions are not sufficiently explored in the literature. In this paper, we present a holistic review of big data privacy in smart farming. The paper utilizes a data lifecycle schema and describes privacy concerns and requirements in smart farming in each of the phases of this data lifecycle. Moreover, it provides a comprehensive review of the existing solutions and the state-of-the-art technologies that can enhance data privacy in smart farming.

Keywords: privacy; big data; security; smart farming; precision agriculture; Internet of Things; machine learning

check for updates

Citation: Amiri-Zarandi, M.; Dara, R.A.; Duncan, E.; Fraser, E.D.G. Big Data Privacy in Smart Farming: A Review. *Sustainability* **2022**, *14*, 9120. https://doi.org/10.3390/su14159120

Academic Editors: Luca Cacchiarelli and Chiara Perelli

Received: 16 May 2022
Accepted: 20 July 2022
Published: 25 July 2022

1. Introduction

Smart farming is an approach for farm management to optimize farming procedures using modern information and communications technologies (ICTs). Increasing farming productivity, enhanced food quality, cost reductions in farm management, and decreased environmental footprint are only some objectives of smart farming. Depending on the application, these objectives are given varying levels of priority. Some modern technologies, such as the Internet of Things (IoT), Artificial Intelligence (AI), and Cloud/Edge Computing, are commonly used in smart agriculture. Through leveraging sensors and smart devices, smart farming enables farmers to collect data regarding weather monitoring, water management, soil health analysis, animal health indicators, and energy consumption. These data can then be analyzed to provide predictions about upcoming situations and to facilitate real-time operational decision-making [1,2].

In Figure 1, an overview of the smart farming ecosystem is demonstrated. In the smart farms, the deployed sensors in the farms interact with the real-world environment to collect data. These data describe different aspects of farming operations, including temperature, humidity, soil nutrition, irrigation, and also livestock and poultry monitoring. In the subsequent stages, these generated data will be utilized by data analytic processes to extract knowledge about farming and facilitate decision making (data analysis component in). Machine learning, data mining, and statistical inference are prevalent approaches in data analytics for smart farming. Machine learning (ML) is a branch of computer science and artificial intelligence that enables computers to learn from data, predict the future, and make decisions with a minimum human of intervention [3]. Data mining and statistical inference are processes of probing data to extract beneficial information and knowledge [4,5].

In the last stage of smart farming procedures (users component in), the information extracted by the analytic techniques is used in value-added services that are provided to the users. The users in the smart farming ecosystem can be farmers, researchers, food companies, or the government. These value-added services can be utilized by decision support systems to improve farming practices such as crop health monitoring, yield prediction, water management, demand forecasting, pesticide and fertilizer management, animal behavior monitoring, livestock health and welfare monitoring, and livestock feed consumption monitoring.

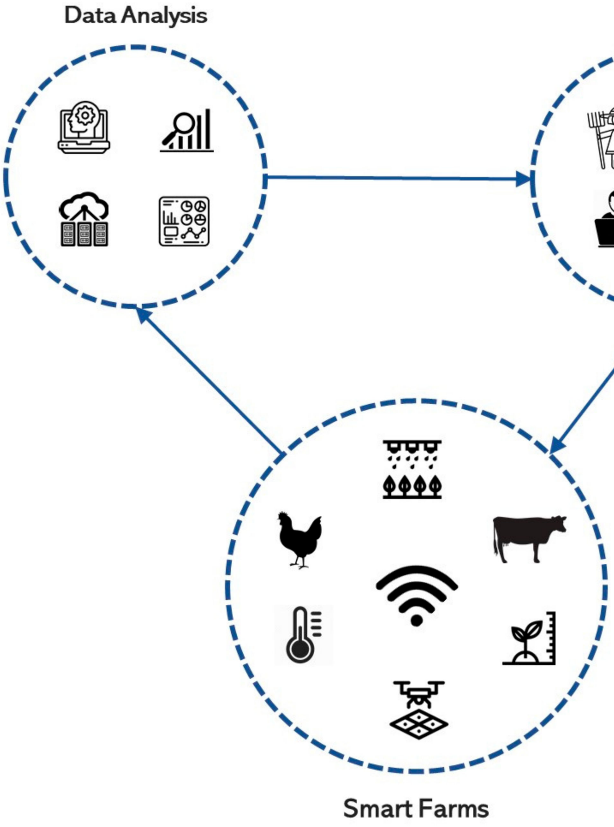

Figure 1. An overview of the smart farming ecosystem showing how Wi-Fi connected drones, livestock and poultry monitoring tools, and other smart farming sensors result in enhanced data analytics that provid users with new insights into how to manage farm operations.

Notwithstanding all benefits raised from the modern smart and interconnected ecosystem in agriculture, they have increased concerns regarding data privacy. Privacy is a major concern for farmers regarding implementing smart farming, or participating in data-sharing practices [6]. Although data security and data privacy are used interchangeably, these are two different concepts. Data security protects data from adversary attacks, while data privacy governs how data is collected, analyzed, stored, and accessed [7]. From this perspective, data security is more about protecting data from attacks, and data privacy is more focused on using data responsibly, according to the users' desire, and protecting data from unauthorized access [8]. This study aims to focus on privacy challenges and solutions in smart farming. Privacy is defined variously under different jurisdictions and applications making it a complicated issue to address. Although it is difficult to precisely define data privacy, in this study, we adopt the definition presented by the Internet Security Glossary (ISG) [9]: "The property that information is not made available or disclosed to unauthorized individuals, entities, or processes."

There have been some preliminary studies exploring the topic of security and privacy concerns in smart farming. Ferrag et al. [10] presented a review on security and privacy issues and challenges in IoT-based agriculture. Gupta et al. [11] discussed the security issues in the smart farming cyber-physical environment. Cybersecurity challenges of smart farming have also been highlighted by Barreto et al. [12]. The primary focus of these studies is security threats and solutions. In this paper, we review privacy requirements, concerns, and solutions in different stages of the smart farming data lifecycle. We aim to make a novel contribution to this literature by focusing this review specifically on big data privacy in smart farming. To this end, we review the papers that explicitly focus on smart farming applications, as well as some studies that consider general IoT applications that can also be applied to smart farming.

The remainder of the paper is structured as follows. Section 2 describes the big data lifecycle in smart farming. In Section 3, privacy concerns and requirements in smart farming are introduced. In Section 4 the state-of-the-art privacy-preserving solutions in the lifecycle stages of smart farming are reviewed. Section 5 reviews the modern technologies utilized for privacy enhancement in smart agriculture. The legislation considerations related to big data privacy in smart farming are discussed in Section 6, and finally, Section 7 provides concluding remarks.

2. Big Data Lifecycle in Smart Farming

A framework of the big data lifecycle is necessary to understand the processes in different stages of data life. Such a framework provides better insight into the processes and actions that are required for data, such as aggregation, encryption, and retention. Arass and N. Souissi [13] detailed a data lifecycle that follows raw data until it is utilized in the big data context. Xu et al. [14] described a big data life cycle framework to investigate security threats. Abouelmehdi et al. [15] presented a big data security lifecycle for healthcare. In this study, we present a big data lifecycle schema from the privacy perspective. This lifecycle provides a better intuition about privacy threats, requirements, and their correlation in different stages of smart farming. Figure 2 demonstrates the main stages of the big data privacy lifecycle.

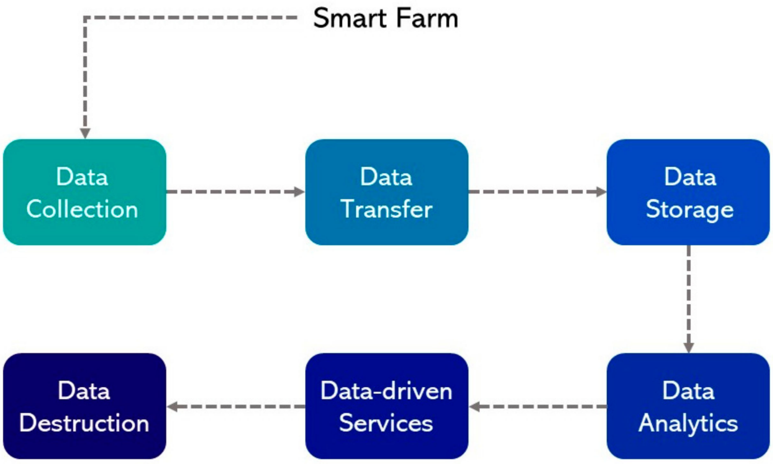

Figure 2. The big data privacy lifecycle in smart farming.

