ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A MODEL FOR RISK ANALYSIS IN THE INDUSTRIAL INTERNET OF THINGS

[1]AMIROVA AKZHIBEK , [2]TOKHMETOV AKYLBEK
[1,2]N. Gumilyov Eurasian national university, Nur-Sultan, Kazakhstan
E-mail: [1]akzhibek.amirova@gmail.com, [2]attohmetov@mail.ru

ABSTRACT

With the rapid development of the industrial Internet of Things (IIoT) the need to respond quickly, detect and prevent intrusions has arisen. IIoT networks have special functions and face unique challenges in defending against cyber attacks. These problems are especially relevant as the predicted growth of IIoT users.

Risk assessment is an important part of the process of information security systems, including industrial complexes. In this document, we present a practical information security risk assessment model. This model is based on simple additive weighting method and fuzzy logic. Fuzzy logic is a suitable model for risk assessment and represents practical results.

Keywords: *Industrial Internet of Things (IIoT), Simple Additive Weighting Method (SAW), Security, Threats.*

1. INTRODUCTION

The Industrial Internet of Things is a system of interconnected computer networks and industrial objects connected to them with built-in sensors and software for collecting and exchanging data, with the possibility of remote control and management in an automated mode, without human intervention. IIoT allows creating industries that are more economical, flexible and efficient than existing ones.

For the development of IIoT, the problem of ensuring an adequate level of cybersecurity remains, perhaps, the only significant obstacle.

According to Market Data Forecast, the global industrial Internet of Things market (including equipment, sensors, sensors, robotic systems, platforms, software and services) in 2019 reached $ 264.22 billion. It will grow from 2021 to 2025 at a CAGR of 18.7%. By 2025, its volume will amount to USD 622 billion. Due to the coronavirus pandemic, market growth in 2020 has been adjusted and will be 0% from 2019 [1].

According to Honeywell, the main trend associated with the development of industrial Internet of Things ecosystems is the involvement of licensors and industrial equipment manufacturers in the development of applications based on the existing IIoT infrastructure, which can subsequently be placed in the application store/ marketplaces. These applications will increase the mobility and productivity of employees in the enterprise, as well as help solve highly specialized tasks of increasing efficiency [2].

Based on the Accenture survey of 1,400 top business executives around the world, the Industrial Internet of Things (IoT) contribution to the global economy will be in the order of $ 14 trillion by 2030. The introduction of IIoT technologies over the same period can add up to $ 6 trillion to the US GDP and at least $ 70 billion to the German economy. An Accenture study shows that the promise and impact of the Industrial Internet of Things is not yet clear to big business. The lack of plans of using such technologies is largely due to their complexity of the potential income [3].

These forecasts further highlight the complexities associated with securing IIoT. While a large number of industrial devices have been migrated to take advantage of more secure communication methods, most of these legacy systems still rely on legacy protocols. This situation persists despite the fact that the public is aware of their inherent vulnerabilities due to the lack of any identification or authentication requirements. The main process of implementing information security management systems is risk assessment [4].

Risk Assessment provides organizations with an accurate assessment of the risks to their assets. This can help them prioritize and develop a comprehensive risk mitigation strategy.

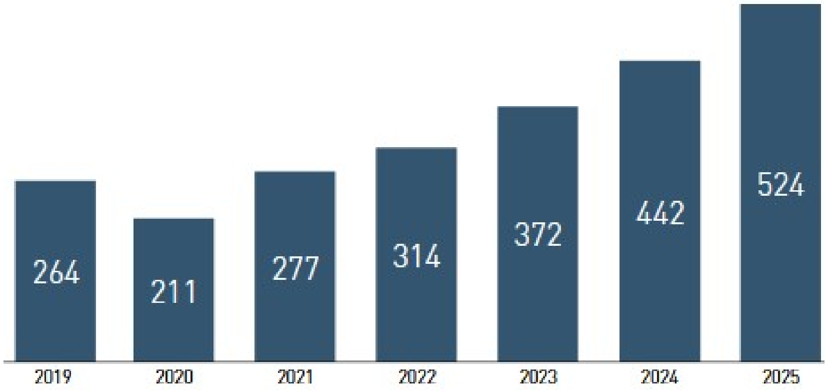

Figure 1: Dynamics of the Global Industrial Internet of Things Market (USD billion) [1]

There are several standards and methodologies for risk assessment, such as NIST and ISO27001, but although they explain general principles and guidelines, they do not contain any implementation details [5]. The European Union Agency for Network and Information Security (ENISA) is a center of expertise, which works to develop advice and recommendations on good practice in information security. Since 2015, ENISA supplies stakeholders with state-of-the-art documents covering security issues in area of IoT and Industrial IoT (IIoT) related with Smart Manufacturing and Industry 4.0 issues. There are practically no risk assessment standards developed specifically for industrial systems [6].

