Integrating Cybersecurity, Data Sovereignty and Trustworthiness in Agri-data Sharing Environments: A Conceptual Framework

Nasibeh Rahbar Nodehi
School of Business
Maynooth University
Maynooth, Ireland
nasibeh.rahbarnodehi.2024@mumail.ie

Fjolla Berisha
Computer Science
Maynooth University
Maynooth, Ireland
fjolla.berisha.2024@mumail.ie

Leidiane Da Silva
School of Business
Maynooth University
Maynooth, Ireland
leidiane.goretedasilva.2021@mumail.ie

Dr. Zohreh Pourzolfaghar
School of Business
Maynooth University
Maynooth, Ireland
· Zohreh.Pourzolfaghar@mu.ie

Prof. Dr. Markus Helfert
School of Business
Maynooth University
Maynooth, Ireland
Markus.Helfert@mu.ie

2024 Cyber Research Conference - Ireland (Cyber-RCI) | 979-8-3503-9010-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/Cyber-RCI60769.2024.10939388

***Abstract*—The increasing use of data-driven technologies in the agriculture industry introduced new opportunities for improving quality, efficiency, and sustainability in the agriculture sector. However, it has also brought major challenges to its agricultural data (agri-data) users, concerning trustworthiness, data sovereignty, and cybersecurity. This paper presents a conceptual framework that integrates these three pillars into a single approach to evaluate the reliability of agri-data sharing environments. The proposed framework offers guidelines for policymakers and agricultural businesses (agri-businesses) to deal with the complex digital agricultural landscape. It enables secure, sovereign, and trustworthy data-sharing environments for all agri-data stakeholders, especially farmers. This paper also highlights a practical application through a real-world case study and recommends directions for future research.**

Keywords—Cybersecurity, Data Sovereignty, Trustworthiness, Agriculture 4.0, Data-sharing Environment, Agri-data, agri-businesses, Data Governance.

I. Introduction

The agricultural sector is undergoing a profound transformation, driven by advancements in digital technologies, big data, and the Internet of Things (IoT). These innovations promise to revolutionize farming by optimizing productivity, improving resource management, and enhancing sustainability [1,2]. However, with the increasing reliance on data for precision agriculture and decision-making processes, a new set of challenges has emerged namely, the governance of agri-data. As agricultural systems become increasingly connected and data-driven, ensuring that data is handled in a secure, transparent, and ethical manner has become a pressing concern for all stakeholders involved [3,4,5].

Agri-Data Governance involves managing, sharing, and protecting data generated from various sources, including sensors, drones, satellites, farm management systems, and other digital tools. This data includes sensitive information about farm operations, crop yields, soil conditions, and environmental factors, all of which are critical to optimising farm productivity. The governance of this data must address several key issues: who owns the data, who has the right to access it, how it is shared, and how it is protected from unauthorised access or misuse. These questions are further complicated by the global nature of agricultural supply chains, where data is often shared across borders, raising concerns about data sovereignty and compliance with international regulations.

One of the core issues in agri-Data Governance is trust [4,6]. For farmers and other stakeholders to be willing to participate in data-sharing environments, they must trust that their data will be used properly [6]. Therefore, data-sharing initiatives that are not trustworthy, may fail to achieve their full potential, limiting the benefits that can be derived from data-driven insights.

Another key concern is data sovereignty, which refers to the rights and control that data owners have over their data. As agri-data becomes increasingly valuable [7], farmers and agri-businesses seek to maintain control over how their data is used and shared [8]. The issue of data sovereignty is particularly important in the context of cloud computing and cross-border data flows, where data may be stored and processed in jurisdictions with different legal frameworks [9]. Ensuring that data owners retain control over their data, even when it is stored or processed by third-party providers, is a critical aspect of any Data Governance framework [10].

Finally, cybersecurity has become a fundamental component of Data Governance, particularly as agricultural systems become more reliant on IoT devices, remote sensors, and cloud platforms [11]. The interconnected nature of these

The Authors are the parts of EnTrust Doctoral Network project funded by the EU's Horizon 2021 research and innovation programme under the MSCA grant agreement No 101073381.

979-8-3503-0952-2/23/$31.00 ©2023 IEEE

systems exposes them to a wide range of cyber threats, including data breaches, ransomware attacks, and system disruptions [12]. Ensuring that agri-data is protected from these cyber-risks requires robust cybersecurity measures that can safeguard the confidentiality, integrity, and availability of data in increasingly complex and distributed systems [13].

This paper proposes a comprehensive framework for agri-Data Governance, integrating three essential components: Trustworthiness, Data Sovereignty, and Cybersecurity. By addressing these components, the framework aims to provide a structured approach to internal and external governance in agri-data sharing environments. The framework emphasizes the importance of transparency, privacy, and control in fostering trust among stakeholders, while also incorporating strong cybersecurity measures to protect data from external threats. In addition, the framework aligns with international regulatory frameworks to ensure that agri-data is managed in compliance with existing laws and best practices.

II. Literature review

The EU's latest agricultural policies, such as the Data Governance Act, aim to clarify Data Governance to boost trust in data middlemen and enhance data-sharing across the EU. However, the discussion mainly focuses on personal and non-personal data without considering how data status can change due to its use, context, and interactions with stakeholders [14]. In addition, different frameworks within and across countries, regions, sectors, and organisations have resulted in a patchwork of policies, frameworks, and practices, leading to a fragmented ecology that poses certain challenges related to trustworthiness, data sovereignty, and cybersecurity to the evolution of a common framework [15].

