http://doi.org/10.35784/iapgos.8133 *received: 21.07.2025 | revised: 05.01.2026 | accepted: 06.01.2026 | available online: 30.06.2026*

FUZZY LOGIC-BASED SECURITY RISK ASSESSMENT IN WIRELESS SENSOR NETWORKS OF INDUSTRIAL IoT

Olena Semenova[1], Natalia Kryvinska[2], Olha Voitsekhovska[3], Andrii Dzhus[1], Volodymyr Martyniuk[1]
[1]Vinnytsia National Technical University, Department of Infocommunication Systems and Technologies, Vinnytsia, Ukraine, [2]Comenius University in Bratislava, Department of Information Management and Business Systems, Bratislava, Slovakia, [3]Vinnytsia National Technical University, Department of System Analysis and Information Technologies, Vinnytsia, Ukraine

Abstract. *Recent years have seen the widespread deployment of wireless sensor networks (WSN), low-cost sensors, industrial clouds and industrial robots. These technological advancements have facilitated the development of Industrial Internet of Things (IIoT) technologies and fostered the emergence of novel digital applications. Thus, the IIoT is a technological concept involving the communication and interaction of mobile devices over wireless networks. Due to the numerous limitations of wireless sensor networks, security is one of the main issues. In the context of interconnected smart devices, the assumption of control over a single device has the potential to compromise the security of the entire network. The identification of these vulnerabilities can be enhanced by the implementation of remote diagnostics for IIoT devices. Whilst Artificial Intelligence (AI) finds extensive application in the solution of complex scientific, technical and practical issues, the present study investigates its use in wireless sensor networks of IIoT. Fuzzy systems, neural networks and genetic algorithms are three examples of AI techniques that are frequently used in wireless networks to improve their optimization and management. This paper proposes a fuzzy logic-based approach that allows intelligent assessment of the security risk levels of IIoT devices. Thus, a fuzzy inference system (FIS) that evaluates the security risk level of an IIoT device was developed. Its parameters were established, including the input and output variables and their membership functions. The developed FIS was optimized thorough other AI techniques. The efficacy of the FIS was evaluated through the use of a computer simulation in the MATLAB.*

Keywords: security, WSN, IoT, fuzzy logic

OCENA RYZYKA BEZPIECZEŃSTWA W OPARCIU O LOGIKĘ ROZMYTĄ W BEZPRZEWODOWYCH SIECIACH CZUJNIKOWYCH PRZEMYSŁOWEGO IoT

Streszczenie. *W ostatnich latach coraz powszechniejsze stało się wdrażanie bezprzewodowych sieci czujników (WSN), niedrogich czujników, chmur przemysłowych oraz robotów przemysłowych. Postępy technologiczne te ułatwiły rozwój technologii Przemysłowego Internetu Rzeczy (IIoT) i sprzyjały pojawieniu się nowych aplikacji cyfrowych. IIoT jest zatem koncepcją technologiczną obejmującą komunikację i interakcję urządzeń mobilnych za pośrednictwem sieci bezprzewodowych. Ze względu na liczne ograniczenia bezprzewodowych sieci czujników jednym z głównych problemów jest bezpieczeństwo. W kontekście połączonych ze sobą inteligentnych urządzeń przejęcie kontroli nad jednym urządzeniem może zagrozić bezpieczeństwu całej sieci. Identyfikację tych słabych punktów można usprawnić poprzez wdrożenie zdalnej diagnostyki urządzeń IIoT. Podczas gdy sztuczna inteligencja (AI) znajduje szerokie zastosowanie w rozwiązywaniu złożonych problemów naukowych, technicznych i praktycznych, niniejsze badanie dotyczy jej wykorzystania w bezprzewodowych sieciach czujników IIoT. Systemy rozmyte, sieci neuronowe i algorytmy genetyczne to trzy przykłady technik sztucznej inteligencji, które są często wykorzystywane w sieciach bezprzewodowych w celu poprawy ich optymalizacji i zarządzania. W niniejszym artykule zaproponowano podejście oparte na logice rozmytej, które umożliwia inteligentną ocenę poziomów ryzyka bezpieczeństwa urządzeń IIoT. W związku z tym opracowano system wnioskowania rozmytego (FIS), który ocenia poziom ryzyka bezpieczeństwa urządzenia IIoT. Ustalono jego parametry, w tym zmienne wejściowe i wyjściowe oraz ich funkcje przynależności. Opracowany system FIS został zoptymalizowany przy użyciu innych technik sztucznej inteligencji. Skuteczność systemu FIS została oceniona za pomocą symulacji komputerowej w programie MATLAB.*

Słowa kluczowe: bezpieczeństwo, WSN, IoT, logika rozmyta

Introduction

The Internet of Things (IoT) has emerged as a transformative force, revolutionizing the manner in which humans interact with technology and the physical world around them. The concept refers to a network of interconnected devices that communicate and exchange digital data seamlessly, paving the way for innovative applications across various industries [31].

There are 4 types of IoT:

- Consumer IoT – is defined as devices and applications designed for personal use, including smart home technology, wearables, and connected vehicles.
- Commercial IoT – the focus of commercial IoT is on applications deployed in business and industrial settings. Examples of such applications include smart buildings, industrial automation systems and asset tracking solutions.
- Industrial IoT – denotes the integration of sensors and connected devices into industrial processes. The implementation of these technologies facilitates real-time monitoring, predictive maintenance, and enhanced operational efficiency.
- Infrastructure IoT – encompasses the implementation of interconnected devices and sensors, with the objective of overseeing and regulating critical infrastructure. Such infrastructure may include transportation systems, energy grids, and smart cities.

The Industrial Internet of Things (IIoT) has transformed modern society and business by driving innovation, efficiency, and sustainability across various sectors. IIoT refers to the network of devices and equipment in industrial environments which collect, exchange, and analyse digital data and are connected to the Internet. This integration of connected devices and software has revolutionized various sectors of industry such as manufacturing, logistics, agriculture and healthcare. Its impact on the modern world is profound as it creates new opportunities for industry and businesses while also improving the quality of life for society.

The IIoT has been demonstrated to facilitate the ongoing observation of industrial systems and processes, resulting in enhanced safety outcomes. IIoT sensors can identify potential hazards in real time mode, such as equipment malfunctions, temperature fluctuations, or gas leaks. These sensors can trigger automatic responses or alerts, thereby preventing accidents from occurring. Furthermore, the IIoT has been proven to play a significant role in the promotion of environmental sustainability. This is achieved by optimizing resource usage and reducing waste. Sensors and connected systems may track energy consumption, water usage, emissions, and waste. This provides analytics that can assist companies in reducing their carbon footprint and enhancing their energy efficiency. IIoT also contributes to public health by improving healthcare systems. Wearable devices, such as smart medical equipment and remote monitoring tools, allow tracking patients' conditions in real time, thus enabling timely medical interventions. In addition, IIoT may help in monitoring public health systems, such as clean water availability, air quality, and sanitation, ensuring better living conditions for people [16]. IIoT has become a vital component of the smart city movement, wherein interconnected systems

promote enhanced management of urban infrastructure and services. IIoT technologies are utilized in various domains, including traffic management, waste disposal, water treatment, and public transportation. This integration of technology has been observed to enhance the efficiency, habitability, and sustainability of cities.

