2021 IEEE International Symposium on Technology and Society (ISTAS) | 978-1-6654-3580-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISTAS52410.2021.9629169

A review of data governance challenges in smart farming and potential solutions

Adesola Anidu
School of Computer Science
University of Guelph
Guelph, Ontario
aanidu@uoguelph.ca

Rozita Dara, IEEE Member
School of Computer Science
University of Guelph
Guelph, Ontario
drozita@uoguelph.ca

***Abstract*—The expectation on the agricultural system is constantly growing to be more productive with less labor, less water and less arable land. To achieve this goal, the use of digital technologies is being promoted. This has resulted in growth in use of wireless sensors, IoTs, cloud computing and other technologies in farms which have fueled the explorational of data. Data collected at farms varies from business operation data (farm management data), transport and farm storage data, land data (water, soil, GPS), machine data, agronomic data, livestock data, climate, and weather data. This large amount of data needs to be managed to ensure confidentiality and other governance requirements and enhance technical capacity and performance such as data integration and processing. This paper reviews the data governance challenges generated in smart farms and provides recommendations on how those challenges can be addressed.**

Keywords—digital agriculture, smart farming, data governance, data lifecycle

I. Introduction

Precision agriculture is defined as “farming management concept using digital techniques for monitoring and optimizing agricultural production processes” [2]. Precision agricultural revolution started with the use of GPS-satellite and aerial imagery, the use of variable rate fertilizer application, weather predictions, remote sensors, and subsequently the collection and use of machine data for improving agricultural practices and increasing productivity leading to what is called smart farming. Smart farming is all about the use of different precision tools that generate data from farms and the utilization of data to gain insights and to increase productivity and improve efficiency [2][3]. Precision agriculture technologies are widespread and have been adopted by many farmers. The driving force for the widespread adoption of digital technology in agriculture is the demand for farmers to increase productivity amidst growing population size, become more efficient, environmentally friendly, and safe.

With the growth of smart farming, there has been improvement in labor and mechanization which has made an impact in the way farmers raise crops and take care of livestock. Many livestock barns are equipped with Wi-Fi and automated feeders, and climate control systems [4]; cows are milked using robotic milking machines and can be monitored during labor from the farmer’s smart phone; dairy herds are fitted with sensors for monitoring their health and daily activities. Also, farming variables such as light, humidity, and water can be monitored using these technologies thereby reducing water and energy consumption. Labor is as well reduced with the use of robots for planting, harvesting and logistics. Moreover, farm operations such as record keeping, quality of food production, and supervision of workers can be automated leading to a significant decrease in labor and cost of farm work. The use of these digital technologies generates a lot of data. This data is subsequently turned into meaningful information that can enable farmers to make better and timely management decisions resulting in more efficiency, productivity, and better care for animals and crops.

Despite all the progress being made by using these digital technologies in farming, there are still some challenges hindering this revolution from reaching its full potential. These challenges include issues relating to data governance such as data ownership, data security and privacy, policy, and interoperability in addition to other challenges such as limited technology literacy and technology issues. This paper presents a survey detailing the existing data governance challenges in smart farming and provides recommendations on improving the smart farm data governance landscape.

II. Motivation

The use of technology in farming generates enormous quantities of data. These data, however, are not being utilized to their full potential. Making the best use of the data available through the various farm technologies is possible if existing barriers/challenges are overcome. For instance, a single farm data do not provide sufficient knowledge. Meaningful decisions can be derived only if it is aggregated with other farms’ data sources. It is even more beneficial if farm data is aggregated with the entire food chain. The benefits of data integration include increased productivity, improved profitability, record keeping, informed policy, real-time information, optimization along the supply chain, quality control and assurance, international collaboration and learning amongst others [5]. However, given all the potential advantages of using farm data, numerous challenges are hindering the growth of what is supposed to be the smart farming revolution. Some of these challenges are on how the data are effectively generated, stored, utilized and made available to various parties so that confidentiality requirements are properly addressed.

978-1-6654-3580-2/21/$31.00 ©2021 IEEE

Fig. 1. Data Life Cycle

In this review, we will look at the challenges in th e context of the farm data value chain. There are several different phases in the data value chain and each phase is characterized by some of its own challenges (Figure 1).

