DOI 10.15622/ia.22.5.5

A.E. ASFHA, A. VAISH

INFORMATION SECURITY RISK ANALYSIS IN FOOD PROCESSING INDUSTRY USING A FUZZY INFERENCE SYSTEM

Asfha A.E., Vaish A. **Information Security Risk Analysis in Food Processing Industry Using a Fuzzy Inference System.**

Abstract. Recently, different attempts have been made to characterize information security threats, particularly in the industrial sector. Yet, there have been a number of mysterious threats that could jeopardize the safety of food processing industry data, information, and resources. This research paper aims to increase the efficiency of information security risk analysis in food processing industrial information systems, and the participants in this study were experts in executive management, regular staff, technical and asset operators, third-party consultancy companies, and risk management professionals from the food processing sector in Sub-Saharan Africa. A questionnaire and interview with a variety of questions using qualitative and quantitative risk analysis approaches were used to gather the risk identifications, and the fuzzy inference system method was also applied to analyze the risk factor in this paper. The findings revealed that among information security concerns, electronic data in a data theft threat has a high-risk outcome of 75.67%, and human resource management (HRM) in a social engineering threat has a low-risk impact of 26.67%. Thus, the high-probability risk factors need quick action, and the risk components with a high probability call for rapid corrective action. Finally, the root causes of such threats should be identified and controlled before experiencing detrimental effects. It's also important to note that primary interests and worldwide policies must be taken into consideration while examining information security in food processing industrial information systems.

Keywords: food processing industry, information security, risk identification, risk analysis, fuzzy inference system, ISO 27005.

1. Introduction. In order to address the problems with nutrition and food security in sub-Saharan Africa, food processing might be extremely important. In actuality, the robustness of the food processing sector directly affects the creation of an abundance of high-quality, wholesome, and secure meals that are accessible to customers and reasonably priced. Processing food is essential to preventing losses after harvest and maximizing harvest usage, especially during drought and seasons of low production, and plays a crucial role in providing income for farmers [1].

In any industry, information is one of the most valuable assets and resources, but it's also the most fragile element, particularly in the food processing industry. It is a value, and every food processing sector has understood that information security threats can negatively affect firm process stability and public image, as well as financial loss, environmental impact, and client and partner satisfaction. Thus, information security applies to the protection of data and information, information systems, and their essential components from unauthorized access, use, exposure, and modification in order to ensure confidentiality, integrity, and availability [2].

In the past, all industries used to be built on mechanical devices and closed systems [3], which meant that most industrial systems were not connected to each other or to public networks such as the Internet. During the risk analysis of these industries, the security-related risks posed by accidental component failures and human errors must be considered. Yet, the scenario is somewhat different now; shifting away from analog or traditional equipment and toward technology offers many advantages in terms of production, but it also has a number of disadvantages [4]. As a result, the most popular sectors are subject to a variety of internal and external security threats, including human, environmental, physical, and natural risks, all of which can have disastrous consequences.

This argument demonstrates that industries are confronting a larger security flaw, an increase in the number and effectiveness of assault scenarios, and increased network complexity [5]. As a result, all industries are confronted with a number of Internet-related concerns, including security risks, intellectual property violations, and personal data privacy. As a result, understanding information security threats in companies is critical in order to prevent future harm.

In reality, in this food processing business, information security risk management is the most important way to reduce losses or damages caused by a variety of security risks. By employing a risk management approach and assuring stakeholders that risks are effectively handled, information security management systems (ISMS) secure the confidentiality, integrity, and availability of information [6].

Therefore, information security risk management aims to protect the security of systems that identify, analyze, and evaluate industrial data, and in order to manage risks, a strategy for assessing the level of risks and identifying potential dangers should exist [7]. Based on ISO 27005, risk analysis is the first step in the risk management process. Evaluating information security risks entails detecting threats and vulnerabilities, calculating the likelihood and impact of known threats, and finally prioritizing the risks to determine the appropriate amount of training and controls needed for effective mitigation [8].

The purpose of this paper is to analyze information security risk in the Sub-Saharan Africa food processing industry information system, and in this study, the authors proposed fuzzy inference system (FIS) methods based on ISO 27005 standards. Inaccuracy and uncertainty in the real world and human thought are modeled by a mathematical technique called fuzzy logic. This essay will demonstrate how fuzzy logic may be used to evaluate risk [9]. In this paper, the authors studied five critical food processing industry assets. Therefore, the five critical assets are briefly characterized

here, such as electronic data, physical hardware, software revenue management systems, food processing industry reputation, or intangible assets, and human resource management (HRM) or employers.

Finally, this paper covers the above-mentioned food industrial assets, the mathematical foundations of fuzzy logic, as well as membership functions, fuzzy sets, and logic rules. Fuzzy expert systems turn input numbers into linguistic values, which are adjusted by if-then rules provided by a human expert. The concept of a fuzzy expert system is explored in detail, along with its rule base and set membership functions.

2. Literature review. Over the years, many studies have been conducted on the topic of information security risk analysis, with various techniques and objectives, but with the fundamental purpose of providing some kind of information about the dangers that could harm an industrial organization's assets. In order to unravel the problem of information security risk analysis, various software packages have been developed based on the developed methods.

There are over 30 methodologies and frameworks that can be used for security risk analysis and assessment. During the risk identification process, potential events are identified based on their positive or negative impact on the main mission goals [10]. Also, the main purpose of the risk analysis is to evaluate the identified risks based on the frequency of their occurrence and their perceived consequences for the mission goals. As a result, one of the most practical methods in this context is to use experts' opinions to identify the rate and potential consequences of risks; thus, after fully recognizing the risks, it is possible to improve opportunities and reduce threats posed by industry risks by implementing risk response strategies [11].