Wireless Sensor Networks (WSNs) are a key component of the Internet of Things, enabling data collection, monitoring, and communication across a wide range of applications. A WSN consists of a large number of spatially distributed sensor nodes, which may gather physical data such as temperature, humidity, pressure, light, motion, and more. These nodes communicate wirelessly with each other and a central processing unit, often referred to as a base station or sink node, which processes and analyses the collected data [14].

1. Problem statement

Wireless Sensor Networks constitute the fundamental infrastructure of numerous IoT applications by facilitating the aggregation of data from the physical environment. In IoT-enabled smart homes, WSNs is used to monitor various environmental factors such as temperature, light, and motion, thus allowing automation systems to optimize energy consumption and enhance security. Smart thermostats, smart light bulbs, smart grids and home security cameras are examples of WSNs [34].

WSNs enable remote patient monitoring and management by aggregating data from wearable sensors that track vital healthcare parameters. In smart city applications, WSNs play a crucial role in traffic monitoring, waste management, energy management, and public safety, thus enabling efficient and sustainable urban management.

However, WSNs also face several challenges such as limited energy and lifetime, network scalability and management, security and privacy [22].

As the data collected by sensors are of sensitive nature, ensuring robust security against cyber threats and maintaining privacy for users are crucial issues. Security in WSNs is fundamental because they are quite vulnerable to physical attacks and unauthorized access due to their wireless nature [18]. Various security measures such as encryption, authentication protocols, and secure data transmission are required to ensure data integrity and to protect sensitive information.

One of the biggest risks in WSNs is unauthorized access. Attackers may gain control over the sensor nodes, then disrupt communication between them or manipulate their data. Through the relevant security level evaluation, various vulnerabilities such as weak authentication protocols, unencrypted data transmission, or poor network segmentation can be identified and mitigated. This reduces the possibility of unauthorized access and ensures that only approved devices and users can communicate in the network.

Wireless Sensor Networks, by nature, are very vulnerable to both physical and cyberattacks. A security assessment helps to identify potential faint areas, such as weaknesses in communication protocols or physical vulnerabilities of sensor devices, which could be used for attacks. Having evaluated these threats, some preventive measures such as secure key exchange protocols, intrusion detection systems, or tamper-resistant hardware could be taken. One of the objectives of a security assessment is to ensure the integrity and availability of the WSN. Attackers could launch Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks to overwhelm the network, making it unavailable or inoperable. Similarly, data integrity could be compromised through malicious data processing. A comprehensive security evaluation can assess the risk of such attacks and thus help to implement some measures such as load balancing, traffic filtering, redundancy to maintain network availability and protect data accuracy.

In the context of IoT, the assessment of security levels in WSNs is critically important due to the sensitive nature of the data they collect and the intrinsic vulnerabilities of these systems [6]. As IoT devices, including sensor nodes of WSNs, are increasingly deployed in various applications like industrial automation, smart homes, healthcare, agriculture, ensuring robust security becomes essential to protect both the networks and the transmitted data. An effective security level assessment helps to identify potential threats, vulnerabilities, and weaknesses, ensuring that appropriate measures are taken to protect the network from cyberattacks and unauthorized access.

A major factor in building trust with users is security. The reliability of an IoT system depends on how well its security measures are designed and implemented. A robust security framework, validated through relevant assessments, improves the trustworthiness of WSNs.

The WSN faces numerous obstacles in developing reliable connectivity in terms of data transfer, quality of service, energy consumption, hardware complexity, and software. WSN limitations are based on compute, storage, and power consumption.

The challenges in the WSN are as follows [25]. Energy efficiency is the main issue because a WSN is a resource constrained network. Energy is consumed during the data packet routing activity and depends on the sensor battery life. Prolonged network lifetime is another challenge, which implies the sensor lifetime extension by reducing power consumption and extending the life cycle of the WSN. Providing Quality of service is still a difficult task as due to the limitations of the physical devices each application has its own QoS requirements and may ask for different QoS processing.

As for the fault tolerance, the sensor nodes must be able to maintain the functions performed by the WSN even in the case of limited battery power, node failure rates and external disturbances.

One more challenge is the dynamic environment as WSN may be deployed in hazardous areas, so they have to withstand difficult environmental conditions.

Providing data and information that is safe from all forms of threats and attacks is the primary objective of the security services in the WSN [28].

The privacy and security issues in WSNs have been thoroughly investigated. In the wireless sensor network, two types of attacks are primarily due to the nature of the transmission medium: active attacks and passive attacks [12]. In active attacks, the attackers attempt to search and corrupt the information, while in passive attacks, the attackers only attempt to steal the useful information such as passwords and confidential data. Nevertheless, in the WSN, the users and organizations need to be aware of both types of attack for secure communication among the sensor nodes.

In [11], WSNs attacks are classified in four categories depending on their impact on the network:

- Attacks introducing packets to the network.
- Attacks introducing noise to the network.
- Attacks introducing both noise and packets to the network.
- Attacks modifying the firmware of sensor nodes.

The following are the different security requirements in WSN [30]:

- Availability. For the message to proceed and for the nodes to be able to use the resource and the network, the resources must be available in the operational network.
- Authorization. It guarantees that the services in the operational network receive information from approved sensors.
- Authentication: It suggests that the communication's sensor nodes are authentic and have the right network access.
- Confidentiality: It ensures that the attackers cannot read or comprehend the message in the network.
- Integrity: It means that during the network communication, the message was not changed or tampered with. One can alter the entire packet by just introducing extra packets.

2. Literature review

Conventional information security technology employs rigorous access control mechanisms and data encryption strategies. However, as attack technology continues to evolve and the sophistication and diversity of attack tools and methods intensifies, these passive security technologies are no longer adequate to satisfy the elevated security requirements of network services that are particularly sensitive to security threats [27].

The huge amount of data transmitted within the network system increases the pressure on the detection system as the rate of network penetration and data transmission rises [4] thus it has become a priority to improve the intrusion detection systems.

An Intrusion Detection System (IDS) is a tool designed for the identification of intrusion attacks within wireless networks. In the event of an intrusion attack being detected by the system, the controller or supervisor will be alerted, enabling them to make informed decisions [35].

A machine-learning based detection method was proposed on [13].

Work [7] suggests an intrusion detection technique for solving malicious attack problems by using Machine Learning.

Study [20] presents the detection system for DDoS based on Deep Learning.

Despite the utilization of neural networks in the domain of intrusion detection, it is essential to acknowledge that prior to employing these networks for intrusion recognition, a substantial number of intrusion samples must be utilized for recognition training. This is imperative to ensure that the system possesses the capacity to accurately classify intrusion behaviours, thereby facilitating the effective identification of intrusions [36].