- Data discovery and generation – Farm data is generated from several devices on the farm such as wireless sensors, the Internet of Things (IoT) [4] devices, UAV, GPS, and others. The challenges in this phase are the ability to collect data, availability of data, lack of standardization in quality and format of data, data ownership issue, data sharing, data security, and technology interoperability.
- Data collection and transmission – The data generated are stored in on-farm devices, edge technologies, on-farm databases or on the cloud. Ensuring data security and integrity is one of the important requirements of this phase for data-in-motion or data-at-rest.
- Data storage and management – this stage deals with the storage, keeping and using data securely. Challenges here include data security and privacy, issues that relate to data ownership, data use and access. Data access control, identity management, data confidentiality and sharing issues, data integration and interoperability needs are only some of the challenges of this phase. Farm data can be found as raw data, processed data, anonymized data, aggregated data, and derivative data. The diversity of data collected from farms with different devices and formats also imposes many technologies and process complications.
- Data processing – In this phase data integration, cleaning, and elimination of redundancy are carried out. Due to the heterogeneity of data sources, some of the challenges are interoperability and data quality. This phase also includes the development of effective models. Alignment of farm data processing with the stakeholders' needs can be challenging. Also, the need for scalability and reliability of data processing can limit the use and analysis of a large amount of data. Real-time data analysis also requires robust infrastructure which can be a limitation.
- Knowledge usage and maintenance – Knowledge should be used in an ethical and responsible manner. Lack of standards and understanding of responsible use of farm technology is one of the challenges of this phase. Business models, collaboration through data sharing, co-creation of value are other challenges. Finally, the dynamic nature of information technology imposes a lot of difficulty on maintaining and expanding the data platforms and infrastructure.

In addition to the above challenges, the success of data in agriculture is dependent on multiple social and technical factors which include the adoption of technologies by the end users, readiness of the stakeholders in sharing and integrating data, the existence of protocols that protects the farmer's right to privacy [5]. Opportunities exist for data analysis, but the problem of data ownership, access, control, and privacy are concerns that are preventing farmers from fully adopting this technology [6].

In the following sections, data governance challenges and potential solutions are explored in-depth.

III. Smart Farm Data Governance Challenges

A. Data ownership, access, and use

For digital technology to transform the food chain, then the issue of trust amongst parties needs to be resolved. Wiseman *et al.* [7] highlighted some of the farmers' concerns such as data ownership/sharing, lack of a suitable business model to share farm data, lack of transparency in the terms of usage of data license/agreements, privacy concerns and inequality in negotiating power. Schuster [8] also argues that the ownership of data is a cause for concern as farmers/producers believe they are the owner of the data generated in their farms. The author further discusses the rules on controlling farm data and points out that they are inadequate and may result in misuse of data.

The economic value of data increases as they are aggregated This causes policy and regulatory problems connected to aggregate versus individual data ownership and users rights for both farmers and developers of digital applications. As the number of users increases, it becomes complicated to define data ownership and data usage rights [9]. With the vast data being produced, farmers have become more cognizant of the value the data can bring hence the issue of who owns or have access to the agricultural data emerges. This issue may even prevent effective data interoperability.

Agricultural data is being governed by private contracts and technology use agreements. These contracts have different data access and use policies most are non-negotiable having a "leave it or take it" option [10]. A recent survey by [10] reveals that most farmers are unaware of the conditions of data contracts they have agreed to. This is one of the reasons for mistrust in the management of agricultural data. Also, the absence of government legislation and lack of consistency in agricultural data contracts makes stakeholders concerned about how the data is accessed and used. This has limited the potential gains that can be derived from utilizing these agricultural data. Moreover legal, and regulatory frameworks around the world do not accept agricultural data as intellectual property further aggravating the issue of data ownership. To address this, various agricultural codes of practice have been implemented but these are voluntary industry standards not a mandatory policy. According to [10], these agricultural codes of practice can be used to fill regulatory gaps and support government regulations thereby facilitating the use of data and thus protecting the security and privacy of farmers and producers.

Based on the review conducted by [10] on agricultural codes of practice particularly the New Zealand's Farm Data Code of Practice and the American Farm Bureau's Privacy and Security Principles for Farm Data, it was noted that these codes of practice do not have an agile agricultural data normative framework and implementation and evaluation methods.