The scenario in information security can be defined as a combination of assets, vulnerability, threat, controls, and consequences [12]. With strong information security, the food processing industry decreases its risk of both inside and outside assaults on information technology systems. They also keep sensitive data safe, protect systems from cyberattacks, provide continuity for the company, and provide peace of mind to everyone in the organization by keeping confidential information safe from security threats.

The risk analysis for seeking goals is very useful due to the definition and nature of risks, and the risk analysis that focuses on examining the effects of risks on industry goals can play a vital role in information security risk management. This, along with risk analysis, is a great help in developing response strategies and reducing unexpected consequences [13]. Accordingly, two general approaches to information security industry risk analysis can be derived by reviewing the existing literature on risk analysis: qualitative and quantitative risk analysis.

To perform a comprehensive assessment of risk in industrial information systems, both quantitative and qualitative methods should be employed. Knowledge of methodology in this area is the prerequisite for accurate risk evaluation, i.e., the combined use of quantitative and qualitative methods ensures more accurate risk estimation [14]. The qualitative method is influenced by subjective judgments and provides poor results for assessing risks because risk analysts mostly depend on their judgments based on their previous knowledge and experiences.

For this purpose and to overcome the inherent limitations in the qualitative approaches to risk analysis, quantitative approaches have been developed, as have various mathematical approaches, for example, fuzzy logic. This method is an advanced model in the information security risk analysis of industrial information systems. Thus, fuzzy logic tools allow us to assess the level of risk using quantitative and qualitative indicators and expert knowledge, whose values are constantly changing over time and which take into consideration the nonlinearity of process growth probabilities and dependability [15].

Fuzzy logic is a type of many-valued logic that deals with approximate reasoning rather than fixed and accurate reasoning, and it is a useful approach to plotting an input space to an output space [16]. It is a type of logic utilized in some expert systems and other artificial intelligence applications in which variables' degrees of truthfulness are represented by a range of values ranging from 0 (false) to 1 (true) [17]. In this way, the membership function of an event on those sets represents the degree to which it belongs to the sets of outcomes and considers a method based on a fuzzy risk matrix that allows expert knowledge to be recorded in an intelligible manner, [18] proves that the fuzzy risk matrix is compatible with the Mamdani fuzzy inference system.

The most important element of risk analysis in the food industry based on fuzzy logic is that the entire process leads to the development of a control system capable of effectively reducing risk. Because of the exact output of analysis and consideration of countermeasures, it can repeat risk analysis on a regular basis with valuable output [19]. Furthermore, it reduced subjectivity to an appropriate standard by using fuzzy logic and methods based on fuzzy logic because of quantitative input data, so subjectivity was moved to the process of creating relations and dependencies between input data and risk assessment, where it could be better controlled [20]. A fuzzy inference engine, a set of fuzzy membership functions, and a set of fuzzy rules are the key elements of a fuzzy expert system. They’re used in a variety of fields, including data analysis, financial systems, pattern recognition, and linear and nonlinear control [21].

Finally, the fuzzy logic approach has been recommended as the appropriate tool to improve food industrial processing information security and may help analyze complex conditions. Thus, the main purpose of this paper is to evaluate risk values in a more reliable, flexible, and objective manner by using this proposed method and prioritizing the level of risk value.

3. Material and Methods. This methodology research was based on ISO 27005, and was completed in 2022. The participants in this study were experts and staff from different sections of the food processing industry in the Sub-Saharan Africa information system (N = 145). The participants were executive management, regular staff, technical and asset operators, and third-party consulting companies.

Participants were asked to evaluate five different information assets based on a scale of ten points (one, two, …. and ten) to estimate the likelihood and severity of the threat and group them into a three-point Likert scale (low, medium, and high) as shown in Table 1. The collected data was analyzed to calculate the likelihood of related threats and their severity. Some specialists in the field of food processing industry information systems confirmed the reliability of the questionnaires. For each question and its corresponding criticality, the average scores were calculated based on the answers of the participants. Finally, all of these average values were used in the FIS model to calculate the final risk values.

Table 1. Likert-scale questionnaires

Likelihood and severity of data collection									
Low			Medium				High		
1	2	3	4	5	6	7	8	9	10

These questionnaires and interviews had three parts, such as:

– Personal information: this is very basic personal information about the participant in the food processing industry;

– The characteristics of systems and the state of information security in the food processing industry's information system (context);

– Risk identification: this part included natural disasters, human threats, and physical and environmental threats.

Based on ISO 27005, the information security risk analysis techniques provide a number of ways. Therefore, it has indicated the following processes.

3.1. Risk Identification Process. The process of recording any hazards that could prevent an organization or program from achieving its goal is known as risk identification. It is the first phase in the risk assessment process, which is used to find, allocate, and describe the types of risks. Therefore, the main goal of risk identification is to determine what,

where, when, why, and how something can impact a company's capacity to operate. All aspects of the risk assessment process are included asset identification and its values, impact level, and threat frequency. This involves eight steps. These steps are:

Step 1. Identify assets and their values. Identifying and valuing food processing industrial assets is a crucial step in determining the appropriate level of protection in the food processing industry. Therefore, an asset's value to any industry, especially the food processing sector, can be quantifiable based on expense, sensitivity, mission criticality, and/or a combination of these factors. In this study, the values of assets were evaluated by executive managers, technical asset operators, and risk management experts in the food processing industry.