Papers [2, 24] focus on the application of genetic algorithms and fuzzy logic for optimizing security measures in WSNs.

A fuzzy logic-based risk estimation technique was proposed in [8].

Work [32] suggest to apply a fuzzy logic method for the attack identification, while [15] discusses a fuzzy defence mechanism.

Paper [5] considers a dynamic DDoS attack detection system, which is based on a fuzzy logic system for selecting the right classification algorithm.

Study [1] discusses a fuzzy logic system to detect the malicious behaviour of the nodes.

Study [26] proposes a fuzzy model for intrusion detection in WSNs.

A model for risk assessment was created in [17]. A new methodology to assess security risk in IoT is proposed in [29]. However, the challenge with the Industrial IoT is that the existing risk assessment approaches may be ineffective in the face of its highly dynamic systems [25].

So, the authors will discuss application of AI techniques for assessing the security risk level of a WSN node in this inquiry.

3. Background

Given the impossibility of constructing a system that is entirely free from vulnerabilities, the field of intrusion detection has emerged as a prominent area of research. The majority of contemporary security techniques, including firewalls, security gateways, code signatures and encryption technologies, constitute passive security defences that are incapable of proactively identifying and responding to threats [9].

Finding hidden covert attacks among a variety of routine communication processes is the main information security challenge. Because AI methods are based on human and natural reasoning, they can lead to improved performance. Telecommunication networks and systems make extensive use of AI technology [33]. Numerous AI techniques, such as fuzzy logic [3, 20], neural networks [19], and genetic algorithms [37], have been extensively used to extract known and unknown infiltration activities from a wide range of intricate and dynamic intrusion detection data. AI has shown encouraging results in detecting the essential components of Internet of Things communication, given its capacity to precisely detect network breaches and attacks.

Fuzzy logic is a mathematical technique that is applied in situations where there is uncertainty and imprecision in the data. Rather than employing rigorous labelling of members or non-members, fuzzy logic permits things to have different degrees of membership in a set. This reasoning allows the evaluation of partial facts.

In the area of security, risk and threat evaluation, fuzzy logic is employed to identify and prioritize threats in accordance with their frequency, detection, and severity.

The IF-THEN inference method is the main technique used by the fuzzy inference system (FIS). Fuzzification, rule base, decision-making, and defuzzification are the four primary components of FIS. The first unit transforms the input value from a crisp to a fuzzy format. The second unit determines the input's level of membership in each fuzzy set. The various fuzzy if-then rules are then subjected to inference. Lastly, the results of the fuzzy inference are used to calculate the output values [10].

Fuzzy models are typically created for fuzzy systems. The capabilities of current models based on fuzzy set theory should be examined in order to create a fuzzy model appropriate for assessing information security threats.

A fuzzy set A in X is defined as the set $A = \{x, \mu_A(x)\},\ x \in X$, where X is a range of values and $\mu_A(x)$ is the membership function, it defines the membership degree of element x to the set A.

The conversion of exact input facts into linguistic conceptions is performed by exploiting membership functions. A variety of membership function types, such as Gaussian, sigmoid, trapezoidal, triangular, singleton functions and others are available for application.

Although there are several kinds of fuzzy models, the Mamdani model is the most widely utilized.

$$If\ (x_1\ is\ A)\ and\ (x_2\ is\ B)\ and\ (x_3\ is\ C)\ Then\ (Y\ is\ D) \quad (1)$$

here x_1, x_2, x_3 are the antecedent part of fuzzy rules, Y is the consequent part of fuzzy rules, A, B, C, and D are fuzzy sets.

The outputs from these rules are determined using a min–max inference method, as follows.

$$\mu_{A\cup B\cup C}(x) = \min[\mu_A(x),\ \mu_B(x),\ \mu_C(x)] |\ x \in X \quad (2)$$

$$\mu_{A\cap B\cap C}(x) = \max[\mu_A(x),\ \mu_B(x),\ \mu_C(x)] |\ x \in X \quad (3)$$

Next, such defuzzification methods as Centre of Area, Bisector of Area, largest of Maximum, Mean of Maximum, Smallest of Maximum, etc. may be applied.

4. Methodology

Therefore, developing a security risk evaluation model based on fuzzy logic includes the following steps:

1. The identification of relevant risk elements is the initial step in constructing a fuzzy logic-based security evaluation model. These elements can be identified through a range of methods, including the review of relevant sources, the examination of testing data, or the consultation of expert perspectives.

2. The employment of membership functions is a method of determining the degree of correlation between a security factor and a specific set. The identification of these functions may be predicated on statistical data or the expertise of the relevant professionals.

3. In order to establish a correlation between the input variables, which represent security factors, and the output variable, which denotes the security risk level, it is necessary to formulate fuzzy production rules.

4. The fuzzy inference system (FIS) plays a fundamental role in the computation of the relationship between input and output variables by implementing membership functions and fuzzy production rules. The utilization of contemporary

software tools, such as MATLAB, can substantially facilitate the testing and implementation of this system.

5. The operability of the developed FIS may be enhanced by integrating it with other AI techniques.

Input linguistic variables of the FIS suggested in this inquiry are connection strength, response time and energy consumption. Its output variable is the security risk level of a particular IIoT device.

The connection strength is determined as the ratio of all responses made by the IIoT device to all requests sent by the server. A lower value indicates a possible threat, while a higher value indicates secure operations. The connection strength refers to the quality, stability, and reliability of the communication between wireless sensors of IIoT. In terms of security, connection strength is crucial for ensuring secure communication and protecting WSN from various vulnerabilities.

The response time of an IIoT sensor is defined as the time required for the sensor to detect a change in its environment and to transmit the corresponding data to the connected system or network. In the event of an attack on the network or unauthorized access, the response time of an IoT sensor increases due to a number of factors, including network congestion, resource depletion, disruption to communication.

The energy consumption of an IoT sensor node is the amount of power it uses for collecting data, processing, and communication with other nodes. When the WSN is under attack or in case of unauthorized access, the energy consumption of the sensor node increases due to the additional processing or data transmission.

The security risk level of an IIoT sensor node is a measure of the potential vulnerability of the node to threats such as attacks, unauthorized access, data interception, or malware, based on its design and the robustness of its security measures.

The considered fuzzy inference system for the security risk level evaluation receives three inputs: connection strength (CS), response time (RT), and energy consumption (EC). These inputs are subsequently processed through a process of fuzzification, and the membership value for each is determined through the application of specific membership functions.

$$CS \in [0,1] \rightarrow \{(CS_{low};\ \mu_{CSlow}),\ (CS_{med};\ \mu_{CSmed}),\ (CS_{high};\ \mu_{CShigh})\} \tag{4}$$

$$RT \in [0,1] \rightarrow \{(RT_{low};\ \mu_{RTlow}),\ (RT_{med};\ \mu_{RTmed}),\ (RT_{high};\ \mu_{RThigh})\} \tag{5}$$

$$EC \in [0,1] \rightarrow \{(EC_{low};\ \mu_{EClow}),\ (EC_{med};\ \mu_{ECmed}),\ (EC_{high};\ \mu_{EChigh})\} \tag{6}$$

The linguistic terms we have chosen for the inputs are "Low," "Medium," and "High," which can be regarded as intuitive categories associated with common assessment terms.

