Article

Cybersecurity Resilience for Low-Income Farmers in Developing Nations: An Asset-Dependency Risk Assessment Inspired by Bayesian Networks

Kossi D Bissadu [1,*], Leela Pavani Velagala [1,*] and Gahangir Hossain [2]

[1] Information Science Department, College of Information, University of North Texas, Denton 76203, United States
[2] Data Science Department, College of Information, University of North Texas, Denton 76203, United States
* Correspondence: bissadukossi02@gmail.com (K.D.B.); leelapavanivelagala@my.unt.edu (L.P.V.)

Abstract

Low-income farmers in developing nations face cybersecurity risks when adopting digital agriculture. This article presents an asset-based assessment that combines an Asset Added Value Tree with a Bayesian-network-inspired dependency graph and expert-derived influence weights. Individual asset risk scores are propagated through the dependency structure using a deterministic weighted aggregation; the approach does not estimate conventional Bayesian conditional probability tables or perform full probabilistic inference. We applied the method to the "Ferme-Ecole" project in Tsevie, Togo. The case study identified elevated scores for configuration data and data storage, and risks associated with personnel interactions. A comparison with previously published fuzzy cognitive map results for 12 common assets yielded an MAE of 0.1467, an RMSE of 0.2051, a Pearson correlation of 0.5129, and 75% qualitative risk-category agreement. These measures describe agreement between model outputs, not predictive accuracy. The assessment was conducted at one farm with five experts and without observed cybersecurity incidents as ground truth. Accordingly, the results illustrate feasibility in the studied setting but do not establish cost-efficiency, general effectiveness, or transferability to other farms.

Keywords: Agricultural Cybersecurity; Cybersecurity Risk Assessment; Smart Farming; Asset Dependency Analysis; Bayesian-Network-Inspired Modeling; Smallholder Farmers.

Citation: Bissadu, K.D.; Velagala, L.P.; Hossain, G. Cybersecurity Resilience for Low-Income Farmers in Developing Nations: An Asset-Dependency Risk Assessment Inspired by Bayesian Networks. *Impact in Agriculture* **2026**, *2*, 10. https://doi.org/10.65500/agriculture-2026-010

Received: 26 July 2026 | Revised: 1 November 2026 | Accepted: 3 November 2026 | Published: 6 November 2026

Copyright: © 2026 by the authors. Licensee Impaxon, Malaysia. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Global food demand is expected to increase by 70% by 2050 to meet the needs of an estimated population of 10.1 billion [1]. It was argued that farmers will need to produce more food than the combined output of all farmers since the inception of the agricultural revolution approximately 10,000 years ago [2]. According to [1], more than 27% of the global population depends directly on agriculture for their livelihoods. Sustainable, resilient, and human-centered agriculture, often associated with the emerging Agriculture 5.0 paradigm, increasingly integrates internet-connected farming systems in which humans interact with sensors, decision-support systems, communication networks, software applications, data-processing systems, and other cyber-physical components [1], [3]. This digital transformation enables farmers to optimize their resource utilization and operations, monitor environmental conditions, and improve production management [2], [4], [5]. This offers many benefits and opportunities for farmers and food security, including enhanced productivity,

resilience, and reduced economic and social inequalities [4], [6].

Despite these potential benefits, digital farming exposes farmers to many cyber threats, especially low-income farmers in developing countries [7], [8]. Figure 1 presents the evolution of agriculture from Agriculture 1.0 to Agriculture 5.0 and its related cybersecurity landscape. These cyberthreats can compromise farm monitoring activities, disrupt operations and undermine the reliability of agricultural decision making [9]

Cybersecurity risk assessment is therefore a critical part of digital agriculture. However, assessing cybersecurity risks should not only focus on individual technological vulnerabilities but also functional dependencies among assets. A compromised asset may affect the reliability of other dependent assets or processes.

Low-income farmers face particular cybersecurity challenges in digital agriculture because of financial constraints, limited cybersecurity expertise, inadequate technical support, and other barriers. These limit conventional cybersecurity risk assessment, especially the estimation of threat likelihoods and potential impacts.

Previous research has examined cybersecurity assessment techniques for digital agriculture. [8] provide a broad understanding of the vulnerabilities and security challenges associated with agricultural technologies, but do not establish a quantitative method for aggregating cybersecurity risk across dependent agricultural assets. [9] conducted a similar investigation but did not develop an analytical framework to translate asset-specific security conditions and functional dependencies into comparable risk scores. Other studies proposed structured threat modeling [10], [11], [12] , quantitative approaches [13], [14] but their application contexts differ from the low-income agricultural environments. Other scientific investigations have proposed and developed cybersecurity risk assessment methods for digital agriculture [9], [11], [15], often relying on standard frameworks (e.g., NIST, IEC) and methodologies [13], [16]. However, applying these approaches can be resource-intensive and costly, creating barriers for low-income farmers in developing countries seeking to adopt sustainable, resilient, and digital farming technologies.

Fuzzy cognitive maps (FCMs) provide another approach [16] but their computational formulation differs from the directed asset-dependency aggregation implemented in the present study. [17] examined cybersecurity resilience for low-income farmers in developing nations through FCM-based risk assessment at Ferme-Ecole in Tsevie, Togo, providing a directly relevant methodological and empirical comparison for this study. However, the present study differs in its explicit use of an Asset Added Value Tree to organize functional asset dependencies, the representation of these dependencies in a Bayesian-network-inspired directed graph, and the calculation of dependency-adjusted risk scores through deterministic aggregation of normalized expert influence weights.

Existing studies have explored cybersecurity threats, risk assessment, and dependency modeling in digital agriculture. However, threat-based approaches primarily focus on identifying vulnerabilities, while conventional Bayesian networks require conditional probability data that may be unavailable in resource-constrained environments. Fuzzy cognitive maps (FCMs) offer an alternative for modeling interconnected risks but differ from directed asset-dependency approaches in their representation and aggregation of risk.

This study addresses the need for asset-dependency risk assessment combining an asset hierarchy, expert-derived influence weights, and deterministic aggregation without historical incident probabilities.

To address this gap, the study combines an Asset Added Value Tree and a Bayesian-network-inspired directed graph for asset-dependency cybersecurity risk assessment. It includes seven steps: asset and threat identification, individual risk computation, dependency modeling, aggregated risk calculation, and classification by asset criticality. The Asset Added Value Tree defines agricultural asset hierarchies, while the directed graph represents dependencies. Normalized expert-derived influence scores support deterministic risk aggregation.

The main objective of this research is to explore an asset-dependency cybersecurity risk method for a resource-constrained digital agriculture. Specifically, the study aims to:

- Develop an asset-based cybersecurity risk assessment method by modeling asset dependencies using Asset Added Value Tree and a Bayesian-network-inspired graph.
- Evaluate the proposed method and compare the results with those of the previous FCM-based study

The main scientific contributions include:

- Combining asset hierarchies, directed dependency modeling, and deterministic risk aggregation.
- Incorporating relationships among interconnected agricultural assets into risk computations.
- Demonstrating the proposed approach using a real-world agricultural case study.