Trustworthiness is a key component for having an effective data-sharing environment. Its absence within the agricultural landscape leads to stakeholders' unwillingness to take part in data-sharing environments [5,6,10]. They are concerned that their data will not be used ethically and transparently, as well as in their best interests [6,7,16]. In practice, these stakeholders are unaware of the fate of their data after it is shared [4,5]. To change this situation, several studies emphasize the importance of transparency, privacy and security of data within data-sharing. Transparency can be achieved by making data processes clear and understandable to stakeholders [5,14,17,18]. A transparent system ensures that data owners and users can see how their data is being collected, processed, and used [14,16].

Privacy also plays a critical role [16] towards trustworthiness, as agri-data often includes sensitive information about farm operations, financial performance, and personal data related to farm owners and workers. Considering the sensitive information, stakeholders need assurance that their data are secured from unauthorized access and breaches. Besides transparency, privacy and security; usability is an equally important aspect of trustworthiness; which is often overlooked. Data-sharing environments must be user-friendly and accessible to all stakeholders to support sharing and traceability of data [16].

Data sovereignty refers to the right of data owners to control how and where their data is stored, processed, and shared. In agriculture 4.0, the concept of data sovereignty is of particular importance, as farmers are increasingly generating vast amounts of data from IoT devices, sensors, drones, and farm management systems. However, control over this data can be easily transferred to third parties, such as technology providers, without clear guidelines or mechanisms for oversight, raising concerns among farmers about potential exploitation or misuse of their data. Bronson and Knezevic (2016) highlight that data sovereignty in agriculture is becoming a pressing issue as agri-businesses and large corporations increasingly gain access to sensitive farm data. Farmers, who are often the primary generators of agri-data [19], may lose control over their own data through complex contracts or cloud storage agreements, leading to power imbalances. The authors argue that ensuring data sovereignty in agriculture requires clear legal frameworks and technological mechanisms that allow farmers to maintain ownership and control over the data they generate. Zhang et al. (2020) further explore the challenges of data ownership and sharing in agriculture, noting that many farmers are reluctant to share their data due to fears of losing control [14]. This hesitance is particularly prevalent in regions where Data Governance laws are underdeveloped or where cross-border data transfers are common. The authors propose that robust data sovereignty policies must be established, especially in cloud computing environments, to ensure that agri-data is stored in jurisdictions with strong legal protections.

Cybersecurity is highlighted when the concept of data-sharing is brought out in the data-exchanged environment. Agriculture 4.0 is an environment that integrates various technologies, such as IoT devices, smart vehicles, drones, edge cloud, and wireless communication [20] to perform specific agricultural tasks across an ecosystem. These sophisticated systems are often outsourced to diverse service providers to process data for various environments and applications, which increases the probability of cyber-attacks [21]. In addition, IoT devices utilized for collecting data in Agriculture 4.0 are vulnerable to various security and privacy breaches, and the data they transmit may not be trustworthy for subsequent analysis [22].

Despite much research on each of the existing technologies' security in the agricultural sector, in most of research, the environmental conditions in which they are used have been neglected [20]. Some cyberattacks are like common ones on the network and computer systems, and in some cases, they are specific to digital environments, which open new weaknesses and security concerns [21]. Hence, Security standards should constantly be revised to keep up with evolving technologies in a rapidly changing digital landscape [23].

For instance, rules and instructions such as the General Data Protection Regulation (GDPR); Findability, Accessibility, Interoperability, and Reusability (FAIR) principles; and the EU code of conduct need specific security requirements [22], including authentication, authorization, data integrity, data reliability, availability, non-repudiation, trust, and privacy, to be followed by agricultural data-sharing systems [23], otherwise could impede the widespread adoption of these advancements [24].