IIoT systems have their own dynamics and uniqueness, which requires new approaches to risk assessment. Risk Assessment provides industrial systems with an accurate assessment of the risks to their assets. This can help them prioritize and develop a comprehensive risk mitigation strategy.

Given the limitations of quantitative approaches, the developed model recommends a qualitative method based on expert opinions and fuzzy methods for assessing information security risks.

Contributions of the paper: This paper offers a model which is based on simple additive weighting method and fuzzy logic for risk assessment in IIoT. This article, in turn, presents the use of the simple additive weighting method and fuzzy logic in the context of the implementation of the risk analysis model in IioT networks.

The rest of this paper is organized as follows. Section 2 gives an insight of the related works. In Section 3 the used methodology is presented. Experimental results are presented in Section 4. Section 5 concludes the paper.give guidance on layout, style, illustrations and references and serve as a model for authors to emulate. Please follow these specifications closely as papers which do not meet the standards laid down, will not be published.

2. RELATED WORKS

As far as the authors know, there is a limited number of works [7--10] devoted to risk assessment in the IIoT environment. Despite this, there are certain solutions that have been discussed below.

[7] presents a methodology for assessing IIoT system risks, which consists of ten steps that cover risk elements to calculate the likelihood that a threat agent investigates one or more vulnerabilities in an IIoT asset, which turns a threat into an incident with consequences for various actors: manufacturers , developers, customers, integrators, service providers and users.

A Vulnerability Analysis Framework (VAF) was developed in [8] to define a measure to describe risk in IIoT environments.

Yu-Long Huang et al. analyzed methods for assessing the risks of an IIoT network, especially for core services running in the cloud for IoT devices. This article also presented a new risk assessment model based on the AHP (Analytic

Hierarchy Process) for the IIoT cloud to self-check its state [9].

Ani and Tiwari [10] provided an assessment of cybersecurity issues in manufacturing infrastructure. The article focuses on the security landscape and discusses vulnerabilities, threats, cyber incidents as well as their impact and threat analysis. In the manufacturing industry, there can be problems with people, problems with processes and problems with technologies. Although a risk assessment has been suggested, there are still no updates in terms of privacy issues.

3. PROPOSED MODEL

To create an information security system, it is necessary to solve problems that are aimed at processing, storing and protecting formalized information. In this case, it is possible to form and using the methods of information theory to calculate fairly accurate parameters reflecting the degree of security of an object or system.

However, for a comprehensive assessment of the degree of security, it is often necessary to use expert methods for evaluating technical parameters that cannot be calculated using the information-theoretic approach. The formation of an information security system of an object requires the solution of a number of tasks related to formalized information - interaction information in the form of documents or exchange signals of technical systems.

In these cases, the methods of mathematical information theory are quite applicable and it is possible to form all the mother values of the parameters characterizing the security of the system. However, to fully assess the security, these parameters have to be compared with the estimates for the impact information that is not directly accessible. For example, it is possible to fairly reliably estimate the probability of recovering a single word in an intercepted voice message, but then it is necessary to establish what probability is considered acceptable.

Such an assessment can only be obtained by expert advice. It is ineffective to apply the methods of information theory in this case, since the result is completely determined by the initial assumptions, which are actually formed arbitrarily. For different situations, different content of phrases, different vocabulary, expert assessments can give results that differ in order. A prerequisite for the use of fuzzy models is the presence of uncertainty due to the lack of information or the complexity of the system, and the availability of qualitative information about the system [2].

The advantages of fuzzy systems include their versatility. According to the study [8], any continuous function can be represented by a fuzzy model with any given accuracy. The special qualities of systems with fuzzy logic make it possible to synthesize a model of an object on the basis of heuristic information received from an expert or as a result of an experiment.