- *Data Collection*: In this step, raw data are collected from devices such as sensors. These sensors can gather data from different aspects of farming, including weather, soil quality, animal movement, and harvest monitoring. Sensors deployed in smart farming applications are commonly limited in energy and computation resources; therefore, these devices are only capable of performing very simple data refinement and processing tasks [16].
- *Data Transfer:* In this stage of the data lifecycle, the collected and aggregated data are transferred to the servers. These servers could be a local computer on the farm or a cloud service used by the technology provider [17]. To this end, a combination of different technologies is utilized including Wi-Fi, cellular, Local Area Network (LAN), and Bluetooth [18].

- *Data Storage:* Data can be stored locally, before transmission, or on the cloud storage servers. In both cases, the privacy of the stored data should be ensured [19]. To reach this goal, an effective access control mechanism is necessary to prevent unauthorized data inquiries [20].
- *Data Analytics:* In this stage, data are analyzed and exploited to extract knowledge. This knowledge improves the farming decision-making processes through the use of analytics methods. Machine learning, statistical inference, and data mining are some of the common approaches for data analytics [21].
- *Data-Driven Services:* These services can provide a wide range of recommendations to farmers regarding aspects such as selecting the most profitable product for the field, designing an optimized procedure from planting to harvesting, forecasting the affecting environmental events, and assessing the market for price negotiation. It is a major motivation for farmers to improve the profitability of their business using data-driven services [22]. Given that these services are usually publicly accessible to various clients, providing privacy protection in these services is a serious requirement [11].
- *Data Destruction:* When the data are no longer useful or when it should be erased based on the preliminary agreements, data destruction needs to occur. For example, these preliminary agreements might set a retention time after which data should be deleted permanently, or at which time, the data owner may request a return of the data [23].

3. Privacy-Preserving Solutions in Big Data Lifecycle

3.1. Data Collection

In smart farming, a large amount of data is generated by the deployed sensors. To decrease the privacy risk in the data collection stage of the data lifecycle, a desirable approach is to aggregate the collected data before transferring it through the network. Using this approach, a preliminary analysis should be performed on the generated data, and then a representative value is sent to the network [24].

Previously, some studies have been conducted on privacy-preserving data collection. Koh et al. [25] suggested using the Gaussian process regression model [26] for sampling and compressing gathered data. In this study, the authors introduced a metric to determine more important data that can be used from the whole collection of data generated by the sensors. Masiero et al. [27] leveraged the principal component analysis (PCA) technique [28] to collect a limited number of signal samples from a central data gathering point and utilize these data to reconstruct the original signals. This method can be used to decrease the transmitted signals from connected digital devices and decrease the privacy risk. In another study, these same authors suggested a combination of PCA and Bayesian estimation [29] for the same goal. Although PCA can be effective in data aggregation, there are some concerns about using this technique in smart farming. PCA requires a great deal of computation to be processed, but the digital devices that are commonly used in smart farming have limited energy and computation resources; thus, some researchers recommend using distribution methods to distribute the computation tasks among diverse available devices. Such a distributed approach is presented in [30] for PCA deployment in wireless sensor networks. This approach can be utilized in wireless sensor deployment in agricultural applications, such as mixed crop farming [31].

Another approach for privacy-preserving in smart farming is anonymization. Data anonymization is a process in which any information that can enable personal identification, including name, address, and geographic identifiers, are removed from data. In [32], an anonymization protection model was used in IoT to obscure the specific location information of the data, while still assuring data openness. In this paper, the authors described that some traditional data anonymization algorithms work just for data streams generated by a single entity, while in some IoT applications (such as smart farming), a single entity can use multiple devices at the same time. To tackle this issue, the authors presented a partitioning approach that extends the k-anonymous privacy model [33] to the IoT data streams. Martin et al. [34] proposed a method for anonymizing point location data in analyzing the spread of avian influenza. This method allows the farmers to share data with experts without disclosing individual farm identities.

Access control, which handles the requests and permissions based on set policies, is an important component of data privacy in smart farming. Additionally, access control determines how smart devices and resources are accessible in the system. One prevailing approach that is used for access control in smart devices is capability-based access control (CBAC). In this approach, each object has a list, called a 'token,' that has a directory of its rights to access other objects, enabling multilevel control. Anggorojati et al. [35,36] presented CBAC mechanisms that use the delegate method to control requests in the IoT. They introduced a module, called 'IoT federation manager,' as a part of a system to keep and manage rules and policies in distributed IoT environments. Mahalle et al. [37] combined CBAC and an elliptic-curve Diffie–Hellman algorithm for a secret-key generation. Because this method is lightweight and distributed, it is suitable for IoT devices in smart farming. Hernández-Ramos et al. [38] optimized the elliptical curve cryptography for real-world applications and used it to design a CBAC mechanism for smart things. This mechanism consists of two parts: firstly, the session key is generated, and in the second step, a capability token is used to access an object. This study is extended [39] by developing a trust evaluator component. In addition to reputation and feedback, this evaluator considered security features and social relationships among devices.

The other access control mechanism is the role-based access control (RBAC) model, in which the permissions are issued based on the role of the nodes in the system. Zhang and Tian [40] leveraged this approach to create an access control model for the IoT. They used contextual data, such as the time and location of IoT users, to improve the access decisions regarding the requests in the system. Jindou et al. [41] presented another role-based mechanism for access control in the IoT. In this study, instead of contextual data, such as time and location, the authors used social networks and enabled the system to leverage data from profiles and social connections to generate access policies. Arka et al. [42] utilized the RBAC approach to enhance the security of the IoT. To reach this goal, they mapped entities of RBAC to WoT components and then used cryptographic keys to implement the access policies. To extend the ideas that were presented in [38,43], Hernandez-Ramos et al. [44] proposed a distributed approach to access control in the IoT. They used public keys and an optimized version of the elliptic curve digital signature algorithm inside the IoT devices to confirm end-to-end authorizing.

Recently, Chukkapalli et al. [20] presented an attribute-based access control (ABAC) solution for smart farm applications. This solution can be utilized for different smart farming applications, including plant agriculture, poultry, or dairy farming. ABAC manages access requests based on the attributes of the actors in the system and provides dynamic permission handling, depending on time and situation. These attributes can be extracted from diverse sources, such as devices, data, users, and the environment. In this study, the authors built a smart farm model with sensors to monitor, weather, soil, tractors, trucks, and labor. The introduced solutions can grant access permissions at different levels, considering the inquirer, requested source, and the time access request. Among the available access control mechanisms, the ABAC approach can be more beneficial in smart farming due to the flexibility and the fine-grained multilevel access control that this approach provides in a system.

3.2. Data Transfer

To address privacy issues in this stage, a potential solution is to add more powerful servers to the farms. These servers are responsible for anonymization and generating summaries from the raw collected data. Although these servers can facilitate many operations in smart farming, cost, space, and energy consumption are the concerns that might lead to small farm owners' hesitation regarding this solution.

Encryption is a classic approach to protecting privacy in communication. It locks the data with a key and turns it into an unreadable format, called 'ciphertext,' so that only individuals with a proper key can decode it. Using this mechanism, even if an adversary agent accesses the sent data in the network, it cannot read the content. Jiang et al. [45] proposed a method that utilizes identity-based encryption to assure privacy and anonymity in big data. In this study, a unique virtual identity, that works as both the identity and the public key, was assigned to each entity in the system. The recovery of the message relies only on the decryption in the destination; thus, using this mechanism, farmers can continue working, even if the data sender is not currently online. In [46], a comprehensive performance evaluation of attribute-based encryption was presented from different aspects, including execution time, energy consumption, data overhead, processing resources, and storage. In [47], the authors described that one drawback of attribute-based encryption is publicly available access policies that put information privacy at risk. This can be a concern for farmers and technology providers because it can allow adversaries to use these public policies to get unauthorized access to smart farms' data. To tackle this issue, the authors proposed a policy-hidden encryption scheme that makes the access policies invisible to third parties and decreases privacy concerns. Davoli et al. [48] presented an anonymity protocol for smart connected objects. They suggest using an anonymity network that enforces privacy on secure end-to-end connections. The presented protocol uses limited cryptographic overhead to provide diverse anonymity path modes and ensures privacy-preserving data transfer for different IoT applications, including agriculture.