Step 2. Threat identification and analysis. A threat is someone, something, an event, or a thought that causes or poses a risk to an asset. By exploiting vulnerabilities or a state of weakness, threats can compromise the confidentiality, integrity, and availability (CIA) of food processing industry assets. Thus, threat analysis is the act of investigating threat detection sources and comparing them to an information system's flaws.

The study's purpose is to identify the threats that could jeopardize an information system in the food processing industry, as the authors noted in the above top five assets in industry information system.

Step 3: Identify the vulnerability and its level. Vulnerability is described as a lack of security in a security system. Threats can take advantage of a vulnerable position because it provides or creates an opportunity for them to do so. The interrelationships between threats and vulnerabilities are examined to determine a likelihood level.

The level of susceptibility is visibly lowered as a high countermeasure is implemented in any manufacturing facility. In this study, just like asset value, the level of vulnerability and threat were evaluated by experts and participants in the food processing industry in Sub-Saharan Africa's information systems.

Step 4. Likelihood. When assessing the likelihood, it needs to be considered how often a specific threat might occur and how easily related vulnerabilities can be exploited. This information can be collected from the food processing industry information system in sub-Saharan Africa through questionnaires and interviews.

The possibility of each situation and its impact occurring must be determined after the incidents have been identified. This can be done using qualitative or quantitative analysis methodologies. The frequency of the threats and the ease with which the vulnerabilities might be exploited should be described.

Step 5. Impact. A degree of loss and harm resulting from some failure might be referred to as event repercussions or impact. Each systemic failure has certain knock-on effects. A failure may result in economic loss, environmental harm, personal injury, or death, among other conceivable outcomes. For various outcome types of facility risk analysis, repercussions need to be quantified using relative or absolute measures.

3.2. FIS process steps. The technique of mapping from a given input set to an output set using fuzzy logic is known as a fuzzy inference system. In our risk assessment model, the Mamdani Fuzzy Inference System (FIS) was employed for fuzzification, rule evaluation, and defuzzification according to Figure 1.

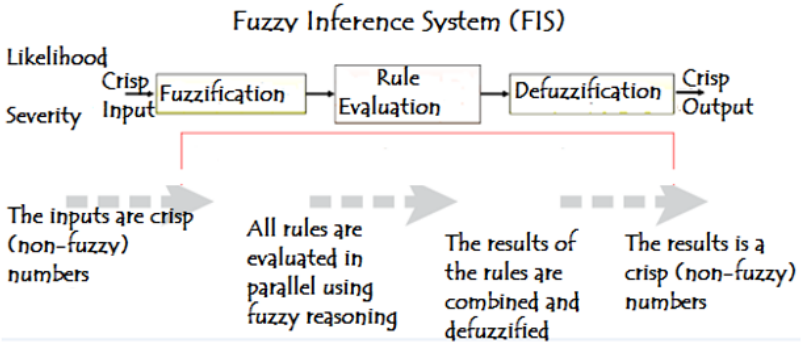

Fig. 1. Risk analysis process based on a fuzzy inference system

Step 6. Fuzzification. The first step is to use membership functions (MF) to assess the inputs' degree of membership in each of the relevant fuzzy sets (fuzzification). In this case, we used MATLAB software to solve all the equations. The fuzzy membership function is a graphical representation of the degree of membership of any value in a particular fuzzy collection. The X-axis of the graph indicates the universe of discourse, while the Y-axis reflects the degree of membership in the range [0, 1]. In this paper, we used Trapezoidal MF (TMF) in likelihood and Gaussian MF (GMF) in severity. TMF has four parameters: “a, b, c, and d”. The Range ‘b’ to ‘c’ represents the element's maximum membership value. And if x is between (a, b) or (c, d), its membership value will be between 0 and 1. A GMF is defined by two parameters, ‘a’ and ‘b’, and can be written as follows: The mean / center of the Gaussian curve is represented by ‘a’ in this function, while the dispersion of the curve is represented by ‘b’.

According to steps 4 and 5, likelihood and ***impact*** (severity) are used as **crisp inputs** to start a FIS process, and the interval range for both indicators is from 0 to 10, as shown in Figure 2.

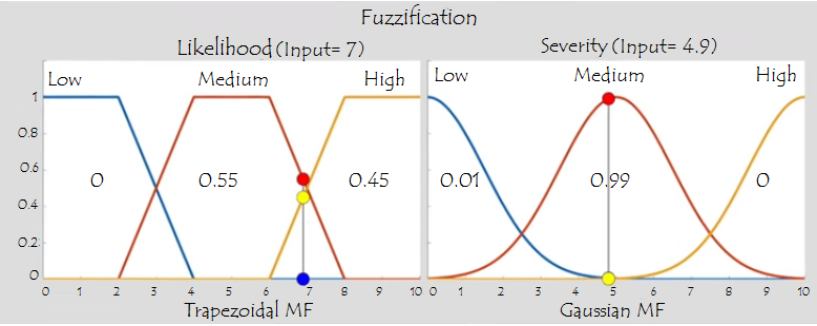

Fig. 2. Fuzzification methods

Step 7. Rule evaluation. Subsequently defining fuzzy membership functions, in this paper, nine fuzzy rules were constructed for the fuzzy inference system (FIS).

Syntax. Based on the Mamdani fuzzy inference system: If (Input 1 is membership function 1) and/or (Input 2 is membership function; 2) then (Output is output membership function). The number of terms used to assess risk variables is assumed to be three, namely *"high", "medium", and "low"* as noted in Table 2.

Table 2. Risk matrix based the above rules

	Severity		
Likelihood	**Low**	**Medium**	**High**
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

Step 7.1. Apply fuzzy operators. After fuzzifying the inputs, you know how well every part of the antecedent fulfills the requirements for each rule. If a rule's antecedent consists of a number of parts, the fuzzy operator is used to generate one number which symbolizes the outcome of the rule's antecedent. This value is subsequently passed on to the output function. The fuzzy operator takes multiple membership values from fuzzified input variables as input. The output consists of a single truth value. In this case, the authors apply the AND operator, as shown below.