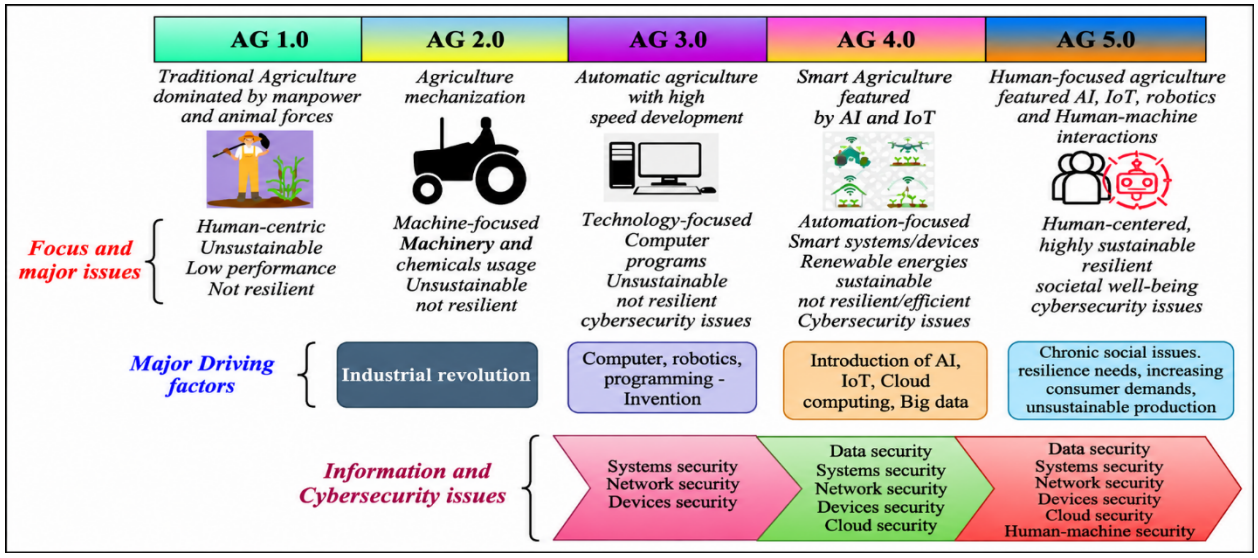


Figure 1. Evolution of Agriculture from Agriculture 1.0 to Agriculture 5.0.

2. Materials And Methods

2.1. Proposed cybersecurity risk assessment method

Our proposed seven-step assessment process is described as operationally lightweight in the limited sense that it uses an asset inventory, a structured questionnaire, and expert judgments rather than historical incident-frequency data. No measurements of assessment time, staffing hours, memory use, hardware requirements, computational cost, or monetary expenditure were collected. Consequently, operational efficiency, cost-efficiency, and scalability remain unverified. The output of one step becomes the input of the next step, as presented in Table 1.

2.1.1. Asset identification

The farm asset inventory was developed through consultation with farm leadership and the technical team, including the farm IT staff.

2.1.2. Threats and existing countermeasures identification.

The asset-based threat identification method enables the identification of potential threats that could affect the farm's information assets. We identified potential threats to each asset and their corresponding existing countermeasures through available resources and literature surveys, and combining methods from [3], [8], [18], [19]. Farm resources and interviews provided additional data for identifying threats and existing countermeasures aimed at mitigating them. After identifying the threats, each threat was mapped to the asset(s) it could directly affect, establishing explicit traceability between the identified threats and the subsequent asset-level risk assessment.

Table 1. Steps involved in the proposed method, their inputs, and outputs.

Steps	Step name	Input(s)	Output(s)
1	Assets identification	-Farm information system topology/architecture documents, - Asset inventory, -Discussion report with the farm leadership	-List of farm digital assets -Asset categories
2	Threats and existing countermeasures identification	-List of farm digital assets -Farm digital topology -Literature survey -Available resources	-List of threats to each identified asset -Existing countermeasures to the identified threats

Steps	Step name	Input(s)	Output(s)
3	Risk calculation for individual assets	- Farm asset vulnerabilities list - Implemented countermeasures	Risk value for each asset
4	Added Value Tree	- Asset list - Asset relationship	Added Value Tree
5	Bayesian-inspired network building	Added Value Tree	Normalized dependency influence weights
6	Aggregated risk computation	- Normalized dependency influence weights -Individual asset risk	Aggregated risk
7	Risk level identification	- Aggregated risk - Risk matrix - Asset criticality	Risk levels for each asset or asset class

2.1.3. Risk computation for individual assets.

This step involves analyzing farm vulnerabilities and assessing the effectiveness of existing countermeasures using a structured questionnaire. The questionnaire was developed to assess the security characteristics and implemented cybersecurity countermeasures of the identified assets and to elicit expert judgments regarding dependencies among the assets. Before its final use, the researchers submitted the initial version of the questionnaire to the expert panel for review and validation. The experts evaluated the relevance, technical appropriateness, clarity, and applicability of the questionnaire items to the cybersecurity assessment of the studied agricultural system. Based on the experts' feedback, the researchers revised the questionnaire and subsequently used the revised version for the assessment. This iterative expert-review process provided content and technical validation before the questionnaire was applied.

The questionnaire was designed to assess distinct technical cybersecurity characteristics and asset relationships rather than multiple indicators of a single latent construct. Consequently, conventional psychometric construct-validation procedures, such as factor analysis, and internal consistency measures, such as Cronbach's alpha, were not considered appropriate for the complete instrument. Instead, we addressed questionnaire validity through expert review of content and technical relevance and evaluated the consistency of the resulting expert judgments using inter-rater reliability analysis.

Five experts with backgrounds in agriculture and cybersecurity reviewed the questionnaire and provided assessments of implementation conditions, importance, and dependency influence.

For each asset, one mutually exclusive implementation category is selected for each applicable security feature. Its corresponding numerical risk value is used in Equation (1), together with the normalized importance weight assigned to that feature. The risk for each individual asset (IAR) is calculated using formula (1), which incorporates the implementation level values l_{ij} assigned to k security features, where $i = 1, \dots, k$ and $j = 1, \dots, n$. Each implementation level is represented by a binary value of either 1 or 0, indicating the presence or absence of the implementation. Therefore, $l_{ij} = 1$ if the $j-th$ implementation level of the $i-th$ security feature is present for an asset, otherwise, $l_{ij} = 0$.

$$IAR = \frac{1}{W}\sum_{i=1}^{k} w_i \sum_{j=1}^{n} C_{ij} l_{ij} + \varepsilon \qquad (1)$$

With $W = \sum_{i}^{k} w_i$ and ε = risk adjustment value to account for the location of the asset.

Equation (1) defines a weighted additive security-condition score plus a physical-access adjustment ε. Feature risk values and importance weights reflect expert judgments, not empirically calibrated incident likelihoods. The feature weights are normalized so that their sum is one.

$$w_j \geq 0 \; ; \; \sum_{j=1}^{m} w_j = 1$$

Based on expert assessment, three physical-access conditions were considered:

- $\varepsilon = 0$ for no physical access for non-authorized users
- $\varepsilon = 0.05$ for limited physical access for non-authorized users.
- $\varepsilon = 0.1$ for easy physical access for non-authorized users.