The fuzzy-based security risk level outcome is denoted as SRL, which is a value defuzzified based on five sets with corresponding membership functions:

$$SRL \in [0,1] \rightarrow \{(SRL_{vl};\ \mu_{SRLvl}),\ (SRL_{low};\ \mu_{SRLlow}),\ (SRL_{med};\ \mu_{SRLmed}),\ (SRL_{high};\ \mu_{SRLhigh}),\ (SRL_{vh};\ \mu_{SRLvh})\} \tag{7}$$

The output classifications for the proposed security FIS are "Very low", "Low," "Medium", "High," and "Very High" that facilitates decision-making.

The authors have decided to use triangle membership and trapezoidal functions in their study because they are simple to use, easy to comprehend, and can aid in the smooth transitions between linguistic phrases.

Trapezoid membership functions for the input variables can be defined as

$$\mu_{low}(CS) = \begin{cases} 1 \ \ if \ \ CS \le 30 \\ \dfrac{50-CS}{50-30} \ \ if \ \ 30 < CS \le 40 \\ 0 \ \ if \ \ CS > 50 \end{cases}$$

$$\mu_{med}(CS) = \begin{cases} 0 \ \ if \ \ CS \le 30 \\ \dfrac{CS-30}{50-30} \ \ if \ \ 30 < CS \le 50 \\ 1 \ \ if \ \ 50 < CS \le 70 \\ \dfrac{90-CS}{90-70} \ \ if \ \ 70 < CS < 90 \\ 0 \ \ if \ \ CS \ge 90 \end{cases}$$

$$\mu_{high}(CS) = \begin{cases} 0 \ \ if \ \ CS \le 70 \\ \dfrac{CS-70}{90-70} \ \ if \ \ 70 < CS \le 90 \\ 1 \ \ if \ \ CS > 90 \end{cases}$$

$$\mu_{low}(RT) = \begin{cases} 1 \ \ if \ \ RT \le 1 \\ \dfrac{2-RT}{2-1} \ \ if \ \ 1 < RT \le 2 \\ 0 \ \ if \ \ RT > 2 \end{cases}$$

$$\mu_{med}(RT) = \begin{cases} 0 \ \ if \ \ RT \le 1 \\ \dfrac{RT-1}{2-1} \ \ if \ \ 1 < RT \le 2 \\ 1 \ \ if \ \ 2 < RT \le 8 \\ \dfrac{10-RT}{10-8} \ \ if \ \ 8 < RT < 10 \\ 0 \ \ if \ \ RT \ge 10 \end{cases}$$

$$\mu_{high}(RT) = \begin{cases} 0 \ \ if \ \ RT \le 8 \\ \dfrac{RT-8}{10-8} \ \ if \ \ 8 < RT \le 10 \\ 1 \ \ if \ \ RT > 10 \end{cases}$$

$$\mu_{low}(EC) = \begin{cases} 1 \ \ if \ \ EC \le 10 \\ \dfrac{50-EC}{50-10} \ \ if \ \ 10 < EC \le 50 \\ 0 \ \ if \ \ EC > 50 \end{cases}$$

$$\mu_{med}(EC) = \begin{cases} 0 \ \ if \ \ EC \le 10 \\ \dfrac{EC-10}{50-10} \ \ if \ \ 10 < EC \le 50 \\ 1 \ \ if \ \ 50 < EC \le 100 \\ \dfrac{200-EC}{200-100} \ \ if \ \ 100 < EC < 200 \\ 0 \ \ if \ \ EC \ge 200 \end{cases}$$

$$\mu_{high}(EC) = \begin{cases} 0 \ \ if \ \ EC \le 100 \\ \dfrac{EC-100}{200-100} \ \ if \ \ 100 < EC \le 200 \\ 1 \ \ if \ \ EC > 200 \end{cases}$$

Membership functions for the output variable, which are of triangular type, are determined as

$$\mu_{vl}(SRL) = \begin{cases} 1 \ \ if \ \ SRL \le 0 \\ \dfrac{25-SRL}{25} \ \ if \ \ 0 < SRL \le 25 \\ 0 \ \ if \ \ 25 < SRL \end{cases}$$

$$\mu_{low}(SRL) = \begin{cases} 0 \ \ if \ \ SRL \le 0 \\ \dfrac{SRL-0}{25} \ \ if \ \ 0 < SRL \le 25 \\ \dfrac{50-SRL}{25} \ \ if \ \ 25 < SRL \le 50 \\ 0 \ \ if \ \ 50 < SRL \end{cases}$$

$$\mu_{med}(SRL)=\begin{cases}0 \ if \ SRL \le 25\\ \dfrac{SRL-25}{25} \quad if \ 25 < SRL \le 50\\ \dfrac{75-SRL}{25} \quad if \ 50 < SRL \le 75\\ 0 \ if \ 75 < SRL\end{cases}$$

$$\mu_{high}(SRL)=\begin{cases}0 \ if \ SRL \le 50\\ \dfrac{SRL-50}{25} \quad if \ 50 < SRL \le 75\\ \dfrac{100-SRL}{25} \quad if \ 75 < SRL \le 100\\ 0 \ if \ 100 < SRL\end{cases}$$

$$\mu_{vh}(SRL)=\begin{cases}0 \ if \ SRL \le 75\\ \dfrac{SRL-75}{25} \quad if \ 75 < SRL \le 100\\ 1 \ if \ 100 < SRL\end{cases}$$

Table 1 outlines the fuzzy rule base for the developed fuzzy inference system. The rule base is a set of if-then rules that define the relationship between input fuzzy variables and the corresponding control actions. The table outlines the possible combinations of input values and a corresponding output value.

Table 1. Rule base

	Connection strength	Response time	Energy consumption	Security risk level
1	Low	Low	Low	High
2	Low	Low	Medium	High
3	Low	Low	High	High
4	Low	Medium	Low	High
5	Low	Medium	Medium	Very high
6	Low	Medium	High	Very High
7	Low	High	Low	High
8	Low	High	Medium	Very high
9	Low	High	High	Very high
10	Medium	Low	Low	Very low
11	Medium	Low	Medium	Medium
12	Medium	Low	High	Medium
13	Medium	Medium	Low	Low
14	Medium	Medium	Medium	Medium
15	Medium	Medium	High	High
16	Medium	High	Low	Medium
17	Medium	High	Medium	Medium
18	Medium	High	High	Very high
19	High	Low	Low	Very low
20	High	Low	Medium	Very low
21	High	Low	High	Low
22	High	Medium	Low	Very low
23	High	Medium	Medium	Very low
24	High	Medium	High	Low
25	High	High	Low	Low
26	High	High	Medium	Low
27	High	High	High	Low

The authors suggest using the Centre of Area approach for defuzzification. It returns the appropriate crisp value after locating the centre of the fuzzy set's area.