Based on Table 2, the authors constructed nine fuzzy rules using the fuzzy operator process.

Rule 1: If likelihood is ***high*** and severity is ***medium*** then risk value is ***high***;

Rule 2: If likelihood is ***medium*** and severity is ***medium*** then risk value is ***medium***;

Rule 3: If likelihood is ***high*** and severity is ***low*** then risk value is ***medium***;

Rule 4: If likelihood is ***medium*** and severity is ***low*** then risk value is ***low***.

Based on Table 2 and Figure 2 membership function, the rules were evaluated in the following process:

Rule 1: Risk value is *high*: $\mu(x_1) = \min(0.45, 0.99) = \mathbf{0.45;}$

Rule 2: Risk value is ***medium***: $\mu(x_2) = \min(0.55, 0.99) = 0.55;$

Rule 3: Risk value is ***medium***: $\mu(x_3) = \min(0.45, 0.01) = 0.01;$

Rule 4: Risk value is *low*: $\mu(x_4) = \min(0.55, 0.01) = \mathbf{0.01;}$

N.B. All other rules have ***zero*** true values. As a result, there is no need to be concerned with them during the composition sub-process.

Step 7.2. Apply Implication Method**.** You must first establish the rule weight before using the implication approach. Every rule has a weight (a value between 0 and 1) that is applied to the antecedent's number. This weight is often 1 and hence has no effect on the implication process. However, you can reduce the impact of one rule compared to the others by changing its weight value from 1 to something else.

The implication approach is used when suitable weighting has been applied to each rule. A consequent is a fuzzy set symbolized by a membership function that properly values the linguistic characteristics assigned to it. The antecedent's function (a single number) is used to alter the consequent. The implication procedure takes a single number from the antecedent and outputs a fuzzy set. The implication is used for each rule, as shown in Figure 3.

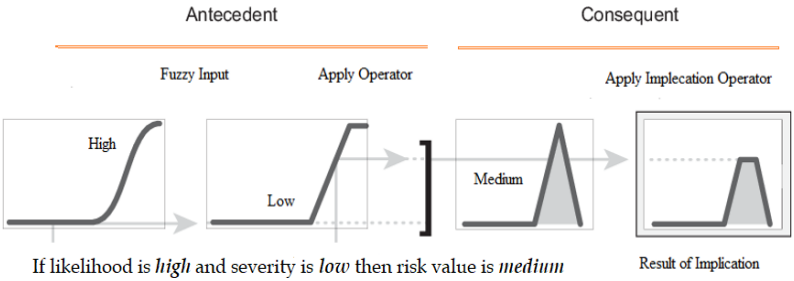

Fig. 3. Implication method

Step 7.3. Aggregate all outputs. The aggregation will be done according to the fuzzy criteria for each risk. The aggregation method seeks to combine all previously scaled and grouped rule consequent MF into a single fuzzy set.

The results of the two rules are alike (as it is for this example: medium), the degree of membership: Based on step 7.2, to be selected OR operator to choice one:

Risk value is ***medium*** = max ($\mu(x_2)$, $\mu(x_3)$) =Max (0.55; 0.01) = **0.55.**

Using the above results:

Risk value is *high*: = **0.45;**

Risk value is *medium* = **0.55;**

Risk value is *low*: = **0.01.**

Step 8. Defuzzification. It is the final step in the fuzzy rule inference model and is used to resolve a crisp value from the results of the FIS process. There are a number of methods available for Defuzzification, for example, max membership principle, centroid method, weighted average method, mean max membership, center of sums, center of largest area, and first or last of maxima. The centroid computation is one of the most used Defuzzification methods**.** In this case, the authors applied the centroid or center of gravity (COG) technique to evaluate the risk value, as shown in Figure 4.

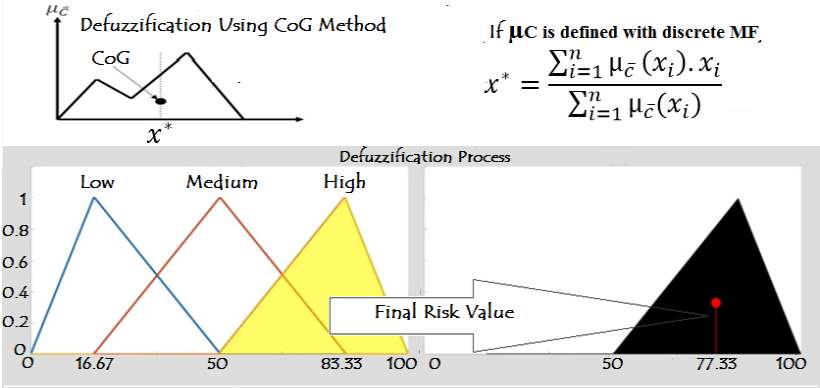

Fig. 4. Defuzzification methods using center of gravity

4. Result and Discussion. This part uses a variety of statistical approaches to evaluate the quantitative data and provide the results of the data analysis in order to test the research hypotheses generated for the current study in the Sub-Saharan Africa food processing industry information system. The response rate of participants is noted in Table 3.

