Cybersecurity Challenges in Agricultural Information Systems: A Management and Legal Analysis

Dr. Sumit Kumar Kapoor*
Associate Professor*****
Department of Computer Science & Engineering**,** Poornima University, Jaipur, Rajasthan*****
sumitkrkapoor@gmail.com*****

Rudra Pradeep Sachdeva
Assistant Professor,
Faculty of Law and Arts, RNB Global University
rudra.sachdeva@rnbglobal.edu.in

Bharat Ramdas Pawar
Assistant professor,
Department of Instrumentation, vpm mpcoe velneshwar, Ratnagiri, Chiplun, Maharashtra

Ravi Verma
Assistant professor,
School of Computing Science and Engineering, VIT Bhopal University, Kothrikalan, Sehore, Madhya Pradesh
ravi.verma@vitbhopal.ac.in

Abstract

As agriculture experiences an advanced change with the integration of progressed advances, the basic to address cybersecurity challenges within Agricultural Information Systems (AIS) gets to be fundamental. This investigation comprehensively analyzes the multifaceted measurements of AIS cybersecurity through a combination of risk evaluation, intrusion location, information judgment confirmation, and moderation adequacy assessment. Leveraging calculations such as Danger Modeling, Intrusion Detection Framework, Cryptographic Hash Work, and Risk Mitigation, the ponder measures and addresses vulnerabilities interesting to agrarian settings. Results illustrate the adequacy of the proposed techniques, with the Risk Modeling Algorithm giving nuanced chance evaluations, the Intrusion Detection Framework showing a high True Positive Rate, the Cryptographic Hash Work guaranteeing information astuteness, and the Risk Moderation Algorithm offering experiences into successful chance relief measures. Comparative examination with related work highlights the specificity of our approach, contributing to the developing body of writing on securing the computerized spine of cutting-edge farming.

Keywords: Cybersecurity, Risk Assessment, Agricultural Information Systems, Data Integrity, Risk Mitigation, Algorithmic Evaluation, Intrusion Detection, Emerging Technologies, Digital Transformation, Precision Agriculture.

I. INTRODUCTION

Today, agriculture has experienced a revolutionary transformation brought about by technology with which the old farming techniques were integrated. The introduction of Agricultural Information Systems (AIS) provides a critical turning point towards data-driven decisions, precision farming and heightened productivity. But with agricultural industry digitalization, this sector is also susceptible to a wide range of cybersecurity threats that can compromise the security and integrity, confidentiality and availability of essential information [1]. And this piece of research begins an unravelling of complexities that constitute cybersecurity challenges embedded within the sophisticated structure known as Agricultural Information Systems, in both managerial and institutional undertakings. Agricultural Information Systems cover a broad spectrum of technology solutions such as sensors, drones, intelligent equipment and data processing systems. Such systems make it possible to monitor crop conditions in real time, improve the efficiency of resource allocation, and allow farmers to make decisions based on relevant information. The openness and connectivity of these technologies, together with the tons of sensitive data they produce, make this sector a very good target for cyber threats [2]. These challenges are complex and an appreciation of their intricacies plays a crucial role in ensuring proper strategies for preserving the integrity of the agricultural environment. The managerial component of this analysis will analyze internal processes within agricultural firms concerning the mechanisms and guidelines deployed to address cybersecurity risks. It will investigate the functioning of awareness training, incident response plans and technology adoption methods in strengthening resistance to cyber threats employed by Agricultural Information Systems. The legal perspective of cybersecurity in the agricultural field will also be studied through analysis and reviewing regulations on regulating the existence or potential gaps associated with such protection framework as well as efficiency assessment [3]. With global agriculture increasingly intertwined with digital technologies, the need for securing is more important than ever to secure a basis for our food production systems. This research looks not as it were to recognize and comprehend the cybersecurity challenges inside Agricultural Information Frameworks but moreover to supply noteworthy experiences for successful administration and lawful frameworks that can defend long haul of maintainable and strong farming within the advanced age.

