# Optimized Fuzzy Secure Scheme for Trust Assessment in IoMT

Olena Semenova, Olha Voitsekhovska, Andrii Dzhus, and Vladyslav Kuzniak

*Vinnytsia National Technical University, Vinnytsia, Ukraine*

https://doi.org/10.26636/jtit.2026.2.2494

**Abstract — Rapid development of technologies associated with the Internet of Medical Things (IoMT) has enabled continuous patient monitoring, diagnosis, and integration of medical devices with various healthcare infrastructures. However, the increasing heterogeneity of IoMT systems and their connectivity-related features introduce also security risks, such as data tampering, unauthorized access, and unsafe behavior of the devices themselves. Traditional trust assessment techniques often fail to handle the uncertainty inherent in medical data and devices. This paper presents a fuzzy logic-based secure trust assessment scheme designed for IoMT, which integrates behavioral and communication indicators to compute trust scores for a device. The scheme employs a fuzzy logic-based approach and provides a trust level evaluation procedure suitable for resource-limited IoMT devices. A fuzzy inference system was developed specifically for this scheme and further optimized by applying evolutionary algorithms. The experimental results demonstrate an improved accuracy of the optimized model in evaluating the trust level of devices and show its enhanced accuracy compared to a classical trust mechanism.**

***Keywords — IoMT, fuzzy logic, trust management, security, optimization***

## 1. Introduction

The emergence of IoMT in healthcare care has transformed the manner in which medical services are provided, as it is capable of significantly enhancing patient care through online monitoring, the use of wearable technology, and the ability to access medical consultations quickly and remotely. However, as IoT technologies continue to evolve, protecting sensitive health information has emerged as a significant challenge for researchers [1]. As data are collected, transmitted, and stored by medical devices, there is, unfortunately, a corresponding increase in cyber incidents, data breaches, and privacy violations associated with medical equipment [2].

The use of IoT devices may result in unauthorized access to confidential patient data, including email accounts, passwords, and private records [3]. Security, privacy, and safety are important factors and pose significant challenges in the implementation of IoT systems. IoT applications encompass numerous devices and generate substantial data volumes. Therefore, in order to ensure data security, it is essential to guarantee that the communicating IoT devices interact in a trustworthy manner [4].

Cryptography and access control are the two conventional approaches to safeguarding IoT networks. If properly implemented, they can be considered hard measures that ensure system security. However, since hacked network nodes might produce false or misleading information while still offering legitimate cryptographic credentials, cryptography alone is not capable of ensuring security in heterogeneous IoT systems. Similarly, typical centralized access control is inappropriate for distributed contexts and access control mechanisms are susceptible to internal harmful attacks. However, trust management, which is regarded a soft security mechanism, can address the aforementioned problems by improving, rather than replacing hard security procedures [5].

Trust management is employed to evaluate and ensure network reliability by assigning a trust value, i.e. its trust level, to each node. Consequently, the information sent by a node with a high trust level is considered reliable [6].

Therefore, trust management has emerged as an important components of IoT security. By analyzing behavioral patterns, data integrity, and communication quality, trust assessment mechanisms aim to quantify the reliability of devices. Traditional trust evaluation models – such as binary classification, threshold-based detection, and probabilistic schemes – offer a quite limited degree of effectiveness when applied in IoT systems. Furthermore, resource-limited medical devices of IoMT may experience communication errors or interruptions that should not be misinterpreted as malicious behavior. These challenges require efficient trust assessment techniques that are capable of differentiating between benign fluctuations and genuine threats.

Artificial intelligence (AI) techniques are a promising solution for assessing trust in IoMT networks, as they involve a data-centric evaluation of device-related and traffic behavior. Unlike traditional static or rule-based mechanisms, AI approaches can consider non-linear dependencies among medical data streams, allowing trust level estimation under complicated network conditions. Approaches based on fuzzy logic, neural networks, and evolutionary optimization offer advanced reasoning, parameter tuning, and efficient searching of complex parameter spaces – features which are essential for handling uncertainty in medical data communication.

Furthermore, AI-based trust modeling may provide continuous improvement as new traffic patterns or threat vectors emerge, ensuring that trust evaluation remains relevant to security challenges. This makes the fuzzy logic theory partic-

ularly suitable for implementation in IoMT, where decisions often depend on slight variations in physiological data.

This paper proposes a fuzzy logic-based trust assessment scheme for IoMT networks. The proposed model integrates several trust indicators concerning both behavioral anomalies and reliability of communication. The designed model computes the trust scores of a device. The resulting trust values may be utilized to establish secure interaction between devices or provide access control, thus increasing resilience against threats.

## 2. Problem Definition

The IoMT can be regarded as a set of connected medical devices, wearable sensors, implantable technologies, and clinical information systems that work together to ensure continuous provision of healthcare to the population. The complexity of IoMT networks stems from the heterogeneity of its devices: from low-power wearable monitors to complex systems and smart equipment. IoMT technology is defined by its vulnerable and unsafe nature, as medical devices operate in a sphere in which even small inaccuracies or delays can lead to severe consequences for patients' health.