5. Simulation

The MATLAB software can be utilized to validate the operability of the designed FIS for security evaluation of a wireless node of IIoT. The software facilitates the visualization and refinement of membership functions, rule bases, and output surfaces, thereby contributing to the development of more accurate decision-making systems. Utilizing MATLAB for the simulation of FISs provides distinct advantages, including the capacity for rapid prototyping and reliable performance evaluation. Furthermore, integrating MATLAB with machine learning and optimization tools allows for the enhancement of the fuzzy inference systems, rendering them more efficient.

Fig. 1 demonstrates the interface of the designed FIS in MATLAB software packet. Here, the FIS Editor displays information about the designed fuzzy inference system. We have chosen the Mamdani Type-1 FIS, it is a fuzzy inference system that applies min-max operations and the centroid method of defuzzification to produce a crisp output value.

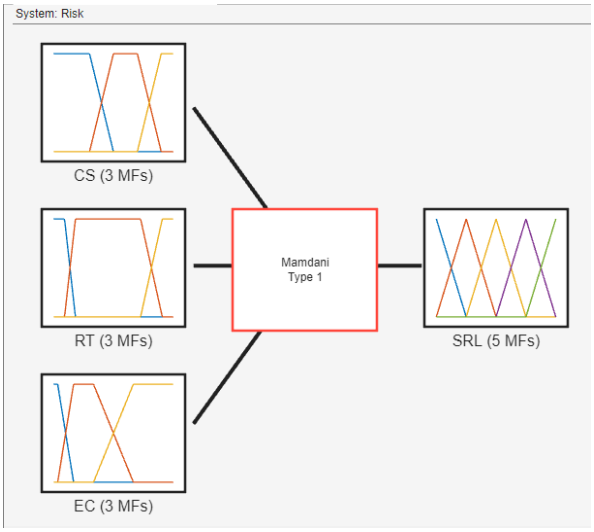


Fig. 1. Fuzzy inference system in MATLAB

We assigned the input and output values. Next, we specified the rule base.

Fig. 2. illustrates the surface of the FIS, it is a representation that shows how the fuzzy inference system maps input variables to output responses based on the defined rule base.

To validate the functionality of the developed FIS, a simulation was performed to generate the required output value.

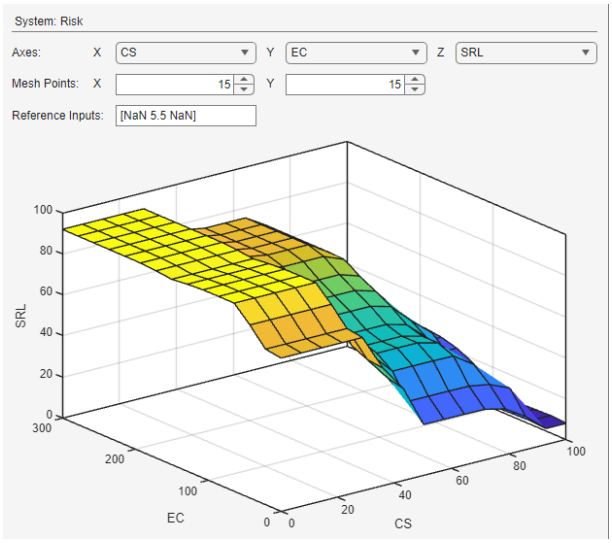


Fig. 2. Surface plot against Security risk level between connection strength and response time

For the first case, let Connection strength be 9%, Response time be 3 s, and the Energy consumption be 15 mW. According to Fig. 3, we get Security risk level of 8.15%. This means that there is a low possibility of malicious attack into the wireless sensor of IIoT.

For the second case, let Connection strength be 25%, Response time be 5.5 s, and Energy consumption be 60 mW. According to Fig. 4, we get Security risk level of 92%. This means that there is a high possibility of malicious attack into the wireless sensor of IIoT.

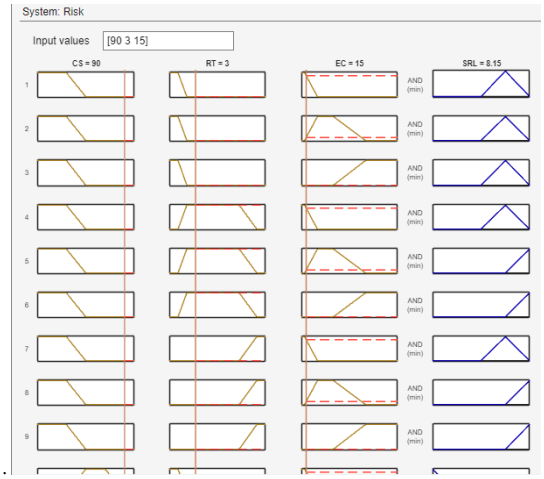


Fig. 3. Simulation outcome (first case)

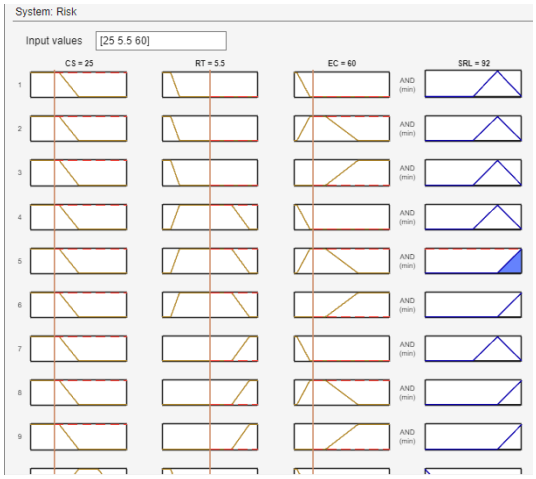


Fig. 4. Simulation outcome (second case)

6. Optimization

To improve the accuracy and efficiency of the developed fuzzy inference system, an optimization was applied in MATLAB to optimize its parameters using AL techniques. The authors employed two techniques, namely Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). Then, results of two optimization processes were compared.

In terms of optimization problem, the fuzzy inference system can be defined as a mapping function:

$$SRL = F(CS, RT, EC; \theta) \tag{8}$$

where θ are all parameters of the FIS to be optimized, namely membership function shapes and fuzzy rule base.

The goal of optimization is to find:

$$\theta^* = arg\min_{\theta} J(\theta) \tag{9}$$

where $J(\theta)$ is the error between the FIS output and target values.

Vector θ^* defines the best membership functions and the most effective fuzzy rule base, so that the FIS produces accurate security risk levels based on IIoT features.

Partial Swarm Optimization is a population-based meta-heuristic that suits well for tuning complex nonlinear systems like FIS.

To optimize the FIS, PSO minimizes the prediction error over a dataset

$$S = \{(CS_i, RT_i, EC_i; SRL_i)\}_{i=1}^{N} \tag{10}$$

where SRL_i is the true security risk level.