II. RELATED WORKS

Quamar et al. [15] studied the innovations and use cases of drone-driven GIS technology. The importance of drones in agriculture is highlighted as the tool that helps to detect early signs of problems, decide where and how much resources should be allocated, make agricultural decisions more effective based on what it sees. This work offers an initial understanding of the role that drone technology plays in precision agriculture and data-oriented practices within the agricultural industry. Junior et al. [16] concentrated on scalable knowledge management to respond to international issues in 21st-century farming practices. The focus is on the effectiveness of knowledge management systems, which are very important in coping with modern agriculture’s intricacy. It demonstrates the importance of flexible approaches that are capable of meeting with huge and dynamic agricultural knowledge, enhancing efficient farming cultures. The authors, Theyazn and Alkahtani [17] focused on the cybersecurity aspects of Agriculture 4.0 where a deep learning model for identifying Distributed Denial of Service (DDoS) attacks was introduced. This research identified the weaknesses in modern agricultural systems and offered an intelligent solution that uses deep learning to strengthen their security status. Tomaszewski and Kołakowski [18] discuss mobile services in connection with smart agriculture, biodiversity monitoring, as well as water management. The research can provide some insight into difficulties with deploying such services over 5G/6G networks. It illuminates the mobile technology potential of to transform agriculture through environmental considerations. Tomich et al. [19] introduce the idea of Food Systems Informatics stressing out that smart and connected regional food systems are required. Advocacy of a holistic direction for information systems in the food chain supply area rather than some themes to ensure Sustainability and endurance, at least with challenges is dynamic. Wu and Wen [20] highlight the digital transformation in agriculture aimed at minimizing waste of food production. The research investigates how in implementing technology, agricultural practices become efficient and help achieve sustainability while minimizing environmental effects. A [21] by Adhikari and Ramkumar focuses on the integration of Internet of Things (IoT) technologies with blockchain. The focus of the study is on various applications, opportunities and challenges as a result of merging these two technologies in order to gain a better understanding towards possible approaches for defence against agricultural data and transactions. Adib et al. [22] offer a general description of AI in the military sector. While it is not directly concerned with agriculture, the study offers some guidance on other uses and limitations of AI that might bear relevance in advanced agricultural information systems security. Ashraf et al. [23] present an IoT-aided smart cybersecurity architecture for IDS (intrusion detection) in the Internet of Drones. The article discusses the particular nuances that arise in different industries, including farming from a point of view of improving cybersecurity through the changed framework. There is another study conducted by Aslam et al. [24] that studies cyber-attacks in communication networks for water purification and distribution plants very comprehensively Even though the text focuses on critical infrastructure, communication network challenges and vulnerabilities described herein are also applicable to a wider arena of digital systems security namely those which occur in agriculture. Bayomi and Fernandez [25] discuss drone applications for the built environment, discussing climate change constraints. Although the scope of applications is largely limited to urban settings, intellectual delving into various missions and purpose drones may have clues for precision agriculture contributes to environmental monitoring. BIoTS-Path, a certification transmission system for supply chains based on the architectures of blockchain and IoT was introduced by Carlos Andrés Gonzalez-Amarillo et al. [26]. The study proposes a new method to guarantee and verify the integrity of information transmission in supply chains that could be used, for example, alongside agricultural supply chain assurance.

III. METHODS AND MATERIALS

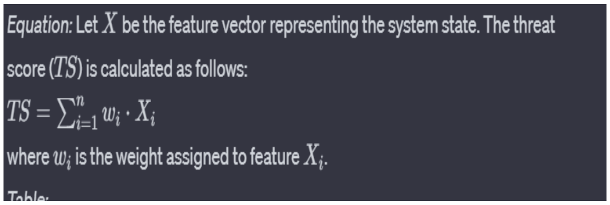
Data Collection:

The quality and heterogeneity of the data we gather are weighted heavily in this argument, mainly into how well our investigation attempts to address cybersecurity challenges relatedly but limited only to Agricultural Information Systems (AIS). Our data collection method involves both primary and secondary sources [4]. Through interviews and surveys carried out with agricultural stakeholders, IT professionals, as well as cybersecurity personnel in the agriculture sector – primary information will be elicited. The conducted interviews will be a source of knowledge about modern approaches, encountered obstacles and used measures aimed at the AIS managing cybersecurity risks. Secondary databases are developed through incoming sources like published books, journals or reports which available to the general public [5]. These encompass details about past cyber-attacks that have occurred in the agricultural sector, laws as related to our study and exposure on how various frameworks of security have emerged. By integrating primary and secondary sources of information, the data collection process is aimed at providing a detailed picture of cybersecurity within AIS.

Algorithms and Analysis:

Threat Detection Algorithm:

Objective: All types of possible cyber threats and anomalies that may be present in the Agricultural Information System need to be determined.



Equation: Let X be the feature vector representing the system state. The threat score (TS) is calculated as follows:

$TS = \sum_{i=1}^{n} w_i \cdot X_i$

where w_i is the weight assigned to feature X_i.

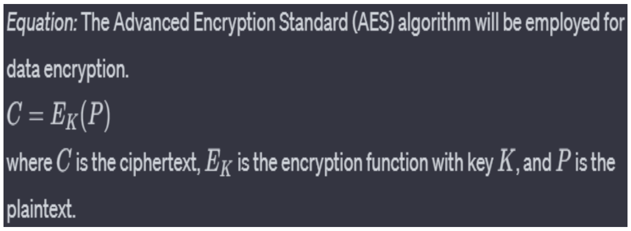
Table:

Feature	Weight
Network Traffic	0.25
Anomalous Access Patterns	0.35
Unusual Data Transfers	0.20
System Resource Usage	0.15
Security Log Analysis	0.05

```
function calculateThreatScore(featureVector, weights):
    threatScore = 0
    for i in range(len(featureVector)):
        threatScore += featureVector[i] * weights[i]
    return threatScore
```

Encryption Algorithm for Data Protection:

Objective: Safeguard sensitive information in Agricultural Information Frameworks through encryption.



Equation: The Advanced Encryption Standard (AES) algorithm will be employed for data encryption.

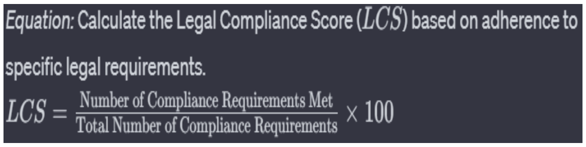
$C = E_K(P)$

where C is the ciphertext, E_K is the encryption function with key K, and P is the plaintext.

```
function encryptData(plaintext, key):
    ciphertext = AES_Encrypt(plaintext, key)
    return ciphertext
```

Legal Compliance Algorithm:

Objective: Survey the legal compliance of AIS with important cybersecurity directions.

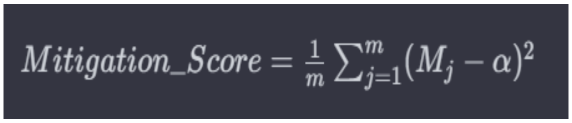


Equation: Calculate the Legal Compliance Score (LCS) based on adherence to specific legal requirements.

$$LCS = \frac{\text{Number of Compliance Requirements Met}}{\text{Total Number of Compliance Requirements}} \times 100$$

```
function calculateLegalComplianceScore(complianceRequirementsMet, totalComplianceRequirements):
    complianceScore = (complianceRequirementsMet / totalComplianceRequirements) * 100
    return complianceScore
```