At the same time, fuzzy systems have such disadvantages as the absence of algorithms for the synthesis of stable models and the low speed of the latter with a large number of control rules [2, 9, 10].

The first stage in the implementation of model is the creation of a representative group of potential experts who will participate in the selection of measures to improve the environmental situation by the “brainstorming” method and the “snowball” method (Figure 2).

Then this group of specialists proceeds to a meaningful analysis of the problematics through collective discussions of the conceptual model, the choice of the most suitable methods for a particular case. Problem analysis includes comprehensive studies of legal and institutional aspects in the field of economics and sociology, as well as the state of the environment. At the stage of modeling the decision-making system, a leading group of experts develops a general model aimed at solving the problem and based on causal relationships using the model.

The purpose of creating a fuzzy information security management model is to determine the values of control variables based on the current state of the protected object, the implementation of which will provide the required level of protection. In classical control theory, the basic model is based on the representation of an object and a process in the form of some systems.

The control object is characterized by a finite set of input and output variables. Input variables are generated using a finite set of sensors. At the output of the control system, a set of output (control) variables is formed. The values of the control variables are fed to the input of the control object and form an adequate control action. If a fuzzy control model is being built, then the classical control system is replaced by a fuzzy control system [10].

As this system, a fuzzy inference system is used with the implementation of all the necessary stages (Fig. 1). The fuzzy inference process is formed on the basis of one of the fuzzy inference algorithms.

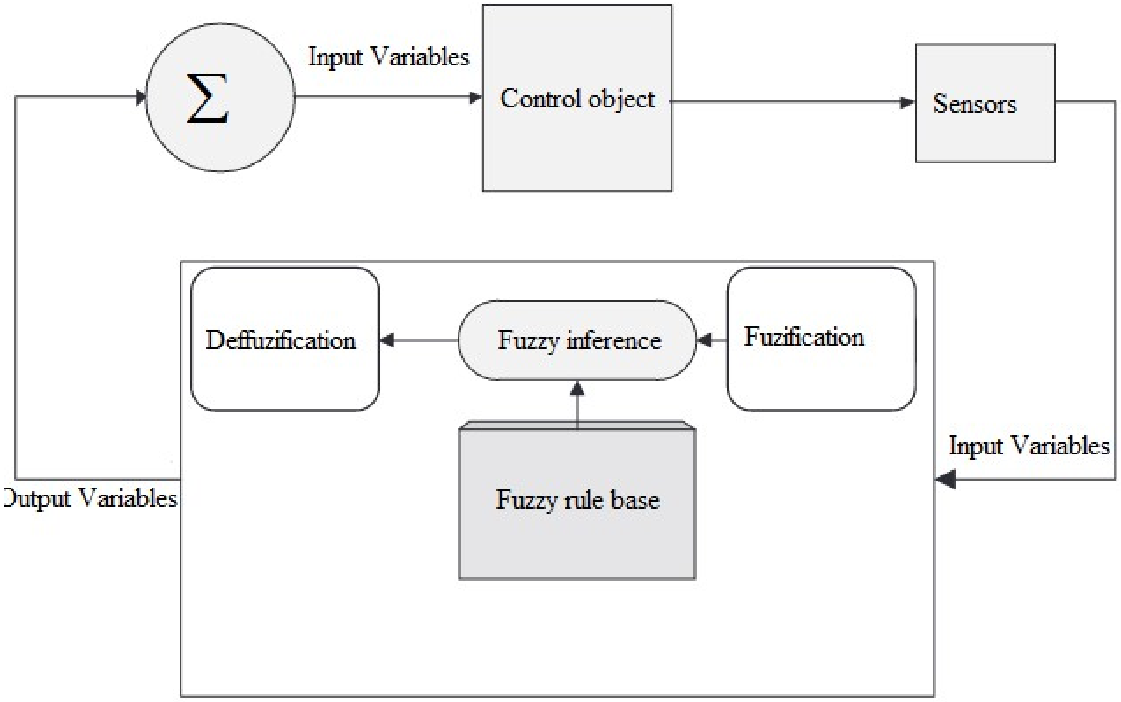

Figure 2: Fuzzy control process diagram

After formalizing the model, an analytical matrix is formed, the elements of which characterize the assessment for each criterion for each alternative. The analytical matrix is an m × n matrix, the elements of which are the estimates (xij) of the alternative aj by the criterion ki.