3.3. Data Storage

Collected data in smart farming applications can be stored in on-site storage devices or remotely, in cloud servers. Like other stages of the big data lifecycle, here we need mechanisms to provide privacy protection. Lain et al. [49] presented a privacy-preserving ciphertext multi-sharing mechanism to accomplish confidentiality and anonymity in big data storage. This mechanism leverages a conditional re-encryption technique in which the encrypted message can be shared with others if some specified conditions are satisfied. Li et al. [50] proposed a scheme for big data protection in data storage that is searchable—meaning that these data are stored in a cloud and encrypted in a way that users are still able to send queries to search data. This scheme increases usability while preserving privacy. In [51], an attribute-based encryption scheme was presented for big IoT data stored in the cloud. This scheme provides an access control mechanism, ensuring accountability for using the user key and authorization center key. In [52], another privacy-preserving auditing scheme was proposed to ensure privacy in the data storage stage of the big data lifecycle. In this study, a novel cryptographic algorithm was utilized to encrypt data and split them up into different files. In this scheme, the entire data file is encrypted and divided into separate files using a cryptographic algorithm. After uploading data to the cloud server, a third party verifies the data integrity using a method with limited computation and communication overheads. Yang et al. [53] proposed a privacy-preserving big data storage system for smart healthcare, which can be utilized for smart farming as well. This system provides secure anonymized data storage and supports smart deduplication to use the big data storage capacity more effectively. The two-fold access control mechanism utilized in this study provides an opportunity for farmers to set different privacy expectation levels for data based on the data content.

The data storage provider cannot disclose data to unauthorized parties and is accountable for all data breaches. On the other hand, the data owner must be able to obtain access to data for farm management purposes at any time.

3.4. Data Analytics

In the data analytics stage of the big data lifecycle, the collected and stored data are processed for knowledge extraction using different analysis techniques. The results from these techniques can be utilized by farmers to inform their farming decisions. Privacy-preserving data analysis encourages data owners to participate in value-added services and increase the performance of different practices by cooperating with other parties.

An example is an architecture proposed by Huning et al. [54] for leaf area index (LAI) calculation in smart farming. LAI is defined as leaf area per horizontal ground surface area and can be utilized for analyzing vegetative processes such as photosynthesis and evapotranspiration. The authors in this study proposed a privacy-preserving architecture that enables an increased spatiotemporal estimation in the LAI calculation.

In many farming applications, achieving complete end-to-end privacy is unreachable because adding auxiliary data to anonymous available data can lead to extra knowledge that reveals private information. In smart farming applications, these auxiliary data can be regional, weather, soil, or production data that help adversaries to infer information from agricultural data. This issue has been discussed by Dwork in [55] and to address this problem, the author defined differential privacy as a metric to measure the privacy degree. This metric quantitatively describes the risk degree of data disclosure. Moreover, in this study, it has been proven that adding noise with different variations provides different levels of differential privacy. In [56], a privacy-preserving deep learning model for disease detection in apple trees was presented. In this study, differential privacy certifies the privacy of the users in the data sharing process. Xu et al. [57] presented a local differential privacy obfuscation (LDPO) framework for data analysis in the IoT. This framework aggregates data before protecting the users' sensitive data. Yan et al. [58] utilized differential privacy for privacy-preserving geographic-based service provision in farming applications. For this purpose, the authors utilized 1500 location points in Nebraska, a typical agricultural-producing state in the U.S. Niemitalo et al. [59] suggested using differential privacy for protecting the privacy of original data points of the drone images acquired from agricultural and forestry research sites.

Zhang et al. [60] proposed an algorithm for quality of service (QoS) prediction in the IoT. In this algorithm, first, some noises are employed on the original data for privacy preservation, then the algorithm predicts the QoS based on the users' preferences and mobility. To achieve better performance, the algorithm leverages the QoS prediction for the same user on other servers, as well as the prediction for similar users on the same server. Xiong et al. [61] designed differentially private machine learning-based algorithms to preserve privacy in IoT applications. In this study, the authors modified the differential privacy k-means algorithm [62] for use in the intelligent electrical service of the IoT.

3.5. Data-Driven Services

In data-driven agriculture, diverse on-farm and off-farm data sources, including field sensors, drones, satellite data, and supply chain data, can be combined and analyzed to provide superior knowledge for different sectors in agriculture. This knowledge is utilized for planning, forecasting, and automatic actions in smart farming. In this stage of the big data lifecycle, it is important to provide data-driven services in a privacy-preserving manner. One of the basic services available in agricultural applications is data sharing. Several platforms are available that enable farmers to share and exchange their data, while ensuring privacy protection. Nordic Cattle Data Exchange (NCDX) [63] is a platform for sharing cattle data that is developed for northern European countries. This platform provides a standard method for data exchange and supports different farm management software. Barto [64] and JoinData [65] provide similar services for data-driven smart farming in Swiss and Netherland markets, respectively. HARA [66] is a blockchain-based data-sharing framework in Indonesia that provides different types of data, including land location and ownership data.

Anonymization is an approach to preserve the privacy of the users in a service provision platform. A system to protect the anonymity of the users interacting through the internet is presented in [67]. The idea proposed in this study is to group the users into a diverse set. The users are anonymized, and the group sends the requests on behalf of the original users and retrieves the information using a randomized routing protocol. Attackers are unable to find the real origin of the request because the probability for all group members to be the source of the request is the same.

One of the other mechanisms that can be used in privacy-preserving service providing is trust evaluation. Using a trust management system, the service provider can assess the trustworthiness of different parties in the system and restrict the activities of the non-trustable users. In [68], a trust model based on software-defined networking (SDN) [69] is presented for IoT systems. In this study, the authors used two reputation evaluation schemes: a behavior-based scheme and an organization-based scheme. Combining these two factors, the proposed model can evaluate the trust factor for each node in the IoT system. Social features of connected digital devices can also be used to enhance trust management in smart farming. From this perspective, Social IoT [70] is a useful concept. It considers that smart devices can be socially connected, like humans in social networks. Using this concept, in addition to the previous experience in the system, the social relations among the IoT devices can be another valuable source of information to evaluate the trustworthiness of devices. Nitti et al. [71] presented social trustworthiness management from two different perspectives: subjective and objective. In the former model, each node uses its own experience and the information from its friends to evaluate the trust factor of other objects, while in the latter approach, the information from nodes will be published in the network and any other objects can utilize it. Another trust management system that leverages social connection among IoT devices is presented in [72]. The proposed system uses blockchain technology to provide a fast and secure trust evaluation mechanism using collaboration among the devices in the system.

3.6. Data Destruction

At the final stage of the big data lifecycle, it is important to make sure that the data are cleaned permanently from data storages to prevent possible data leakage in the future. Fengzhe et al. [73] discussed the privacy concerns regarding data destruction and suggested a time-constrained mechanism to remove data from storage servers. In this proposed mechanism, all sensitive data are irreversibly removed at a specified time, with no user intervention. In [73], the authors proposed a scheme for data destruction in multi-tenant data storage. The focus of this study was to provide a way to track customers' data and ensure the destruction of the original data, as well as all copies. Farmers can leverage these destruction mechanisms and set a retention time for their data in the agreements. Based on this retention time, data holders are responsible to make sure the data are removed from the servers permanently and irreversibly.

4. Privacy-Preserving Technologies in Smart Farming

4.1. Machine Learning

Machine learning is a method to enable machines to learn based on their experience. Using machine learning, the farmers can analyze the collected data and discover patterns, predict the future, and increase the performance of their businesses. In smart farming, the deployed sensors are responsible to collect data from different aspects of the farm, and then this data will be analyzed by machine learning models to provide an insightful analysis regarding diverse applications, such as yield prediction, quality assessment, water management, disease prediction, and livestock monitoring. Because machine learning models utilize data for the learning process, it is essential to design the learning models in a way that sensitive information remains protected [74]. Therefore, some studies have provided privacy-preserving machine learning-based solutions for smart agriculture.

De Souza et al. [75] presented a machine learning model to detect sensors that are used to monitor the forests and are suspicious to perform malicious activities. The presented solution was tested on four forest areas of the Roosevelt National Forest (U.S). These areas were selected since minimum disturbances caused by human activities are seen in these areas. In this study, the authors describe that because the behavior of the sensors is highly affected by environmental conditions, it is not easy to determine if the behavior of a sensor is normal and trustable. To tackle this problem, the authors presented a machine learning-based algorithm to identify suspicious sensors in a wireless sensor network based on the goals that are defined by the users, including accuracy, power saving, and thermal efficiency. Udendhran and Balamurugan [56] proposed a secure deep learning system for disease detection in apple orchards. The presented method analyzes the images of apple tree leaves that suffer from multiple foliar diseases. The utilized dataset includes more than 3500 images captured with diverse angles and illuminations. This architecture connects people who are not willing to share their data. These people can use the proposed local classifier, without sharing the data with other parties. Chukkapalli et al. [76] designed a framework for weed quality analysis that provides a privacy-preserving mechanism for data sharing among the farmers. The presented framework used data perturbation techniques to add noise to raw data and consequently, protect data privacy. In this study, the authors suggested a noise-adding procedure that does not impact the data analysis results. The framework gathers the perturbed data from various farmers and detects the low-quality products using anomaly detection.