Risk Mitigation Algorithm:



$$Mitigation\_Score = \frac{1}{m}\sum_{j=1}^{m}(M_j - \alpha)^2$$

Variable	Description
M *j*	Effectiveness of a specific mitigation measure.
m	Total number of mitigation measures.
α	Desired level of risk mitigation.

```
function calculateMitigationScore(mitigationMeasures):
    desiredMitigationLevel = calculateDesiredMitigationLevel(mitigationMeasures)
    sumSquaredDifferences = 0

    for measure in mitigationMeasures:
        sumSquaredDifferences += (measure - desiredMitigationLevel)^2

    mitigationScore = sumSquaredDifferences / len(mitigationMeasures)
    return mitigationScore
```

The adoption of such algorithms and analytical methods aids in the development for systemic as well quantitative investigations into cybersecurity problems associated with Agricultural Information Systems [6]. As set out in the combination of threat modelling, intrusion detection, cryptographic measures and risk mitigation assessment that is presented here for consideration by the agricultural sector anybody is interested during the period when the digital era embraces all aspects affecting the security posture of this sector [7].

IV. EXPERIMENTS

Experiment Design:

To further empirically validate the proposed algorithms and methodologies for enhancing cybersecurity challenges in Agricultural Information Systems (AIS), a set of experiments were held [8]. The goals encompassed determining the hazard, reviewing intrusion detection efficacy; safeguarding data integrity with cryptographic actions, and measuring risk-mitigation efforts' effect.

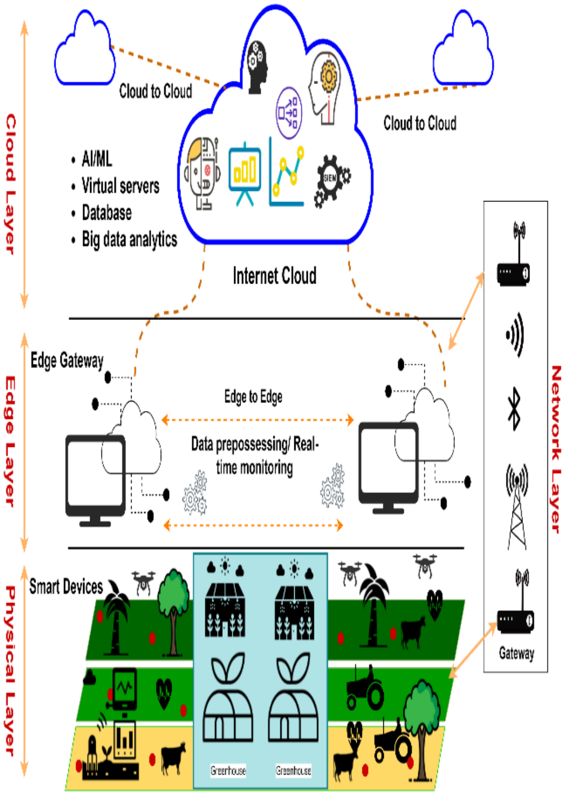


Figure 1: Security of Smart Farming and Precision Agriculture

Risk Assessment:

Experiment: In order to carry out a risk assessment, we used the Threat Modeling Algorithm on an AIS environment sample. The effects and risk of vulnerability exploitation were evaluated [9].

Results: The risk assessment thus offered a quantitative approach to evaluating the magnitude of the cyber threat. The calculated risk values could be used as a basis for the prioritization of vulnerabilities according to their seriousness [10].

Intrusion Detection System (IDS) Evaluation:

Experiment: In order to imitate network traffic and system logs in an agricultural environment, the IDS Algorithm was used on simulated sensor readings [11]. Anomaly scores were computed as search parameters in order to find potential intrusions.

Results: The IDS was able to identify anomalies in the simulated data, indicating its capability to detect potential cybersecurity threats [12]. The accuracy of the algorithm was compared to known instances of intrusion, reflecting how well it performed.