B. Data privacy

The fear of data falling into the wrong hands particularly producer's competitors is paramount in the heart of producers' concerns. Presently, no federal law is protecting agricultural data similar to health (HIPAA) and financial data. Moreover, the privacy policies available deal with personal information and not agricultural data. This is a threat to the growth of digital agriculture. Data privacy and sharing problems need to be resolved because data systems depend on farmers/producers trusting data aggregators on the use and sharing of their data which is often difficult for producers [11]. Farmers are concerned about how information relating to their farming activities is used by competitor farms [12].

C. Lack of regulatory laws

The lack of legal and regulatory laws focusing on how agricultural data is collected, shared, and used contributes to the problems being encountered by farmers in adopting digital technologies. Laws relating to agricultural data are not consistent. Wiseman et al. [7] stated that lack of clarity and transparency on issues centered around data ownership, trust, privacy, liability, and portability in the business relationship governing smart agriculture is a contributing factor to the reluctance among farmers in sharing their data. A legal framework needs to be put in place.

D. Security

Security concerns data, IoT, cloud and network. Most of the cyber threats being faced in the agricultural industry are similar to the threat vectors in other connected sectors. The same tactics used in other industries are being utilized here such as improper use of USB thumb drives, spear-phishing, and other cyber-attacks which can lead to reputation loss, data theft, destruction of equipment and other issues. Also, the generally accepted mitigation techniques can be used in preventing such attacks. In information security, the three main threats are to confidentiality, integrity, and availability [13].

Confidentiality is the security principle designed to ensure that data and information are not accessed by unauthorized users. Threats to confidentiality could be a deliberate theft of data generated or accidental leakage of data to third parties which could be a result of not implementing patching and appropriate security controls. This could also occur if user agreements, privacy controls are not well structured. It can also be through remote access to unmanned aerial system (UAS) data and unethical sale of confidential data which could be possible through insider threat.

Integrity is the security principle that assures the accuracy and completeness of data throughout its lifecycle. It guards against data modification in an unauthorized manner. As digital agriculture is being embraced using robotics, IoT, machine learning, there are threats to data integrity which includes intentional falsification of data that can come from adversarial attacks corrupting the machine learning model or the data itself leading to incorrect categorization /prediction. Also, introducing rogue data into a sensor network corrupts the data leading to falsification of results and insufficiently vetted machine learning model.

Availability in security ensures that information is readily available and accessible to authorized users. Threats to availability include disruption to positioning, navigation and timing (PNT)systems either space-based or ground-based and disruption to communication networks through DDoS.

E. Security and Privacy of Connected Devices

The use of IoT is the driving force for smart farming. The Internet of Thing devices are prone to cyber-attacks as most of these devices are not made with security in mind. These devices can be attacked remotely creating an unproductive and unsafe farming environment. Attacks on IoT devices can be against integrity, privacy, confidentiality, authentication, and availability [14]. Attacks against privacy could be a result of an attacker trying to access the private data and subsequently compromise the privacy of the system. Attacks against authentication is a type of attack that creates identities to imitate authorized nodes such as IoT devices. These attacks can be in the form of replay attack, impersonation attack, spoofing attack, and masquerade attack. Attacks against confidentiality are attacks that attempt to spy on the network traffic between IoT devices compromising confidentiality subsequently leading to wrong decisions. Examples of such attacks include brute force attacks, known key attacks and tracing attacks. Attacks against availability can be in form of Distributed Denial of Service (DDoS) thereby making the required service unavailable. Attacks against integrity can be in the form of a biometric template attack, forgery attack, trojan horse attack, and man-in-the-middle (MITM) attack. Cyber- attacks on farms can lead to devasting effects capable of disrupting the economy of a nation that is solely dependent on agriculture.

F. Interoperability

Data interoperability is the ability of exchanging data between systems and devices without interference as per established processes and protocols. There are different standards that enables how the different data generated by devices can be seamlessly integrated. There are four dimensions to interoperability namely

- Legal—this ensures that organizations/agricultural sectors operating under different laws, policies and legal frameworks can exchange data.
- Semantic—this category is related to the interpretation of data and information and how they are exchanged, understood and preserved. It needs both structured data which is commonly understood and codification of the data to be exchanged. It is divided into two aspects: syntactic and semantic. Semantic is the interpretation of data elements and the connection between them. Syntactic deals with describing the format of information to be interchanged with respect to format and grammar
- Organizational—this category is concerned with how business processes, expectations and responsibilities are aligned towards common goals and objectives making services accessible and user-focused. To tackle the issue of organizational interoperability, it is necessary to document business processes using a commonly accepted modelling technique [15].
- Technical—Technical integration of systems and services such as data, secure communication protocol, and the process is critical [16].

