EVOLUTION OF COMPUTER HARDWARE FOR AGRICULTURAL SECURITY

Emanuel ACHIREI[1], Alexandrina RATA[2], Mia MERTICARIU[3], Mihaela Catalina FROICU [3]

e-mail: froicucatalina8@gmail.com

Abstract

The article looks at the challenges and solutions for data privacy in agriculture. The use of advanced technologies in agriculture, such as sensors, IoT, data analytics, and AI, has brought several benefits to the industry. However, protecting sensitive data is a significant challenge in using these technologies, especially in the agricultural sector, where personal and business data, such as agricultural production and financial and customer information, can be vulnerable to theft or misuse. The article discusses solutions for data protection in agriculture, including data encryption, zero-knowledge proofs, decentralized identities, multi-party computing, and homomorphic encryption. The article also highlights the importance of compliance with GDPR and other data protection regulations. Protecting sensitive data in agriculture is essential as modern farming relies heavily on technology for decision-making and management. This paper proposes an ideal approach to secure data by deploying advanced weather-resistant computing systems designed to operate under harsh conditions while employing sophisticated cryptographic techniques. Although constrained by current technological limitations, the ideal implementation of these systems offers numerous advantages, such as improved data protection, enhanced data availability, facilitation of collaborative farming practices, and potential integration with IoT devices. Further research and development in this area could lead to significant advancements in agricultural technology and data security, making the proposed solution a model for future efforts.

Key words: IoT, data privacy, data protection, GDPR (General Data Protection Regulation).

Agriculture has undergone a major digital transformation in recent years, with the increasingly widespread use of advanced technologies such as sensors, the Internet of Things (IoT), data analytics, and artificial intelligence (AI) (Shabbir J. *et al*, 2015). These technologies can offer a wide range of benefits, from increasing crop yields and improving the efficiency of agricultural operations to reducing environmental impact. However, a significant challenge in using these technologies is protecting sensitive data. Agriculture relies on a large amount of personal and commercial data, such as information on agricultural production, finances, and customers, which can be vulnerable to theft or misuse. In addition, data about soil and crops, which can be considered a competitive advantage for a farmer or agricultural company, can be just as vulnerable to breaches of confidentiality.

In this article, we will focus on the data privacy challenges in agriculture and the solutions available for protecting this data. Specifically, we will discuss the collection and storage of data in agriculture, the risks associated with breaching data privacy, and regulations governing data protection and user rights (Alboaie S. *et al*, 2022; Alboaie L., 2017). We will also explore the technologies and solutions available for protecting data in agriculture and provide relevant case studies and examples of best practices. Moreover, our analysis suggests that an ideal solution would involve farmers controlling the computing systems, at least for key management in the case of using cloud resources. Generally, for optimal privacy, it would be ideal for the hardware to be locally controlled by the farmers and able to function without internet access. These computers could be small IoT devices or systems that manage data (in databases). This article proposes improvements and specific features for this imagined hardware as the ideal solution. This article explores potential improvements and specific features for this envisioned hardware, treating it as the ideal solution for agricultural data security. Some of the proposed enhancements may include advanced weather-resistant materials and design,

[1] "Alexandru Ioan Cuza" University of Iasi, Romania

[2] AXIOLOGIC SAAS, Iasi, Romania

[3] Iasi University of Life Sciences, Romania

robust encryption and authentication methods, and user-friendly interfaces tailored to the needs of farmers. By focusing on these characteristics, we aim to provide a comprehensive blueprint for future development in this area, ultimately contributing to advancing agricultural technology and data protection.

MATERIAL AND METHOD

Data protection is a critical issue in business, especially regarding sensitive data (Alboaie S. et al, 2022). In business, sensitive data can include information about customers, employees, business partners and owners. This data can include sensitive information such as names, addresses, phone numbers and emails, identification information, and financial and business information. In addition, companies collect and store data about employees, including information on income, benefits, and performance.