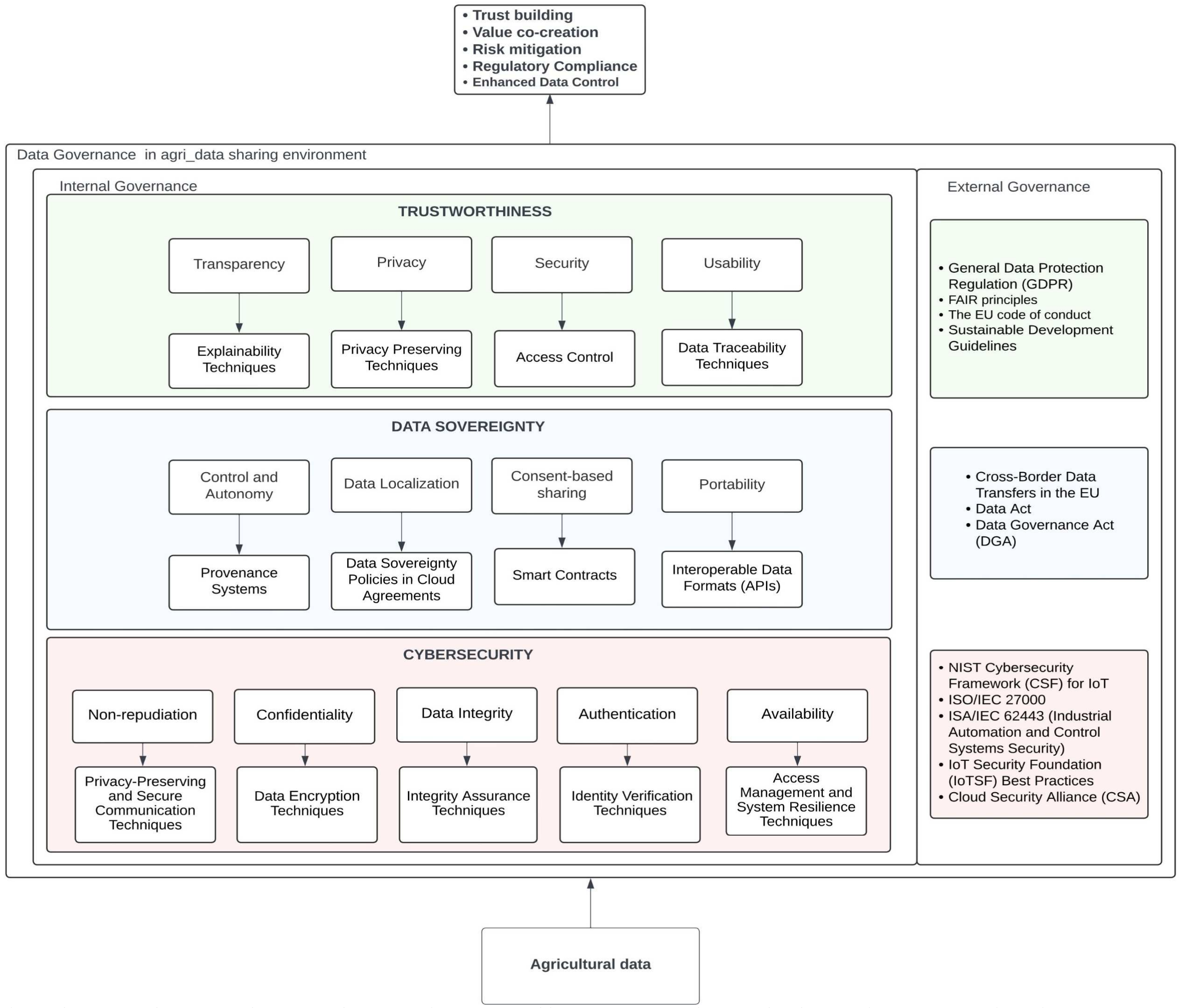
• Trust building
• Value co-creation
• Risk mitigation
• Regulatory Compliance
• Enhanced Data Control
Data Governance in agri_data sharing environment
Internal Governance
TRUSTWORTHINESS
Transparency
Privacy
Security
Usability
Explainability Techniques
Privacy Preserving Techniques
Access Control
Data Traceability Techniques
DATA SOVEREIGNTY
Control and Autonomy
Data Localization
Consent-based sharing
Portability
Provenance Systems
Data Sovereignty Policies in Cloud Agreements
Smart Contracts
Interoperable Data Formats (APIs)
CYBERSECURITY
Non-repudiation
Confidentiality
Data Integrity
Authentication
Availability
Privacy-Preserving and Secure Communication Techniques
Data Encryption Techniques
Integrity Assurance Techniques
Identity Verification Techniques
Access Management and System Resilience Techniques
External Governance
• General Data Protection Regulation (GDPR)
• FAIR principles
• The EU code of conduct
• Sustainable Development Guidelines
• Cross-Border Data Transfers in the EU
• Data Act
• Data Governance Act (DGA)
• NIST Cybersecurity Framework (CSF) for IoT
• ISO/IEC 27000
• ISA/IEC 62443 (Industrial Automation and Control Systems Security)
• IoT Security Foundation (IoTSF) Best Practices
• Cloud Security Alliance (CSA)
Agricultural data

Fig 1. The proposed Conceptual Framework: Integrating Trustworthiness, Data Sovereignty and Cybersecurity components in agri-Data Governance

III. The Proposed Conceptual Framework

The conceptual framework developed in this paper is designed to address the governance of agri-data sharing environments by integrating three key elements: Trustworthiness, Data Sovereignty, and Cybersecurity. When data flows across the different layers of a shared network (from the application layer to the physical layer, adapted from the OSI model), its governance faces many challenges. As shown in Fig 1., the trustworthiness component is located at the top because it is entwined with building trust via the various applications and platforms tailored for stakeholders. In addition, the nature of data Sovereignty stems from the data life cycle, so it is in the middle of this Framework to show that its considerations are related to the middle layers of the OSI model. Subsequently, cybersecurity is suited at the bottom because the physical, data link and network layers are associated with cyber risks and implementing cybersecurity protocols.

These components are critical for ensuring that agri-data is managed securely, transparently, and in compliance with the expectations and legal rights of stakeholders [6,25]. Given the complexities and sensitivity of agri-data, such a governance framework is essential for protecting stakeholder interests and promoting the responsible use of agricultural information. This framework is divided into Internal Data Governance Mechanisms and External Data Governance Mechanisms, where the former focuses on operational, technical, and managerial approaches to governing data within an organisation, and the latter ensures compliance with laws, policies, and international standards [5].

The framework is centred around agri-data and aims to meet the complex needs of various stakeholders, including farmers, agri-businesses, regulators, and technology providers. Effective Data Governance requires that these stakeholders have clear control over their data, while also ensuring that external regulations are adhered to in cross-border and multi-party data-sharing ecosystems [26].