In the literature, some studies have been conducted on using privacy-preserving machine learning approaches in general IoT applications. These studies can be utilized in different smart farming applications. Da et al. [77] used neural networks for IoT device authentication. In this study, channel state information (CSI) of connected digital devices was utilized in a deep long short-term memory (LSTM) learning method for device authentication. In [78], a privacy concern regarding the analysis of CSI in wireless sensor networks was studied. In this study, the authors described how the channel state information can be used to identify the behavior pattern of the users and any malicious actions. Canedo and Skjellum [79] suggested using machine learning to detect anomalies in data transferred by IoT devices. To achieve this goal, they utilized neural networks to identify invalid data points.

Machine learning has also been used to develop intelligent access control mechanisms in IoT environments [80]. The presented solution in this study used the support vector machine (SVM) method that analyzes behavior data from the devices to detect adversarial actions. Another machine learning-based access control was presented in [81]. In this study, a neural network was designed for controlling access to media in wireless sensor networks. To train this model, the features from the physical layer of the devices, in addition to network data, were collected and analyzed. Outchakoucht et al. [82] proposed a reinforcement learning model based on the blockchain platform that manages access control decisions in IoT. This model collects behavior information from smart IoT devices and dynamically adjusts the access policies.

Recently, federated learning as a distributed learning approach that assures a high level of data privacy has gained a lot of attention [83]. This technique distributes the learning model among different smart devices and eliminates the need for a central unit to perform all processes. Using this approach, the users can keep their data private on the local servers, while these data are utilized by the learning model. This approach reduces privacy concerns and motivates farmers to participate in the data analysis programs. One of the studies that uses this approach was proposed in [84]. In this paper, the authors combined federated learning with reinforcement learning on mobile devices in edge-enhanced IoT. Wang et al. [85] utilized federated learning on IoT resource-constrained devices. To this end, the authors designed a control algorithm to maximize the accuracy of the learning model by building a balance between local updates and global aggregation of the parameters in gradient descendent-based machine learning models.

4.2. Edge Computing

In many smart farming structures, there are two main types of communication among devices. One is device-to-device communication, in which the digital devices communicate directly, with no intermediate. In this communication mechanism, two devices create a peer-to-peer connection to exchange data between each other. The second class of communication is device-to-server, in which IoT devices make independent connections to data and computation servers (usually cloud servers) to transfer data. Recently, some researchers introduced another communication class. In this class, digital devices use middleware, called the edge nodes, to transfer data through the network. This middleware collects data from end-users (e.g., sensors) and performs some pre-processing tasks, such as data or protocol change algorithms to reduce the volume of transferred data. Edge nodes usually have more computational power than the sensors and can process larger tasks on data before transforming through the network. This enhances data privacy by reducing the volume of transmitted data in the network. By performing pre-processing tasks at the edge of the network, it is not necessary to transfer all the raw data to the cloud servers, and most of these data will stay in private storage, which enhances data protection. The other advantage of making use of edge-enhanced architecture is having more computing resources, which enables using more sophisticated algorithms for data aggregate encryption before transmission through the network.

Guardo et al. [86] highlighted how edge computing technology can significantly reduce the amount of transmitted data via the network. To this end, they presented a two-tier edge computing framework and utilized it for farm management. In [87], another edge-based platform was proposed that decreases the amount of transformed data to the cloud server while leveraging automated pest management, agricultural monitoring, and image processing. Malik et al. [88] designed a simulator to examine edge-based farming scenarios. This simulator considers different factors influencing edge-based smart farming, such as device placement, sensor coverage area, mobility models for moving elements, and energy consumption. Rezk et al. [89] proposed a decision support system to predict crop productivity and drought in smart farming. For this purpose, the authors designed an intelligent AI-based method that leverages classification and wrapper feature selection. Using edge computing, the transformed data to the main server is lessened, helping to reduce the privacy risks for personal information. In [90], it was described that due to a limited budget, many farmers are only willing to use a few digital devices on their property. Thus, the authors present a service offloading-oriented edge server placement method for smart farming. This method decreases the data transmission delay and also balances the workload among different edge servers.

Caria et al. [91] introduced a privacy-preserving system for animal welfare monitoring. They suggest using low-cost devices, such as Raspberry Pi, as edge servers to work with the sensors deployed for monitoring livestock and farm environments. They demonstrate that their low-cost solution can effectively control multiple factors of animal welfare monitoring, such as room temperature, body temperature, humidity, and motion. Taneja et al. [92] proposed an edge-assisted system for the analysis of animal behavior and health monitoring in dairy farming. This system brings a major portion of data analysis from cloud servers to the local edge servers that are placed at the farm. This analysis system provides notices regarding livestock health to detect diseases in the early stages. They extended their work using real data from dairy cows in [93]. In [94], a platform is presented that leverages different technologies, including edge computing, machine learning, and blockchains, to improve the quality of service and privacy. The designed platform monitors dairy cattle and feed grain. In this study, it has been shown that the edge nodes can lessen the data traffic transferred between edge nodes and cloud servers. These examples show that edge computing is widely recommended for smart farming, and it can be an effective solution to protect privacy.

4.3. Blockchain

Blockchain is a state-of-the-art technology that has recently been widely used in diverse applications [95]. This technology is a distributed ledger that records all previous transactions on the public ledgers and utilizes mathematical algorithms to prevent data manipulations and certify the validation of data. It was originally introduced as Bitcoin [96], a cryptocurrency for financial applications, but it is also utilized in other applications, such as data management and smart contract-based automation. Smart contracts are computer programs that can be deployed and executed on a blockchain network [97].

Blockchain reduces privacy concerns by eliminating the central point of vulnerability in the system. All clients can have a copy of the ledgers, and nobody has full control to store, use, and delete the whole data. Data on the blockchain is transparent and immutable; therefore, all previous records are traceable. Blockchain platforms also deploy a cryptographic private key, in addition to the ring signature, ensuring privacy and confidentiality for the users [96]. Different blockchain-based mechanisms have been introduced in recent years. Some technical features that can describe the difference among these architectures are:

(1) The permission mechanism which indicates the method that is utilized for authentication.
(2) The consensus algorithm that is the mathematical algorithm to decide how to add a new block to the blockchain.
(3) The smart contract/cryptocurrency which points out if the blockchain is used for smart contract deployment, financial payment, or both [98].

Blockchain has gained a lot of attention in smart farming applications, such as water management [99,100], food traceability [101], and supply chain [102,103]. Geethanjali and Muralidhara [104] suggested using a blockchain that monitors the growth and supply chain of the fruit in banana production. In this study, the authors indicated that blockchain technology enables farmers to securely save data and attract more investments in their businesses. In [104], a blockchain was used for fish farms to ensure data integrity. The authors developed smart contracts to run fish farm processes automatically. Using this approach, there is no need for a third party to store data and execute the process, which reduces privacy risks. Yadav and Singh [104] reviewed the issues of Indian farmers and suggested that a mobile app that utilizes blockchains can address these issues. This mobile app handles traceability, monitoring, and informative systems and utilizes smart contracts. A three-layer concept for decentralized trust management in IoT was proposed in [104]. This architecture is scalable and secure, as it deploys trust management on distributed ledgers and automates the process using smart contracts. Another blockchain-based trust management system is presented in [105]. In this paper, social information about the IoT devices, in addition to information entropy, evaluated the trustworthiness of the nodes in IoT environments and described the trust using three metrics: reputation, cooperativeness, and community-interest. Tahar et al. [106] presented a distributed blockchain-based authentication mechanism for IoT on the public Ethereum. It was shown that the proposed mechanism can provide robust identification and authentication to ensure data integrity and availability.

An intelligent system for agriculture that protects data security and privacy was proposed in [107]. This system applies dark web technology to cover the IDs of the servers and also leverages a fast authentication mechanism for blockchain information. Moreover, the presented system enhanced privacy and integrity by applying encryption and using hash technology. Sahid et al. [108] proposed a blockchain-based solution for the agri-food supply chain. In the presented system, all transactions are first written to the blockchain, then a summary of data is uploaded to other external storage systems. This procedure decreases the saved data on the distributed ledgers and accelerates data access. Furthermore, an access control strategy monitors authenticated access to data and ensures data privacy and confidentiality. Salah et al. [109] suggested a system that leverages blockchains to ensure soybean traceability. In the introduced framework, business transactions regarding the soybean supply chain are stored on a blockchain platform, and smart contracts automate procedures related to monitoring the transactions. In this paper, it has been described how this solution can eliminate the centralized authority in the system.