As IoMT systems become increasingly connected, they are also exposed to emerging cybersecurity threats. Attackers can manipulate physiological data streams, impersonate medical devices, inject unauthorized control commands, or exploit vulnerabilities in wireless communication protocols. Furthermore, data collected by these devices are often noisy, incomplete, or suffer from sudden fluctuations and distortions caused by patient movement or environmental factors. These uncertainties complicate the discovery of benign anomalies and malicious actions. Finally, regulatory frameworks can impose strict requirements related to confidentiality and integrity, thus requiring the introduction of effective security mechanisms.

Although IoMT holds considerable potential, concerns about security and privacy have hindered its extensive implementation within the healthcare sector [7], [8]. This problem is exacerbated by the introduction of new technologies, including mobile devices, cloud services, and remote applications that are being integrated into the healthcare system [9].

The lack of attention to security and privacy in IoMT hinders the complete utilization of these technologies to address existing issues in healthcare. Thus, it is essential to define security and privacy within the healthcare sector.

Although these technologies improve data processing in the healthcare sector, they also significantly increase the risk of security and privacy breaches of medical information. The growing reliance on these technologies can lead to an increased vulnerability of health data, leaving health-related information open to various threats and misuse, which could result in sever consequences for both patients and organizations [10].

The need for effective methods capable of identifying attacks and malicious devices within IoT networks stems from their vulnerability to threats and attacks. The lack of adequate focus on security and privacy in healthcare IoT technologies is a major obstacle preventing these technologies from being effectively used to address current problems. Therefore, a need to investigate security-related factors exists.

Given these challenges, accurate assessment of the reliability of IoMT devices continues to remain a complex problem. Traditional trust assessment methods, which use deterministic thresholds or probabilistic evaluations, often fail to take into account the variability of wireless communication environments. Moreover, they are typically quite rigid when faced with incomplete information.

These limitations justify the need for a more uncertainty-aware trust assessment mechanism.

## 3. Literature Review

Researchers encounter several obstacles in the IoT area, such as guaranteeing a sufficient level of security while exchanging data, ensuring trust between IoT components, addressing concerns related to data confidentiality in IoT technologies, creating safe communication with various components on the edge network, and finding ways to save energy by applying reliable smart devices and infrastructure [11].

The degree of trust placed in engineering solutions depends on their capability to interprtet data in various psychological and economic contexts and varies rather considerably. Additionally, it differs with the contexts in which they are applied [12].

Trust is closely related to guaranteeing the security of a given system and the safety of its users. It involves not only security, but also other elements, including integrity, resilience, dependability, accessibility, and capability, making it more complex and challenging to provide [13].

In [14], trust is defined as a key feature for establishing trust between devices in order to guarantee secure services and applications.

An IoT device interacts with the physical environment to collect data and operates by relaying on communication technologies. However, IoT devices may become faulty, compromised, or can misbehave due to internal factors or external threats, such as cyberattacks. In such cases, the data collected and transmitted by these devices can become unreliable, which may significantly affect the decision making process, particularly in critical domains such as IoT-based healthcare. Establishing trust in devices and the data they generate can increase end-user confidence in IoT systems. Estimated trust status (trusted, uncertain, or untrustworthy) is to be used as a reputation indicator for healthcare applications [15].

In [16], a trust management mechanism based on architecture modeling is proposed. The IoT is decomposed into three layers, each of them controlled by a special purpose trust management system (self-organized, affective routing and multi-service). The final decision making process is conducted based on trust-related information.

To ensure data and information security, it is essential to verify that any IoT device that interacts with other system elements is trustworthy. To address these challenges, various methods have been proposed, for example, in [17], [18]. Several trust frameworks have been proposed to address the issue of node security to protect devices from being attacked or damaged, which can lead to unavailability of resources [19]–[21].

In [22], a centralized trust management scheme was created for lightweight IoT devices. This system facilitates service exchange between devices, as it manages trust certificates without performing trust calculations. In terms of cooperation and compatibility, additional observations of direct trust are quantified. Recommendations, meanwhile, are used to assess indirect trust.

The authors of [23] introduced a behavior-based reputation system to establish trust between nodes. They proposed an architecture that integrates software-defined networks within the IoT and a cross-layer authorization protocol in trust management. In [24], a dynamic trust management model was created that allows network nodes to autonomously assess the behavior of their peer nodes and dynamically assign rewards and penalties. This method identifies malicious nodes, categorizing them into three levels: mild, moderate, and severe.

Artificial intelligence methods are also widely used in trust assessment. Paper [25] considers the behavior of users in the trusted model to identify anomalous patterns. The established model takes into account specific indicators, such as security, authentication, operation, and efficiency, to assess the user's past behaviors and compare them with the current state of the their actions. The framework developed utilizes fuzzy logic to evaluate both comprehensive and direct trust values.