A. *Agri-data as the Core*

At the heart of the framework lies Agri-data, generated from numerous sources such as IoT devices, drones, satellites, sensors, and farm management systems. Agri-data includes sensitive and vital information about farm operations, crop conditions, soil health, weather patterns, and productivity metrics [27]. Proper governance of this data is crucial, as it can be used to drive precision farming, optimize resource management, improve yield predictions, and support supply chain logistics [28].

Given the sensitive nature of agri-data, its governance must focus on protecting the data from unauthorized use, ensuring that stakeholders maintain control over how the data is used and shared, and safeguarding the data from external threats such as cyberattacks [29]. The proposed framework seeks to meet these needs by surrounding agri-data with layers of governance that address trust, control, and security. Agri-data not only has economic value but also social and environmental implications, making its proper governance essential for sustainable agriculture practices [30].

B. *Internal Governance Mechanisms*

In Agriculture 4.0, High-level planning and control and governance efforts over data management [31] should encompass a wide range of factors including policy, standards, ethics, and management of risks for both institutions and individuals, especially regarding sensitive data and data-sharing agreements [6,36]. Data Governance is distinct from data management; Data Governance works alongside data management but does not serve as a substitute for it. The definition of Data Governance is a structured framework of responsibilities and decision-making authority for information processes, implemented based on pre-established guidelines outlining permissions, actions, timing, conditions, and methodologies [31].

1) *Trustworthiness component*

Establishing a trustworthy data-sharing environment requires transparency in data processes, strong privacy protections, and robust security measures to prevent unauthorized access or misuse of data [5,6,18]. Moreover, usability must also be incorporated to ensure that sharing and tracking data will be user-friendly and accessible to all stakeholders. In line with the trustworthiness aspects highlighted in this study, the following mechanisms are applied:

- Transparency: One of the primary methods for ensuring transparency is through explainability techniques [1], which make complex algorithms and decision-making processes more comprehensible. Therefore, it fosters trust among farmers and agri-businesses, who can better understand how their data contributes to the decision-making process [19,32].
- Privacy: Privacy-preserving techniques, such as differential privacy and anonymization [1], are essential to protect this data from misuse. Differential privacy ensures that individual data points cannot be reverse-engineered from aggregate datasets, while anonymization removes personally identifiable information (PII) from datasets [1]. These techniques ensure that data can be shared while still protecting the privacy of the data owners.
- Security: Access control mechanisms are used to manage who has permission to access specific datasets. Role-Based Access Control (RBAC) is one such method, where access rights are assigned based on the role of the user [33]. For example, a farm manager may have access to detailed operational data, while a technology provider may only have access to anonymized summaries. This approach minimizes the risk of unauthorized access and misuse of data.
- Usability: Data traceability techniques enhance usability by allowing stakeholders to easily track the history and provenance of their data [1], This ensures that users can see where their data originated, how it has been used, and who has accessed it. This type of traceability not only improves trust but also helps in auditability and accountability within the data-sharing environment.

These mechanisms altogether make stakeholders feel more confident in sharing their agri-data.

2) *Data Sovereignty component*

Data Sovereignty refers to the rights and control that data owners have over their data, including how and where it is stored, processed, and shared. In agriculture, data sovereignty is a key concern for farmers and agri-businesses, as they seek to maintain control over the data generated from their farms [9]. The data sovereignty layer of the framework addresses this concern through four key elements: Control and Autonomy, Data Localization, Consent-Based Sharing, and Portability.

Control and Autonomy ensure that data owners retain the power to decide how their data is used and shared. This is particularly important in agriculture, where farmers may be hesitant to share data with large agri-businesses or technology providers without clear assurances that they will maintain control over how their data is used. The framework proposes the use of provenance systems to track the lifecycle of agri-data [12]. Provenance systems provide a detailed record of the origins of data, the transformations it undergoes, and the entities with which it is shared. These systems ensure accountability and provide farmers with the transparency they need to maintain control over their data.

Data Localization refers to the practice of ensuring that data is stored and processed within specific legal jurisdictions. This is particularly important for agri-data that may be subject to varying legal requirements depending on where it is stored [34]. Data sovereignty policies in cloud agreements are one way to enforce data localization, ensuring that data is stored within the borders of a country or region that has favourable legal protections for data owners. For example, European farmers may prefer to store their data within the EU to benefit from the protections afforded by the GDPR.

Consent-Based Sharing ensures that data owners have control over how their data is shared with third parties. The framework incorporates smart contracts as a mechanism for automating and enforcing consent-based sharing agreements. Smart contracts, built on blockchain technology, allow data owners to set conditions for sharing their data, such as specifying which parties can access the data, for what purposes, and under what circumstances [35]. Once these conditions are met, the data is automatically shared according to the terms of the contract. This gives data owners greater autonomy and control over their data-sharing practices.

Portability is another critical aspect of data sovereignty, ensuring that data owners can move their data across different systems and platforms without encountering barriers. In agriculture, data portability is essential as farmers may need to share data across various farm management systems, agribusiness platforms, and governmental databases. The framework supports portability through the use of interoperable data formats Application Programming Interfaces (API) that ensure data can be easily transferred between systems [36]. This reduces vendor lock-in and gives farmers more flexibility in choosing the platforms and services that best meet their needs.

By ensuring that data owners maintain control over their data, the data sovereignty mechanisms in this framework address the concerns of stakeholders who may be reluctant to share their data due to fears of losing control or being exploited by larger entities.