At the Design stage, the analytical matrix is processed by one of three multi-attributive decision-making methods that allow you to rank many alternatives. Each of the methods evaluates n alternatives, which are variants of activities, each of which corresponds to m attributes.

1. One of the most famous and widely used methods of multi-institutional decision-making is the simple additive weighting method (SAW). Using this method, the decision maker (DM) can obtain an overall rating for each alternative by multiplying the rating scale value for each attribute value by the weight assigned to the attribute, and then summing these values across all attributes. Thus, the decision maker receives an alternative with the highest score (the highest average weight), which is the answer to the decision-making problem.

2. The TOPSIS method (Ideal point method) is based on the concept that the chosen alternative should have the shortest distance to the ideal solution and the largest distance to the ideal negative solution [11].

3. The ELECTRE method (Method of exclusion and choice reflecting reality) consists in pairwise comparison of alternatives based on the assessment of alternatives and preference weights, confirming or rejecting the relationship of pair dominance between alternatives.

Since our goal is a practical model for any organization, the SAW methodology was chosen for implementation. In addition, since risk assessment refers to ambiguous topics, fuzzy logic is suitable for assessing uncertain subjects, and using it, experts can express their opinion in the form of linguistic variables, such as "very high", "low", etc.

Different domains of Information Technology (IT) assets are identified based on ENISA document “Industry 4.0 Cybersecurity: Challenges & Recommendations (2019)” [12]. Table 1 defines the categories and types of assets in IIoT systems, taking into account the necessary digital and physical elements.

Table 1: The Categories and Types of Assets in IIoT Systems

Category	Type
Hardware or physical	Building, location, device, gateway, edge IIoT end devices (sensors, actuators)
Software	Application, platform, system, middleware, operational system, firmware
Communication	Cloud, ICS communication networks & components (switches, wireless access points, power supply)
Information	Data-At-Rest (DAR), Data-In-Use (DIU), Data-In-Motion (DIM)
Servers and Systems	Historians , Application Servers, Database Servers ,Enterprise operations systems, Manufacturing operations systems
Security equipment	Antivirus, firewall, SIEM IDS/IPS
Human	Human, knowledge and skills of the personnel

Table 2:Attacks in IIoT

Category	Attacks
Hardware or physical	Denial of Service attacks, Ransomware, Vurises, Trojan horses, Spyware, Exploit kits, Denial of Service attacks, Advanced Persistent Threat, Wireless attack, Unautorised access, Brute force, Physical attacks, Power supply outage, Failure or malfunction of a sensor/actuator, Man-in-the-Middle attack, Session hijacking
Software	Control device configuration manipulation, SCADA, MES, Historian data manipulation, Loss of support services (MES, ERP, CRM), Software vulnerabilities exploitation, Unauthorized update of information, Unauthorized access to software, Entering false information into the software, Human error in the software
Communication	Communication disruption, Denial of Service attacks, Industrial robot manipulation, Remote controller devices manipulation, Attacks using AI, Wireless attack, Unautorised access,

	Brute force, Physical attacks, Communication network outage, Power supply outage, Enviromental disasters, Failure or disruption of service providers, Sniffing IoT communication protocol hijacking Tunneling
Information	Password disclosure Disclosure of information Active eavesdropping Theft of information Modification of information Detection of information Loss of data Attacks using AI Abuse of personal data SQL Injection
Servers and Systems	Denial of Service Malware Manipulation of Information Unintentional change of data
Security equipment	Theft Dissatisfied personnel Shortage of skilled personnel Dependency to personnel Human error
Human	Theft Dissatisfied personnel Shortage of skilled personnel Dependency to personnel Human error

Then threats relative to each domain are determined based on [14]. The occurrence probability of threats manifestation of damage done are two main factors in risk level estimation. Therefore, in each area, two decision tables are compiled to assess these two factors. Each expert then determines the importance of each criterion and the value of each alternative in relation to each criterion using linguistic variables.

In the end, using the SAW method, the manifestation of the damage caused and the likelihood of each threat occurring will be refined, and the level of risk is calculated by multiplying these two factors.