The three ε values (0, 0.05, 0.10) are illustrative expert-defined scenarios for no, limited, and easy unauthorized

physical access; they are not independently validated coefficients. The adjustment can materially change the score and should not be interpreted as an estimated physical-attack probability. Consequently, $\varepsilon \in [0, 0.10]$, and increasing ε produces a monotonic increase in IAR while leaving the relative contributions of the security-feature weights unchanged. This assumption is further examined through sensitivity analysis. Table 2 shows an example of a questionnaire used to collect the inputs required to compute individual asset risks.

Table 2. Sample questionnaire used to collect countermeasures implemented and their weights.

Security feature C_i	j=1	l_{i1}	j=2	l_{i2}	J=3	l_{i3}	w_i
SSL use for communication	Yes	0.0	No	1.0	Cannot verify	0.5	1.0
Antivirus use	Yes	0.1	No	0.9	Limited use	0.4	0.6
Password encryption in local database	Yes	0.0	No	0.9	Weak key	0.5	1.0

Assuming an agricultural farm implements SSL communications for asset A, installs antivirus for the asset, and uses weak data encryption for its transmitted and stored data. Asset A has no physical access for non-authorized users. The IAR value for the asset is computed as follows:

$$IAR = \frac{1}{(1.0 + 0.6 + 1.0)}(1.0 * (1 * 0) + 0.6 * (0.1 * 1) + 1.0 * (0.5 * 1)) + 0 = 0.2154$$

The calculated IAR for Asset A is approximately 0.2154, indicating the weighted security-condition risk under the assumed implementation levels and physical-access conditions. This value is used as the baseline for the sensitivity analysis presented in Table 3, where variations in the physical-access adjustment factor and selected security-feature weights are examined.

2.1.4. Sensitivity analysis of the individual asset risk

The sensitivity analysis varies ε from 0 to 0.10 and selected expert-derived feature weights while renormalizing weights. Table 3 reports effects on the individual asset risk (IAR) for an illustrative baseline of 0.2154.

For ε, because it is additive, the mathematical sensitivity is particularly straightforward.

If:

$$IAR = \sum_{j=1}^{m} w_j x_j + \varepsilon,$$

Then:

$$\frac{\partial IAR}{\partial \varepsilon} = 1.$$

The local sensitivity of IAR to the physical-access adjustment factor is obtained from $\partial IAR/\partial \varepsilon = 1$. Thus, holding all other parameters constant, an increase of 0.01 in εincreases IAR by 0.01. The relationship is linear and monotonic over the specified interval $0 \leq \varepsilon \leq 0.10$.

For a security-feature weight:

$$\frac{\partial IAR}{\partial w_j} = x_j.$$

Similarly, before weight renormalization, the local sensitivity of IAR to the weight assigned to security feature j is $\partial IAR/\partial w_j = x_j$. Consequently, changes in the weights associated with security features having higher implementation-related risk values have a greater effect on IAR. Table 3 presents a sample of the sensitivity analysis of the IAR computed.

For the illustrative baseline in Table 3, varying ε from 0 to 0.10 changes IAR from 0.2154 to 0.3154 (46.43% relative increase), showing that the physical-access assumption can materially affect scores. Changes in selected feature weights also alter IAR. These are local input-sensitivity results only; they do not establish robustness of final aggregated scores, asset rankings, or risk classifications.

2.1.5. Construction of asset added value tree (AAT)

The concept of an asset added value tree comes from the need to establish relationships between an asset and its dependent assets. This relationship is crucial because the risk value of an asset that depends on another asset is influenced by the risk profile of the dependent asset. AAT is a hierarchical structure of assets where assets at lower levels contribute value to higher-level assets.

Assets are also classified into functional groups called asset class. Figure 2 provides an example of an asset added value tree. The first digit after the word "Asset" indicates the asset's hierarchical level. Assets at the top level (or first level) depend on assets at the second or middle level, while middle-level assets depend on third-level assets, and so on. The number of levels varies depending on the topology and architecture of the farm's digital assets. Experts build the added value tree using their knowledge and discussions with farm technical teams.

Table 3. Sensitivity analysis of individual asset risk (IAR) to variations in the physical-access adjustment factor and normalized security-feature weights.

Parameter varied	Variation	Parameter value	Resulting IAR	Absolute change from baseline	Relative change
Baseline	—	—	0.2154	—	—
ε	Baseline	0.000	0.2154	0.0000	0.00%
ε	+0.025	0.025	0.2404	+0.0250	+11.61%
ε	+0.050	0.050	0.2654	+0.0500	+23.21%
ε	+0.075	0.075	0.2904	+0.0750	+34.82%
ε	+0.100	0.100	0.3154	+0.1000	+46.43%
SSL weight w_1	−20%	0.80	0.2333	+0.0179	+8.33%
SSL weight w_1	−10%	0.90	0.2240	+0.0086	+4.00%
SSL weight w_1	Baseline	1.00	0.2154	0.0000	0.00%
SSL weight w_1	+10%	1.10	0.2074	−0.0080	−3.70%
SSL weight w_1	+20%	1.20	0.2000	−0.0154	−7.14%
Antivirus weight w_2	−20%	0.48	0.2210	+0.0056	+2.59%
Antivirus weight w_2	−10%	0.54	0.2181	+0.0027	+1.27%
Antivirus weight w_2	Baseline	0.60	0.2154	0.0000	0.00%
Antivirus weight w_2	+10%	0.66	0.2128	−0.0026	−1.21%
Antivirus weight w_2	+20%	0.72	0.2103	−0.0051	−2.36%
Password-encryption weight w_3	−20%	0.80	0.1917	−0.0237	−11.01%
Password-encryption weight w_3	−10%	0.90	0.2040	−0.0114	−5.29%
Password-encryption weight w_3	Baseline	1.00	0.2154	0.0000	0.00%
Password-encryption weight w_3	+10%	1.10	0.2259	+0.0105	+4.89%
Password-encryption weight w_3	+20%	1.20	0.2357	+0.0203	+9.44%

2.1.6. Bayesian-network-inspired asset dependency graph

A conventional Bayesian Network is a directed acyclic graph (DAG) with a conditional probability distribution for each node given its parents. The present implementation uses the DAG to represent asset dependencies but does not elicit or estimate complete conditional probability tables (CPTs). Expert influence scores are converted to normalized relative weights for deterministic aggregation. Thus, the method is Bayesian-network-inspired in its graph structure but does not implement standard BN posterior inference or supply a fully specified joint probability distribution.

An edge from a supporting asset to a dependent asset records an assessed functional dependency. Unlike a conventional BN edge, it is not accompanied by a calibrated conditional probability distribution. Accordingly, the local Markov property and probabilistic factorization of a fully specified Bayesian network cannot be assumed to hold for the implemented deterministic risk computation.

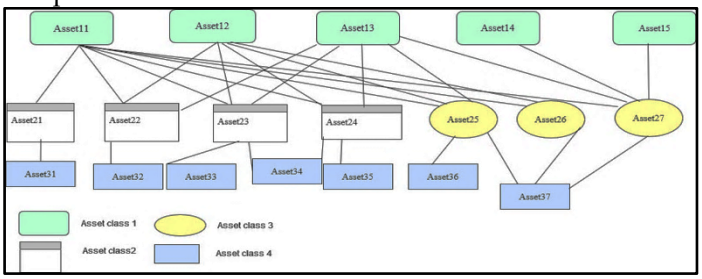


Figure 2. Example of an Asset Added Value Tree comprising four asset classes.