3) Cybersecurity component

Along with new opportunities that Agriculture 4.0 has offered to agricultural sectors and all involved stakeholders [37], a lot of new cyberattacks have been developed due to the usage of thousands of IoT devices [24] and receiving services from infrastructure providers in open fields [20]. These modern technologies have not been fundamentally tailored for the agricultural context and have led to a lack of focus on security concerns [38]. Although some cyber risks are such as common attacks on the network and computer systems, in some cases, they are specific to digital environments, which open up new vulnerabilities and security issues that decrease stakeholder control over data [21].

Like all smart systems, this data-sharing environment includes some layers: from collecting data on the farms to upper layers that work with processed data in decision-making platforms [39]. The following are the most common security vulnerabilities in multilayer systems often targeted by cyber attackers [23,40]:

- Confidentiality could result in unauthorised access to vital data, leading to theft of crucial information and posing significant threats to the privacy of agriculture system users.
- Authentication verifies the identity of participants in a network. Fake attackers can impersonate legitimate individuals and infiltrate the smart agriculture system. The potential outcomes could include data breach/loss, alteration, service unavailability, loss of device connectivity, or damage to smart farming agriculture systems.
- Data integrity ensures data remains unaltered during transmission, processing, or storage. The data exchange between devices and individuals in agriculture can result in financial or authentication fraud if the information is not deemed accurate enough.
- Availability guarantees prompt system responses and service accessibility. The unavailability of the services offered may cause business interruptions, potential erosion of customer trust, and revenue losses.
- Non-repudiation is essential for recognizing legitimate transactions. Information repudiation enables an attacker to deny the power usage, data creation, and production methods within an agricultural Information and Communications Technology (ICT) system, potentially resulting in a denial of services, authentication data, or data transmissions via the system's nodes.
- Privacy safeguards user information from unauthorized access, ensuring data confidentiality for authorized users. Possible invasion of privacy can lead to theft and vandalism.

When at least one of the above security requirements is threatening, popular cyber security Rules and instructions such as the ISO, NIST, etc. use a combination of three elements to tackle it [41].

Prevention is the common tactic for stopping cyber-attacks from occurring in advance. In this situation, any suggested approach must have ability to create strategies to protect against the particular type of attack(s), such as Intrusion prevention mechanisms. So, the initial step in risk management involves identifying the risks and vulnerabilities. But when an attacker surpasses the prevention measures, or the level of risk exceeds the acceptable level of risk, the system must react via detection procedures [42]. Mitigation refers to the last step of addressing attacks post-incident [41]. Table 1. shows which solution is used for each security requirement violation in this environment [43].

TABLE I. CYBER_ATTACKS GOALS AND SOLUTIONS IN AGRI-DATA SHARING ENVIRONMENT

CYBERATTACK GOAL	SOLUTIONS
CONFIDENTIALITY	DATA ENCRYPTION, MIXING NOISE, HIDING LOCATION
DATA INTEGRITY	HASHING, MESSAGE AUTHENTICATION CODES
AUTHENTICATION	DIGITAL SIGNATURES, IDENTITY-BASED CRYPTOGRAPHY, GROUP SIGNATURES, MULTI-FACTOR AUTHENTICATION
AVAILABILITY	ACCESS CONTROL, FAULT-TOLERANCE
NON-REPUDIATION	PSEUDONYMS, BLIND SIGNATURES, PRIVATE ANONYMOUS CHANNELS, POINT-TO-POINT CHANNELS, MULTI-PARTY PROTOCOLS WITH UNCONDITIONAL SECURITY, TRACEABLE META-DATA, DIGITAL SIGNATURES

C. External Governance

While internal governance mechanisms focus on operational and technical controls, external governance mechanisms ensure that the system complies with international laws, regulations, and standards. In the context of agri-Data Governance, external governance mechanisms are particularly important for ensuring compliance with data protection laws, cross-border data transfer regulations, and industry-specific standards. The global nature of agricultural systems means that Data Governance must navigate complex legal environments, where data ownership, privacy, and security are regulated by various jurisdictions [44,45].

The framework incorporates several external governance mechanisms, including the General Data Protection Regulation (GDPR), the Data Governance Act (DGA), and the Cybersecurity Frameworks (CSF**)**. These mechanisms provide guidelines for protecting the privacy, security, and sovereignty of agri-data. Each plays a crucial role in shaping how agri-data can be collected, processed, shared, and protected in compliance with both regional and international requirements.

a) General Data Protection Regulation (GDPR)

The GDPR is particularly relevant in the context of data sovereignty, as it provides strict rules on how personal data can be collected, stored, and shared within the European Union. The GDPR requires that data owners provide explicit consent before their data is shared with third parties and mandates that personal data be stored and processed within the EU, or in jurisdictions that have comparable levels of protection [46]. This is especially significant for farmers and agri-businesses that work with cloud platforms or third-party data processors outside the EU. The framework ensures compliance with the GDPR by incorporating consent-based sharing mechanisms that give data owners control over their data, and data localization policies that restrict where agri-data can be stored to ensure it is subject to appropriate regulatory oversight [47].

b) Data Governance Act (DGA)

DGA complements the GDPR by providing a framework for the safe and secure sharing of non-personal data across borders. The DGA promotes the creation of trusted data-sharing spaces where stakeholders can exchange data under clear governance rules [48]. The DGA is particularly important for ensuring that agri-data, even when anonymized or aggregated, is still protected under strong governance structures when shared across countries or between organisations. By establishing the conditions for trusted data exchanges, the DGA reduces the risks associated with sharing agri-data, such as potential breaches of privacy or unauthorized use of data for commercial purposes.