In addition to these papers, some studies have suggested using blockchains for distributed access control. Ouaddah et al. [110,111] used blockchains to design a distributed framework for access control in IoT. The presented framework leverages smart contracts to automate complying with access permissions and managing access requests. Similarly, Zhang et al. [112] utilized smart contracts to control access requests in IoT environments. The proposed framework can not only manage static access permissions, but it can also dynamically change the permissions based on the objects' behavior. Novo [113] presented another access control mechanism for arbitrating roles and permissions in IoT. The presented solution is scalable, and the IoT devices are not directly connected to the blockchain. This design addresses the concerns related to the limited energy and computation resources of IoT devices and makes it easier to adopt current IoT devices for the proposed architecture.

5. Legal Considerations

The promising goals of smart farming are achievable when farmers trust other parties to share data and participate in value-added services. However, studies have shown that the farmers are not always willing to share data [6,114,115]. Some of the concerns that reduce farmers' motivation to share data come from their attitude that laws do not support their rights concerning data privacy and business benefits [116]. Recently some privacy and security principles and data codes of conduct have been proposed in an attempt to address the farmers' concerns.

In 2014, the American Farm Bureau Federation established Privacy and Security Principles for Farm Data (PSPFD) in the U.S. [117]. These principles touch on different privacy concerns, especially on data sharing practices. Here are some core principles of PSPFD [117]:

1. *Ownership*: Farmers own the information collected in the farming operations, but it is also their responsibility to negotiate and agree on data sharing with other parties. It is also the farmers' responsibility to make sure only the data they own have been included in an agreement.
2. *Collection, Access, and Control*: Any access and use of farm data should be explicitly permitted by the farmer in the signed contracts or other types of legal agreements.
3. *Notice*: Not only should farmers be clearly informed that their data are being collected, but they must also be aware of how their data are going to be used and disclosed by the technology provider or any other third party. These notices should be provided in an easily located and readily accessible format.
4. *Choice*: Technology providers must provide choices for farmers to opt in, opt out, or cancel the services.
5. *Portability*: The farmers should be able to transfer their data to other systems, except for the data that have been aggregated or anonymized.
6. *Disclosure, Use, and Sale Limitation*: The technology provider should notify the farmer if they decide to sell or disclose the collected data, and they should also provide the chance for the farmer to cancel the service or remove the data. Working with a new third party should be based on the agreements consistent with the primary agreement between the parties.
7. *Data Retention and Availability*: Technology and service providers should provide mechanisms to erase or return farm data based on the farmer's request, either immediately or after an agreed-upon timespan.

AFBF has developed a tool called the Ag Data Transparency Evaluator to ensure the compliance of policies and agreements with the PSPFD principles in all designed smart farming services. This tool evaluates the agreements among smart farming actors against the principles provided in the PSPFD. If this procedure is successful, the contract receives an Ag Data Transparency seal that certifies the service has passed the required evaluation.

All stakeholders in the smart farming ecosystem must continuously adapt their products, agreements, and services to the available privacy policies and regulations. However, it is costly and time-consuming for the smart farming actors to manually ensure compliance, considering the extensive amount of data and complexity of legal documents. A promising approach in this field that has recently gained a lot of attention is to manage the compliance processes automatically. Data Capsule [118] is a paradigm designed for the automatic compliance checking of data privacy. This paradigm uses a formal language that is designed specifically to describe the privacy policies in an abstract format. This abstract format formulizes the privacy policies and their requirements.

Finally, although the available codes of conduct provide useful initial attempts in defining privacy in a standard way and automizing compliance using digital platforms for smart farming, current practices are not enough to protect farm data. These best practices do not set out requirements and standards for data privacy to be followed by smart farming actors. Therefore, standardized best practices that are applicable in different regions are important for the smart farming ecosystem.

6. Discussion and Future Directions

In this paper, we investigated different aspects of data privacy in smart farming. Privacy-preserving smart farming requires data protection in different stages of data lifecycles. Security is a major requirement to safeguard agricultural applications against potential attacks, but it is not sufficient for data protection. Privacy is also a crucial requirement in smart farming applications to ensure data confidentiality and integrity in collecting, analyzing, and storing procedures. Data privacy should be considered a core value for the different stakeholders in the smart farming ecosystem. In the literature, several solutions have been provided for preserving farming data privacy throughout the data lifecycle stages. In spite of all these efforts, a unified approach that provides a clear and concrete mechanism for data protection in all stages of smart farming applications is still a gap. In the following, we review some challenges and future research directions in the privacy-preservation of agricultural data which we believe require the most attention.

Standardization: Numerous IoT devices are connected through the IoT. These devices utilize various technologies, configurations, and protocols. The heterogeneity of these devices is an issue in developing privacy-preserving solutions to work in different farming practices. Without standardization, the interconnection mechanisms in agriculture are highly complex because different technology providers use different formats for their system operations such as sensing, transmission, storage, routing, and service management. Standardization addresses this issue by providing unified approaches to be followed by technology providers and farming actors, consequently improving the privacy-preserving solutions for smart farming.

Trust: Previous studies show that trust is a bottleneck in data sharing and collaborative service production in smart farming [6]. Trust evaluation is a complimentary act to the data protection mechanisms provided in farming applications. Trust evaluation reduces the concerns of agricultural sectors regarding data sharing procedures and encourages these actors to participate in collaborative value-adding services. To this end, the trustworthiness of an actor in the agricultural ecosystem can be evaluated based on investigating the background of the actor and analyzing recommendations from other businesses that have previous experience in working with the actor. Automatic tools and services that manage this process accelerate the trust evaluation process and reduce the threats to the privacy of data in smart farming.

Legal Frameworks: Smart farming requires legal frameworks that clearly discuss different aspects of data privacy, including responsibilities and accountability. These frameworks can indicate the requirements for different agricultural sectors to access, utilize, and make profits from available data. Such best practices should also determine the responsibilities of farming actors in each stage of the data lifecycle and set requirements to ensure data privacy. Moreover, the legal frameworks should clearly elaborate on the accountability of each actor and the potential consequences in the case of data leakage.

Blockchain: Blockchain is a promising technology that has gained considerable attention in smart farming. Despite the advantages of this technology, some concerns and issues have affected the development of blockchain-based solutions in real-world agricultural applications. A major concern in this regard is scalability. Since numerous smart devices are working in farming applications, the blockchain-based method must be able to provide solutions that manage all the transactions transmitted through the system in a reasonable time. The other concern in leveraging the blockchain in farming is that the mining procedures commonly require a great amount of computation and energy resources, which is a constraint in many farming smart devices. A potential research direction can be investigating the solutions that reduce these concerns.

7. Conclusions

Digital technologies have reshaped agriculture by collecting and analyzing data from different aspects of farming. These massive amounts of data that are continuously generated in digital agriculture have been considered as a widespread application of big data in the real world. These data have improved farming practices from different aspects, such as crop health monitoring, yield prediction, water management, and demand forecasting. However, utilizing digital tools that are interconnected and remotely accessible raises concerns related to the privacy of available big data. The privacy issues in agriculture reduce the farmers' willingness to engage in data collection activities and affect the progress of smart farming. To address these concerns, privacy assurance mechanisms should be used in different stages of the data lifecycle. In this paper, we provided a scheme of the big data lifecycle, from a privacy perspective, and classified the privacy concerns and requirements in this area. In addition, we reviewed the state-of-the-art existing technologies which impact big data privacy in smart farming. Additionally, we provided a consideration on the legislation that affects farmers' enthusiasm for sharing data and their contribution to smart farming practices. Smart farming has a great potential to improve agriculture globally, and through this review, it has become clear that there are many solutions for addressing privacy concerns that do not limit the adoption of big data and modern technologies in this ecosystem.

Author Contributions: Conceptualization, M.A.-Z. and R.A.D.; methodology, M.A.-Z.; formal analysis, M.A.-Z., E.D. and R.A.D.; in-vestigation, M.A.-Z., E.D., E.D.G.F. and R.A.D.; writing—original draft preparation, M.A.-Z.; writing—review and editing, M.A.-Z., E.D., E.D.G.F. and R.A.D.; supervision, R.A.D. and E.D.G.F.; funding acquisition, R.A.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded grants from the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery and the Ontario Ministry of Agriculture, Food, and Rural Affairs (OMAFRA), awarded to R. Dara.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Coble, K.H.; Mishra, A.K.; Ferrell, S.; Griffin, T. Big data in agriculture: A challenge for the future. *Appl. Econ. Perspect. Policy* **2018**, *40*, 79–96. [CrossRef]
2. Astill, J.; Dara, R.A.; Fraser, E.D.G.; Roberts, B.; Sharif, S. Smart poultry management: Smart sensors, big data, and the internet of things. *Comput. Electron. Agric.* **2020**, *170*, 105291. [CrossRef]
3. Alzubi, J.; Nayyar, A.; Kumar, A. Machine Learning from Theory to Algorithms: An Overview. *J. Phys. Conf. Ser.* **2018**, *1142*, 012012. [CrossRef]
4. Amiri-Zarandi, M.; Fard, M.H.; Yousefinaghani, S.; Kaviani, M.; Dara, R. A Platform Approach to Smart Farm Information Processing. *Agriculture* **2022**, *12*, 838. [CrossRef]
5. Hubbard, R.; Haig, B.D.; Parsa, R.A. The Limited Role of Formal Statistical Inference in Scientific Inference. *Am. Stat.* **2019**, *73*, 91–98. [CrossRef]
6. Jakku, E.; Taylor, B.; Fleming, A.; Mason, C.; Fielke, S.; Sounness, C.; Thorburn, P. 'If they don't tell us what they do with it, why would we trust them?' Trust, transparency and benefit-sharing in Smart Farming. *NJAS Wagen. J. Life Sci.* **2019**, *90*, 100285. [CrossRef]
7. Chen, D.; Zhao, H. Data security and privacy protection issues in cloud computing. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; Volume 1, pp. 647–651.
8. Shin, D.H. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interact. Comput.* **2010**, *22*, 428–438. [CrossRef]