The table 3 shows the effective criterions for determining the likelihood and impact intensity of threats:

Table 3: Effective Criterions for Determining the manifestation of damage done and occurrence probability of Threats

Effective Criterion	Effective Criterion
For manifestation of damage done	For occurrence probability
Financial cost	Attraction of information asset
Time cost	Vulnerability
Damage to reputation	Existing control

The algorithm (Figure 3) for implementing this model contains 9 stages [14, 15]:

1. Get expert opinions in the form of linguistic variables about the importance of each area. This should be done on the basis of the decision table (Table 4), which indicates the weight of each criterion.

2. Obtain expert opinions of each domain about of the manifestation of damage done and occurrence probability of each threat related to each domain in the form of linguistic variables (Table 5).

3. Replace linguistic variables with fuzzy variables based on Tables 3 and 4. Combine all expert opinions in each area and create a decision matrix. x_{ij} and w_j are triangular fuzzy numbers, and suppose our decision group consists of n people [14].

$$x_{ij} = (a_{ij}, b_{ij}, c_{ij}) \quad (1)$$

$$w_j = (w_{ij}, w_{ij}, w_{ij}) \quad (2)$$

$$x_{ij} = \frac{1}{n}\left[x_{ij}^{1}(+)x_{ij}^{2}(+) \dots x_{ij}^{n}(+)\right] \quad (3)$$

$$w_{ij} = \frac{1}{n}\left[w_{ij}^{1}(+)w_{ij}^{2}(+) \dots w_{ij}^{n}(+)\right] \quad (4)$$

The fuzification stage consists in applying decision rules to the input data (expert estimates of the likelihood and damage of the threat) and serves to convert the clear input data to a fuzzy format.

4. Linear normalization of consolidated matrix.

5. Deffuzification of combined weights using signed distance and normalization method:

$$w_j = \frac{w_j}{\sum_j w_j}$$

6. Calculate weight matrix

7. Multiply the fuzzy values of manifestation of damage done and occurrence probability of each threat and calculate the probability of the threat occurring in each domain.

8. Deffuzification of fuzzy values by Signed Distance method for each threat and calculation of the risk level for each domain.

9. Calculate the overall risk level of organization by multiplying the risk level of threat with every domain importance Coefficient.

4. EXPERIMENTAL RESULTS

In this model, linguistic variables are used to get experts opinion for weights of criteria and rate of alternatives, with respect to various criteria whose fuzzy equivalent is as in Tables 4, 5 [15].

In our evaluation, 70 threats and 7 domains had been defined in advance. At first, to determine the importance of each domain, experts proposed their opinion in the form of linguistic variables.

Table 6 illustrates the importance of each domain (Step1).

Table 7 illustrates the threats related to the servers domain. We continue the presentation of our results with this domain and eventually with the results of all domains.

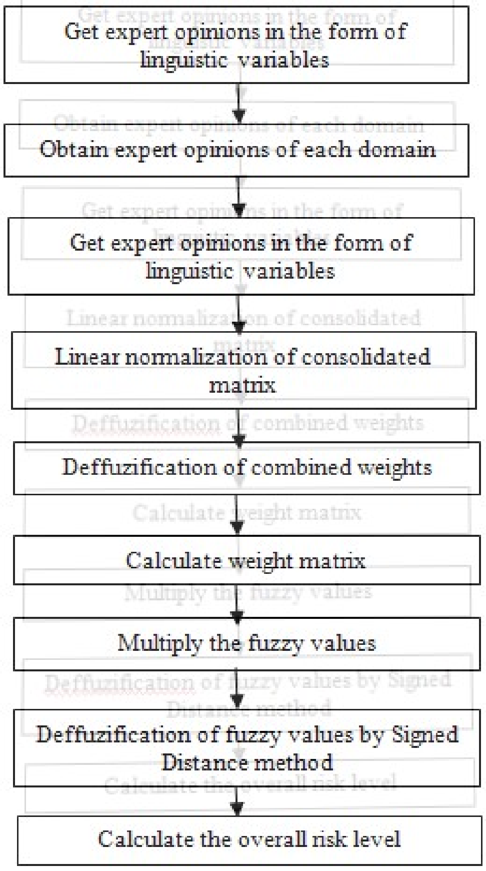
Get expert opinions in the form of linguistic variables
Obtain expert opinions of each domain
Get expert opinions in the form of linguistic variables
Linear normalization of consolidated matrix
Deffuzification of combined weights
Calculate weight matrix
Multiply the fuzzy values
Deffuzification of fuzzy values by Signed Distance method
Calculate the overall risk level