Regarding agriculture, data collection and storage are essential to increase crop yields and improve the efficiency of agricultural operations. However, the risks associated with data privacy (Ferris J., 2017**)** breaches are just as significant in agriculture. The data collected can include information about agricultural production, soil, crops, and financial and business information. This data can be vulnerable to theft, unauthorised use, or destruction, negatively affecting farm owners or agricultural producers.

In addition, the risks of breaching data privacy can be significant in agriculture because the data collected and stored in this sector is often sensitive and unique to each farm or agricultural producer. However, technologies and solutions are available to protect this data, including data encryption and other data security techniques, developing secure data collection and storage platforms, and employee training to prevent data privacy breaches. Data protection is an important concern for business and agriculture, as the sensitive data of customers, employees, and business partners is essential to business success and must be protected. Additionally, the data collected in agriculture is important for increasing crop yields and improving the efficiency of agricultural operations but must be protected from risks such as theft and unauthorised use.

According to a report by the United Nations Conference on Trade and Development (UNCTAD), 137 out of 194 countries have implemented legislation to secure data protection and privacy (UNCTAD, 2023). The EU General Data Protection Regulation (GDPR) (Wilgenbusch J. et al, 2021) is also an important regulation that provides data protection. The European Data Protection Board (EDPB) has published guidelines on data subject rights, including the right of access (EDPB, 2022). GDPR (General Data Protection Regulation) is a European Union (GDPR, 2016) law that regulates the protection of the personal data of EU citizens. This law applies to all organisations that collect and store the personal data of EU citizens, regardless of the organisation's location. Agriculture is no exception and must comply with GDPR regarding the personal data of farmers, employees, and customers.

The implications of GDPR (Wilgenbusch J. et al, 2021) in agriculture include the responsibility to protect personal data and to ensure that data is stored securely and used in compliance with regulations. This can be a disadvantage for agricultural producers, as data regarding production, soil, and crops may be important for managing their business and improving the efficiency of agricultural operations. However, there are ways to collect and use data in compliance with GDPR so that agricultural producers can take advantage of the benefits of technology without compromising data privacy.

RESULTS AND DISCUSSIONS

Data protection has become a critical issue in agriculture. The sensitive data collected and stored in this sector is vulnerable to risks such as theft, unauthorised use, or destruction. To address these risks, various technical measures have been developed to protect data, including data encryption, zero-knowledge proofs, decentralised identities, multi-party computation, and homomorphic encryption. Data encryption (Saikumar I., 2017) is a cryptographic technique that converts data into an unreadable format, so unauthorised users cannot read it. Encryption can be used to protect stored and transferred data. Various encryption methods are available, including symmetric-key encryption, asymmetric-key encryption, and hashing (Alboaie S., Cosovan D., 2017). While encryption is a useful tool for protecting data, it can also introduce performance overhead and may only be suitable for some use cases.

Zero-knowledge proofs (Zkps) (Bączkowski A., 2022) are cryptographic techniques used to prove the authenticity of data without revealing the data itself. Using this technique, two parties can confirm the validity of a statement without revealing any additional information apart from the statement itself. Zero-knowledge proofs can be used to ensure that data is authentic without revealing the data itself, which can be useful for data privacy. Decentralised identities (W3C, 2022) are a privacy-enhancing technology that allows individuals to control their digital identity without needing a central authority. Users can authenticate themselves using decentralised identities and access services without revealing personal information. This can

help protect data privacy while still enabling access to services. Multi-party computation (Damgård I. et al, 2012) is a cryptographic technique that allows multiple parties to jointly compute a function on their private data without revealing their data to each other. This technique is useful for collaborative data analysis while preserving data privacy. Multi-party computation can be used to enable data sharing between multiple parties while still preserving data privacy. Homomorphic encryption (Damgård I. et al, 2012) is a cryptographic technique that allows computation on encrypted data without first decrypting it. This technique can protect sensitive data while still allowing data analysis and computation. Homomorphic encryption can be useful for protecting data privacy in applications where data analysis is necessary.