Table 3. Response rate of participant in this study

Questionnaire	Number	Percentage
Distributed	165	100 %
Received	150	90.90%
practical	145	96.67%
Impractical	5	3.33%

Based on Table 3, considering the chosen strategy of handing out the questionnaires to specific individuals one at a time, and 165 were distributed. As a consequence, 145 of the 150 questionnaires received were complete and functional, yielding a response rate of 96.67%, which is regarded as excellent in research using a survey method and is displayed in Table 3. However, 15 employees failed to submit their surveys, and the remaining five – representing 3.33% of the impractical forms – were incomplete and contained inconsistent answers.

In this study, the distribution of participants in Sub-Saharan Africa's food processing industry is shown in Table 4.

Table 4. Distribution of participant in this study

Sex	**Men**		**Female**	
	N = 122, 84.14%		N=23, 15.86%	
Average Age	34.33± 6.79			
Position	Management and Executive Management	Regular Staff	Technical and Asset operators	Third-party consultancy companies
	N=21, 14.48%	N=48, 33.10%	N=67, 46.21%	N=9, 6.21%
Work of experience	=< 2 years	>2 & ≤ 5	>5 & ≤ 10	>10 years
	N=18, 12.41%	N=48, 33.10%	N=67, 46.21%	N=12, 8.28%
Education	Ph.D.	MSc	BSc/Diploma	Vocational and =<High school
	N=7, 4.83%,	N=15, 10.34%	N=50, 34.48%	N=73, 50.34%

Based on Table 4, the majority of respondents had between five and ten years of work experience, which may imply a fair amount of knowledge of the physical security system. The majority of respondents, however, had only completed high school and a vocational program, making up 50.34% of the total and demonstrating a high level of knowledge. A bachelor's degree (BSc) and diploma are the next most common levels of education, coming in at 34.48%, and the Ph.D. level is the least common, at 4.83%.

Additionally, job position data show that workers at the technical and asset operator's personnel level were the most prevalent, totaling 46.21%, followed by "regular staff" at 33.10%, and third-party consultant organizations, the lowest, represented by 6.21% of the total respondents.

According to the risk identification process, the identification of threats for each asset is listed in Table 5.

Table 5. Asset, threat, and vulnerability outcome in this study

Asset Name	Threat Code	Threat	Vulnerability
Electronic Data (ED)	T1	SQL injection	Outdated DBMS
	T2	Data theft	Breaching legal requirements
	T3	User error	Negligence
Physical Hardware (PH)	T4	Power interruptions	Inability to operate without power supply
	T5	Heat	Vulnerability of Processor Chips to melt at high temperatures
	T6	Fire	Vulnerability physical problem/damage
Software Revenue Management System (SRMS)	T7	Cross-site Scripting	Vulnerability to malicious code
	T8	Stack-Overflow attacks	Bad coding conducts
	T9	Denial-of-Service (DoS)	Low memory resources
Industry Reputation or intangible asset (IRIA)	T10	Fraud	Staff deceitfulness
	T11	Data breach	Outdated Security Software
	T12	Misuse of resources	Poor resources management
Human Resource Management /Employee (HRME)	T13	Accident	Ignorance to precaution
	T14	Social engineering	Inclination to improved status gain
	T15	Illness	Illness due to change of weather

Based on sections 3.1 and 3.2, the final risk level of each asset is noted in Table 6 and also ranked from maximum to minimum risk value.

Table 6. Final risk values in this study

	Threats	**Likelihood Level**	**Severity Level**	**Risk Level %**	**Rank**
		Input variable to Fuzzification		Defuzzification	
		Level Value: 0-10	**Level Value: 0-10**	**Value: 100%**	
ED	T1	7	8	66.33	3
	T2	5	9.1	75.67	1
	T3	4	4	48.33	8
PH	T4	8.5	2.5	57.67	5
	T5	5.5	3.4	45.67	10
	T6	9.4	8	70	2
SRMS	T7	2.9	5.2	39.67	13
	T8	3	7	42	11
	T9	7.5	1.5	50.67	6
IRIA	T10	1.8	8.8	48.33	8
	T11	7	4.6	58.67	4
	T12	8.1	0.1	50	7
HRME	T13	1.5	5.8	38.67	14
	T14	4.8	1.5	26.67	15
	T15	3.5	6.1	40.67	12

Based on the fuzzy logic designer, nine fuzzy rules were constructed. The inference engine maps input fuzzy sets (likelihood and severity) into fuzzy output sets (risk value). Figure 5 shows the number of if-then rules in order to provide a better understanding of the proposed fuzzy inference system framework, and with the input of likelihood of occurrence and risk severity, the risk size can be calculated. For instance, with 5 and 5 for likelihood and risk severity, the risk size would be 50%. A likelihood of 5 is related to rules 4-6, and a risk severity of 5 is related to rules 2, 5, and 8. The fuzzy model designed by combining these rules estimates the risk value.

The authors generated and plotted an output surface map for the food processing industry information system fuzzy model using surface viewer to visualize the dependence of one of the outputs on any one or two of the inputs. According to Mamdani, Figure 6 depicts the food processing fuzzy model's output surface viewer.

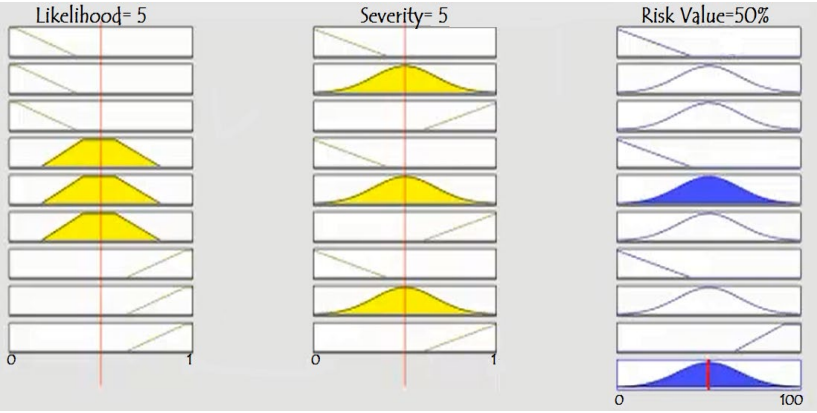

Fig. 5. Fuzzy rules according to Mamdani method

Based on Tables 5 and 6, electronic data in T2 (data theft) has a high effect risk of 75.67%, and human resource management in T14 (social engineering) has a low-risk impact of 26.67%. As a result of this risk assessment, the food processing industry's high-probability risk items necessitate immediate remedial action to mitigate the risk (Figure 7).