9. Shirey, R. Internet Security Glossary, Version 2 RFC 4949. Available online: https://www.rfc-editor.org/rfc/rfc4949 (accessed on 15 May 2022).
10. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. *IEEE Access* **2020**, *8*, 32031–32053. [CrossRef]
11. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access* **2020**, *8*, 34564–34584. [CrossRef]
12. Barreto, L.; Amaral, A. Smart farming: Cyber security challenges. In Proceedings of the 2018 International Conference on Intelligent Systems (IS), Funchal, Portugal, 25–27 September 2018; pp. 870–876.
13. Arass, M.E.; Souissi, N. Data Lifecycle: From Big Data to SmartData. In Proceedings of the 2018 IEEE 5th International Congress on Information Science and Technology (CiSt), Marrakech, Morocco, 22–24 October 2018; pp. 80–87.
14. Xu, L.; Jiang, C.; Wang, J.; Yuan, J.; Ren, Y. Information security in big data: Privacy and data mining. *IEEE Access* **2014**, *2*, 1149–1176.
15. Abouelmehdi, K.; Beni-Hessane, A.; Khaloufi, H. Big healthcare data: Preserving security and privacy. *J. Big Data* **2018**, *5*, 1. [CrossRef]
16. Srbinovska, M.; Gavrovski, C.; Dimcev, V.; Krkoleva, A.; Borozan, V. Environmental parameters monitoring in precision agriculture using wireless sensor networks. *J. Clean. Prod.* **2015**, *88*, 297–307. [CrossRef]
17. Anidu, A.; Dara, R. A review of data governance challenges in smart farming and potential solutions. In Proceedings of the 2021 IEEE International Symposium on Technology and Society (ISTAS), Waterloo, ON, Canada, 28–31 October 2021; pp. 1–8.
18. Madushanki, R.; Wirasagoda, H.; Halgamuge, M. Adoption of the Internet of Things (IoT) in agriculture and smart farming towards urban greening: A review. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 11–28. [CrossRef]
19. Zamora-Izquierdo, M.A.; Santa, J.; Martínez, J.A.; Martínez, V.; Skarmeta, A.F. Smart farming IoT platform based on edge and cloud computing. *Biosyst. Eng.* **2019**, *177*, 4–17. [CrossRef]
20. Chukkapalli, S.L.L.; Piplai, A.; Mittal, S.; Gupta, M.; Joshi, A. A Smart-Farming Ontology for Attribute Based Access Control. In Proceedings of the 2020 IEEE 6th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing,(HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), Baltimore, MD, USA, 25–27 May 2020; pp. 29–34.
21. Adi, E.; Anwar, A.; Baig, Z.; Zeadally, S. Machine learning and data analytics for the IoT. *Neural Comput. Appl.* **2020**, *32*, 16205–16233. [CrossRef]
22. Steup, R.; Dombrowski, L.; Su, N.M. Feeding the world with data: Visions of data-driven farming. In Proceedings of the 2019 on Designing Interactive Systems Conference, Online, 18 June 2019; pp. 1503–1515.
23. Nandhini, M.; Jenila, S. Time Constrained Data Destruction in Cloud. *Int. J. Innov. Res. Comput. Commun. Eng.* **2014**, *3*, 2228–2231.
24. Guan, Z.; Zhang, Y.; Wu, L.; Wu, J.; Li, J.; Ma, Y.; Hu, J. APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. *J. Netw. Comput. Appl.* **2019**, *125*, 82–92. [CrossRef]
25. Kho, J.; Rogers, A.; Jennings, N.R. Decentralized Control of Adaptive Sampling in Wireless Sensor Networks. *ACM Trans. Sens. Netw.* **2009**, *5*, 1–35. [CrossRef]
26. Quinonero-Candela, J.; Rasmussen, C.E. A Unifying View of Sparse Approximate Gaussian Process Regression. *J. Mach. Learn. Res.* **2005**, *6*, 1939–1959.
27. Masiero, R.; Quer, G.; Munaretto, D.; Rossi, M.; Widmer, J.; Zorzi, M. Data Acquisition through joint Compressive Sensing and Principal Component Analysis. In Proceedings of the GLOBECOM 2009–2009 IEEE Global Telecommunications Conference, Honolulu, HI, USA, 30 November–4 December 2009; pp. 1–6.
28. Wold, S.; Esbensen, K.; Geladi, P. Principal component analysis. *Chemom. Intell. Lab. Syst.* **1987**, *2*, 37–52. [CrossRef]
29. Masiero, R.; Quer, G.; Rossi, M.; Zorzi, M. A Bayesian Analysis of Compressive Sensing Data Recovery in Wireless Sensor Networks. In Proceedings of the 2009 International Conference on Ultra Modern Telecommunications & Workshops, St. Petersburg, Russia, 12–14 October 2009; pp. 1–6.
30. Macua, S.V.; Belanovic, P.; Zazo, S. Consensus-based distributed principal component analysis in wireless sensor networks. In Proceedings of the IEEE 11th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Marrakech, Morocco, 20–23 June 2010; pp. 1–5.
31. Ndzi, D.L.; Harun, A.; Ramli, F.M.; Kamarudin, M.L.; Zakaria, A.; Shakaff, A.Y.M.; Jaafar, M.N.; Zhou, S.; Farook, R.S. Wireless sensor network coverage measurement and planning in mixed crop farming. *Comput. Electron. Agric.* **2014**, *105*, 83–94. [CrossRef]
32. Xie, M.; Huang, M.; Bai, Y.; Hu, Z. The Anonymization Protection Algorithm Based on Fuzzy Clustering for the Ego of Data in the Internet of Things. *J. Electr. Comput. Eng.* **2017**, *2017*, 2970673. [CrossRef]
33. Casino, F.; Domingo-Ferrer, J.; Patsakis, C.; Puig, D.; Solanas, A. A k-anonymous approach to privacy preserving collaborative filtering. *J. Comput. Syst. Sci.* **2015**, *81*, 1000–1011. [CrossRef]
34. Martin, M.K.; Helm, J.; Patyk, K.A. An approach for de-identification of point locations of livestock premises for further use in disease spread modeling. *Prev. Vet. Med.* **2015**, *120*, 131–140. [CrossRef]
35. Anggorojati, B.; Mahalle, P.N.; Prasad, N.R.; Prasad, R. Capability-based Access Control Delegation Model on the Federated IoT Network. In Proceedings of the 15th International Symposium on Wireless Personal Multimedia Communications, Taipei, Taiwan, 24–27 September 2012; pp. 604–608.