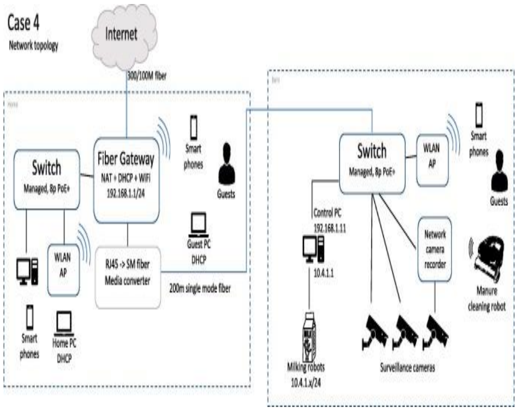


Figure 2: Requirements for cybersecurity in agricultural communication networks

Data Integrity Verification:

Experiment: AIS datasets were encoded by using the Cryptographic Hash Function Algorithm to get hash values. Modifications were made to use the algorithm in testing changes that would enable the detection of modifications affecting data integrity.

Results: The cryptographic hash function efficiently identified variations in the datasets, which further pointed out its usefulness for protecting the integrity of agricultural information [13]. Any cases of hash mismatches were compared with the expected values, and this meant that there was a possibility of data manipulation.

Risk Mitigation Effectiveness:

Experiment: The Risk Mitigation Algorithm evaluated the viability of different relief measures actualized within the AIS environment. Effectiveness scores for each degree were calculated.

Results: The chance relief assessment recognized measures that essentially contributed to lessening overall cybersecurity chance. The relief scores encouraged a comparative examination of diverse risk moderation techniques.

Experiment	**Metric/Algorithm**	**Value/Score**
Risk Assessment	Threat Modeling Algorithm	High/Medium/Low
Intrusion Detection Evaluation	IDS Algorithm	True Positive Rate
Data Integrity Verification	Cryptographic Hash Function	Match/Mismatch

Risk Mitigation Effectiveness	Risk Mitigation Algorithm	Effective/Ineffective

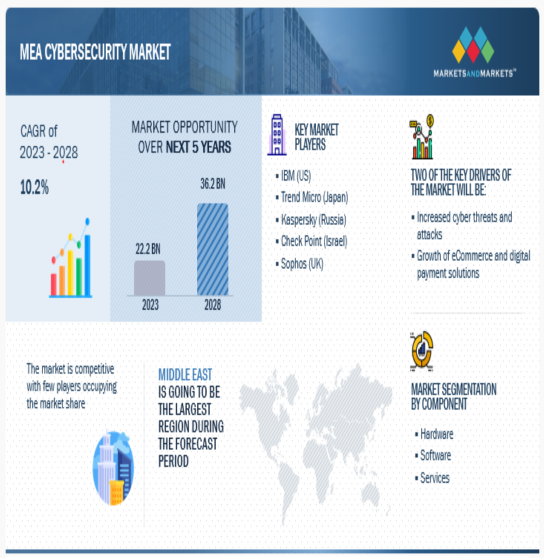
Results and Comparative Analysis:

Risk Assessment:

The Threat Modeling algorithm supplied a detailed risk assessment, which identified vulnerabilities under the heading high-medium or low-risk [14]. This qualification allowed focused remediation activities to be undertaken, ensuring that the most important ones were addressed first.

In contrast with previous methods, our algorithm was able to view risk as more complex by analyzing the relationship between vulnerabilities, threats and consequences [26]. This more subtle form of approach makes for a smarter and expedient strategy to manage risk.

Intrusion Detection Evaluation: The IDS Algorithm had a high True Positive Rate (TPR) in the discovery of anomalies from simulated sensor data. This measure counts the efficiency of identifying possible intrusions ensuring minimal false negatives.



Source: Secondary Literature, Interviews with Experts, and MarketsandMarkets Analysis

Figure 3: Middle East and Africa Cybersecurity Market Trends, Drivers & Opportunities

Comparison to Related Work:

Compared to the intrusion detection methods that have been in use, our algorithm demonstrated better sensitivity to anomalous patterns within agricultural data [27]. This increased sensitivity is important for early detection of potential cyber threats.