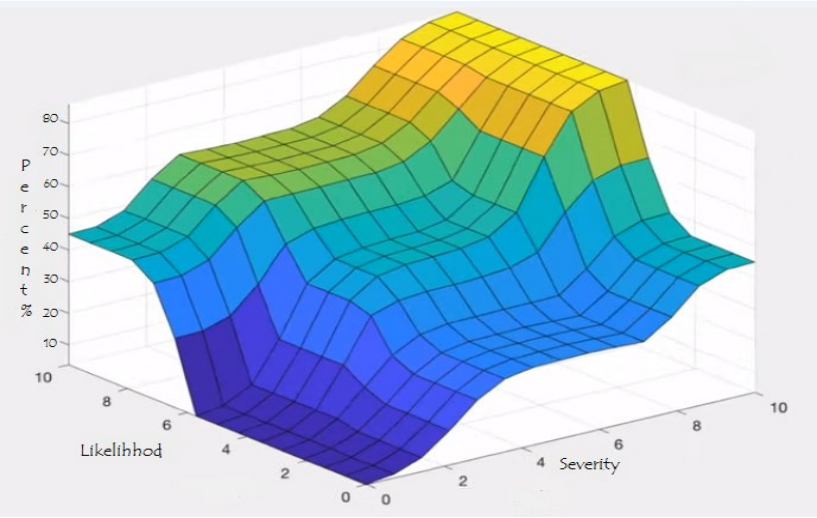

Fig. 6. 3D plots for 9 rules according to Mamdani method

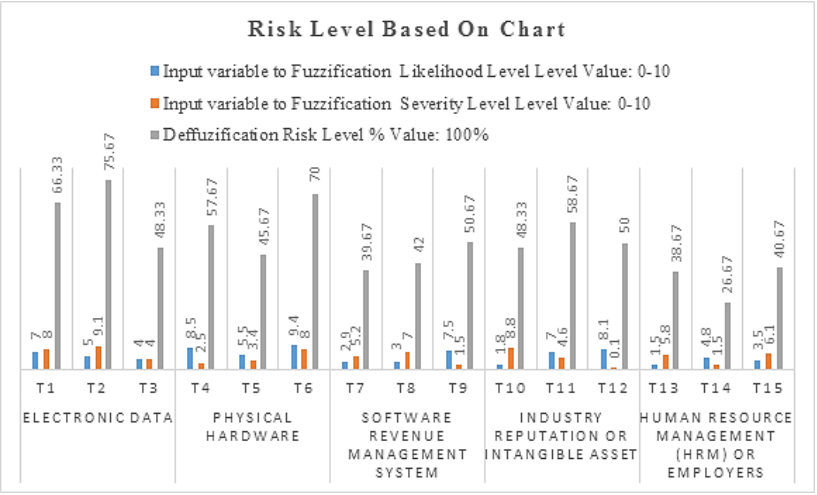

Fig. 7. Risk level based on the chart

5. Conclusion. According to the results of this study, the authors developed a flow model for assessing the risks of activities in the Sub-Saharan food industry. The authors identified five critical food processing industry information systems, including electronic data, physical hardware, software revenue management systems, food processing industry reputation (intangible) assets, and human resource management (HRM).

In order to obtain a more reliable and less subjective method for the risk assessment process, a fuzzy inference system has been used in this model. Nine fuzzy decision rules were constructed for some of the chosen risks by using likelihood, severity, and risk values. Finally, the risk values were calculated in the aggregation and defuzzification processes. Finally, based on the final information security risk values, the risks were ranked from maximum to minimum risk values obtained in the Sub-Saharan African food processing industry.

References

1. Food processing in Sub-Saharan Africa: Solutions for African Food Enterprises. TechnoServes, 2017. 44 p. Available at: https://www.technoserve.org/wp-content/uploads/2018/04/solutions-for-african-food-enterprises-final-report.pdf. (accessed 26.07.2023).
2. Whitman M.E., Mattord H.J. Principles of Information Security. Cengage Learning. 2018. 750 p.
3. Kriaa S., Bouissou M., Laarouchi Y. A Model Based Approach for SCADA Safety and Security Joint Modelling: S-Cube. 10th IET System Safety and Cyber-Security Conference. 2015. DOI: 10.1049/cp.2015.0293.