The technique introduced in [26] is based on fuzzy logic and aims to identify untrusted nodes. The authors created a reliable messaging method for IoT communication among nodes to ensure the security of the entire IoT system. However, the model suffers from certain limitations related to scalability, energy efficiency, and data storage.

A trust management scheme constructed on the principles of Bayesian learning and collaborative filtering was proposed in [27]. To quickly reflect behavioral changes, the scheme is regularly updated after a designated interval, applying a decay factor to the currently computed scores. Nevertheless, Bayesian inference presents certain limitations in trust calculations, including the challenge of trust subjectivity with the element of randomness.

The study described in [28] introduced a trust calculation model that is capable of yielding precise trust evaluations. The approach quantitatively assesses individual trust characteristics and categorizes them to derive the ultimate trust values. The investigation presented in [29] examined a trust model which offers an effective approach to routing protocols for lossy networks, allowing to categorize untrustworthy nodes. The designed model utilizes the logistic regression technique to assess the behavior of a specific node.

The investigation described in [30] proposed a trust-oriented model utilizing a decision tree algorithm to detect malicious activities within the Internet of Battlefield Things environment. In [31], the authors introduced conditional packet manipulation attacks, known as targeted insider attacks. The presented scheme maintains restricted trust performance metrics for every node, indicating the potential for initial attacks, such as forwarding packets with specific values.

The investigation presented in [32] introduced an adaptive trust protection scheme designed specifically for industrial IoT networks, using a deep neural network alongside a supervised learning algorithm. This approach successfully identified various types of attacks without the need for any prior knowledge of their characteristics and eliminated the need for manual intervention.

LSTM and multi-attribute rating techniques for trust management in IoT devices were proposed in [33]. A multi-attribute rating algorithm was applied to compute the trust values, while LSTM was utilized to determine the trust threshold based on behavioral changes.

Although previous studies presented a general examination of security- and privacy-related issues affecting IoT, a significant gap continues to exist in the literature as far as the layered structure of IoT is concerned, specifically within the healthcare context [34].

Paper [35] proposes a fuzzy trust management mechanism to prevent Sybil attacks in IoMT. Moreover, this mechanism can recognize untrustworthy nodes in the system. Study [36] proposes a blockchain-based fuzzy trust management framework to detect Sybil nodes in IoMT networks, while [37] discusses an intelligent trust cloud management method where individual trust clouds of IoMT devices are established by fuzzy trust recommending. The suggested trust classification scheme can determine whether an IoMT device is malicious and can be relied upon for secure clustering.

Although the number of published studies focusing on trust assessment in IoT networks is quite substantial, insufficient attention has been devoted to hybrid approaches that integrate several AI techniques and combine their advantages in order to improve model accuracy – a feature this paper focuses on.

## 4. Methodology

In this paper, fuzzy logic was chosen over other AI techniques because it does not require large training datasets and can operate effectively, since fuzzy logic deals with expert knowledge and linguistic rules, which makes it well suited for cases in which IoMT data may be limited or inprecise. Moreover, unlike black-box models (e.g. deep neural networks), fuzzy systems provide high interpretability and are transparent operationaly, while retaining low computational complexity.

At the foundation of the scheme lies the selection and integration of indicators that reflect the secure behavior of a specific IoMT device. The architecture of the proposed fuzzy logic-based trust assessment scheme for IoMT is shown in Fig. 1.

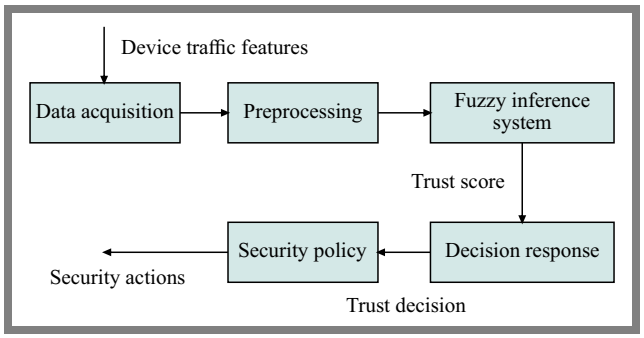


**Fig. 1.** Fuzzy-based secure trust assessment scheme.

The trust assessment scheme for IoMT medical devices comprises several functional units. The data acquisition unit collects the behavior characteristics of traffic from medical devices of the IoMT network. The preprocessing unit performs the data cleaning and normalization stage. Next, the fuzzy inference system processes the normalized numerical features and gives the trust score of each device. The decision response unit interprets the trust score produced by the FIS and determines the appropriate reaction, such as classifying devices as trusted, suspicious or malicious. By applying relevant security rules, the security policy unit implements this trust-related decision (access control, device isolation, and alert generation) to protect the IoMT network.