Figure 3:Algorithm for risk analysis in the IIoT

TABLE 4: Linguistic Variables and Fuzzy Equivalent for the Importance Weight of Each Criterion

Linguistic Variables	Fuzzy Triangular
Very low (VL)	(0, 0, 0.1)
Low (L)	(0, 0.1, 0.3)
Medium low (ML)	(0.1, 0.3, 0.5)
Medium (M)	(0.3, 0.5, 0.7)
Medium high (MH)	(0.5, 0.7, 0.9)
High (H)	(0.7, 0.9, 1.0)
Very high (VH)	(0.9, 1.0, 1.0)

TABLE 5: Linguistic Variables and Fuzzy Number for the Ratings

Linguistic Variables	Fuzzy Triangular
Very poor (VP)	(0, 0, 1)
Poor (P)	(0, 1, 3)
Medium poor (MP)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Medium good (MG)	(5, 7, 9)
Good (G)	(7, 9, 10)
Very good (VG)	(9, 10, 10)

Table 6: Relative Importance of Different Domains in the Organization

Category	Initial Weight	Normalized Weight
Hardware or physical	0.8192	0.131
Software	0.7630	0.122
Communication	0.7296	0.117
Information	0.6374	0.102
Servers	0.7023	0.113
Security equipment	0.5987	0.096
Human	0.6478	0.104

Table 7: Threats of the Servers Domain

	Threats
T1	Denial of Service
T2	Malware
T3	Manipulation of Information
T4	Unintentional change of data

Table 8: Importance Weight of Criteria Related to the probability of occurrence

	DM1	DM2
Cr1 Attraction of information asset	H	H
Cr2 Vulnerability	H	MH
Cr3 Existing control	MH	H

Table 9: Importance Weight of Criterion Related to manifestation of damage done

	DM1	DM2
Cr4 Financial cost	H	MH
Cr5 Time cost	MH	H
Cr6 Damage to reputation	M	ML

Table 10: The Ratings of the Four Threats of Servers by Decision Makers Under All Criterions

Criteria	Threat	DM 1	DM 2
Cr 1	T1	F	MG
	T2	MG	G
	T3	G	MG
	T4	MG	F
Cr 2	T1	F	MG
	T2	G	MG
	T3	MG	VG
	T4	G	G
Cr 3	T1	G	G
	T2	F	MG
	T3	F	MG
	T4	F	MG
Cr 4	T1	G	G
	T2	G	MG
	T3	G	MG
	T4	G	G
Cr 5	T1	G	MG
	T2	G	G
	T3	F	G
	T4	F	G
Cr 6	T1	P	MP
	T2	MP	MP
	T3	MG	G
	T4	MG	MG

Table 11: The Fuzzy Decision Matrix and Fuzzy Weights of the probability of occurrence in Servers Domain

	Cr1	Cr2	Cr3
Weight	(0.7, 0.9, 1)	(0.6, 0.8, 0.95)	(0.6, 0.8, 0.95)
T1	(4, 6, 8)	(4, 6, 8)	(7, 9, 10)
T2	(6, 8, 9.5)	(6, 8, 9.5)	(4, 6, 8)
T3	(6, 8, 9.5)	(7, 8.5, 9.5)	(4, 6, 8)
T4	(3, 5, 7)	(7, 9, 10)	(4, 6, 8)

Table 12: The Fuzzy Decision Matrix and Fuzzy Weights of the manifestation of damage done in Servers Domain

	Cr4	Cr5	Cr6
Weight	(0.6, 0.8, 0.95)	(0.6, 0.8, 0.95)	(0.2, 0.4, 0.6)
T1	(7, 9, 10)	(6, 8, 9.5)	(0.5, 2, 4)
T2	(6, 8, 9.5)	(5, 7.5, 8.5)	(1, 3, 5)
T3	(6, 8, 9.5)	(5, 7.5, 8.5)	(6, 8, 9.5)
T4	(7, 9, 10)	(7, 9, 10)	(5, 7, 9)

Table 13: The Fuzzy Normalized Decision Matrix Of The Probability Of Occurrence In Servers Domain