4. Shin J., You I., Seo J.T. Investment priority analysis of ICS information security resources in smart mobile IoT network environment using the analytic hierarchy process. Mobile Information Systems. 2020. vol. 2020. DOI: 10.1155/2020/8878088.
5. Shamala P., Ahmad R., Zolait A.H., Bin Sahib S. Collective information structure model for information security risk assessment (ISRA). Journal of Systems and Information Technology. 2015. vol. 17. no. 2. pp. 193–219. DOI: 10.1108/JSIT-02-2015-0013.
6. Abbass W., Baina A., Bellafkih M. Improvement of information system security risk management. 4th IEEE International Colloquium on Information Science and Technology (CiSt). 2016. pp. 182–187. DOI: 10.1109/CIST.2016.7805039.
7. Yang M. Information Security Risk Management Model for Big Data. Advances in Multimedia. 2022. vol. 2022. DOI: 10.1155/2022/3383251.
8. Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. Risks. 2022.
9. Ebrat M., Ghodsi R. Construction project risk assessment by using adaptive-network-based fuzzy inference system: An empirical study. KSCE Journal of Civil Engineering. 2014. vol. 18. pp. 1213–1227. DOI: 10.1007/s12205-014-0139-5.
10. Stebbins-Wheelock E.J., Turgeon A. Guide to Risk Assessment and Response. The University of Vermont, 2018. 17 p.
11. Sobel P.J., Prawitt D.F., Dohrer R.D., Murdock D.C., Thomson J.C., Miller P.K. Compliance risk management: applying the COSO ERM framework. Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2020. 48 p.
12. Chandra N.A., Ramli K., Ratna A.A.P., Gunawan T.S. Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. Risks. 2022. vol. 10(8). no. 165. DOI: 10.3390/risks10080165.
13. Crotty J., Daniel E. Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. Applied Computing and Informatics. 2022. DOI: 10.1108/ACI-07-2022-0178.
14. Carlsson E., Mattsson M. The MaRiQ model: A quantitative approach to risk management in cybersecurity. 2019. Uppsala: Uppsala Universitet, 2019. 97 p.
15. Fadyeyeva I., Gryniuk O. Fuzzy modelling in risk assessment of oil and gas production enterprises' activity. Baltic Journal of Economic Studies. 2017. vol. 3. no. 4. pp. 256–264.
16. Papageorgiou E.I., Aggelopoulou K., Gemtos T.A., Nanos G.D. Development and Evaluation of a Fuzzy Inference System and a Neuro-Fuzzy Inference System for Grading Apple Quality. Applied Artificial Intelligence. 2018. vol. 32. no. 3. pp. 253–280. DOI: 10.1080/08839514.2018.1448072.
17. Blasi A.H. The use of Fuzzy Logic Control in Manufacturing Systems. 2020. 12 p.
18. Kotenko I., Saenko I., Ageev S. Countermeasure Security Risks Management in the Internet of Things Based on Fuzzy Logic Inference. IEEE TrustCom/BigDataSE/ISPA. 2015. pp. 654-659. DOI: 10.1109/Trustcom.2015.431.
19. Hadacek L., Sivakova L., Sousek R., Zeegers M. Assessment of security risks in railway transport using the fuzzy logical deduction method. Communications – Scientific Letters of the University of Zilina. 2020. vol. 22. no. 2. pp. 79–87. DOI: 10.26552/com.C.2020.2.79-87.
20. Kaka S., Hussin H., Khan R., Akbar A., Sarwar U., Ansari J. Fuzzy logic-based quantitative risk assessment model for hse in oil and gas industry. Universiti Teknologi PETRONAS, 2022. DOI: 10.17605/OSF.IO/WVG2H.
21. Zhao Y., Talha M. Evaluation of food safety problems based on the fuzzy comprehensive analysis method. Food Science and Technology. 2021. vol. 42. no. e47321. DOI: 10.1590/FST.47321.

Asfha Amanuel — Post-graduate student, ITMO University. Research interests: information security methods and systems, information and cyber security, risk management. The number of publications — 3. baquesti2003@gmail.com; 49, Kronverksky Av., 197101, St. Petersburg, Russia; office phone: +7(952)378-2147.

Vaish Abhishek — Ph.D., Assistant professor, It department, Indian Institute of Information Technology, Allahabad. Research interests: information security, information security laws and regulations, cyber diplomacy, network security, IT Governance, enterprise recourses planning. The number of publications — 66. abhishek@iiita.ac.in; Uttar Pradesh, 211015, Deghat Jhalwa, India; office phone: +91(790)535-6150.

УДК 004.056 **DOI** 10.15622/ia.22.5.5

А.Э. Асфха, А. Вайш

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПИЩЕВОЙ ПРОМЫШЛЕННОСТИ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ НЕЧЕТКОГО ВЫВОДА

Асфха А.Э., Вайш А. **Анализ рисков информационной безопасности в пищевой промышленности с использованием системы нечеткого вывода.**

Аннотация. В последнее время предпринимались различные попытки охарактеризовать угрозы информационной безопасности, особенно в промышленном секторе. Тем не менее, существует ряд загадочных угроз, которые могут поставить под угрозу безопасность данных, информации и ресурсов пищевой промышленности. Целью данного исследования было изучение рисков для информационной безопасности в информационной системе пищевой промышленности, а участниками этого исследования были эксперты исполнительного руководства, штатный персонал, технические и активные операторы, сторонние консалтинговые компании и управление рисками, специалисты пищевой промышленности в информационной системе стран Африки к югу от Сахары. Анкета и интервью с различными вопросами с использованием подходов качественного и количественного анализа рисков были использованы для сбора идентификаций рисков, а также метод системы нечётких выводов, приманенный для анализа фактора риска в этой статье. Выводы показали, что среди проблем информационной безопасности электронные данные в угрозе кражи данных имеют высокий риск 75,67%, а управление человеческими ресурсами (HRM) в угрозе социальной инженерии имеет низкий риск воздействия 26,67%. В результате факторы риска с высокой вероятностью требуют оперативных действий. Компоненты риска с высокой вероятностью требуют быстрых корректирующих действий. В результате необходимо выявить и контролировать первопричины таких угроз до того, как возникнут пагубные последствия. Также важно отметить, что при изучении информационной безопасности в промышленных информационных системах пищевой промышленности необходимо принимать во внимание основные интересы и глобальную политику.