The dependency graph structure is constructed from the asset dependency relationships identified in the added value tree. First, each asset identified in the tree is represented as a node in the graph. Second, the functional dependencies established in the added value tree are translated into directed edges. When the functionality of an

asset depends on a supporting asset, the supporting asset is defined as its parent, and a directed edge is introduced from the supporting asset to the dependent asset. Assets that do not depend on other identified assets are represented as root nodes. Third, the edge directions follow the hierarchical dependency structure of the added value tree, from supporting lower-level assets to the higher-level assets that depend on them. Finally, the strength of each identified parent-child relationship is elicited from the experts using the five linguistic influence levels—no influence, low, moderate, significant, and high—which are mapped to numerical values of 0, 0.25, 0.50, 0.75, and 1, respectively. The numerical values assigned to the five linguistic influence levels were selected as an equally spaced ordinal-to-numerical transformation over the normalized interval. The endpoints represent the absence of an identified influence (0) and the maximum influence considered in the assessment (1), while the intermediate categories are positioned at equal intervals of 0.25.

To assess whether the choice of numerical values for the linguistic influence levels affected the results, we conducted a sensitivity analysis using two alternative monotonic mappings. The baseline scale $\{0, 0.25, 0.50, 0.75, 1.00\}$ was compared with Alternative 1 $\{0, 0.20, 0.50, 0.80, 1.00\}$ and Alternative 2 $\{0, 0.10, 0.40, 0.70, 1.00\}$. We recoded the original expert assessments under each scenario, then aggregated and normalized them using the same computational procedure as the baseline model.

Alternative 1 produced a mean absolute change of 0.0028 and a maximum absolute change of 0.0114 in the normalized influence values, while Alternative 2 produced a mean absolute change of 0.0058 and a maximum absolute change of 0.0236. Spearman rank correlations between the baseline and alternative normalized influence values were 0.997 and 0.994, respectively (Table 4). These results indicate that reasonable modifications of the numerical representation of the linguistic categories produce only small changes in the normalized dependency weights and preserve the overall ordering of the asset-dependency relationships. Therefore, the dependency parameterization is relatively stable at the intermediate normalized-weight level for the mappings examined; effects on final AAR and classifications were not calculated.

A conventional Bayesian network (BN) is represented by a directed acyclic graph $\big(G = (C, E)\big)$, where $(C = C_1, C_2, \ldots, C_n)$ denotes the set of nodes representing random variables associated with agricultural assets, and (E) represents the set of directed edges between these nodes. The joint probability distribution of a fully specified BN can be factorized as shown in Equation (2). This formulation is included for theoretical comparison, as the proposed method does not estimate the conditional probability distributions required for Bayesian inference.

$$P(C_1, C_2, \ldots, C_n) = \prod_{i=1}^{n} P\left(C_i \mid PA(C_i)\right) \quad (2)$$

In Equation (2), $PA(C_i)$ denotes the set of parent nodes of C_i, while $P\big(C_i \mid PA(C_i)\big)$represents the conditional probability distribution of C_i given its parents. This factorization applies to a fully specified Bayesian network. The proposed method does not calculate these conditional probabilities. Instead, the five linguistic influence levels (0, 0.25, 0.50, 0.75, and 1.00) are converted into numerical influence scores and normalized for deterministic risk aggregation. These scores represent expert-assessed dependency importance rather than probabilities of cybersecurity incidents.

Table 4. Sensitivity of normalized dependency weights to alternative linguistic scales

Scale	Numerical mapping	Mean absolute change	Maximum absolute change	Spearman ϱ
Baseline	0, 0.25, 0.50, 0.75, 1.00	—	—	—
Alternative 1	0, 0.20, 0.50, 0.80, 1.00	0.0028	0.0114	0.997
Alternative 2	0, 0.10, 0.40, 0.70, 1.00	0.0058	0.0236	0.994

2.1.7. Aggregated risk computation using normalized influence weights

Aggregated asset risk (AAR) is a deterministic weighted score derived from the individual risk of an asset and the scores of supporting parent assets. Normalized influence weights sum to one across the contributing parent assets.

For example, the risk score of software can be affected by the risk score of supporting hardware. Experts assign each dependency one of five ordered influence levels, mapped to 0, 0.25, 0.50, 0.75, and 1. These nonnegative scores are normalized to form relative contribution weights. No negative influence values are defined in the stated scale.

The resulting weights indicate assessed dependency importance, not the probability of failure or attack.

Mathematically, the dependency relationship between assets c_i and c_j can be represented using an $(m \times m)$ influence matrix $(E = [e_{ij}])$, where (e_{ij})denotes the expert-assessed influence score assigned to the directed edge from $(C_i)to(C_j)$.

In addition to the expert validation of the questionnaire, the consistency of the expert-derived influence assessments was evaluated using Kendall's coefficient of concordance (W). Kendall's W was selected because the same five experts evaluated multiple asset-dependency relationships using an ordered linguistic scale. We coded responses according to the numerical scale used in the model: no influence = 0, low = 0.25, moderate = 0.50, significant = 0.75, and high = 1.00. We excluded self-relationships and relationships with incomplete ratings across the five experts from the agreement analysis, resulting in 51 asset-dependency relationships with complete ratings. The analysis produced a Kendall's coefficient of concordance of $W = 0.739$, with $\chi^2(50) = 184.744$ and $p < 0.001$, indicating strong and statistically significant concordance among the five experts.

The proposed method uses deterministic risk aggregation based on expert-assessed asset dependencies. Influence scores are exponentially normalized into relative weights using Equation (3), which are subsequently used to compute the aggregated asset risk using Equation (4).

$$\bar{e}_{ji} = \begin{cases} 0, & e_{ji} = 0, \\ \dfrac{\exp(e_{ji})}{\sum_{k \in PA(C_i),\, e_{ki}>0} \exp(e_{ki})}, & e_{ji} > 0. \end{cases} \quad (3)$$

In Equation (3), each nonzero parent influence score is transformed and divided by the sum of transformed scores for the same dependent asset. The resulting nonnegative weights sum to one across included parents. They are relative influence weights, not empirically estimated conditional probabilities; zero-influence relationships are excluded from normalization.

$$0 \le \bar{e}_{ji} \le 1$$

$$\sum_{j \in PA(C_i)} \bar{e}_{ji} = 1$$

The aggregated asset risk (AAR) is computed using the normalized influence weights and individual asset risk scores, as expressed in Equation (4), following the aggregation approach discussed in [10].

$$AAR(C_i) = \sum_{j \in PA(C_i)} \overline{e}_{ji}\ IAR(C_j) \quad (4)$$

In Equation (4), $IAR(C_j)$represents the individual risk score of parent asset C_j, while $\bar{e}_{ji}$ denotes its normalized influence weight on dependent asset C_i. The resulting AAR represents a dependency-weighted risk score rather than a probability of compromise. Therefore, it should not be interpreted as a posterior probability obtained through Bayesian inference.