There is also the need for interoperability that enables communication, exchange and use of data from various software applications and information technology systems. Past research highlighted four main problems of using open data through interoperability framework which are granularity of data, mismatch entity naming and data unit, heterogeneities of the schema, and inconsistency of data [17].

IV. Recommendations

To solve some of the challenges listed above, diverse technology, process, and policy solutions are required to address them holistically. This section provides some recommendations on how data governance requirements can be satisfied (Table I).

A. Standards

The use of standardized language helps address interoperability problems. There are several proposed standardized languages such as agroXML [18] which is an XML dialect that describes the farm production processes and the real-world objects needed in conducting them. Other existing data exchange standards include Crop Ontology, Semantic Sensor Network (SSN) [19], Open Geospatial Consortium (OGC) [20]. Also, the use of ontological models for IoT includes Fiesta-IoT ontology which includes openIoT, IoT-O, IoT-Lite, and Sensei [21]. Smart Appliances Reference (SAREF) ontology enables interoperability between solutions from different providers. It provides semantic interoperability needed to share the information carried by the data. SAREF4AGRI addresses smart agriculture and food chain [22]. An ontology-based approach is also proposed by [23] to describe and extract the semantics of agriculture objects for the purpose of reusing and sharing of agriculture knowledge.

In addition, the development of agricultural industry standards for both technical ISO standards for data and equipment, privacy or use standards for agricultural data generated, transparency standards on how information is generated, used, and shared should be encouraged. AgGateway, a non -profit organization has ADAPT framework, which is an open source software kit based on a global data model through which translation between various proprietary data formats is enabled. This makes data exchange easier leading to improved decision making [24]. Other non-profit organizations developing standards to leverage data are Ag Data Coalition and Open Ag Data Alliance.

Henriyadi [17] highlighted four main problems of using open data through interoperability framework which are granularity of data, mismatch entity naming and data unit, heterogeneities of the schema, and inconsistency of data. The authors have suggested the use of ontology matching to overcome schema heterogeneity; granularity alignment to overcome the problem of granularity of data; ontology mapping for overcoming mismatch entity naming and data unit; and for the problem of inconsistency of data, the use of ontology selection algorithm for the selection of the best external data source from more than two external sources within data problems.

B. Platforms

Open data platforms have been advocated by [9] to combat the challenges of data ownership, access, and use. Open Data is a methodology that involves enhanced data availability in an accessible form for both machines and humans, allowing everyone with a license to access, use and share [25] [26]. An open data and API platform called API-AGRO [26] is proposed to enhance interoperability standards for farm operations. Application Programming Interface (API) is a software intermediary that permits the interaction of two applications with each other. API-AGRO platform enables access to data in private or open mode and a set of Private or Open-APIs. This encourages data sharing and can encourage innovation and promotion of the development of web applications for digital agriculture. Another example is GODAN that supports open data in agriculture and nutrition for research. These resources are available to small non-industrial farmers which enables them to have a degree of autonomy over their data [27]. Open data also comes with its own challenges such as standards. According to [9], there should be transparency in data collection i.e. individuals should have knowledge about how their data is being collected and used. Also, the data sharing model must be worked out for both the data suppliers (farmers) and data users (companies).

An open and interoperable platform known as FOODIE is proposed by [28] for the management of farm data. FOODIE provides a secured platform where stakeholders can publish their datasets thus, making it available as open linked data which can be used for making an informed decision. Also, FIWARE is an open source development environment having reusable components (Generic Enablers Repository) that provides easy integration with other tools and platforms [29]. To solve the problem of lack of connectivity, the creation of a hybrid platform of edge, fog, and cloud computing to enable smart farming applications in areas where the quality of service of wireless networks is bad or not available is proposed by [30]. In addition, interaction with agricultural information systems through open farm information system data exchange platform was proposed by [31] to promote data sharing.

Also, having a connected platform could be a step in the right direction as most of the platforms presently being used in digital agriculture are standalone. They are fragmented and the exchange of information cannot be made with other platforms. Having a connected platform by using a distributed ledger technology such as a blockchain can solve this problem.