The objective function of optimization is the mean squared error (MSE) between predicted and target outputs:

$$J(\theta) = \frac{1}{N}\sum_{i=1}^{N}\left[F(CS_i, RT_i, EC_i; \theta) - SRL_i\right]^2 \tag{11}$$

In the optimization process each particle represents a candidate solution θ_i. Next, each particle updates its position in the search space based on its own best solution and the global best found so far.

The set of n particles in the swarm is denoted as

$$P = \{\theta_1, \theta_2, \ldots, \theta_n\} \tag{12}$$

Velocity update is performed as:

$$v_i(t+1) = wv_i(t) + c_1r_1(p_i - \theta_i(t)) + c_2r_2(g - \theta_i(t)) \tag{13}$$

where v_i is the velocity of particle i, w is inertia weight, c_1, c_2 are cognitive and social coefficients, r_1, r_2 are random numbers in [0,1], p_i is the personal best solution of particle i, g is global best, t is the current iteration.

Position update is performed as:

$$\theta_i(t+1) = \theta_i(t) + v_i(t+1) \tag{14}$$

Thus, the PSO continues until convergence, or a maximum number of iterations. If the global best fitness value does not improve beyond a small threshold for several consecutive iterations the PSO also stops.

Therefore, in this study, the PSO algorithm was used to adjust the parameters of the membership functions and rule weights to minimize the discrepancy between the FIS output and the desired values, which is typically measured by a cost function such of MSE. Figure 5 shows the optimization process graph.

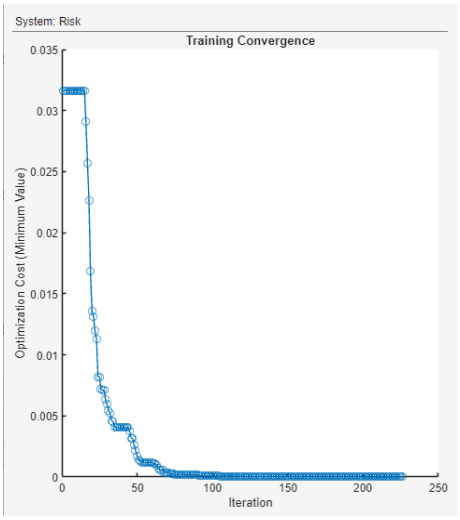


Fig. 5. Partial swarm optimization

The GA aims to find the optimal set of parameters θ^*, which define the membership functions and rule base, by minimizing the difference between the FIS output and the actual target values in the dataset S (10).

In GA optimization objective function is the same as the one for the PSO, defined by (11).

In the optimization process each chromosome encodes membership function parameters for each input and output membership functions and rule structure.

Here, such GA operators are applied as selection (for choosing the best-performing individuals), crossover (for exchanging segments of chromosomes), mutation (for changing some gene values randomly).

Thus, the GA searches for θ^* that minimizes the MSE.

GA stops after a fixed number of generations or when the fitness improvement is below a threshold.

Therefore, a genetic algorithm was employed for optimization of the developed FIS in MATLAB. This optimization process also focused on tuning the membership function parameters and rule weights to minimize the error between the predicted and desired output values. In MATLAB environment, the objective function evaluated the FIS output against a predefined dataset using a fitness metric such as MSE. Through successive generations involving selection, crossover, and mutation operations, the GA iteratively improved the FIS parameters. Figure 6 shows the GA optimization process graph.

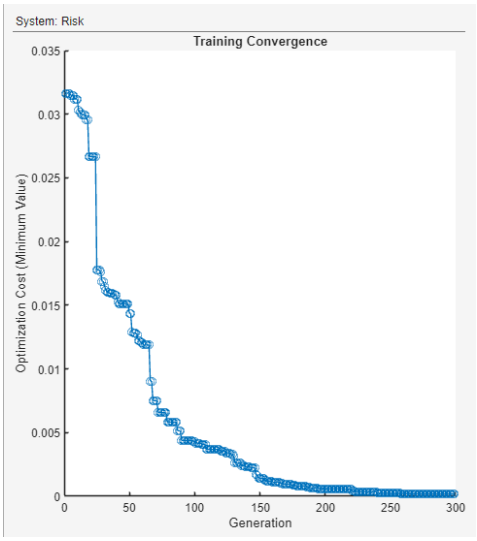


Fig. 6. Optimization with genetic algorithm

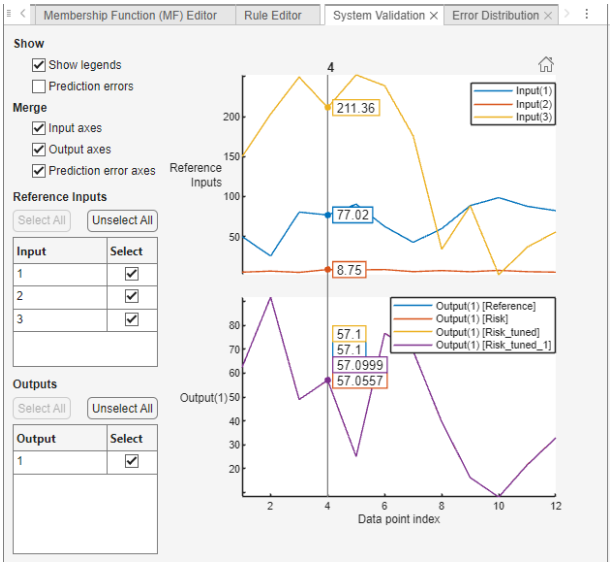


Fig. 7. Validation of the FIS

While both methods successfully enhanced the FIS, some differences in performance were observed.

PSO generally required fewer iterations to converge compared to GA. Due to its simpler structure and fewer control parameters, PSO exhibited faster convergence and lower computational cost in most simulation runs. The FIS optimized with PSO achieved lower mean squared compared to the GA-optimized FIS. This suggests that PSO was more effective in finding a near-optimal solution in the parameter space. GA demonstrates better exploration capabilities due to its genetic diversity mechanisms such as crossover and mutation, which helped avoid local minima. However, this comes at the cost of slower convergence and higher variability between runs. Overall, PSO proved to be more efficient and slightly more accurate in optimizing the FIS. However, GA may be preferred in other cases, for instance in combination with artificial neural networks.

Next, the system validation was performed for the initial FIS and its optimized versions obtained via GA and PSO. The validation involved testing the models on an independent dataset not used during the training or optimization phases, to objectively assess their generalization performance. Figure 7 shows the FIS validation graph. The results indicated that both optimized FIS models outperformed the original, with the PSO-optimized FIS achieving the lowest error values confirming its superior prediction capability. These findings demonstrate that optimization significantly improves the accuracy of fuzzy inference systems.

Therefore, the optimized FIS achieved better accuracy, ensuring more efficient and reliable decision-making within the wireless sensor network, that makes it suitable for dynamic and uncertain environments, such as wireless sensor networks.