The trust assessment scheme can be used as part of a security management module integrated into IoMT gateways, edge servers, or organization network controllers to evaluate the trustworthiness of connected devices. Based on the calculated trust score, the scheme can control network access by prioritizing trusted devices for data transmission, and may restrict or isolate devices with suspicious behavior.

The core component of the proposed trust assessment scheme is the fuzzy inference system (FIS), which performs the decision-making process. It processes several indicators – behavioral and network characteristics of IoMT devices – and transforms them to a unified continuous trust score. To transform these features into a trust score, the FIS applies a fuzzification process that converts numerical indicator values into linguistic terms such as “low”, “medium” or “high”. These terms are represented by membership functions. Next, the inference stage takes place, where the fuzzy inference engine applies the rule base which encodes expert knowledge to produce fuzzy outputs. Then, defuzzification is performed to produce a single value trust score that represents the device’s current level of trustworthiness on a continuous numerical scale.

To evaluate the performance of the trust assessment phase, the FIS should be validated using a real dataset. In this study, the CICIoMT2024 dataset is applied, as it offers a comprehensive and up-to-date representation of network traffic and cyberattacks, which are specific for IoMT. This data set includes various attack scenarios and realistic benign traffic, thus allowing to objectively evaluate and validate the specific intrusion and attack detection methods [38].

The proposed FIS has four inputs, which correspond to selected features of the CICIoMT2024 dataset and determine essential traffic and security-related properties, enabling the FIS to model both normal and malicious patterns effectively. These chosen features are inter-arrival time, flow duration, tot_size, and SYN flag number.

The inter-arrival time feature measures the time difference between subsequent packets sent by a medical device, reflecting its communication behavior. This feature can indicate anomalies, such as irregular or suspicious transmission patterns that may indicate compromised or misbehaving devices.

The flow duration feature represents the total time of a given network flow, showing the duration of the period over which the device communicates during a session. Abnormal flow durations – either unusually short or excessively long – may indicate suspicious activity or potential security breaches. The Tot_size feature represents the total size of packets transmitted in a network flow, reflecting the volume of data exchanged by a device. Unusually large or small values can indicate abnormal behavior, such as data exfiltration or communication suppression.

The Syn flag number feature counts the TCP packets from a device, reflecting how often it attempts to establish communication. Abnormally high Syn counts may indicate suspicious behaviors such as scanning, flooding, or unauthorized connection attempts.

The output of the proposed FIS is the trust score, which represents the reliability or trustworthiness of an IoMT device evaluated based on its observed network behavior. In this study, the Mamdani-type FIS was selected due to its common rule-based structure and high interpretability, as well as a clear representation of expert knowledge in the trust assessment process. The Mamdani FIS represents a non-linear approach to mapping between a four-dimensional input vector $\mathbf{x} = [x_1, x_2, x_3, x_4]$ and a scalar output variable $y$. Each input variable $x_1, i = 1, \ldots, 4$, is characterized by three linguistic terms presented as Gaussian membership functions, while the output variable is described by five Gaussian membership functions. The Gaussian membership function corresponding to the $j$-th linguistic term of the $i$-th input can be expressed as:

$$\mu_{A_{ij}}(x_i) = \exp\left( - \frac{(x_i - c_{ij})^2}{2\sigma_{ij}^2} \right), \tag{1}$$

where $c_{ij}$ and $\sigma_{ij}$ are the center and standard deviation of the Gaussian function, respectively and $j = 1, 2, 3$.

Next, the $k$-th membership function of the output variable can be defined as:

$$\mu_{B_k}(y) = \exp\left( - \frac{(y - c_k)^2}{2\sigma_k^2} \right). \tag{2}$$

The fuzzy rule base designed for this case consists of 12 Mamdani type fuzzy if-then rules which encode expert knowledge about the system’s behavior. The $r$-th rule can be written as:

$$\begin{aligned} R_r : \text{if } x_1 \text{ is } A_{1j_1^r} \text{ and } x_2 \text{ is } A_{2j_2^r} \text{ and } x_3 \text{ is } A_{3j_3^r} \\ \text{and } x_4 \text{ is } A_{4j_4^r} \text{ then } y \text{ is } B_{k^r}\ , \end{aligned} \tag{3}$$

where $r = 1, \ldots, 16$, $j_i^r \in \{1, 2, 3\}$, and $k^r \in \{1, \ldots, 5\}$ are the indices of the previous and next membership functions, respectively.