C. Security and privacy

Data privacy can be addressed by the use of differential privacy for data, confidential computing, and multi-party computation. Also, open data principles and FAIR data principles (Findable, Accessible, Interoperable and Reusable), interoperability and metadata standards, new models for collective governance for agriculture and data, digital property rights and data access rights. Also, using de-identified open data access, where datasets are accessible through a platform (e.g. GODAN initiative), can be considered for the protection of data privacy. Also, remote analysis systems where analysts submit statistical queries through the interface, analysis are carried out in a secured environment and the user receives the results of analysis [32].

European Union agri-food chain which instituted the EU code of conduct on ag-data sharing is designed for data privacy. In many recommendations, end-to-end security is achieved using GSMA IoT Security guidelines. Best practices for securing the design, development, and deployment of IoT services are being promoted by these guidelines. In addition, the technical standards and specifications which address the need for a common machine-to-machine communication or M2M service layer in IoT are developed by oneM2M [33].

The adoption of some of the baseline security controls in other sectors for solving security and privacy problems is encouraged. Some of these controls are implementing web browser and email protection, limiting and controlling network ports, services, and protocols, inventory and control of software and hardware assets, data protection, account monitoring and control, secure configurations for software and hardware on laptops, servers, mobile devices, and workstations.

Other solutions include incident response, management and implementation of physical controls. Authentication of IoT devices can be performed by using secure lightweight multi-factor authentication protocols. Also, quantum-based cryptography is being investigated for secure end-to-end communication in IoT devices [34][35]. Privacy-preserving protocol which uses message authentication codes (MAC) is proposed by [35] to protect authentication and integrity of IoT applications. Lightweight integrity verification architecture has been proposed by [36] to ensure secure content access which can provide integrity verification.

To ensure privacy in digital agriculture, we must ensure privacy by design practices which encompasses principles such as privacy embedded into design, privacy protection throughout the lifecycle of data, visibility and transparency, and proactive privacy protection. This should be ensured particularly when data is collected by UAV which collects location data amongst others in order to protect the privacy of farmers [2]. Privacy of communication channels and metadata should also be ensured. Obfuscation – data sanitized through suppression randomization or generalization to reduce privacy concerns. Location cloaking can also be done to address location privacy [37]. Privacy-preserving data aggregation and trust evaluation can be adapted to prevent false injection of data. Blockchains can be used to enhance privacy and security in IoT [38][14]. Blockchain can also be used for encrypted data sharing.

D. Policies

There should be laws guiding the collection and use of agricultural data. Presently, there are agricultural codes of practice for the use of agricultural data. In [10], it is recommended that these codes of practice need credible administration, monitoring, and accreditation to solve the problem of data ownership, access, and use. Furthermore, laws and best practices should be developed for legal, social, technical and other aspects of safeguarding privacy in AI ecosystems [1].

Also, the creation of an agricultural data governance framework which will provide clarity on the different roles and responsibilities relating to agricultural data, minimize the risks associated with collecting, storing and use of data and also increase the value of agricultural data should be given a high priority. In order to implement an agricultural data governance framework, dynamic data standards and licensing arrangements should be established [39].

E. Data analytics

To gain meaningful insights from the aggregated data, there is a need to apply powerful data analytics, predictive algorithms and machine learning to gain valuable insights from the data. Open source data analytic tools and platforms for farmers have been designed to enable farmers have control over their data and analyze their data. ISOBlue, is an open source project of Purdue University that helps farmers with capturing and storing their data independently. FarmLogs is an organization that sells data analytic software. This software enables the farmer to manage their data and analyze it. The OpenAg Data helps farmers access and control their data [40]. Collaboration between subject matter experts, data scientists, and decision makers to build more powerful analytic tools and platforms is recommended.