Data protection (Alboaie S., Cosovan D., 2017; Alboaie L., 2017) is a critical issue in agriculture, and various technical measures have been developed to protect sensitive data. Each measure has advantages and disadvantages and should be selected based on the use case. Organisations can protect their data from theft, unauthorised use, or destruction by implementing these technical measures while enabling data analysis and collaboration.

Weather and shock-resistant hardware require robust materials, protective enclosures, and specific design features to withstand harsh environmental conditions, such as extreme temperatures, moisture, and physical stress. However, integrating these protective elements while accommodating the computational demands of advanced cryptographic techniques can be a complex task.

This chapter addresses the tension between advanced cryptography and hardware constraints (Mustafa G. et al, 2018), which is essential for developing effective weather and shock-resistant computing systems that can ensure the security and privacy of agricultural data in challenging environments.

OpenDSU technology (Ursache C. et al, 2022; OpenDSU, 2023) is a decentralised identity and access management platform that enables the creation of Digital Trust Ecosystems in agriculture. The technology integrates various data protection solutions such as encryption, zero-knowledge proofs, decentralised identities, multi-party computation, and homomorphic encryption. Digital Trust Ecosystems provide a secure and trustworthy environment that facilitates data sharing between stakeholders without compromising data privacy or security. Two case studies demonstrate OpenDSU technology's effectiveness in managing livestock and crop production data. OpenDSU technology (Ursache C. et al, 2022; OpenDSU, 2023) provides a comprehensive data protection solution that can be applied across various sectors, including agriculture. In the contemporary agricultural landscape, data protection is paramount. With the increasing reliance on technology for farm management and decision-making processes, securing sensitive data and maintaining its integrity is crucial. In light of current technological limitations, the ideal approach is deploying advanced weather-resistant computing systems capable of enduring harsh conditions while employing sophisticated cryptographic techniques to safeguard data access.

The proposed weather-resistant computing systems would be specifically designed to operate under challenging environmental conditions often encountered in agricultural settings. These systems would be built with materials capable of withstanding high temperatures, water-resistant enclosures, and rugged design features to resist physical shocks, vibrations, and other forms of mechanical stress. Computers constructed with these characteristics can be installed in various locations on the field or farm, ensuring continuous data collection and processing even in adverse conditions.

To safeguard sensitive agricultural data, advanced cryptographic methods will be integrated into weather-resistant computing systems. Techniques like Public Key Cryptography, Zero-Knowledge Proofs, and Secure Multi-Party Computation ensure secure data access and sharing. Designing hardware that balances these computational demands with resilience against harsh conditions requires careful consideration of factors like heat dissipation, energy consumption, and component placement, as well as innovative materials and efficient algorithms.

The ideal implementation of these weather-resistant computing systems with advanced cryptographic techniques would provide numerous advantages for the agricultural sector, such as improved data protection, enhanced data availability, facilitation of collaborative farming practices, and potential integration with IoT devices (Torky M. et al, 2020) for comprehensive farm management. Although realising this ideal approach is constrained by current technological limitations, further research and development could lead to significant advancements in agricultural technology and data security. Considering the potential benefits and applications, the proposed solution is a model for future efforts to enhance data protection in agriculture.

CONCLUSIONS

Data protection is a critical issue in agriculture, and the sensitive data collected and stored in this sector is vulnerable to risks such as theft, unauthorised use, or destruction. To address these risks, various technical measures have been developed to protect data, including data encryption, zero-knowledge proofs, decentralised identities, multi-party computation, and homomorphic encryption. Technical measures protect data from unauthorized access while enabling analysis and collaboration. Organizations must evaluate and select suitable data protection solutions to maintain security, privacy, and trust. Implementing advanced weather-resistant computing systems with cryptographic techniques can enhance agricultural data protection. Despite current technological limitations, this approach highlights the potential benefits and applications that could be achieved with continued research and development. By considering the advantages of improved data protection, enhanced data availability, collaborative farming practices facilitation, and potential IoT device integration (Torky M. et al, 2020), the proposed solution is a valuable model for future efforts to bolster data security and overall farm management in the agricultural sector.