The firing strength of the $r$-th rule is calculated using the minimum $t$-norm as:

$$\alpha_r = \min\left\{\mu_{A_{1j_1^r}}(x_1), \ldots, \mu_{A_{4j_4^r}}(x_4)\right\} . \tag{4}$$

Each fuzzy rule contributes to the output fuzzy set by modifying its consequent membership function according to its firing strength:

$$\mu_{B_r}^{\text{out}}(y) = \min\left\{\alpha_r, \mu_{B_{k^r}}(y)\right\} . \tag{5}$$

The aggregated output fuzzy set is obtained by applying the maximum operator over all rules:

$$\mu_{\text{agg}}(y) = \max_{r=1,\ldots,16} \mu_{B_r}^{\text{out}}(y) . \tag{6}$$

Finally, the final crisp output is calculated using the centroid defuzzification method:

$$y^* = \frac{\int y\mu_{\text{agg}}(y)dy}{\int \mu_{\text{agg}}(y)dy} . \tag{7}$$

To improve the accuracy of the FIS, evolutionary algorithms are employed to optimize the parameters of the membership functions and the structure of the fuzzy rule base.

First, the developed FIS is optimized by applying a genetic algorithm (GA). Here, a GA chromosome is encoded as a vector that includes all membership function parameters and the indices defining the fuzzy rules. The membership function parameters are encoded as:

$$\mathbf{z}_{\text{MF}} = \left[c_{11}, \sigma_{11}, \ldots, c_{43}, \sigma_{43}, c_1, \sigma_1, \ldots, c_5, \sigma_5\right] , \tag{8}$$

while the fuzzy rules are encoded as:

$$\mathbf{z}_{\text{R}} = \left[j_1^1, j_2^1, j_3^1, j_4^1, k^1, \ldots, j_1^{16}, j_2^{16}, j_3^{16}, j_4^{16}, k^{16}\right] , \tag{9}$$

where the previous indices $j_i^r$ and subsequent indices $k^r$ are integer-coded.

The complete chromosome can be written as:

$$\mathbf{z} = \left[\mathbf{z}_{\text{MF}}, \mathbf{z}_{\text{R}}\right]^{\cdot} , \tag{10}$$

For a given chromosome $\mathbf{z}$, the parameters of the fuzzy inference system are determined and its performance is evaluated through a fitness function expressed as the mean squared error between the desired output $y^{ref}$ and the actual output $y^*$:

$$J(\mathbf{z}) = \frac{1}{N}\sum_{n=1}^{N}\left(y_n^{ref} - y_n^*(\mathbf{z})\right)^2 , \tag{11}$$

where $N$ is the number of training samples.

The genetic algorithm iteratively minimizes $J(\mathbf{z})$ by applying selection, crossover, and mutation operators to evolve the chromosomes toward an optimal FIS configuration.

Another evolutionary algorithm, particle swarm optimization (PSO), is applied to the same FIS. In PSO, each particle represents a candidate solution with the same dimensionality and structure as the GA chromosome:

$$\mathbf{x}_p = \left[\mathbf{x}_{p,MF}, \mathbf{x}_{p,R}\right] \in \mathbb{R}^D , \tag{12}$$

where $D$ is the total number of optimized parameters and denotes the particle index.

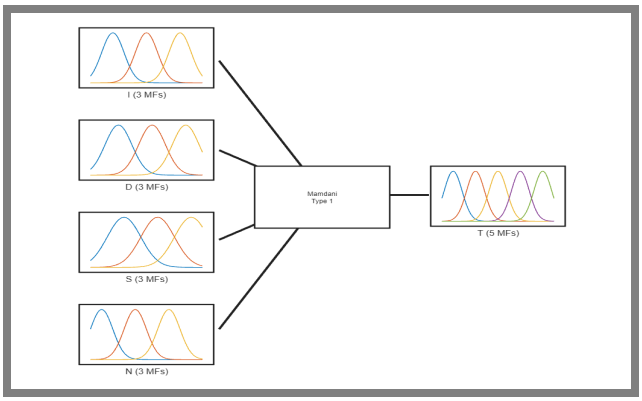


**Fig. 2.** Fuzzy inference system developed in Matlab.

Each particle is associated with a velocity vector $\mathbf{v}_p \in \mathbb{R}^D$, and its evolution in the search space is determined by:

$$\begin{aligned}\mathbf{v}_p(t+1) = \omega\mathbf{v}_p(t) + c_1 r_1\left[\mathbf{p}_p - \mathbf{x}_p(t)\right] \\ + c_2 r_2\left[\mathbf{g} - \mathbf{x}_p(t)\right] ,\end{aligned} \tag{13}$$

$$\mathbf{x}_p(t+1) = \mathbf{x}_p(t) + \mathbf{v}_p(t+1) , \tag{14}$$

where $\omega$ is the inertia weight, $c_1$ and $c_2$ are cognitive and social acceleration coefficients, respectively, $r_1$ and $r_2$ are vectors of random variables uniformly distributed in [0, 1], $\mathbf{p}_p$ denotes the personal best position found by particle $p$ and $\mathbf{g}$ represents the global best position discovered by the swarm. During evaluation, the rule-related components of $\mathbf{x}_p$ are discretized to the nearest valid linguistic index. The fitness of each particle is computed using the same objective function $J(\cdot)$ as in the genetic algorithm.