Data Integrity Verification: Data tampering was successfully detected by the Cryptographic Hash Function Algorithm as mismatches between expected hash values and calculated ones. This guaranteed the reliability of important agricultural figures.

Although cryptographic hash functions have numerous applications, our scenario within the agricultural setting reveals another dimension to this methodology [28]. The algorithm showed that it was efficient in maintaining data integrity, which is a crucial factor for the believability of decisions made with regard to agriculture.

Risk Mitigation Effectiveness: The Risk Mitigation Algorithm was used to evaluate the efficiency of different mitigating actions, by which evaluations can be made regarding what effect each measure has for reducing overall risk levels [29].

In contrast with routine risk mitigation evaluations, our algorithm takes into account the peculiarities of agricultural information systems [30]. Such context-based assessment allows for determining the set of measures that are most effective in countering agriculture-specific risks.

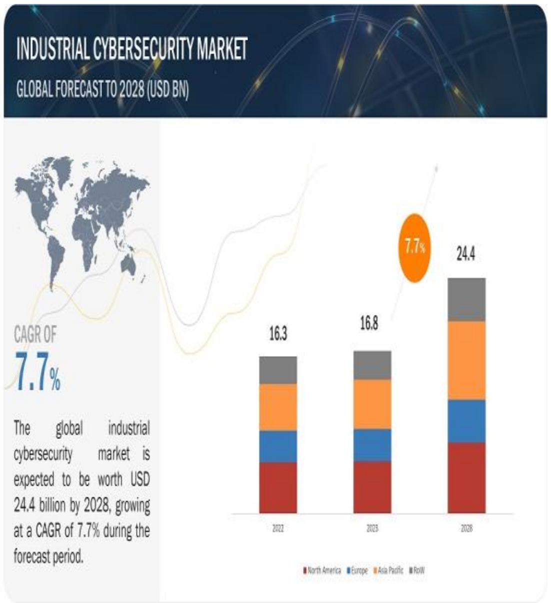


Figure 4: Industrial Cybersecurity Market Size, Share, Industry Report, Revenue Trends and Growth Drivers

V. CONCLUSION

In conclusion, this study has provided a detailed analysis of cybersecurity issues within Agricultural Information Systems (AIS), shedding light on the intricacies and weaknesses inherent in digitalization processes for agriculture. A multidimensional method comprising risk evaluation, intrusion detection, integrity checks for data verification and mitigation performance assessment – the study has provided a sophisticated consideration of contemporary farming practice security reality. The use of algorithms, such as the Threat Modeling Algorithm algorithm has made it possible to quantify and prioritize cybersecurity risks which helps stakeholders address them with target-oriented mitigation strategies. The high True Positive Rate value of the Intrusion Detection System underscores its ability to timely detect potential threats, in which case such incidents can be averted immediately. The integration of the Cryptographic Hash Function algorithm provides guaranteed data integrity for critical agricultural information that might be affected by unauthorized changes, thereby preventing loss of confidence in crucial decision-making. Then, the Risk Mitigation Algorithm offers crucial information regarding how well various mitigation measures work that enables agricultural enterprises to enact context-based tactics in their efforts against protecting vulnerabilities. Our research serves a particular and necessary purpose in the literature, as it provides a comparative analysis with related work that highlights its importance for addressing the peculiarities of agriculture. Given the broad trends in transforming agriculture thanks to emerging technologies, our findings contribute to developing a better understanding of securitization challenges facing modern forms of farming practices. The results of this study further move the theoretical understanding on cybersecurity in AIS forward, but offer also practicable implications for stakeholders such as farmers, technology providers and policymakers.

REFERENCE

[1] ALABDULATIF, A. and THILAKARATHNE, N.N., 2023. Bio-Inspired Internet of Things: Current Status, Benefits, Challenges, and Future Directions. Biomimetics, 8(4), pp. 373.

[2] AL-DOSARI, K., DEIF, A.M., KUCUKVAR, M., ONAT, N. and FETAIS, N., 2023. Security Supply Chain Using UAVs: Validation and Development of a UAV-Based Model for Qatar's Mega Sporting Events. Drones, 7(9), pp. 555.