36. Anggorojati, B.; Mahalle, P.N.; Prasad, N.R.; Prasad, R.; Theoleyre, F.; Pang, A. Secure access control and authority delegation based on capability and context awareness for federated iot. In *Internet of Things and M2M Communications*; Aalborg University: Aalborg, Denmark, 2013; pp. 135–160.
37. Mahalle, P.N.; Anggorojati, B.; Prasad, N.R.; Prasad, R.R. Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *J. Cyber Secur. Mobil.* **2013**, *1*, 309–348. [CrossRef]
38. Hernández-ramos, J.L.; Jara, A.J.; Marín, L. DCapBAC: Embedding authorization logic into smart things through ECC optimizations. *Int. J. Comput. Math.* **2014**, *93*, 37–41. [CrossRef]
39. Bernabe, J.B.; Ramos, J.L.H.; Gomez, A.F.S. TACIoT: Multidimensional trust-aware access control system for the Internet of Things. *Soft Comput.* **2016**, *20*, 1763–1779. [CrossRef]
40. Zhang, G.; Tian, J. An extended role based access control model for the Internet of Things. In Proceedings of the 2010 International Conference on Information, Networking and Automation (ICINA), Kunming, China, 17–19 October 2010; Volume 1, pp. V1-319–V1-323.
41. Jindou, J.; Xiaofeng, Q.; Cheng, C. Access Control Method for Web of Things based on Role and SNS. In Proceedings of the 2012 IEEE 12th International Conference on Computer and Information Technology, Chengdu, China, 27–29 October 2012; pp. 316–321.
42. Barka, E.; Mathew, S.S.; Atif, Y. *Securing the Web of Things with Role-Based Access Control*; Springer: Cham, Switzerland, 2015; pp. 14–26.
43. Gusmeroli, S.; Piccione, S.; Rotondi, D. A capability-based security approach to manage access control in the Internet of Things. *Math. Comput. Model.* **2013**, *58*, 1189–1205. [CrossRef]
44. Hernández-Ramos, J.L.; Jara, A.J.; Marín, L.; Skarmeta, A.F. Distributed Capability-based Access Control for the Internet of Things. *J. Internet Serv. Inf. Secur.* **2013**, *3*, 1–16.
45. Jiang, L.; Li, T.; Li, X.; Atiquzzaman, M.; Ahmad, H.; Wang, X. Anonymous Communication via Anonymous Identity-Based Encryption and Its Application in IoT. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 6809796. [CrossRef]
46. Wang, X.; Zhang, J.; Schooler, E.M.; Ion, M. Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 10–14 June 2014; pp. 725–730.
47. Belguith, S.; Kaaniche, N.; Laurent, M.; Jemai, A.; Attia, R. PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT. *Comput. Netw.* **2018**, *133*, 141–156. [CrossRef]
48. Davoli, L.; Protskaya, Y.; Veltri, L. An anonymization protocol for the Internet of Things. In Proceedings of the 2017 International Symposium on Wireless Communication Systems (ISWCS), Bologna, Italy, 28–31 August 2017; Volume 2017, pp. 459–464.
49. Liang, K.; Susilo, W.; Liu., J.K. Privacy-preserving ciphertext multi-sharing control for big data storage. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1578–1589. [CrossRef]
50. Li, S.; Li, M.; Xu, H.; Zhou, X. Searchable encryption scheme for personalized privacy in IoT-based big data. *Sensors* **2019**, *19*, 1059. [CrossRef] [PubMed]
51. Li, J.; Zhang, Y.; Ning, J.; Huang, X.; Poh, G.S.; Wang, D. Attribute Based Encryption with Privacy Protection and Accountability for CloudIoT. *IEEE Trans. Cloud Comput.* **2020**, *10*, 762–773. [CrossRef]
52. Anbuchelian, S.; Sowmya, C.M.; Ramesh, C. Efficient and secure auditing scheme for privacy preserving data storage in cloud. *Cluster Comput.* **2019**, *22*, 9767–9775. [CrossRef]
53. Yang, Y.; Zheng, X.; Guo, W.; Liu, X.; Chang, V. Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. *Inf. Sci.* **2019**, *479*, 567–592. [CrossRef]
54. Huning, L.; Bauer, J.; Aschenbruck, N. A Privacy Preserving Mobile Crowdsensing Architecture for a Smart Farming Application. In Proceedings of the First ACM Workshop on Mobile Crowdsensing Systems and Applications, Delft, The Netherlands, 5 November 2017; Volume 2017, pp. 62–67.
55. Dwork, C. *Differential Privacy in Encyclopedia of Cryptography and Security*; Springer: Cham, Switzerland, 2006; pp. 338–340.
56. Udendhran, R.; Balamurugan, M. Towards secure deep learning architecture for smart farming-based applications. *Complex Intell. Syst.* **2020**, *7*, 659–666. [CrossRef]
57. Xu, C.; Ren, J.; Zhang, D.; Zhang, Y. Distilling at the edge: A local differential privacy obfuscation framework for IoT Data Analytics. *IEEE Commun. Mag.* **2018**, *56*, 20–25. [CrossRef]
58. Yan, Q.; Lou, J.; Vuran, M.C.; Irmak, S. Scalable Privacy-preserving Geo-distance Evaluation for Precision Agriculture IoT Systems. *ACM Trans. Sens. Netw.* **2021**, *17*, 1–30. [CrossRef]
59. Niemitalo, O.; Koskinen, E.; Hyväluoma, J.; Lientola, E.; Lindberg, H.; Koskela, O.; Kunttu, I. A year acquiring and publishing drone aerial images in research on agriculture, forestry, and private urban gardens. *Technol. Innov. Manag. Rev.* **2021**, *11*, 5–16. [CrossRef]
60. Zhang, Y.; Pan, J.; Qi, L.; He, Q. Privacy-preserving quality prediction for edge-based IoT services. *Future Gener. Comput. Syst.* **2021**, *114*, 336–348. [CrossRef]
61. Xiong, J.; Ren, J.; Chen, L.; Yao, Z.; Lin, M.; Wu, D.; Niu, B. Enhancing Privacy and Availability for Data Clustering in Intelligent Electrical Service of IoT. *IEEE Internet Things J.* **2018**, *6*, 1530–1540. [CrossRef]
62. Blum, A.; Dwork, C.; McSherry, F.; Nissim, K. Practical Privacy: The SuLQ Framework. In Proceedings of the Twenty-Fourth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, Baltimore, ML, USA, 13–15 June 2005; pp. 128–138.
63. Kyntäjä, J.; Frandsen, J.; Ilomäki, J.; Jafner, N.; Jóhannesson, G.; Mikalsen, V. Nordic Cattle Data eXchange-a shared standard for data transfer. *ICAR Tech. Ser.* **2018**, *23*, 99–100.