To sum up, the proposed mathematical models provide a comprehensive description of a Mamdani-type fuzzy inference system and its optimization using two evolutionary algorithms and can be utilized to develop the required trust assessment FIS.

## 5. Simulations

Matlab can be used to examine and verify the operation of the developed FIS for trust assessment in IoMT. Running FIS simulations in Matlab enables fast model prototyping, structured performance testing, and convenient experimental analysis. Moreover, it is possible to integrate FIS with optimization toolboxes and machine learning techniques such as

| | Rule | Weight | Name |
|---|---|---|---|
| 1 | If IT is L and FD is L and TS is L and FN is L then TS is VH | 1 | rule1 |
| 2 | If IT is L and FD is M and TS is L and FN is L then TS is H | 1 | rule2 |
| 3 | If IT is M and FD is L and TS is M and FN is L then TS is H | 1 | rule3 |
| 4 | If IT is M and FD is M and TS is M and FN is L then TS is M | 1 | rule4 |
| 5 | If IT is H and FD is M and TS is H and FN is M then TS is L | 1 | rule5 |
| 6 | If IT is M and FD is H and TS is H and FN is M then TS is L | 1 | rule6 |
| 7 | If IT is L and FD is H and TS is H and FN is H then TS is VL | 1 | rule7 |
| 8 | If IT is H and FD is H and TS is M and FN is H then TS is VL | 1 | rule8 |
| 9 | If IT is M and FD is M and TS is H and FN is L then TS is M | 1 | rule9 |
| 10 | If IT is H and FD is L and TS is M and FN is M then TS is M | 1 | rule10 |
| 11 | If IT is L and FD is M and TS is M and FN is H then TS is L | 1 | rule11 |
| 12 | If IT is H and FD is H and TS is H and FN is H then TS is VL | 1 | rule12 |

**Fig. 3.** Rule base of the FIS.

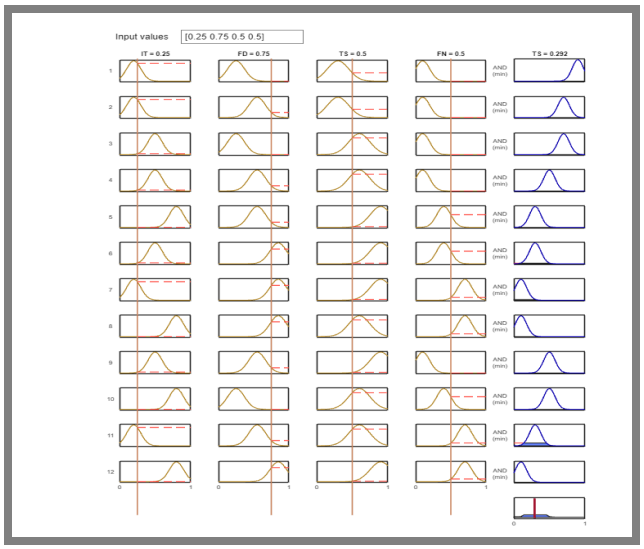


**Fig. 4.** FIS simulation results.

neural networks, which increases the effectiveness of fuzzy inference systems and promotes their improvement.

The initial phase of creating the FIS interface involved assigning input and output variables. The membership functions for the inputs and outputs were defined as well (Fig. 2).

The rule base was specified (Fig. 3). Following this, we allocated the input values and executed the simulation process to generate outputs, thus verifying the functionality of the proposed FIS.

To verify the operability of the developed FIS, a series of simulations was performed. Figure 4 illustrates a scenario with the following input values: the interarrival time value $I_T$ was 0.25, the flow duration value $F_D$ was 0.75, the total size value $T_S$ was 0.5, and the Syn flag number value $F_N$ was 0.5. The simulated FIS yielded the trust score of the device equal to 0.292. This means that this device has a low trust score and can be regarded malicious.

The GA was then applied to adjust both the parameters of the Gaussian membership functions and the structure of the fuzzy rule base, allowing the FIS to better reflect the nonlinear relationships within the features of the CICIoMT2024 dataset.

The convergence analysis of the GA-based optimization shows that the evolutionary search successfully refined the parameters of the proposed FIS within 86 iterations (Fig. 5). The convergence behavior verifies that the GA reached a near-optimal solution. After optimization, the Gaussian membership functions were better positioned around informative data regions. The GA also refined the rule base.

The Mamdani-type FIS was also optimized using the PSO tool. Representing each particle as a candidate FIS configuration and iteratively updating particle positions according to individual and global best performance values, PSO also adjusted the parameters of the Gaussian membership functions and refined the fuzzy rule base. The PSO-based optimization of the proposed FIS reached convergence after 310 iterations, demonstrating a gradual but steady improvement in the fitness value as the swarm explored the search space (Fig. 6).