c) Cybersecurity Frameworks (CSF)

- *IoT Cybersecurity Management Frameworks*

These kinds of frameworks provide IoT devices with the best practices and well-rounded cybersecurity act, which include strategies on monitoring systems, responding to disaster incidents, deploying new applications, periodically evaluating implemented security, isolating systems, restricting physical and logical systems access, acceptable use policies, the enforcement of proper security and privacy policies, and compliance. Such as Cloud Security Alliance IoT Security Controls Framework 2019, IoT Cybersecurity Improvement Act of 2019 (S.734), NIST Considerations for Managing IoT Cybersecurity and Privacy Risks (NISTIR 8228), Foundational Cybersecurity Activities for IoT Device Manufacturers (NISTIR 8259), Standard for an Architectural Framework for the Internet of Things (IEEE P2413), and Industrial Internet Consortium Security Framework (IISF) [49].

- *Cloud Cybersecurity Management Frameworks*

The lack of computational capacity to process or store data in IoT devices causes edge or cloud resource usage through the network layer in this environment for agri-data processing [39]. The widespread application of edge or cloud computing has necessitated the development of numerous cloud protocols. The most common frameworks are ISO/IEC 27017, ISO/IEC 27018, NIST Special Publication 800-53, Privacy in Cloud Computing, SP 800-210, OWASP Secure Coding Practices, FedRAMP (The Federal Risk and Authorization Management Programme), and CSA-STAR [50].

IV. Discussion

This framework proposes a comprehensive approach for governing agri-data within data-sharing environments. By unifying those components, it undertakes the key governance needs of agricultural stakeholders. Trustworthiness mechanisms, such as transparency and privacy-preserving techniques, strengthen the confidence in the systems and enable stakeholders to feel more encouraged to share their agri-data. The Data sovereignty mechanisms give data owners control over their data, addressing concerns about ownership and autonomy. For instance, Provenance systems, data localization policies, and smart contracts enable data owners to retain control over their data and share it based on their terms. The mechanisms for cybersecurity provide robust protections against external threats while securing and protecting data from unauthorized access or alteration. In addition, to the above mechanisms, external governance is also incorporated into the framework. Therefore, the system complies with international laws and standards, such as the GDPR and the NIST or ISO Cybersecurity Frameworks. As a result, these mechanisms altogether ensure that agri-data sharing environments are aligned with the best practices in Data Governance.

V. Conclusion

Many of today's businesses have acknowledged the value of data as an asset in the research and development of new products [51] and are trying to take full advantage of this by providing an appropriate and secure platform to gain a greater share of the marketplace. The same as all data-sharing environments, agri-data is the main core of Agriculture 4.0. However, the fear of losing control over data usage and releasing sensitive data are the important challenges stakeholders in this ecosystem encounter.

The most serious questions that may come to the mind of participants framed this study are: what if this shared data is subjected to manipulation and the agri-data quality does not remain correct? How can they rely on data-driven analysis when they don't know the decisions are made based on whose data? What are the prevention, detection, and mitigation strategies for tackling emerging cyberattacks? To overcome these barriers and build trust in this ecosystem, this study follows well-rounded practices to reinforce the Data Governance perspective by developing a conceptual framework to deal with all vulnerabilities related to cyberspace, data sovereignty, and trustworthiness to increase the level of certainty and produce new opportunities.

The proposed framework in this paper depicts the importance of having a secure, sovereign, and trustworthy environment, and shows the position of each of these three components according to the layers of the OSI model. The complexity of Agricultural 4.0 when the aim is to protect this ecosystem against losing control over collected data, highlights the necessity of adhering to the offered practical practices by this framework for all stakeholders including policymakers, agri-businesses, and farmers.

In addition, this research can be applied in developing Information systems conceptually where the sharing of data is the main core of that. This framework can also widen those researchers' horizons, designing data-sharing protocols and standards and struggling with different challenges in trust building, data tracking, and external attacks as parts of Data Governance’s considerations.

Acknowledgment

The sincere thanks to Dr. Aoibhin Moore Heslin, Dr. Paul O'Keeffe from Airfield Estate, and Dr. Peter Mooney from the School of Computer Science of Maynooth University for their continuous support and mentorship.

Also, all the first three authors contributed equally.

References

[1] Bukhari, S.N.H. (2024) Data-Driven Farming Harnessing the Power of AI and Machine Learning in Agriculture. Boca Raton, FL: CRC Press.

[2] Fraser, A. (2018). Land grab/data grab: precision agriculture and its new horizons. The Journal of Peasant Studies, 46(5), 893–912. https://doi.org/10.1080/03066150.2017.1415887.

[3] Wolfert, S., Ge, L., Verdouw , C. And Bogaardt, M.J. (2017) ‘Big Data in smart farming – a review’, Agricultural Systems, 153, pp. 69–80. doi:10.1016/j.agsy.2017.01.023.

[4] Wiseman, L., Sanderson, J., Zhang, A. And Jakku, E. (2019) ‘Farmers and their data: An examination of farmers’ reluctance to share their data through the lens of the laws impacting smart farming’, NJAS: Wageningen Journal of Life Sciences, 90–91(1), pp. 1–10. doi:10.1016/j.njas.2019.04.007.