For decision-making, we translated the aggregated risk values into linguistic terms (e.g., very low risk, low risk, moderate risk, high risk, very high risk) based on asset criticality using the guide depicted in Figure 3. By computing risk values with and without all countermeasures, we established a risk-value range uniformly segmented into five intervals: negligible, minor, moderate, major, and catastrophic. We used a risk matrix based on the above information to convert numerical risk values into more human-understandable language for risk analysis and response strategy development.

Asset Criticality	AAR	Negligeable	Minor	Medium	Major	Catastrophic
	<Day	M	H	H	VH	VH
	Day	L	M	H	H	VH
	<Week	L	L	M	H	H
	Week	VL	L	L	M	H
	Month	VL	VL	L	L	M

Figure 3. Risk assessment matrix used for classifying various risk levels

Legend: (VL = Very Low, L=Low, M= Moderate, H= High, VH = Very High)

Recognizing that low-income farmers with limited resources and expertise struggle to accurately assess potential risks to their farm operations, we adopted an asset criticality index to replace financial impact or severity. Asset criticality refers to the allowable downtime that a farm can tolerate for a specific asset. For instance, an attack on an asset involved in hourly irrigation could significantly impact farming operations (e.g., disruption of soil moisture, increased water stress), potentially resulting in near-total loss of plant yield. Assets with the highest criticality have a tolerable downtime of less than a day, whereas less critical assets can withstand downtime of more than a week.

2.2. Application of the Method to a low-income farm called "Ferme-Ecole" of Tsevie in Togo

The proposed method was tested using a small modern farm in Togo, West Africa. It is an agricultural production

and training center that specializes in sustainable agriculture and bio-energies, emphasizing health and environmental protection while integrating social, cultural, demographic, and economic considerations of local populations. Its integrated system comprises the following components:

- Green energy utilization, including solar panels powering the farming system
- Soil and soilless farming for organic product cultivation
- Animal husbandry and fishery operations
- Water management, featuring water recycling with a filtration system for potable water production
- Hybrid dryers for crop drying
- Biodigesters for biogas production
- Agrometeorological stations for data collection
- Technology-driven automated systems for monitoring and action implementation

3. Results

3.1. Architecture, identified assets, and added value tree of "Ferme-Ecole" of Tsevie

To evaluate the overall architecture, we analyzed organizational documents, including architectural, topology, and administrative documents. We also gathered further insights through a questionnaire administered to leadership and IT staff (one individual). Figure 4 illustrates the farm's overall architecture.

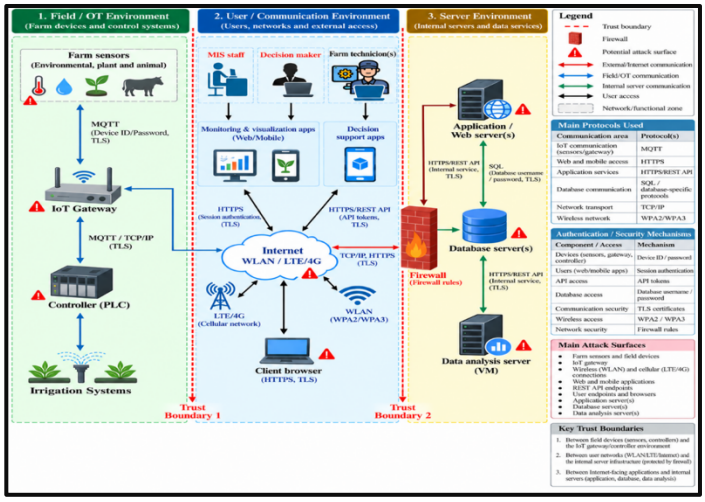


Figure 4. The Overall Architecture of the "Ferme-Ecole" of Tsevie

From a cybersecurity perspective, the Ferme-Ecole architecture can be organized into three main functional environments: the field/operational technology (OT) environment, the user and communication environment, and the server environment. The field/OT environment comprises farm sensors, the IoT gateway, controllers, and irrigation systems. The user and communication environment includes farm technicians, MIS staff, decision makers, client browsers, monitoring and visualization applications, and decision-support applications. The server environment comprises the application/web server, database server, and data-analysis server. Communication among these components is supported by Internet connectivity, WLAN, and LTE/4G, while MQTT is used for IoT-related data exchange, HTTPS and HTTPS/REST APIs are used for communication with web, mobile, and application services, SQL/database-specific protocols are used for database communication, and TCP/IP provides the underlying network communication.

The assets identified from the architecture presented in Figure 4 include:

- Processes: remote monitoring, Actionable decision-making (decision support), and actuation.
- Services: data storage, data transfer, data analysis and visualization, notifications (Email, SMS), and field actuation.
- Data: configuration, input and control data, environmental conditions data, plant/animal data.
- Software: Apache server, data analysis and visualization, sensor software, database, web, and mobile application.
- Hardware: firewall, application server, database server, data analysis server, PLC, gateways, farming machinery.
- Communication: cellular phone protocol (LTE and 4G), WLAN, and internet.
- People: Decision maker(s), farm technicians, Management information system (MIS) staff.
- Cyber-physical infrastructure: buildings, farm management office, etc.

After identifying all assets, the added value tree was constructed by linking lower-level assets (parent nodes) to their corresponding higher-level assets (child nodes) and establishing connections among each asset, as depicted in Figure 5. In this added value tree, risks related to people, software, communication, and hardware influence the risk profiles of the data objects class and services class. Risks related to data objects and services influence the risk profile of all the agricultural processes at the top of the tree hierarchy.

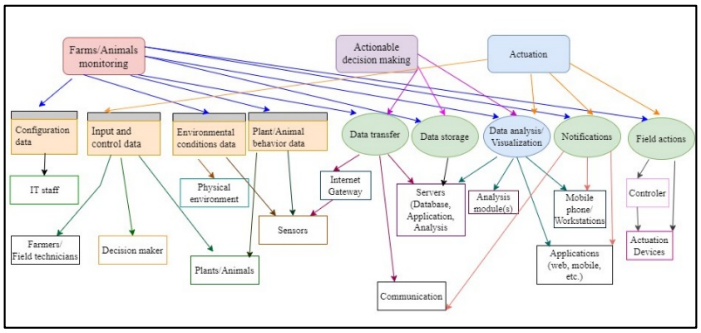


Figure 5. Added value tree hierarchy for "Ferme-Ecole" of Tsevie.

3.2. Threats identified and aggregated risk

In this study, fourteen threat categories were identified based on existing sources. These include viruses and other malware, rogue security software, Trojan software, adware, spyware, ransomware, worms, denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, phishing, rootkits, SQL injection, man-in-the-middle (MitM) attacks, illegal data access, data modification, and data destruction. A comprehensive description of these threats is provided in [11].