Table I: Summary of proposed solutions/recommendations from literatures

Problem	Proposed solutions/recommendations from literatures
Data Privacy	- Implementation of data privacy laws such as EU GDPR, regulations such as the EU code of conduct on agricultural data sharing, GSMA IoT Security guidelines to provide end-to-end security [31]. - Anonymization techniques, differential privacy, hashing, and encryption [43] - Use of remote analysis system [32]
Data security	- Authentication of IoT devices using secure lightweight multi- factor authentication protocols. Also, quantum-based cryptography for secure end to end communication for IoT devices[33] [35] - Use of baseline security controls
Data ownership, access, and use	- Federal regulation of data practices of organizations involved inthe collection of agricultural data [44] - Development of open platforms [9] - Creation of an agricultural data governance framework [40] - Credible administration, accreditation, and monitoring of codes of practice [10] - Implementation of agricultural codes of practices and agriculturaldata core principles such as - Reviewing of data licenses before entering contractualagreement [10] - Use of open source data analytic tools for farmers such asOpenAg data [41] - Encouragement of open access of data such as GODAN
Lack of regulatory laws	- Creation of legal, social, technical, and other areas that safeguardprivacy as AI systems [1]
Interoperability	IoT interoperability - Agri-IoT semantic framework for IoT based farm applications [45] - Use of metadata based on Sensor Model Language (SensorML) [29] Legal - Existing legislation must be checked to identify interoperability barriers such as geographical/sectoral restrictions in the storage and use of data, outdated security and data protection needs - Legal interoperability through RDA-CODATA principles [46] Semantic - Use data driven design coupled with linked technology [16] - Use of standardized language such as agroXML [18] - Use of ontological models for IoT include Fiesta-IoT ontologywhich include openIoT, IoT-O, IoT-Lite, Sensei etc, [21] - Use of shared data models [21] - Use of Linked Data which is based on data and its links to other data. An example is the AGROVOC from Food Agriculture Organization (FAO) [47] - Implementation of ontology-based services such as AgroPortal [48] Organizational - Document business processes using a commonly acceptedmodelling technique [16] Technical The use of formal technical specifications, (open specifications)[16]

F. Identity management

Identity management is the process which is employed to identify, authenticate, and authorize a person, an item, or a product to have access to data or information by associating the rights and restrictions with established identities [41]. Identity management is expanding from just identifying and authenticating people to identifying devices, monitors, and sensors, and managing their access to different types of data for instance agriculture products. This helps to prevent malicious activities and data breaches thereby safeguarding the security and privacy of IoT devices and data.

G. Processes and procedures

To solve the problem of interoperability in information systems, shared data models can be employed [21]. Data models such as OGC (Open Geospatial Consortium), Observations and Measurements (O&M), Open Connectivity Foundation and World Wide Web Consortium Thing Description.

Also, to solve the issue of data sharing and fair use technology, use agreements should be adopted and clear terms in privacy contracts should be included so that farmers clearly understand what policies they are committing to. There should also be an option to opt-in or opt-out at any time.

H. User centered design

User centered design is an optimistic approach to inventing new solutions tailored to individual needs. However, in digital agriculture, most system designs do not meet the end users need. User centered design is encouraged for system design and development in smart farming technologies. User centered design is focused on understanding the needs of the user and designing a solution based on their perspective. Famers have several challenges and if the farmer’s perspective is taken into consideration, innovative digital tools and solutions that satisfy the need of the farmer can be developed. This will encourage the adoption of digital tools and technologies.

V. Conclusion

The use of smart farming technologies has recently gained a lot of momentum. These technologies generate a large amount of data from diverse and fragmented sources, in different formats, and under different legal agreements. To take advantages of these data, standardized and consolidated approaches are required to integrate, process, exchange, and analyze such data. This study reviews the smart farming data governance shortcomings and provides recommendations on addressing those challenges.

References

[1] G. Hatim, P. Lara, R. Jennifer, S. C. Tran, C. Huiping, M. Satyajayant, L. Boucheron, T. Razzaghi, S. Sandoval, D. Daniel, C. Mora and A. Faruk, "Artificial Intelligence Applications in Agriculture," Climate Adaptive Smart Systems for Future Agricultural and Rangeland Production, 2019.

[2] M. Kritikos, "Precision agriculture in Europe: Legal, social and ethical considerations," European Union, Brussels, 2017.

[3] K. Karandeep, "The Agriculture Internet of Things: A review of the concepts and implications of implementation," International Journal of Recent Trends in Engineering & Research, vol. 2, no. 4, 2016.

[4] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow and M. N. Hindia, "An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges," IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3758-3773, 2018.

[5] E. Jakku, B. Taylor, A. Fleming, C. Mason, S. Fielke, C. Sounness and P. Thorburn, ""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 -Wageningen Journal of Life Sciences, Vols. 90-91, 2019.