64. Barto. Available online: https://www.barto.ch (accessed on 15 May 2022).
65. Join Data. Available online: https://www.join-data.nl (accessed on 15 May 2022).
66. Wahyu, R.; Zuhri, I.; Jatra, A. HARA Token Whitepaper. Available online: https://www.scribd.com/document/392346486/HARA-Token-White-Paper-v20180923 (accessed on 15 May 2022).
67. Reiter, M.K.; Rubin, A.D. Crowds: Anonymity for web transactions. *ACM Trans. Inf. Syst. Secur.* **1998**, *1*, 66–92. [CrossRef]
68. Chen, J.; Tian, Z.; Cui, X.; Yin, L.; Wang, X. Trust architecture and reputation evaluation for internet of things. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 3099–3107. [CrossRef]
69. Kreutz, D.; Ramos, F.M.; Verissimo, P.E.; Rothenberg, C.E.; Azodolmolky, S.; Uhlig, S. Software-Defined Networking: A Comprehensive Survey. *Proc. IEEE* **2014**, *103*, 14–76. [CrossRef]
70. Atzori, L.; Iera, A.; Morabito, G. From "Smart Objects" to "Social Objects": The Next Evolutionary Step of the Internet of Things. *IEEE Commun. Mag.* **2014**, *52*, 97–105. [CrossRef]
71. Nitti, M.; Girau, R.; Atzori, L. Trustworthiness Management in the Social Internet of Things. *IEEE Trans. Knowl. Data Eng.* **2014**, *26*, 1253–1266. [CrossRef]
72. Amiri-Zarandi, M.; Dara, R.A.; Fraser, E. LBTM: A lightweight blockchain-based trust management system for social internet of things. *J. Supercomput.* **2022**, *78*, 8302–8320. [CrossRef]
73. Zhang, F.Z.; Chen, J.; Chen, H.B.; Zang, B. Lifetime privacy and self-destruction of data in the cloud. *J. Comput. Res. Dev.* **2011**, *48*, 1155.
74. Amiri-Zarandi, M.; Dara, R.A.; Fraser, E. A survey of machine learning-based solutions to protect privacy in the Internet of Things. *Comput. Secur.* **2020**, *96*, 101921. [CrossRef]
75. De Souza, P.S.S.; Rubin, F.P.; Hohemberger, R.; Ferreto, T.C.; Lorenzon, A.F.; Luizelli, M.C.; Rossi, F.D. Detecting abnormal sensors via machine learning: An IoT farming WSN-based architecture case study. *Measurement* **2020**, *164*, 108042. [CrossRef]
76. Chukkapalli, S.S.L.; Ranade, P.; Mittal, S.; Joshi, A. A Privacy Preserving Anomaly Detection Framework for Cooperative Smart Farming Ecosystem. In Proceedings of the 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Atlanta, GA, USA, 13–15 December 2021; pp. 340–347.
77. Das, R.; Gadre, A.; Zhang, S.; Kumar, S.; Moura, J.M.F. A Deep Learning Approach to IoT Authentication. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
78. Shi, C.; Liu, J.; Liu, H.; Chen, Y. Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-enabled IoT. In Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Chennai, India, 10–14 July 2017; pp. 1–10.
79. Canedo, J.; Skjellum, A. Using machine learning to secure IoT systems. In Proceedings of the 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016; pp. 219–222.
80. Ni, Q.; Lobo, J. Automating Role-based Provisioning by Learning from Examples. In Proceedings of the 14th ACM Symposium on Access Control Models and Technologies, Online, 3 June 2009; pp. 75–84.
81. Kulkarni, R.V.; Venayagamoorthy, G.K. Neural network based secure media access control protocol for wireless sensor networks. In Proceedings of the 2009 International Joint Conference on Neural Networks, Atlanta, GA, USA, 14–19 June 2009; pp. 1680–1687.
82. Outchakoucht, A.; Hamza, E.S.; Leroy, J.P. Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 7. [CrossRef]
83. Konečný, J.; McMahan, H.B.; Ramage, D.; Richtárik, P. Federated Optimization: Distributed Machine Learning for On-Device Intelligence. *arXiv* **2016**, arXiv:1610.02527.
84. Wang, X.; Han, Y.; Wang, C.; Zhao, Q.; Chen, X.; Chen, M. In-Edge AI: Intelligentizing Mobile Edge Computing, Caching and Communication by Federated Learning. *IEEE Netw.* **2019**, *33*, 156–165. [CrossRef]
85. Wang, S.; Tuor, T.; Salonidis, T.; Leung, K.K.; Makaya, C.; He, T.; Chan, K. Adaptive Federated Learning in Resource Constrained Edge Computing Systems. *IEEE J. Sel. Areas Commun.* **2018**, *37*, 1205–1221. [CrossRef]
86. Guardo, E.; Stefano, A.D.; Corte, A.L.; Sapienza, M.; Scatà, M. A fog computing-based IoT framework for precision agriculture. *J. Internet Technol.* **2018**, *19*, 1401–1411.
87. Hsu, T.C.; Yang, H.; Chung, Y.C.; Hsu, C.H. A Creative IoT agriculture platform for cloud fog computing. *Sustain. Comput. Inform. Syst.* **2018**, *28*, 100285. [CrossRef]
88. Malik, A.W.; Rahman, A.U.; Qayyum, T.; Ravana, S.D. Leveraging Fog Computing for Sustainable Smart Farming Using Distributed Simulation. *IEEE Internet Things J.* **2020**, *7*, 3300–3309. [CrossRef]
89. Rezk, N.G.; Hemdan, E.E.D.; Attia, A.F.; El-Sayed, A.; El-Rashidy, M.A. An efficient IoT based smart farming system using machine learning algorithms. *Multimed. Tools Appl.* **2020**, *80*, 773–797. [CrossRef]
90. Zhang, J.; Li, X.; Zhang, X.; Xue, Y.; Srivastava, G.; Dou, W. Service offloading oriented edge server placement in smart farming. *Softw. Pract. Exp.* **2020**, *51*, 2540–2557. [CrossRef]
91. Caria, M.; Schudrowitz, J.; Jukan, A.; Kemper, N. Smart farm computing systems for animal welfare monitoring. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017; pp. 152–157.
92. Taneja, M.; Byabazaire, J.; Davy, A.; Olariu, C. Fog assisted application support for animal behaviour analysis and health monitoring in dairy farming. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; Volume 2018, pp. 819–824.

93. Taneja, M.; Jalodia, N.; Byabazaire, J.; Davy, A.; Olariu, C. SmartHerd management: A microservices-based fog computing–assisted IoT platform towards data-driven smart dairy farming. *Softw. Pract. Exp.* **2019**, *49*, 1055–1078. [CrossRef] [PubMed]
94. Alonso, R.S.; Sittón-Candanedo, I.; García, Ó.; Prieto, J.; Rodríguez-González, S. An intelligent Edge-IoT platform for monitoring livestock and crops in a dairy farming scenario. *Ad Hoc Netw.* **2020**, *98*, 102047. [CrossRef]
95. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
96. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://www.debr.io/article/21260.pdf (accessed on 15 May 2022).
97. Founder, G.W.; Gavin, E. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Available online: https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper.pdf (accessed on 15 May 2022).
98. Ge, L.; Brewster, C.; Spek, J.; Smeenk, A.; Top, J.; Diepen, F.V.; Klaase, B.; Graumans, C.; Wildt, M.D.R.D. *Blockchain for Agriculture and Food: Findings from the Pilot Study*; Wageningen University & Research: Wageningen, The Netherlands, 2017.
99. Bordel, B.; Martin, D.; Alcarria, R.; Robles, T. A Blockchain-based Water Control System for the Automatic Management of Irrigation Communities. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; pp. 17–18.
100. Bodkhe, U.; Tanwar, S.; Bhattacharya, P.; Kumar, N. Blockchain for precision irrigation: Opportunities and challenges. *Trans. Emerg. Telecommun. Technol.* **2020**, *1*, e4059. [CrossRef]
101. Lin, J.; Zhang, A.; Shen, Z.; Chai, Y. Blockchain and IoT based food traceability for smart agriculture. In Proceedings of the 3rd International Conference on Crowd Science and Engineering, Singapore, 28–31 July 2018; pp. 1–6.
102. Casado-Vara, R.; Prieto, J.; Prieta, F.D.L.; Corchado, J.M. How blockchain improves the supply chain: Case study alimentary supply chain. *Procedia Comput. Sci.* **2018**, *134*, 393–398. [CrossRef]
103. Kamble, S.S.; Gunasekaran, A.; Sharma, R. Modeling the blockchain enabled traceability in agriculture supply chain. *Int. J. Inf. Manag.* **2020**, *52*, 101967. [CrossRef]
104. Geethanjali, B.; Muralidhara, B.L. A Framework for Banana Plantation Growth Using Blockchain Technology. In *ICT Analysis and Applications*; Springer: Cham, Switzerland, 2020; pp. 615–620.
105. Amiri-Zarandi, M.; Dara, R.A. Blockchain-based Trust Management in Social Internet of Things. In Proceedings of the 2020 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 17–22 August 2020; pp. 49–54.
106. Tahar, M.; Hammi, B.; Bellot, P. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Comput. Secur.* **2018**, *78*, 126–142.
107. Wu, H.T.; Tsai, C.W. An intelligent agriculture network security system based on private blockchains. *J. Commun. Netw.* **2019**, *21*, 503–508. [CrossRef]
108. Shahid, A.; Almogren, A.; Javaid, N.; Al-Zahrani, F.A.; Zuair, M.; Alam, M. Blockchain-Based Agri-Food Supply Chain: A Complete Solution. *IEEE Access* **2020**, *8*, 69230–69243. [CrossRef]
109. Salah, K.; Nizamuddin, N.; Jayaraman, R.; Omar, M. Blockchain-Based Soybean Traceability in Agricultural Supply Chain. *IEEE Access* **2019**, *7*, 73295–73305. [CrossRef]
110. Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. In *Europe and MENA Cooperation Advances in Information and Communication Technologies*; Springer: Cham, Switzerland, 2017; pp. 523–533.
111. Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. FairAccess: A new Blockchain-based access control framework for the Internet of Things: FairAccess: A new access control framework for IoT FairAccess: A new Blockchain-based access control framework for the Internet of Things. *Secur. Commun. Netw.* **2016**, *9*, 5943–5964. [CrossRef]
112. Zhang, Y.; Kasahara, S.; Shen, Y.; Jiang, X.; Wan, J. Smart Contract-Based Access Control for the Internet of Things. *IEEE Internet Things J.* **2018**, *6*, 1594–1605. [CrossRef]
113. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet Things J.* **2017**, *5*, 1184–1195. [CrossRef]
114. Wiseman, L.; Sanderson, J.; Zhang, A.; Jakku, E. Farmers and their data: An examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming. *NJAS Wagen. J. Life Sci.* **2019**, *90*, 100301. [CrossRef]
115. Regan, Á. "Smart farming" in Ireland: A risk perception study with key governance actors. *NJAS Wagening. J. Life Sci.* **2019**, *90*, 100292. [CrossRef]
116. Van der Burg, S.; Wiseman, L.; Krkeljas, J. Trust in farm data sharing: Reflections on the EU code of conduct for agricultural data sharing. *Ethics Inf. Technol.* **2021**, *23*, 185–198. [CrossRef]
117. AFBF. Privacy and Security Issues for Farm Data. Available online: https://www.fb.org/issues/technology/dataprivacy/privacyandsecurityprinciplesforfarmdata (accessed on 15 May 2022).
118. Wang, L.; Near, J.P.; Somani, N.; Gao, P.; Low, A.; Dao, D.; Song, D. Data Capsule: A New Paradigm for Automatic Compliance with Data Privacy Regulations. In *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*; Springer: Cham, Switzerland, 2019; Volume 11721, pp. 3–23.