[5] Jakku, E. et al. (2019) ‘“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, 90–91(1), pp. 1–13. doi:10.1016/j.njas.2018.11.002.

[6] van der Burg, S., Wiseman, L. and Krkeljas, J. (2020) ‘Trust in farm data sharing: Reflections on the EU code of conduct for Agricultural Data Sharing’, Ethics and Information Technology, 23(3), pp. 185–198. doi:10.1007/s10676-020-09543-1.

[7] Wysel, M., Baker, D. And Billingsley, W. (2021) ‘Data Sharing Platforms: How value is created from Agricultural Data’, Agricultural Systems, 193, p. 103241. doi:10.1016/j.agsy.2021.103241.

[8] K. Bronson and I. Knezevic, "Big Data in food and agriculture," Big Data & Society, vol. 3, no. 1, pp. 1-5, Jan. 2016. doi: 10.1177/2053951716648174.

[9] A. Zhang, R. Heath, K. McRobert, R. Llewellyn, J. Sanderson, L. Wiseman, R. Rainbow,” Who will benefit from big data? Farmers’ perspective on willingness to share farm data”, Journal of Rural Studies, Volume 88, 2021, Pages 346-353.

[10] Fleming, A., Jakku, E., Lim-Camacho, L., Taylor, B. And Thorburn, P. (2018) ‘Is big data for big farming or for everyone? perceptions in the Australian grains industry’, Agronomy for Sustainable Development, 38(3). doi:10.1007/s13593-018-0501-y.

[11] FAO (2021) The State of Food and Agriculture [online]. Available at: https://openknowledge.fao.org/server/api/core/bitstreams/125b023c-002f-4387-9150-dc7fbbd86cbc/content.

[12] K. Spanaki, E. Karafili, and S. Despoudi, “AI applications of data sharing in agriculture 4.0: A framework for role-based data access control,” International Journal of Information Management, vol. 59, p. 102350, Aug. 2021.

[13] NIST, "Framework for improving critical infrastructure cybersecurity," National Institute of Standards and Technology, 2018. [Online]. Available: https://www.nist.gov/cyberframework. Accessed: Sept. 2024.

[14] Brown, C., Regan, A. and van der Burg, S. (2022) ‘Farming futures: Perspectives of Irish agricultural stakeholders on data sharing and Data Governance’, Agriculture and Human Values, 40(2), pp. 565–580. doi:10.1007/s10460-022-10357-8.

[15] S. Marcucci, A. Natalia González, S. G. Verhulst, and E. Wüllhorst, "Informing the Global Data Future: Benchmarking Data Governance Frameworks," (in English), Data & Policy, vol. 5, Aug 2023, doi: https://doi.org/10.1017/dap.2023.24.

[16] Durrant, A. et al. (2021) ‘How might technology rise to the challenge of Data Sharing in agri-food?’, Global Food Security, 28, p. 100493. doi:10.1016/j.gfs.2021.100493.

[17] Dibbern, T., Romani, L.A. and Massruhá, S.M. (2024) ‘Main drivers and barriers to the adoption of Digital Agriculture Technologies’, Smart Agricultural Technology, 8, p. 100459. doi:10.1016/j.atech.2024.100459.

[18] Šestak, M. & Copot, D. (2023) ‘Towards trusted data sharing and exchange in Agro-Food Supply Chains: Design principles for Agricultural Data Spaces’, Sustainability, 15(18), p. 13746. doi:10.3390/su151813746.

[19] Copa-Cogeca et al. (2018) EU Code of Conduct on Agricultural Data Sharing by Contractual Agreement. Available at: https://fefac.eu/wp-content/uploads/2020/07/eu_code_of_conduct_on_agricultural_data_sharing-1.pdf

[20] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," IEEE Access, vol. 8, pp. 34564-34584, 2020, doi: 10.1109/ACCESS.2020.2975142.

[21] A. N. Alahmadi, S. U. Rehman, H. S. Alhazmi, D. G. Glynn, H. Shoaib, and P. Solé, "Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture," Sensors, vol. 22, no. 9, doi: 10.3390/s22093520.

[22] M. T, K. Makkithaya, and N. V.G, "A trusted IoT data sharing and secure oracle based access for agricultural production risk management," Computers and Electronics in Agriculture, vol. 204, p. 107544, 2023/01/01/ 2023, doi: https://doi.org/10.1016/j.compag.2022.107544.

[23] K. Al-Dosari and N. Fetais, "Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach," Electronics, vol. 12, no. 17, doi: 10.3390/electronics12173629.

[24] H. H. A. Theyazn and H. Alkahtani, "Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model," (in English), Mathematics, vol. 11, no. 1, p. 233, 2023

[25] L. Wiseman, J. Sanderson, A. Zhang, and E. Jakku, “Farmers and their data: An examination of farmers’ reluctance to share their data through the lens of the laws impacting smart farming,” NJAS - Wageningen Journal of Life Sciences, vol. 90–91, no. 1, pp. 1–10, Dec. 2019.

[26] M. Ur Rahman, F. Baiardi and L. Ricci, "Blockchain Smart Contract for Scalable Data Sharing in IoT: A Case Study of Smart Agriculture," 2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), Dubai, United Arab Emirates, 2020, pp. 1-7.

[27] Costabile, C. and Øvrelid, E. (2023) Identifying governance mechanisms for data sharing in collaborative platform ecosystems. https://aisel.aisnet.org/ecis2023_rp/283/.