ACKNOWLEGMENTS

This research is co-financed by the European Fund for Regional Development through the Competitiveness Operational Program 2014 – 2020, project “Establishment and implementation of partnerships for the transfer of knowledge between the Iasi Research Institute for Agriculture and Environment and the agricultural business environment”, acronym “AGRIECOTEC”, SMIS code 119611.

REFERENCES

Alboaie S., Ursache C., Lenuta Alboaie, 2022 - *Self-Sovereign Applications: return control of data back to people, Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 24th International Conference KES2020,* vol. 176, 16-18 Septembrie 2020, online available at: https://doi.org/10.1016/j.procs.2020.09.164.

Alboaie L., 2017 - *Towards a smart society through personal assistants employing executable choreographies,* ISD 2017, 6-8 Sep 2017 26th International Conference on Information Systems Development, online available at: https://aisel.aisnet.org/isd2014/proceedings2017/Security/5/.

Bączkowski A., 2022 - Fundamentals: What Are Zero-knowledge Proofs?, online available at: https://alephzero.org/blog/fundamentals-zero-knowledge-proofs/.

Damgård I., Pastro V., Smart N. and Zakarias S., 2012 - *Multiparty computation from somewhat homomorphic encryption*, Crypto 2012, vol. Springer LNCS 7417, pp. 643-662, 2012, online available at: http://dx.doi.org/10.1007/978-3-642-32009-5_38.

Alboaie S., Cosovan, D., 2017 - *Private Data System Enabling Self-Sovereign Storage Managed by Executable Choreographies*, available at http://dx.doi.org/10.1007/978-3-319-59665-5_6

EDPB, 2022 - *Guidelines 01/2022on data subject rights - Right of access*, European Data Protecetion Board, Version 1.0, Adopted on 18 January 2022, online available at: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf

Ferris J., L., 2017 - *Data Privacy and Protection in the Agriculture Industry: Is Federal Regulation Necessary?,* available online at:https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1422&context=mjlst.

GDPR, 2016 - General Data Protection Regulation, online available at: https://gdprinfo.eu/.

Mustafa G., Ashraf, R., Mirza, M.A. and Jamil, A., 2018 - A review of data security and cryptographic techniques in IoT based devices. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems (pp. 1-9).

OpenDSU, 2023 - *OpenDSU Documentation*, online available at: https://opendsu.com/.

Saikumar I., 2017 - *DES-Data Encryption Standard.* International Research Journal of Engineering and Technology, 4(3).

Shabbir J., and Anwer, T., 2015 - *Artificial Intelligence and its Role in Near Future,* available online at: https://arxiv.org/pdf/1804.01396.pdf.

Torky M., Hassanein, A., E., 2020 - *Integrating blockchain and the internet of things in precision: agriculture: Analysis, opportunities, and challenges*, available at https://www.sciencedirect.com/science/article/abs/pii/S0168169919324329.

UNCTAD, 2023 - "Data Protection and Privacy Legislation Worldwide", United Nations Conference on Trade and Development, available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

Ursache C., Sammeth, M., & Alboaie, S., 2022 - OpenDSU: Digital Sovereignty in PharmaLedger. *arXiv preprint arXiv:2209.14879*, online available at: https://doi.org/10.48550/arXiv.2209.14879.

W3C, 2022 - *Decentralized Identifiers (DIDs) v1.0, Core architecture, data model, and representations*, World Wide Web Consortium , online available at: https://www.w3.org/TR/did-core/#abstract.

Wilgenbusch J., Lynch, B., Hospodarsky, N., and Pardey, P., 2021 - *Addressing new data privacy realities affecting agricultural research and development: A tiered-risk, standards-based approach*, available at https://acsess.onlinelibrary.wiley.com/doi/10.1002/agj2.20968.