	Cr1	Cr2	Cr3
Weight	0.26	0.23	0.23
T1	(0.42, 0.63, 0.84)	(0.4, 0.6, 0.8)	(0.7, 0.9, 1)
T2	(0.63, 0.84, 1)	(0.6, 0.8, 1)	(0.4, 0.6, 0.8)
T3	(0.63, 0.84, 1)	(0.7, 0.9, 1)	(0.4, 0.6, 0.8)
T4	(0.32, 0.53, 0.74)	(0.7, 0.9, 1)	(0.4, 0.6, 0.8)

Table 14: The Fuzzy Normalized Decision Matrix Of The Manifestation Of Damage Done In Servers Domain

	Cr4	Cr5	Cr6
Weight	0.23	0.23	0.12
T1	(0.7, 0.9, 1)	(0.6, 0.8, 1)	(0.05, 0.21, 0.42)
T2	(0.6, 0.8, 1)	(0.5, 0.8, 0.9)	(0.11, 0.32, 0.53)
T3	(0.6, 0.8, 1)	(0.5, 0.8, 0.9)	(0.63, 0.84, 1)
T4	(0.7, 0.9, 1)	(0.7, 0.9, 1)	(0.53, 0.74, 0.95)

Table 15: The Fuzzy Weighted Normalized Decision Matrix Of The Probability Of Occurrence In Servers Domain

	Cr1	Cr2	Cr3
T1	(0.11, 0.16, 0.22)	(0.09, 0.14, 0.18)	(0.16, 0.21, 0.23)
T2	(0.16, 0.22, 0.26)	(0.14, 0.18, 0.23)	(0.09, 0.14, 0.18)
T3	(0.16, 0.22, 0.26)	(0.16, 0.21, 0.23)	(0.09, 0.14, 0.18)
T4	(0.08, 0.14, 0.19)	(0.16, 0.21, 0.23)	(0.09, 0.14, 0.18)

Table 16: The Fuzzy Weighted Normalized Decision Matrix Of The Manifestation Of Damage Done In Servers Domain

	Cr4	Cr5	Cr6
T1	(0.16, 0.21, 0.23)	(0.14, 0.18, 0.23)	(0.01, 0.03, 0.05)
T2	(0.14, 0.18, 0.23)	(0.12, 0.18, 0.21)	(0.01, 0.04, 0.06)
T3	(0.14, 0.18, 0.23)	(0.12, 0.18, 0.21)	(0.08, 0.1, 0.12)
T4	(0.16, 0.21, 0.23)	(0.16, 0.21, 0.23)	(0.06, 0.09, 0.11)

Table 17: The Value Of The Occurrence Probability In Servers Domain

Threat	Fuzzy Triangular
T1	(0.36, 0.51,0.63)
T2	(0.39, 0.54, 0.66)
T3	(0.42, 0.54, 0.66)
T4	(0.33, 0.48, 0.6)

Table 18: The Value Of The Manifestation Of Damage Done In Servers Domain

Threat	Fuzzy Triangular
T1	(0.3, 0.42, 0.51)
T2	(0.27, 0.39, 0.51)
T3	(0.22, 0.45, 0.57)
T4	(0.39, 0.48, 0.51)

Table 19: The Probability Of Threat Occurring In Servers Domain As Fuzzy

Threat	Fuzzification Values of Risk Level	Defuzzification Values
T1	(0.11, 0.21, 0.32)	0.21
T2	(0.11, 0.21, 0.34)	0.22
T3	(0.09, 0.24, 0.38)	0.24
T4	(0.13, 0.23, 0.31)	0.22

Table 20: Final Results Of Risk Level In Servers Domain

Threat	Risk Level
T1	23.73
T2	24.86
T3	27.12
T4	24.86

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Based on the data in Table 21, it can be concluded that the estimated level of risk for the servers domain is medium.

Table 21: Estimated Levels Of Risk Related To Different Scenarios

Estimated levels of risk	Range
Very Low	0.00-0.1
Medium Low	0.11-2.0
Low High	2.01-15.0
Meduim	15.01-51.0
High Low	51.01-100.0
Medium high	100.01-123.0
Very High	123.01

5. CONCLUSION

Implementing industrial internet systems requires a powerful tool for assessing the risks of industrial systems. In this article, an expert system based on fuzzy logic has been proposed for assessing the risks of industrial systems. In the proposed model, a fuzzy method was used to link expert opinions with linguistic variables. These linguistic variables more accurately reflect expert opinions. As a result, using this process, we can calculate the risk level of all threats related to the other domains. The recommended model in this study is a promising idea for a correct analysis of the safety of industrial systems. This model can be used in real industrial IoT systems, as it considers updated data on possible threats. At the same time, the model can be updated with new types of attacks.