To establish the relationship between the identified cybersecurity threats and the assessed assets, a threat–asset matrix was developed, as presented in Table 5. Each of the fourteen threats was mapped to the assets that could be directly exposed to or affected by it. A check mark (✓) indicates an identified direct relationship, while a dash (—) indicates that no direct relationship was identified. The matrix provides traceability between threat identification and asset-level risk assessment but is not used as an additional numerical parameter in the proposed model. Instead, the identified threats inform the evaluation of asset security conditions used to calculate the Individual Asset Risk (IAR). The Aggregated Asset Risk (AAR) is subsequently computed by incorporating the dependency relationships among assets.

Table 5. Threat–Asset Matrix

Threat	Farm & Animal Monitoring	Decision Support	Actuation	Data Storage	Configuration Data	Field Data	Data Analysis	Notifications	Data Transfer	Hardware	Software Module	Sensors	Communication	People
T1 Viruses and Malware	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—	—	✓
T2 Rogue Security Software	✓	✓	—	✓	✓	—	✓	✓	—	✓	✓	—	—	✓
T3 Trojan Software	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	✓
T4 Adware and Spyware	✓	✓	—	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	✓
T5 Ransomware	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	✓	—	—	✓
T6 Worms	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—
T7 DoS/DDoS	✓	✓	✓	✓	—	—	✓	✓	✓	✓	✓	✓	✓	—
T8 Phishing	✓	✓	—	✓	✓	✓	✓	✓	—	✓	✓	—	—	✓
T9 Rootkits	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—
T10 SQL Injection	✓	✓	—	✓	✓	✓	✓	✓	—	—	✓	—	—	—
T11 Man-in-the-Middle (MitM)	✓	✓	✓	—	✓	✓	✓	✓	✓	—	✓	✓	✓	—
T12 Illegal Data Access	✓	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	✓	✓	✓
T13 Data Modification	✓	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	✓	✓	—
T14 Data Destruction	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	✓	✓	—	—

The aggregated risk analysis focuses primarily on the three upper-tier asset classes: processes, data, and services. The computed relative risk scores range from 0.18 to 0.93, with assets at the higher levels of the added value tree generally exhibiting greater aggregated risk. Within the processes class, actionable decision-making recorded the highest risk score (0.61), followed by actuation (0.59) and farm monitoring (0.49), as shown in Figure 6.

Within the data asset class, configuration data recorded the highest aggregated risk score (0.93), followed by input and

control data (0.73), environmental data (0.68), and plant and animal data (0.64). In the services asset class, data storage exhibited the highest aggregated risk score (0.85), followed by field actions. These findings indicate variations in dependency-weighted risk across the assessed assets.

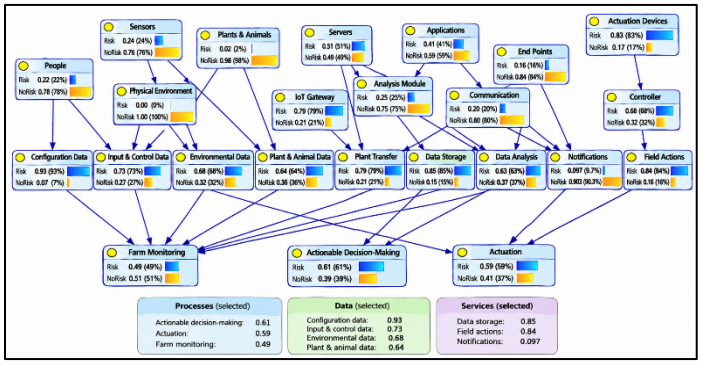


Figure 6. Aggregated asset risk (AAR) scores using dependency-weighted aggregation.

To evaluate whether the selection of numerical values for the linguistic influence levels affected the results, we conducted a sensitivity analysis using two alternative monotonic mappings. We compared the baseline scale {0, 0.25, 0.50, 0.75, 1.00} with Alternative 1 {0, 0.20, 0.50, 0.80, 1.00} and Alternative 2 {0, 0.10, 0.40, 0.70, 1.00}. We recoded the original expert assessments under each scenario, aggregated them, and normalized them using the same computational procedure as the baseline model.

The alternative linguistic mappings changed intermediate normalized influence weights by mean absolute differences of 0.0028 and 0.0058, with maximum differences of 0.0114 and 0.0236, respectively. Spearman correlations with baseline weights were 0.997 and 0.994. These results concern weights only; final AAR, rankings, and category stability were not recomputed from the available information.

3.3. Risk levels identified

Figure 7 shows the qualitative categories assigned to assessed assets using their risk scores and criticality. The highest-scoring assets warrant priority review, especially where personnel interact with configuration and operational data. The categories are relative prioritization outputs, not empirically measured attack probabilities. Notification services received a lower score, but this does not establish immunity from cyber threats.

3.4. Comparison of the results with similar study

The findings from the current study were compared with a similar study conducted by [17]. The authors conducted a similar study using fuzzy cognitive mapping (FCM) approach to assess cybersecurity risk of low-income farmers in developing countries. They used "Ferme Ecole of Tsevie" as a case study. We assessed the effectiveness of our proposed method by comparing its results with those of their study. The comparison was done using three criteria:

1. Variability in the risk values predicted across assets: BN-inspired dependency-weighted scores range from 0.18 to 0.93, whereas the previously reported FCM scores range from 0.50 to 0.68 [17]. The means are 0.614 and 0.615, respectively. Different dispersion does not establish that either method performs better without observed ground-truth risk outcomes.
2. Asset by asset risk values comparison: We compared the AAR values for each asset within their class for both models, as shown in Figure 8. In most cases, the predicted values for both models follow the same trend, except for the data transfer and notification service.
3. Paired comparison of model outputs: The BN-inspired and FCM approaches evaluated the same 12 assets; therefore, paired observations were analyzed. We assessed the normality of the paired differences using the Shapiro–Wilk test ($W = 0.8360$, $p = 0.0247$). Because normality was not supported, we used the two-sided Wilcoxon signed-rank test as the primary comparison ($W = 30.0$, $p = 0.5044$) and report a paired t-test as supplementary analysis ($t(11) = -0.0269$, $p = 0.9790$). Neither test detected a systematic difference at the 0.05 significance level. However, non-significance does not demonstrate equivalence, efficiency, or predictive accuracy. The small sample and potential asymmetry of paired differences limit inference.

Asset	Risk level	Asset criticality
Notifications	Very Low	Month
Input and control data	Moderate	Week
Data transfer	Moderate	Day
Configuration data	High	Week
Data storage	High	Week
Data analysis & visualization	High	Day
Farm monitoring	High	<Day
Decision making	High	Day
Actuation	Very High	<Day
Environmental data	Very High	<Day
Plant & animal data	Very High	<Day
Field actions	Very high	<Day

Figure 7. Risk Level for each Asset identified in the top three asset classes.

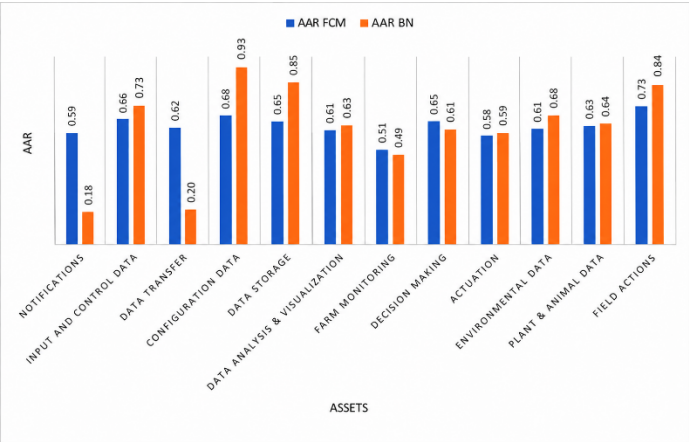


Figure 8. AAR values comparison between FCM and BN techniques

Table 6. Paired statistical comparison of BN-inspired and FCM aggregated asset risk estimates for 12 common assets.