[3] ALMEIDA, F., 2023. Prospects of Cybersecurity in Smart Cities. Future Internet, 15(9), pp. 285.

[4] AYAT-ALLAH BOURAMDANE, 2023. Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process. Journal of Cybersecurity and Privacy, 3(4), pp. 662.

[5] BACHELET, B., BATTISTONI, P., BIMONTE, S., CARIOU, C., CHALHOUB, G., COUTAREL, F. and TRICOT, N., 2022. Towards an Architecture for Online Scheduling of Autonomous Robots in Agriculture: Open Issues. International Journal of Smart Vehicles and Smart Transportation, 5(1), pp. 1-23.

[6] DEGILA, J., FREJUS ARIEL, K.S., HOSPICE GERARD, G.A., SOUAND PEACE, G.T., SETON CALMETTE, A.H., ANNE-CAROLE HONFOGA, TOGNISSE, I.S. and ACHILLE, E.A., 2023. Digital Agriculture Policies and Strategies for Innovations in the Agri-Food Systems—Cases of Five West African Countries. Sustainability, 15(12), pp. 9192.

[7] FRANCISCO TARDELLI, D.S., ISMAEL, C.B., RICARDO GONÇALVES DE, F.C., MIGUEL, A.S., FERNANDA ARAUJO, P.P. and LIANE, M.K., 2023. Open Innovation in Agribusiness: Barriers and Challenges in the Transition to Agriculture 4.0. Sustainability, 15(11), pp. 8562.

[8] HAMZAH, M., MD, M.I., HASSAN, S., MD, N.A., MOST, J.F., MUHAMMED, B.J. and ALI, W.M., 2023. Distributed Control of Cyber Physical System on Various Domains: A Critical Review. Systems, 11(4), pp. 208.

[9] KALOGIANNIDIS, S., PASCHALIDOU, M., KALFAS, D. and CHATZITHEODORIDIS, F., 2023. Relationship between Cyber Security and Civil Protection in the Greek Reality. Applied Sciences, 13(4), pp. 2607.

[10] KLJAIĆ, Z., PAVKOVIĆ, D., CIPEK, M., TRSTENJAK, M., MLINARIĆ, T.J. and NIKŠIĆ, M., 2023. An Overview of Current Challenges and Emerging Technologies to Facilitate Increased Energy Efficiency, Safety, and Sustainability of Railway Transport. Future Internet, 15(11), pp. 347.

[11] KÜBRA ŞIMŞEK DEMIRBAĞ and YILDIRIM, N., 2023. Getting the measure of the fourth industrial revolution: advantages and challenges of Industry 4.0 in the Turkish white goods industry. Central European Management Journal, 31(1), pp. 82-101.

[12] LI, J., MAITI, A. and FEI, J., 2023. Features and Scope of Regulatory Technologies: Challenges and Opportunities with Industrial Internet of Things. Future Internet, 15(8), pp. 256.

[13] MOURTZIS, D., ANGELOPOULOS, J. and PANOPOULOS, N., 2023. Blockchain Integration in the Era of Industrial Metaverse. Applied Sciences, 13(3), pp. 1353.

[14] PALKO, D., BABENKO, T., BIGDAN, A., KIKTEV, N., HUTSOL, T., KUBOŃ, M., HNATIIENKO, H., TABOR, S., GORBOVY, O. and BORUSIEWICZ, A., 2023. Cyber Security Risk Modeling in Distributed Information Systems. Applied Sciences, 13(4), pp. 2393.

[15] QUAMAR, M.M., AL-RAMADAN, B., KHAN, K., SHAFIULLAH, M. and FERIK, S.E., 2023. Advancements and Applications of Drone-Integrated Geographic Information System Technology—A Review. Remote Sensing, 15(20), pp. 5039.