[28] Jussen, I. et al. (2024) 'Issues in Inter-Organisational Data Sharing: Findings from Practice and Research Challenges,' Data & Knowledge Engineering, 150, p. 102280.

[29] Abraham, C., Schneider, C. and vom Brocke, J., 2019. Data Governance in Digital Platforms: Insights from Platform Ecosystem Research. Journal of Strategic Information Systems, 28(2), pp.110-128.

[30] de Lima Fontão, D., Heimburg, J. and Wiesche, M., 2019. The Role of Dual Actors in Digital Platform Ecosystems. Journal of Information Technology, 34(3), pp.236-255.

[31] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "A systematic literature review of Data Governance and cloud Data Governance," (in English), Personal and Ubiquitous Computing, vol. 23, no. 5-6, pp. 839-859, Nov 2019 2023-12-03 2019, doi: https://doi.org/10.1007/s00779-017-1104-3.

[32] C. Eastwood, L. Klerkx, M. Ayre, and B. Dela Rue, "Managing socio-cultural drivers in the development of precision agriculture systems: A responsible research and innovation perspective," Agricultural Systems, vol. 176, 2019. doi:10.1016/j.agsy.2019.102672.

[33] de Carvalho Junior, M.A. and Bandiera-Paiva, P. (2018) 'Health Information System role-based access control current security trends and challenges', *Journal of Healthcare Engineering*, 2018, pp. 1–8. doi:10.1155/2018/6510249.

[34] Van den Broek, T. and Van Veenstra, A.F., 2015. Modes of Governance in Inter-organisational Networks. Information Systems Journal, 25(3), pp. 89-121.

[35] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, May 2016. doi: 10.1109/ACCESS.2016.2566339.

[36] N. Kshetri, "Big data's impact on privacy, security, and consumer welfare," Telecommunications Policy, vol. 38, no. 11, pp. 1134-1145, Oct. 2014. doi: 10.1016/j.telpol.2014.10.002.

[37] S. Padhy et al., "AgriSecure: A Fog Computing-Based Security Framework for Agriculture 4.0 via Blockchain," (in English), Processes, vol. 11, no. 3, p. 757, 20232023-12-03 2023, doi: https://doi.org/10.3390/pr11030757.

[38] M. W. Sitnicki et al., "Regional Perspective of Using Cyber Insurance as a Tool for Protection of Agriculture 4.0," (in English), Agriculture, vol. 14, no. 2, p. 320, 2024, doi: https://doi.org/10.3390/agriculture14020320.

[39] A. Rettore de Araujo Zanella, E. da Silva, and L. C. Pessoa Albini, "Security challenges to smart agriculture: Current state, key issues, and future directions," Array, vol. 8, p. 100048, 2020/12/01/ 2020, doi: https://doi.org/10.1016/j.array.2020.100048.

[40] K. Demestichas, N. Peppes, and T. Alexakis, "Survey on Security Threats in Agricultural IoT and Smart Farming," Sensors, vol. 20, no. 22, doi: 10.3390/s20226458.

[41] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures," IEEE Communications Surveys & Tutorials, vol. 22, pp. 616-644, 11/13 2019, doi: 10.1109/COMST.2019.2953364.

[42] A. Zarreh, H. Wan, Y. Lee, C. Saygin, and R. A. Janahi, "Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach," Procedia Manufacturing, vol. 38, pp. 605-612, 2019/01/01/ 2019, doi: https://doi.org/10.1016/j.promfg.2020.01.077.

[43] A. Vangala, A. K. Das, V. Chamola, V. Korotaev, and J. J. P. C. Rodrigues, "Security in IoT-enabled smart agriculture: architecture, security solutions and challenges," (in English), Cluster Computing, vol. 26, no. 2, pp. 879-902, Apr 2023, doi: https://doi.org/10.1007/s10586-022-03566-7.

[44] Costabile, C. and Øvrelid, E. (2023) Identifying governance mechanisms for data sharing in collaborative platform ecosystems. https://aisel.aisnet.org/ecis2023_rp/283/.

[45] Lynch, T. and Gregor, S. (2004b) 'User participation in decision support systems development: Influencing system outcomes,' European Journal of Information Systems, 13(4), pp. 286–301.

[46] European Commission, "Data protection in the EU," 2020. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection_en. Accessed: Sept. 2024.

[47] Bertino, E., Kundu, A., & Sura, Z. (2019). Data transparency with blockchain and AI ethics. Journal of Data and Information Quality (JDIQ), 11(4), 1-8.

[48] European Parliament, "The Data Governance Act: A new regulation for data sharing," 2021. [Online]. Available: https://www.europarl.europa.eu. Accessed: Sept. 2024.

[49] L. Anderson, "The Internet of Things: Security and Insecurity Challenges," M.S., Utica College, United States -- New York, 28495210, 2021. [Online]. Available: https://may.idm.oclc.org/login?url=https://www.proquest.com/dissertations-theses/internet-things-security-insecurity-challenges/docview/2537760411/se-2?accountid=12309

[50] F. Abdullayeva, "Cyber resilience and cyber security issues of intelligent cloud computing systems," Results in Control and Optimization, vol. 12, p. 100268, 2023/09/01/ 2023, doi: https://doi.org/10.1016/j.rico.2023.100268.

[51] L. Veldkamp, "Valuing Data as an Asset*," Review of Finance, vol. 27, no. 5, pp. 1545-1562, 2023, doi: 10.1093/rof/rfac073.