A distinctive feature of this article is that there were categories and types of assets in IIoT systems, taking into account the necessary digital and physical elements. As far as the authors know, the previous articles did not update the base of attacks and threats in industrial systems. It is also worth noting that this model considers the determination of the manifestation of damage and the likelihood of threats to be effective criteria. The authors tried to combine the methods of mathematical information theory and an expert system to create a risk analysis model in IioT.

REFERENCES:

[1] Industrial IoT Market Research Report," Market Data Forecast. India, Feb, 2020 [Online]. Available: https://www.marketdataforecast.com/market-reports/industrial-ioT-market. [Access date: 01.05.2021].

[2] A.Amirova, A.Tokhmetov, A.Zhanasbaeva, "Researching the requirements for building a model for securing the industrial Internet of things," *Bulletin of the Scientific and Technical Society "Kahak"*, vol.70, no.3, pp.8-16, 2020.

[3] A.Amirova, A.Tokhmetov, A.Zhanasbaeva, "Overview of the main security issues in the industrial internet of things", *Bulletin of D. Serikbayev East Kazakhstan technical university,* vol.91, no.1, pp.82-90, 2021.

[4] International Standard Organization, ISO/IEC 27005, Information Security Risk Management, 2008.

[5] A. Shameli-Sendi, N. Ezzati-Jivan, M. Jabbarifar, and M. Dagenais, "Intrusion response systems: survey and taxonomy," *Int. J. Comput. Sci. Netw.Secur.*, vol. 12, no. 1, pp.1-14, 2012.

[6] V. Sklyar and V. Kharchenko, "ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios," *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2019, pp. 1046-1049, doi: 10.1109/IDAACS.2019.8924452.

[7] E. T. Nakamura and S. L. Ribeiro, "A Privacy, Security, Safety, Resilience and Reliability Focused Risk Assessment Methodology for IIoT Systems Steps to Build and Use Secure IIoT Systems," in the *Global Internet of Things Summit (GIoTS),* 2018, pp. 1-6, doi: 10.1109/GIOTS.2018.8534521.

[8] S.Figueroa-Lorenzo, J.Añorga, and S. Arrizabalaga, "A Survey of IIoT Protocols: A Measure of Vulnerability Risk Analysis Based on CVSS," *ACM Comput. Surv.* Vol. 53, no. 2, pp. 53–60, 2020, DOI:https://doi.org/10.1145/3381038.

[9] Y. Huang and W. Sun, "An AHP-Based Risk Assessment for an Industrial IoT Cloud," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, Lisbon, Portugal, 2018, pp. 637-638, doi: 10.1109/QRS-C.2018.00112.

[10] U.Ani and A.Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective," *Journal of Cyber Security Technology*, vol.1, no.1, pp. 32-74, 2017.

[11] K.Omari, S.Harchi, L.Ouchaouka, Z.Rachik, M.Moussetad and L.Labriji, “Application the fuzzy topsis and fuzzy electre in the serious games evaluation tool”, *Journal of Theoretical and Applied Information Technology,* vol.99. no 9, pp.1931-1942, 2021.

[12] Good Practices for Security of Internet of Things in the context of Smart Manufacturing, ENISA, 2018, 118 p.

[13] Industry 4.0 Cybersecurity: Challenges & Recommendations, ENISA, 2019, 13 p.

[14] S. Y. Chou, Y. H. Chang, and C. Y. Shen, “A fuzzy simple additive weighting system under group decision-making for facility location selection with objective/subjective attributes,” *Oper.Res.,* vol. 189, pp.132-145, 2008.

[15] A. Shameli-Sendi, M. Shajari, M. Hassanabadi, M. Jabbarifar, M. Dagenais, “Fuzzy Multi-Criteria Decision-Making for Information Security Risk Assessment,” *The Open Cybernetics & Systemics Journal*, no 6, pp.26-37, 2012.