Evaluation metric	Result	Interpretation
Number of paired assets	12	Same assets evaluated by both methods
Mean AAR – FCM	0.6158	Sample SD = 0.0448
Mean AAR – BN-inspired	0.6142	Sample SD = 0.2338
Mean paired difference (BN − FCM)	−0.0017	95% t-based CI: [−0.1378, 0.1345]
Shapiro–Wilk normality test	W = 0.8360; p = 0.0247	Normality of paired differences not supported
Wilcoxon signed-rank test (two-sided)	W = 30.0; p = 0.5044	Primary paired comparison; no detected systematic difference
Paired t-test (supplementary)	t(11) = −0.0269; p = 0.9790	Interpret cautiously given non-normal differences
Mean absolute error (MAE)	0.1467	Mean absolute paired discrepancy
Root mean square error (RMSE)	0.2051	Root mean squared paired discrepancy
Pearson correlation (r)	0.5129	Linear association between outputs
Spearman rank correlation (ϱ)	0.7088	Rank association between outputs

The FCM and BN-inspired mean AAR values were 0.6158 and 0.6142, respectively. The mean paired difference (BN − FCM) was −0.0017 (95% t-based confidence interval: −0.1378 to 0.1345). The recalculated MAE was 0.1467, RMSE was 0.2051, Pearson correlation was 0.5129, and Spearman rank correlation was 0.7088. The corresponding standard deviations were 0.0448 (FCM) and 0.2338 (BN-inspired), indicating greater dispersion of BN-inspired scores. The marked differences for data transfer (0.20 versus 0.62) and notifications (0.18 versus 0.59) illustrate why similar overall means do not imply asset-level equivalence. These agreement metrics compare model outputs, not predictions against observed incidents.

Asset risk level prediction comparison: One key element of risk assessment is providing a human-understandable risk categorization. Therefore, we compared each asset's risk levels across both models. Table 7 shows the comparative results for each asset's risk categorization. The results show that both models agree on 9 of 12 assets, for a 75% agreement rate. The models differ in categorizing 25% of the assets. A thorough analysis shows that disagreement occurs only within the services asset class, with asset risks differing by one level. For instance, BN categorizes notification services risk into the 'very low' risk level, while FCM puts the same asset into the 'low' risk level category, a one-category difference. This difference may reflect differences in how the two models aggregate asset-level risks.

Table 7. Comparison between FCM and BN predictions of asset risk levels

Asset	Risk level BN	Risk level FCM	Asset criticality
Notifications	Very Low	Low	Month
Input and control data	Moderate	Moderate	Week
Data transfer	Moderate	High	Day
Configuration data	High	High	Week
Data storage	High	Moderate	Week
Data analysis & visualization	High	High	Day
Farm monitoring	High	High	<Day
Decision making	High	High	Day
Actuation	Very High	Very High	<Day
Environmental data	Very High	Very High	<Day
Plant & animal data	Very High	Very High	<Day
Field actions	Very high	Very High	<Day

4. Discussion

The proposed method provides a structured representation of the relationships among heterogeneous assets within the agricultural system considered in this case study. Integrating the Asset Added Value Tree and Bayesian

Network represents asset dependencies and associated cybersecurity risks within a common assessment framework. These characteristics suggest the approach may provide an accessible way to support cybersecurity risk assessment in small-scale agricultural environments where specialized cybersecurity expertise and historical incident data are limited [12]. Bayesian Networks also provide a useful framework for representing uncertainty and dependencies among interconnected assets [9],[10].

In the present case study, the proposed approach produced results that showed some agreement with the fuzzy cognitive map method previously applied to cybersecurity risk assessment in a comparable agricultural context [17]. However, these findings should be interpreted within the scope of the Ferme-Ecole case study. The method was evaluated in a single agricultural environment, and several assessment parameters were derived from expert judgments. Therefore, the present results do not establish universal applicability or effectiveness across all small- and medium-sized farms. The framework may be adaptable to other small- and medium-sized agricultural systems with comparable characteristics, but further validation across multiple farms, technological configurations, geographical contexts, and larger expert panels is required before broader generalization can be established.

The method provides an asset inventory, an explicit dependency structure, and a way to prioritize security attention using expert-derived scores. Its graph resembles a Bayesian Network, but the implemented computation lacks CPTs and posterior probabilistic inference. It is therefore more accurately characterized as Bayesian-network-inspired dependency-weighted assessment. Operational resource requirements were not measured, and no claim of demonstrated computational efficiency or cost savings is warranted.

5. Conclusion

This study developed an asset-dependency cybersecurity risk-assessment framework that combines an Asset Added Value Tree with a Bayesian-network-inspired graph and deterministic normalized expert influence weights. Unlike a conventional Bayesian Network, it does not specify full conditional probability tables or calculate posterior probabilities. Its application to the "Ferme-Ecole" of Tsevie, Togo, illustrates relative asset-risk prioritization within one case study.

The case study distinguished risk scores among assets. For the 12 common assets, the inter-model comparison yielded an MAE of 0.1467, RMSE of 0.2051, Pearson correlation of 0.5129, and Spearman rank correlation of 0.7088. The Wilcoxon signed-rank test did not detect a systematic paired difference ($p = 0.5044$); this does not establish model equivalence or predictive accuracy in the absence of empirical incident outcomes.

The reported Kendall's coefficient of concordance $W=0.739$ ($p < 0.001$) for the five experts is a measure of agreement in the assessed dependency rankings, not independent validation of the dependencies. Alternative linguistic scales yielded Spearman correlations of 0.997 and 0.994 for normalized influence weights.

The highest reported scores, including configuration data (0.93) and data storage (0.85), suggest practical priorities. Configuration data warrant restricted administrative access, strong authentication, change control, and staff training; data storage warrants access review, secure backup and recovery procedures, and protection of database credentials. These are proposed mitigations, not interventions tested at the farm. For any control improvement, the scoring framework predicts a change in IAR equal to its normalized feature weight multiplied by the change in the corresponding feature risk value, provided other inputs and ε are unchanged. A numerical before-and-after AAR cannot be reported without the complete asset-specific feature and dependency inputs.

Limitations include a single farm, five experts, one local IT informant, incomplete reporting of individual elicitation records, subjective and uncalibrated feature scores and physical-access adjustments, and no empirical incident ground truth. The method does not implement conventional Bayesian posterior inference. Neither assessment cost nor execution time, memory, hardware requirements, final AAR sensitivity, or countermeasure outcomes were measured. Consequently, claims of efficiency, cost-effectiveness, predictive accuracy, and broad applicability cannot be established.