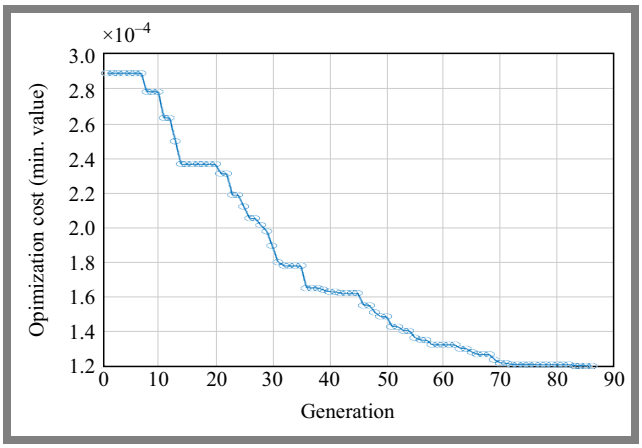


**Fig. 5.** FIS optimization with GA.

The performance of the original FIS, GA-optimized FIS, and the PSO-optimized FIS were validated in Matlab to ensure that the proposed trust assessment scheme demonstrates measurable improvement throughout the optimization stages. During validation, the FIS variants were evaluated according to a predefined fitness metric that reflects the accuracy of the trust estimate. Through this validation procedure, the authors verified whether GA and PSO optimization provided significant performance gains over the original FIS. The validation results show that both optimization algorithms improved the performance of the original FIS, while the PSO-optimized FIS showed the highest accuracy in estimating trust scores from IoMT traffic features (Fig. 7).

The original FIS produced comparatively less precise trust scores, caused by limitations of manually configured membership functions and fuzzy rules. The validation results indicate that optimization significantly improves the performance of the proposed FIS for trust assessment in IoMT. Despite the lower error, the GA-optimized FIS outperformed the original FIS. The PSO-optimized FIS achieved the best results, as it surpassed both the original and the GA-enhanced models. This improvement confirms that swarm-based optimization provided better parameter refinement and convergence.

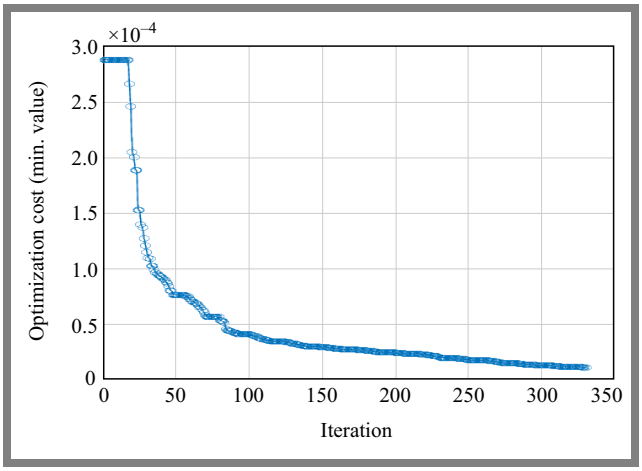


**Fig. 6.** FIS optimization with PSO.

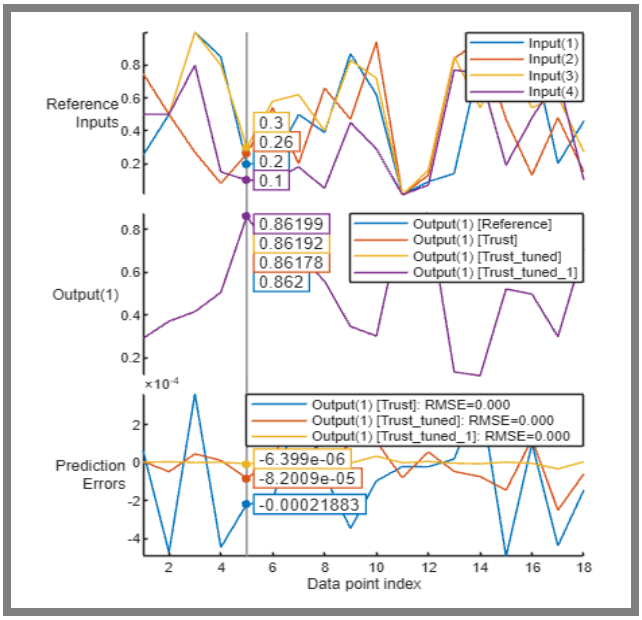


**Fig. 7.** FIS validation results.

## 6. Evaluation

To evaluate and compare the performance of the trust assessment models, simulations were performed in Matlab using traffic features extracted from the CICIoMT2024 dataset. Four models were examined: the original Mamdani type FIS, its GA-optimized and PSO-optimized variants, and a weighted sum trust scheme (WSTS), which is a traditional non-AI trust assessment method.