[6] S. Himesh, E. P. Rao, K. Gouda, K. Ramesh, V. Rakesh, G. Mohapatra, B.K. Rao, S. Sahoo and P. Ajilesh, "Digital revolution and Big Data: a new revolution in agriculture," CAB Reviews, vol. 13, no. 021, 2018.

[7] L. Wiseman, J. Sanderson, A. Zhang and E. Jakku, "Farmers and their data: An examination of farmer's reluctance to share their data through the lens of the laws impacting smart farming," NJAS - Wageningen Journal of Life Sciences, Vols. 90-91, 2019.

[8] J. Schuster, "Big Data Ethics and the Digital Age of Agriculture," Resource Magazine, vol. 24, no. 1, pp. 20-21, 2017.

[9] World Bank Group, "Future of Food: Harnessing Digital Technologies to Improve Food System Outcomes," World Bank Group, Washington , 2019.

[10] J. Sanderson, L. Wiseman and S. Poncini, "What’s behind the ag-data logo? An examination of vcoluntary agricultural data codes of practice," International Journal of Rural Law and Policy, no. 1, 2018.

[11] K. H. Coble, A. K. Mishra, S. Ferrell and T. Griffin, "Big Data in Agriculture: A Challenge for the Future," Applied Economic Perspectives and Policy, vol. 40, no. 1, pp. 79-96, 2018.

[12] M. Carolan, "Agro-Digital Governance and Life Itself: Food Politics at the Intersection of Code and Affect," Sociologia Ruralis, vol. 57, no. S1, pp. 816-835, 2016.

[13] Public-Private Analytic Exchange Program, "Threats to Precision Agriculture," 2018.

[14] M. A. Ferrag, L. Shu, X. Yang, A. Derhab and L. Maglaras, "Security and Privacy for Green IoT- Based Agriculture: Review, Blockchain Solutions, and Challenges," IEEE Access, vol. 8, no. 2020, pp. 32031-32053, 2020.

[15] S. Talari, M. Shafie-Khah, P. Siano, V. Loia, A. Tommasetti and J. Catalão, "A Review of Smart Cities Based on the Internet of Things Concept," Energies, vol. 10, no. 4, pp. 421-444, 2017.

[16] "NIFO - National Interoperability Framework Observatory," [Online]. Available: joinup.ec.europa.eu/collection/nifo-national-interoperability-framework- observatory/3-interoperability-layers. [Accessed 8 July 2021].

[17] Henriyadi, "The model of data interoperability in farm management information system," in Doctoral Consortium at International Semantic Web Conference (ISWC 2019), Auckland, 2019.

[18] D. Martini, "Semantic Interoperability in Agriculture," Semantic Interoperability Centre Europe.

[19] W3C, "Semantic Sensor Network Ontology," 19 October 2017. [Online]. Available: www.w3.org/TR/vocab-ssn/. [Accessed 10 July 2021].

[20] OGC, "OGC Standards and Resources," [Online]. Available: www.ogc.org/standards. [Accessed 10 July 2021].

[21] J. A. López-Morales, J. A. Martínez and A. F. Skarmeta, "Digital Transformation of Agriculture through the Use of an Interoperable Platform," Sensors, vol. 20, no. 4, 2020.

[22] ETSI, "SAREF4AGRI: an extension of SAREF for the agriculture and food domain," 30 April 2019. [Online]. Available: saref.etsi.org/saref4agri/v1.1.2/. [Accessed 10 July 2021].

[23] S. Hu, H. Wang, C. She and J. Wang, "AgOnt: Ontology for Agriculture Internet of Things," in Computer and Computing Technologies in Agriculture IV. CCTA 2010. IFIP Advances in Information and Communication Technology, Volume 344, Berlin, Heidelberg, Springer, 2011, pp. 131-137.

[23] IOF, "Seamless interoperability between farm machines and software is a step closer," 1 March 2018. [Online]. Available: www.iof2020.eu/latest/press/2018/03/seamless- interoperability-between-farm-machines-and-software. [Accessed 11 July 2021].

[24] Sunlight Foundation, "Ten Principles for Opening Up Government Information," 2010. [Online]. Available: sunlightfoundation.com/policy/documents/ten-open-data- principles/. [Accessed 19 July 2021].