Ключевые слова: пищевая промышленность, информационная безопасность, идентификация рисков, анализ рисков, система нечеткого вывода, ISO 27005.

Литература

1. Food processing in Sub-Saharan Africa: Solutions for African Food Enterprises. TechnoServes, 2017. 44 p. Available at: https://www.technoserve.org/wp-content/uploads/2018/04/solutions-for-african-food-enterprises-final-report.pdf. (accessed 26.07.2023).
2. Whitman M.E., Mattord H.J. Principles of Information Security. Cengage Learning. 2018. 750 p.
3. Kriaa S., Bouissou M., Laarouchi Y. A Model Based Approach for SCADA Safety and Security Joint Modelling: S-Cube. 10th IET System Safety and Cyber-Security Conference. 2015. DOI: 10.1049/cp.2015.0293.
4. Shin J., You I., Seo J.T. Investment priority analysis of ICS information security resources in smart mobile IoT network environment using the analytic hierarchy process. Mobile Information Systems. 2020. vol. 2020. DOI: 10.1155/2020/8878088.
5. Shamala P., Ahmad R., Zolait A.H., Bin Sahib S. Collective information structure model for information security risk assessment (ISRA). Journal of Systems and Information Technology. 2015. vol. 17. no. 2. pp. 193–219. DOI: 10.1108/JSIT-02-2015-0013.

6. Abbass W., Baina A., Bellafkih M. Improvement of information system security risk management. 4th IEEE International Colloquium on Information Science and Technology (CiSt). 2016. pp. 182–187. DOI: 10.1109/CIST.2016.7805039.
7. Yang M. Information Security Risk Management Model for Big Data. Advances in Multimedia. 2022. vol. 2022. DOI: 10.1155/2022/3383251.
8. Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. Risks. 2022.
9. Ebrat M., Ghodsi R. Construction project risk assessment by using adaptive-network-based fuzzy inference system: An empirical study. KSCE Journal of Civil Engineering. 2014. vol. 18. pp. 1213–1227. DOI: 10.1007/s12205-014-0139-5.
10. Stebbins-Wheelock E.J., Turgeon A. Guide to Risk Assessment and Response. The University of Vermont, 2018. 17 p.
11. Sobel P.J., Prawitt D.F., Dohrer R.D., Murdock D.C., Thomson J.C., Miller P.K. Compliance risk management: applying the COSO ERM framework. Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2020. 48 p.
12. Chandra N.A., Ramli K., Ratna A.A.P., Gunawan T.S. Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. Risks. 2022. vol. 10(8). no. 165. DOI: 10.3390/risks10080165.
13. Crotty J., Daniel E. Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. Applied Computing and Informatics. 2022. DOI: 10.1108/ACI-07-2022-0178.
14. Carlsson E., Mattsson M. The MaRiQ model: A quantitative approach to risk management in cybersecurity. 2019. Uppsala: Uppsala Universitet, 2019. 97 p.
15. Fadyeyeva I., Gryniuk O. Fuzzy modelling in risk assessment of oil and gas production enterprises' activity. Baltic Journal of Economic Studies. 2017. vol. 3. no. 4. pp. 256–264.
16. Papageorgiou E.I., Aggelopoulou K., Gemtos T.A., Nanos G.D. Development and Evaluation of a Fuzzy Inference System and a Neuro-Fuzzy Inference System for Grading Apple Quality. Applied Artificial Intelligence. 2018. vol. 32. no. 3. pp. 253–280. DOI: 10.1080/08839514.2018.1448072.
17. Blasi A.H. The use of Fuzzy Logic Control in Manufacturing Systems. 2020. 12 p.
18. Kotenko I., Saenko I., Ageev S. Countermeasure Security Risks Management in the Internet of Things Based on Fuzzy Logic Inference. IEEE TrustCom/BigDataSE/ISPA. 2015. pp. 654-659. DOI: 10.1109/Trustcom.2015.431.
19. Hadacek L., Sivakova L., Sousek R., Zeegers M. Assessment of security risks in railway transport using the fuzzy logical deduction method. Communications – Scientific Letters of the University of Zilina. 2020. vol. 22. no. 2. pp. 79–87. DOI: 10.26552/com.C.2020.2.79-87.
20. Kaka S., Hussin H., Khan R., Akbar A., Sarwar U., Ansari J. Fuzzy logic-based quantitative risk assessment model for hse in oil and gas industry. Universiti Teknologi PETRONAS, 2022. DOI: 10.17605/OSF.IO/WVG2H.
21. Zhao Y., Talha M. Evaluation of food safety problems based on the fuzzy comprehensive analysis method. Food Science and Technology. 2021. vol. 42. no. e47321. DOI: 10.1590/FST.47321.

Асфха Амануэль Эстифанос — аспирант, Университета ИТМО. Область научных интересов: методы и системы защиты информации, информационная и кибербезопасность, управление рисками. Число научных публикаций — 3. baquesti2003@gmail.com; Кронверкский проспект, 49, 197101, Санкт-Петербург, Россия; р.т.: +7(952)378-2147.

Вайш Абхишек — Ph.D., доцент, кафедра информационных технологий, Индийский институт информационных технологий, Аллахабад. Область научных интересов: информационная безопасность, законы и нормативные акты в области информационной безопасности, кибердипломатия, сетевая безопасность, управление ИТ, планирование ресурсов предприятия. Число научных публикаций — 66. abhishek@iiita.ac.in; Уттар-Прадеш, 211015, Дегхат Джалва, Индия; р.т.: +91(790)535-6150.