The developed and optimized fuzzy inference system can be effectively utilized in wireless sensor networks to evaluate the security risk level of individual sensor nodes. By analysing key input parameters such as connection strength, response time, and energy consumption, the system enables intelligent and context-aware assessment of possible node-level vulnerabilities. This facilitates proactive security monitoring and supports the implementation of adaptive defence mechanisms within the WSN infrastructure, thus enhancing the overall resilience of the network against potential threats

7. Conclusion

In the context of Industrial IoT, Wireless Sensor Networks are integral to a wide range of applications that impact society and business. However, their wireless nature and often limited resources make them particularly susceptible to security threats. A thorough security level assessment is crucial to identify vulnerabilities, protect sensitive data, and ensure the overall integrity and availability of these networks. By regularly assessing and improving the security posture of WSNs, businesses can safeguard their IIoT systems, maintain compliance, and foster trust among users, all while minimizing the risk of data breaches and cyberattacks. Security should be a continuous process, as the rapid evolution of IoT technologies and cyber threats demands ongoing vigilance and adaptation.

AI techniques, including fuzzy logic, neural networks and genetic algorithms, have demonstrated their efficacy in a wide range of challenges. This inquiry considers a fuzzy logic-based approach that has the potential to enhance the informational security of IIoT networks. The fuzzy inference system developed by the authors of this study evaluates the security risk level of an IIoT device and may be employed as part of IIoT security measures. The methodology developed in this paper is intended for practical application. The methodology outlined in this paper involves the definition of three input and one output linguistic variables, their terms and membership functions. The rule base comprising twenty-seven rules was developed. Using the fuzzy inference system in WSN of the Industrial Internet of Things is supported by the simulation results. Other parameters can be taken into consideration to improve the developed FIS. In future inquiries, the security risk level evaluation mechanism is to be improved by revising other AI techniques.

References

[1] A. P., H., & K., K. (2019). Secure-MQTT: An efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. *EURASIP Journal on Wireless Communications and Networking*, *2019*(1), 90. https://doi.org/10.1186/s13638-019-1402-8

[2] Al Hayali, S., Ucan, O., Rahebi, J., & Bayat, O. (2019). Detection of Attacks on Wireless Sensor Network Using Genetic Algorithms Based on Fuzzy. *International Journal of Renewable Energy Development*, *8*(1), 57–64. https://doi.org/10.14710/ijred.8.1.57-64

[3] Almseidin, M., Al-Sawwa, J., & Alkasassbeh, M. (2021). Anomaly-based Intrusion Detection System Using Fuzzy Logic. *2021 International Conference on Information Technology (ICIT)*, 290–295. https://doi.org/10.1109/ICIT52682.2021.9491742

[4] Alqahtani, M., Gumaei, A., Mathkour, H., & Maher Ben Ismail, M. (2019). A Genetic-Based Extreme Gradient Boosting Model for Detecting Intrusions in Wireless Sensor Networks. *Sensors*, *19*(20), 4383. https://doi.org/10.3390/s19204383

[5] Alsirhani, A., Sampalli, S., & Bodorik, P. (2019). DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark. *IEEE Transactions on Network and Service Management*, *16*(3), 936–949. https://doi.org/10.1109/TNSM.2019.2929425

[6] Alsumayt, A., Alshammari, M., Alfawaer, Z. M., Al-Wesabi, F. N., El-Haggar, N., Aljameel, S. S., Albassam, S., AlGhareeb, S., Alghamdi, N. M., & Aldossary, N. (2024). Efficient security level in wireless sensor networks (WSNs) using four-factors authentication over the Internet of Things (IoT). *PeerJ Computer Science*, *10*, e2091. https://doi.org/10.7717/peerj-cs.2091

[7] Arunkumar, M., & Ashok Kumar, K. (2022). Malicious attack detection approach in cloud computing using machine learning techniques. *Soft Computing*, *26*(23), 13097–13107. https://doi.org/10.1007/s00500-021-06679-0