[25] M. Sine, H. Theo-Paul and E. Emeric, "API - AGRO: An Open Data and Open API platform to promote interoperability standards for Farm Services and Ag Web Applications," Journal of Agricultural Informatics., vol. 6, no. 4, pp. 56-64, 2015.

[26] "GODAN," GODAN, [Online]. Available: www.godan.info/pages/godan-open-data- challenge. [Accessed 19 July 2021].

[27] K. Charvat, M. A. Esbri, W. Mayer, K. C. Jr, A. Campos, R. Palma and Z. Krivanek, "FOODIE – Open Data for Agriculture," in 2014 IST-Africa , Le Meridien, 2014.

[28] FIWARE, [Online]. Available: www.fiware.org/about-us/. Accessed 26 July 2021.

[29] H. Gao, H. Shi, K. Ho, D. J. Z. Peng, J. Connier, F. Pinet, H. Zhou, X. Diao, C. d. Vaulx and e. al, "Interoperability and sensor integration for smart farming," in New and smart information communication science and technology to support sustainable development: France-China workshop, Shiyan, 2018.

[30] J. Y. Kim, C. G. Lee, S. H. Baek and J.-Y. Rhee, "Open farm information system data-exchange platform for intercation with agricultural information systems," Agricultural Engineering International: CGIR Journal, vol. 17, no. 2, pp. 296-309, 2015.

[31] Internet of Food & Farm , "IOF2020 Reference architecture for interoperability, replicability and reuse".

[32] G. DeBoe and M.-A. Jouanjean, "Digital Opportunities for Better Agriculral Policies: Insights from Agri-environmental Policies," Organisation for Economic Co-operation and Development, 2019.

[33] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali and S. Sarkar, "Quantum cryptography for IoT: APerspective," in 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, 2017.

[34] T. Song, R. Li, B. Mei, J. Yu, X. Xing and X. Cheng, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," IEEE Internet o f Things Journal, vol. 4, no. 6, pp. 1844-1852, 2017.

[35] M. Gupta, M. Abdelsalam, S. Khorsandroo and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," IEEE Access, vol. 8, no. 2020, pp. 34564-34584, 2020.

[36] Q. Li, X. Zhang, Q. Zheng, R. Sandhu and X. Fu, "LIVE: Lightweight Integrity Verification and Content Access Control for Named Data Networking," IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 308-320, 2015.

[37] D. Eckhoff and I. Wagner, "Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions," IEEE Communications surveys and tutorials, vol. 20, no. 1, pp. 489-516, 2018.

[38] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang and X. Shen, "CPAL: A Conditional Privacy-Preserving Authentication With Access Linkability for Roaming Service," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 46-57, 2014.

[39] A. Dorri, S. S. Kanhere and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," 2016.

[40] L. Wiseman and J. Sanderson, "Accelerating Precision Agriculture to Decision Agriculture : enabling digital agriculture in Australia," Griffith University; USC Australia, Australia, 2017.

[41] I. M. Carbonell, "The ethics of big data in big agriculture," Internet policy review, vol. 5, no. 1, 2016.

[42] Wikipedia, "Identity management," [Online]. Available: en.wikipedia.org/wiki/Identity_management. [Accessed 26 July 2021].

[43] J. Curzon, A. Almehmadi and K. El-Khatib, "A survey of privacy enhancing technologies for smart cities," Pervasive and Mobile Computing, vol. 55, pp. 76-95, 2019.

[44] J. L. Ferris, "Data Privacy and Protection in the Agriculture Industry: Is Federal Regulation Necessary," Minnesota Journal of Law, Science and Technology, vol. 18, no. 1, pp. 309-342, 2017.

[45] A. Kamilaris, F. Gao, F. X. Prenafeta-Boldu and M. I. Ali, "Agri-IoT: A semantic framework for Internet of Things-enabled smart farming applications," in IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016.

[46] RDA-CODATA Legal Interoperability Interest Group, "Legal Interoperability of Research Data: Principles and Implementation Guidelines," Research Data Alliance, 2016.

[47] K. J. Caracciolo Caterina, "A Framework for Knowledge sharing and Interoperability in Agricultural Research for Development," FAO, 2011.

[48] J. Clement, D.-Y. Esther, A. Elizabeth and L. Pierre, "AgroPortal : a proposition for ontology- based services in the agronomic domain," in IN-OVIVE, Rennes, 2015.