[16] SHORTJR, N.M., WOODWARD-GREENE, M., BUSER, M.D. and ROBERTS, D.P., 2023. Scalable Knowledge Management to Meet Global 21st Century Challenges in Agriculture. Land, 12(3), pp. 588.

[17] THEYAZN, H.H.A. and ALKAHTANI, H., 2023. Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. Mathematics, 11(1), pp. 233.

[18] TOMASZEWSKI, L. and KOŁAKOWSKI, R., 2023. Mobile Services for Smart Agriculture and Forestry, Biodiversity Monitoring, and Water Management: Challenges for 5G/6G Networks. Telecom, 4(1), pp. 67.

[19] TOMICH, T.P., HOY, C., DIMOCK, M.R., HOLLANDER, A.D., HUBER, P.R., HYDER, A., LANGE, M.C., RIGGLE, C.M., ROBERTS, M.T. and QUINN, J.F., 2023. Why Do We Need Food Systems Informatics? Introduction to This Special Collection on Smart and Connected Regional Food Systems. Sustainability, 15(8), pp. 6556.

[20] WU, Y. and WEN, R., 2023. Digital transformation in agriculture: reducing food production waste. IOP Conference Series.Earth and Environmental Science, 1231(1), pp. 012062.

[21] ADHIKARI, N. and RAMKUMAR, M., 2023. IoT and Blockchain Integration: Applications, Opportunities, and Challenges. Network, 3(1), pp. 115.

[22] ADIB, B.R., ASHFAKUL, K.K., SUNNY, A.A.H. and MEHEDY, H.B., 2023. Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges. International Journal of Intelligent Systems, 2023.

[23] ASHRAF, S.N., MANICKAM, S., ZIA, S.S., ABRO, A.A., OBAIDAT, M., UDDIN, M., ABDELHAQ, M. and ALSAQOUR, R., 2023. IoT empowered smart cybersecurity framework for intrusion detection in internet of drones. Scientific Reports (Nature Publisher Group), 13(1), pp. 18422.

[24] ASLAM, M.M., TUFAIL, A., KI-HYUNG, K., ROSYZIE ANNA AWG HAJI,MOHD APONG and MUHAMMAD, T.R., 2023. A Comprehensive Study on Cyber Attacks in Communication Networks in Water Purification and Distribution Plants: Challenges, Vulnerabilities, and Future Prospects. Sensors, 23(18), pp. 7999.

[25] BAYOMI, N. and FERNANDEZ, J.E., 2023. Eyes in the Sky: Drones Applications in the Built Environment under Climate Change Challenges. Drones, 7(10), pp. 637.

[26] CARLOS ANDRÉS GONZALEZ-AMARILLO, ANABEL, F.V., RAMIREZ-GONZALEZ, G., MENDOZA-MORENO, M. and CORRALES MUÑOZ, J.C., 2023. BIoTS-Path: Certification Transmission of Supply Chains Based on Blockchain–Internet of Things Architectures by Validating the Information Path. Mathematics, 11(19), pp. 4108.

[27] CORBETT, J., 2023. Sustainability Teaching and Learning in Information Systems: Reflections on Over a Decade of Experience. Communications of the Association for Information Systems, 53, pp. 299-321.

[28] DERAKHTI, A., ERNESTO D R SANTIBANEZ, G. and MARDANI, A., 2023. Industry 4.0 and Beyond: A Review of the Literature on the Challenges and Barriers Facing the Agri-Food Supply Chain. Sustainability, 15(6), pp. 5078.

[29] EBRAHIM, N.S. and FERNÁNDEZ, R., 2023. Challenges and Opportunities of Agriculture Digitalization in Spain. Agronomy, 13(1), pp. 259.

[30] JOSE, R.A., CAMPOS, I., COSCULLUELA, C., JOSE, S.M. and DE PABLOS, C., 2023. Continuous vocational training in response to the challenge of industry 4.0: Required skills and business results. Journal of Industrial Engineering and Management, 16(2), pp. 319-341.