[8] Atlam, H. F., & Wills, G. B. (2019). An efficient security risk estimation technique for Risk-based access control model for IoT. *Internet of Things*, *6*, 100052. https://doi.org/10.1016/j.iot.2019.100052
[9] Bajpai, P., Sood, A. K., & Enbody, R. J. (2018). The art of mapping IoT devices in networks. *Network Security*, *2018*(4), 8–15. https://doi.org/10.1016/S1353-4858(18)30033-3
[10] Devi, R., Jha, R. K., Gupta, A., Jain, S., & Kumar, P. (2017). Implementation of Intrusion Detection System using Adaptive Neuro-Fuzzy Inference System for 5G wireless communication network. *AEU – International Journal of Electronics and Communications*, *74*, 94–106. https://doi.org/10.1016/j.aeue.2017.01.025
[11] Diaz, A., & Sanchez, P. (2016). Simulation of Attacks for Security in Wireless Sensor Network. *Sensors*, *16*(11), 1932. https://doi.org/10.3390/s16111932
[12] Ee, S. J., Tien Ming, J. W., Yap, J. S., Lee, S. C. Y., & Tuz Zahra, F. (2020). *Active and Passive Security Attacks in Wireless Networks and Prevention Techniques*. https://doi.org/10.36227/techrxiv.12972857
[13] He, Z., Zhang, T., & Lee, R. B. (2017). Machine Learning Based DDoS Attack Detection from Source Side in Cloud. *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 114–120. https://doi.org/10.1109/CSCloud.2017.58
[14] Huanan, Z., Suping, X., & Jiannan, W. (2021). Security and application of wireless sensor network. *Procedia Computer Science*, *183*, 486–492. https://doi.org/10.1016/j.procs.2021.02.088
[15] Iyengar, N. Ch. S. N., Banerjee, A., & Ganapathy, G. (2022). A Fuzzy Logic Based Defense Mechanism against Distributed Denial of Services Attack in Cloud Environment. *International Journal of Communication Networks and Information Security (IJCNIS)*, *6*(3). https://doi.org/10.17762/ijcnis.v6i3.864
[16] Kaur, R. (2024). Internet of things: An Overview. *International Journal For Multidisciplinary Research*, *6*(2), 14323. https://doi.org/10.36948/ijfmr.2024.v06i02.14323
[17] Khambhammettu, H., Boulares, S., Adi, K., & Logrippo, L. (2013). A framework for risk assessment in access control systems. *Computers & Security*, *39*, 86–103. https://doi.org/10.1016/j.cose.2013.03.010
[18] Kumar, S. A., Vealey, T., & Srivastava, H. (2016). Security in Internet of Things: Challenges, Solutions and Future Directions. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 5772–5781. https://doi.org/10.1109/HICSS.2016.714
[19] Ma, T., Wang, F., Cheng, J., Yu, Y., & Chen, X. (2016). A Hybrid Spectral Clustering and Deep Neural Network Ensemble Algorithm for Intrusion Detection in Sensor Networks. *Sensors*, *16*(10), 1701. https://doi.org/10.3390/s16101701
[20] Mittal, M., Kumar, K., & Behal, S. (2023). Deep learning approaches for detecting DDoS attacks: A systematic review. *Soft Computing*, *27*(18), 13039–13075. https://doi.org/10.1007/s00500-021-06608-1
[21] Moradi, M., Moradkhani, M., & Tavakoli, M. B. (2022). A Real-Time Biometric Encryption Scheme Based on Fuzzy Logic for IoT. *Journal of Sensors*, *2022*, 1–15. https://doi.org/10.1155/2022/4336822
[22] Naskar, S. (2023). Wireless Sensor Networks Challenges and Solutions. In J. Sen, M. Yi, F. Niu, & H. Wu (Eds), *Wireless Sensor Networks—Design, Applications and Challenges*. IntechOpen. https://doi.org/10.5772/intechopen.109238
[23] Nguyen, T. M., Vo, H. H.-P., & Yoo, M. (2024). Enhancing Intrusion Detection in Wireless Sensor Networks Using a GSWO-CatBoost Approach. *Sensors*, *24*(11), 3339. https://doi.org/10.3390/s24113339
[24] Nurse, J. R. C., Creese, S., & De Roure, D. (2017). Security Risk Assessment in Internet of Things Systems. *IT Professional*, *19*(5), 20–26. https://doi.org/10.1109/MITP.2017.3680959
[25] Patel, N. R., & Kumar, S. (2018). Wireless Sensor Networks' Challenges and Future Prospects. *2018 International Conference on System Modeling & Advancement in Research Trends (SMART)*, 60–65. https://doi.org/10.1109/SYSMART.2018.8746937
[26] Sathishkumar, P., Gnanabaskaran, A., Saradha, M., & Gopinath, R. (2024). Dos attack detection using fuzzy temporal deep long Short-Term memory algorithm in wireless sensor network. *Ain Shams Engineering Journal*, *15*(12), 103052. https://doi.org/10.1016/j.asej.2024.103052
[27] Sharma, R., Vashisht, V., & Singh, U. (2020). eeTMFO/GA: A secure and energy efficient cluster head selection in wireless sensor networks. *Telecommunication Systems*, *74*(3), 253–268. https://doi.org/10.1007/s11235-020-00654-0
[28] Sharma, S., Yadav, A., Panchal, M., & Vyavahare, P. D. (2019). Classification of Security Attacks in WSNs and Possible Countermeasures: A Survey. *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 1–6. https://doi.org/10.1109/ANTS47819.2019.9118119
[29] Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. (2018). A risk assessment methodology for the Internet of Things. *Computer Communications*, *129*, 67–79. https://doi.org/10.1016/j.comcom.2018.07.024
[30] Sinha, P., Jha, V. K., Rai, A. K., & Bhushan, B. (2017). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. *2017 International Conference on Signal Processing and Communication (ICSPC)*, 288–293. https://doi.org/10.1109/CSPC.2017.8305855
[31] Tamrakar, A. K., Shukla, A., Kalifullah, A. H., Reegu, F. A., & Shukla, K. (2022). Extended review on internet of things (IoT) and its characterisation. *International Journal of Health Sciences*, 8490–8500. https://doi.org/10.53730/ijhs.v6nS2.7177
[32] Wang, J., Li, R., Wang, J., Ge, Y., Zhang, Q., & Shi, W. (2020). Artificial intelligence and wireless communications. *Frontiers of Information Technology & Electronic Engineering*, *21*(10), 1413–1425. https://doi.org/10.1631/FITEE.1900527
[33] Wang, J., & Yang, G. (2008). An intelligent method for real-time detection of DDoS attack based on fuzzy logic. *Journal of Electronics (China)*, *25*(4), 511–518. https://doi.org/10.1007/s11767-007-0056-6
[34] Yilmaz, S., & Dener, M. (2024). Security with Wireless Sensor Networks in Smart Grids: A Review. *Symmetry*, *16*(10), 1295. https://doi.org/10.3390/sym16101295
[35] Zhang, F., Kodituwakku, H. A. D. E., Hines, J. W., & Coble, J. (2019). Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. *IEEE Transactions on Industrial Informatics*, *15*(7), 4362–4369. https://doi.org/10.1109/TII.2019.2891261
[36] Zhang, J. (2022). Network Security Situational Awareness Based on Genetic Algorithm in Wireless Sensor Networks. *Journal of Sensors*, *2022*, 1–11. https://doi.org/10.1155/2022/8292920
[37] Zhang, Y., Li, P., & Wang, X. (2019). Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. *IEEE Access*, *7*, 31711–31722. https://doi.org/10.1109/ACCESS.2019.2903723

Ph.D. Olena Semenova
e-mail: semenova.o.o@vntu.edu.ua

Received the Ph.D. degree in Computer Systems and Elements from Vinnytsia National Technical University in 2007. She is currently an associated professor at Department of Infocommunication Systems and Technologies, Vinnytsia National Technical University. She has over 170 scientific papers.
Her research interests include telecommunication networks and artificial intelligence.

https://orcid.org/0000-0001-5312-9148

Prof. Ing. Natalia Kryvinska
e-mail: natalia.kryvinska@uniba.sk

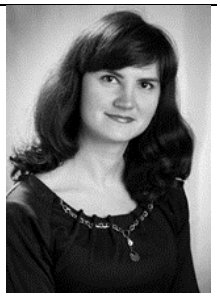
Received the Ph.D. degree in Electrical & IT Engineering from Vienna University of Technology, and the habilitation degree in Management Information Systems from Comenius University in Bratislava. She is a full professor at Department of Information Management and Business Systems, Comenius University in Bratislava. She has over 450 scientific papers.
Her research interests include complex service systems engineering, service analytics, applied mathematics.

https://orcid.org/0000-0003-3678-9229

Ph.D. Olha Voitsekhovska
e-mail: o_voytsekhovska@vntu.edu.ua

Received the Ph.D. degree in System Analysis from Vinnytsia National Technical University in 2022. She is currently an associated professor at Department of System Analysis and Information Technologies, Vinnytsia National Technical University. She has over 90 scientific papers.
Her research interests include system analysis and artificial intelligence.

https://orcid.org/0000-0001-8504-1204



M.Sc. Andrii Dzhus
e-mail: dzhuz1988@gmail.com

Received the M.Sc. degree in Telecommunication and Radiotechnics from Vinnytsia National Technical University in 2010. He is currently a Ph.D. student at the Department of Infocommunication Systems and Technologies, Vinnytsia National Technical University.
His research interests include telecommunication networks, artificial intelligence, and programming.

https://orcid.org/0009-0005-3583-5766

M.Sc. Volodymyr Martyniuk
e-mail: vm4ukr@gmail.com

Received the M.Sc. degree in Telecommunication and Radiotechnics from Vinnytsia National Technical University in 2010. He is currently a Ph.D. student at the Department of Infocommunication Systems and Technologies, Vinnytsia National Technical University.
His research interests include telecommunication networks, artificial intelligence, and programming.

https://orcid.org/0009-0006-8421-0348