Future work should disclose the complete expert-level scoring and dependency matrices; recalculate final AAR values, rankings, and categories under parameter perturbations; test the framework against observed incidents; and evaluate performance, assessment time, and cost across multiple farms. The present paired comparison is limited to 12 common assets and should not be interpreted as proof of equivalence.

Author Contributions: K.D.B.: Conceptualization, Methodology, Writing – Original Draft Preparation; L.P.V.: Visualization, Figure Preparation, Manuscript Formatting and Finalization; G.H.: Supervision, Writing – Review and

Editing. All the authors have read and approved the final version of the manuscript.

Funding: This research received no specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data supporting the findings of this study are available from the corresponding author upon reasonable request, subject to applicable copyright restrictions. Third-party copyrighted materials are excluded unless appropriate permissions are obtained from the respective copyright holders.

Acknowledgments: The authors thank the leadership and technical team of "Ferme Ecole" of Tsevie for their availability and support.

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

AI Use Declaration: During the preparation of this manuscript, the authors used ChatGPT (OpenAI) solely for limited language refinement to improve the clarity and readability of selected paragraphs originally written by the authors. All AI-assisted revisions were carefully reviewed and edited to ensure that the intended meaning and scientific accuracy were preserved. The authors take full responsibility for the content, accuracy, and integrity of the manuscript.

References:

1. S. Rudrakar and P. Rughani, "IoT based Agriculture (Ag-IoT): A detailed study on Architecture, Security and Forensics," *Information Processing in Agriculture*, 11.4 (2024): 524-541. https://doi.org/10.1016/j.inpa.2023.09.002.
2. E. D. G. Fraser and M. Campbell, "Agriculture 5.0: Reconciling Production with Planetary Health," *One Earth*, vol. 1, no. 3, pp. 278–280, Nov. 2019, https://doi.org/10.1016/j.oneear.2019.10.022.
3. G. Toader, D. Trifan, L. Rîșnoveanu, C.-I. Enea, A.-I. Ghiorghe, E. Lungu, V. Chiurciu, P. Chițonu, L. Lazăr, and L. Ilie, "From traditional agriculture to digital agriculture (Agriculture 5.0)—Trend, changes, importance," *Research Journal of Agricultural Science*, vol. 53, no. 1, p. 162, 2021.
4. N. Baryshnikova, P. Altukhov, N. Naidenova, and A. Shkryabina, "Ensuring Global Food Security: Transforming Approaches in the Context of Agriculture 5.0," *IOP Conf. Ser.: Earth Environ. Sci.*, vol. 988, no. 3, p. 032024, Feb. 2022, https://doi.org/10.1088/1755-1315/988/3/032024.
5. V. Martos, A. Ahmad, P. Cartujo, and J. Ordoñez, "Ensuring Agricultural Sustainability through Remote Sensing in the Era of Agriculture 5.0," *Applied Sciences*, vol. 11, Art. no. 13, Jan. 2021, https://doi.org/10.3390/app11135911.
6. M. J. Carrer, H. M. D. S. Filho, M. D. M. B. Vinholis, and C. I. Mozambani, "Precision agriculture adoption and technical efficiency: An analysis of sugarcane farms in Brazil," *Technological Forecasting and Social Change*, vol. 177, p. 121510, Apr. 2022, https://doi.org/10.1016/j.techfore.2022.121510.
7. Z. Angyalos, S. Botos, and R. Szilagyi, "The importance of cybersecurity in modern agriculture," *JAI*, vol. 12, no. 2, Jan. 2022, https://doi.org/10.17700/jai.2021.12.2.604.
8. K. Demestichas, N. Peppes, and T. Alexakis, "Survey on Security Threats in Agricultural IoT and Smart Farming," *Sensors*, vol. 20, no. 22, Art. no. 6458, Jan. 2020, https://doi.org/10.3390/s20226458.
9. 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, Art. no. 3520, Jan. 2022, https://doi.org/10.3390/s22093520.
10. Md. R. A. Asif, K. F. Hasan, M. Z. Islam, and R. Khondoker, "STRIDE-based Cyber Security Threat Modeling for IoT-enabled Precision Agriculture Systems," in *2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, Dec. 2021, pp. 1–6. https://doi.org/10.1109/STI53101.2021.9732597.
11. E. Kristen, R. Kloibhofer, V. H. Díaz, and P. Castillejo, "Security Assessment of Agriculture IoT (AIoT) Applications," *Applied Sciences*, vol. 11, no. 13, Art. no. 5841, Jan. 2021, https://doi.org/10.3390/app11135841.
12. G. J. Rosline, P. Rani, and D. Gnana Rajesh, "Comprehensive Analysis on Security Threats Prevalent in IoT-Based Smart Farming Systems," in *Ubiquitous Intelligent Systems*, P. Karuppusamy, I. Perikos, and F. P. García Márquez, Eds., in Smart Innovation, Systems and Technologies. Singapore: Springer, 2022, pp. 185–194. https://doi.org/10.1007/978-981-16-3675-2_13.
13. K. Herland, H. Hämmäinen, and P. Kekolahti, "Information Security Risk Assessment of Smartphones Using Bayesian Networks," *JCSANDM*, Aug. 2015, https://doi.org/10.13052/2245-1439.424.
14. K. Huang, C. Zhou, Y.-C. Tian, W. Tu, and Y. Peng, "Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks," in *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, Nov. 2017, pp. 1–6. https://doi.org/10.1109/ATNAC.2017.8215355.
15. M. Walkowski, J. Oko, and S. Sujecki, "Vulnerability Management Models Using a Common Vulnerability Scoring System," *Applied Sciences*, vol. 11, no. 18, Art. no. 8735, Jan. 2021, https://doi.org/10.3390/app11188735.
16. Szwed, Piotr, and Paweł Skrzyński. "A new lightweight method for security risk assessment based on fuzzy cognitive maps." *International Journal of Applied Mathematics and Computer Science*, vol. 24, no. 1, University of Zielona Góra, 2014, pp. 213-225. https://doi.org/10.2478/amcs-2014-0016.
17. K. Bissadu, G. Hossain, and L. P. Velagala, "A Enhancing Cybersecurity Resilience for Low-Income Farmers in Developing Nations: A Fuzzy Cognitive Mapping Approach," in *2024 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA: IEEE, Jan. 2024, pp. 1–6. https://doi.org/10.1109/ICCE59016.2024.10444324.
18. Kariri, E. "IoT Powered Agricultural Cyber-Physical System: Security Issue Assessment". *IETE Journal of Research,* 1–11. 2022. https://doi.org/10.1080/03772063.2022.2032848
19. K. Kok, "The potential of Fuzzy Cognitive Maps for semi-quantitative scenario development, with an example from Brazil,"

Global Environmental Change, vol. 19, no. 1, pp. 122–133, Feb. 2009, https://doi.org/10.1016/j.gloenvcha.2008.08.003.

Disclaimer: All views, interpretations, and data presented in Impaxon publications are the sole responsibility of the respective authors. These do not necessarily reflect the opinions of Impaxon or its editorial team. Impaxon and its editors assume no liability for any harm or loss arising from the use of information, procedures, or materials discussed in the published content.

Publisher's Note: Impaxon remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.