Figure 8 illustrates the trust scores across sample measures related to how the four models assign trust values to IoMT traffic samples. The weighted-sum method produces relatively smoother and less discriminative trust variations. The original FIS exhibits more adaptive trust fluctuations, as it has improved sensitivity to non-linear relations in the input data. GA-optimized FIS gives more stable high-trust scores for benign samples and lower trust scores for suspicious ones. The PSO-optimized FIS shows the clearest separation between trusted and untrusted samples.

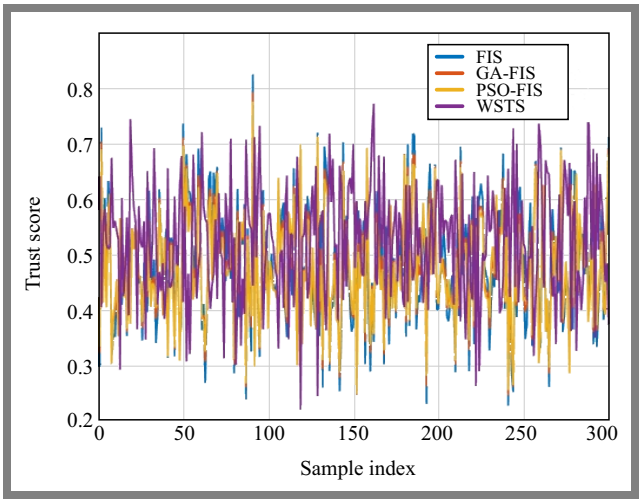


**Fig. 8.** Trust scores across samples.

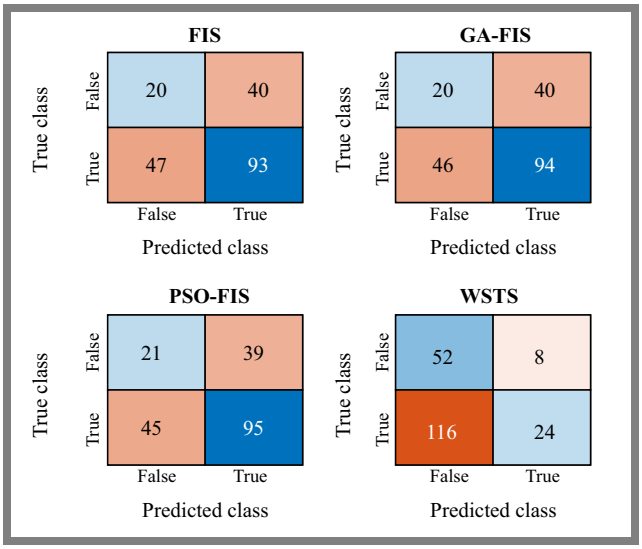


**Fig. 9.** Confusion matrices for models considered.

The confusion matrix plots confirm these trends, showing a reduced number of misclassified samples in both optimized models, where PSO-FIS shows the lowest false-negative rate (Fig. 9).

Receiver operating characteristic (ROC) curves and the corresponding area under the curve (AUC) values highlight the discriminatory strength of each method. The PSO-FIS curve was placed farthest from the random-guess diagonal line, indicating superior separability between trusted and untrusted samples, followed by GA-FIS, the original FIS, and finally WSTS (Fig. 10).

The simulation results demonstrate a significant advantage of the intelligent approach to trust assessment, as the developed fuzzy-based trust assessment model outperforms the traditional method in terms of accuracy and classification reliability.

The integration of fuzzy inference with optimization techniques leads to more precise modeling of complex and nonlinear relationships among IoMT traffic features, i.e., to improved discrimination between trusted and malicious devices.

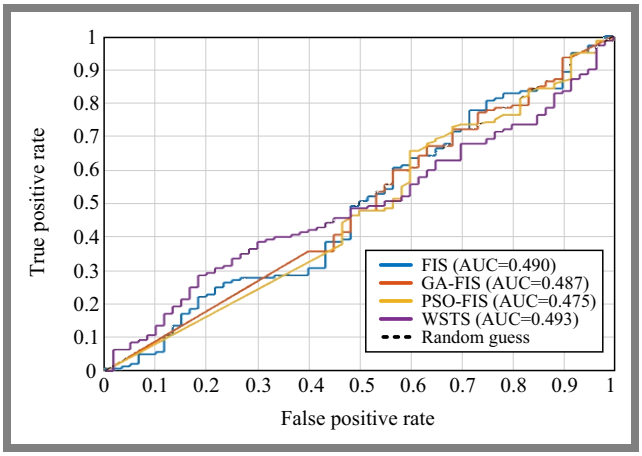


**Fig. 10.** ROC and AUC curves.

## 7. Discussion

The proposed fuzzy secure scheme for trust assessment can be implemented within a layered IoMT architecture, consisting of three layers: the perception layer, the edge/fog layer, and the cloud layer (Fig. 11). The trust assessment scheme is implemented at the edge layer. Deploying at the edge provides several advantages, such as reduced latency to transfer decisions, visibility of aggregated traffic, and sufficient computational capacity. Based on the calculated trust score, the edge/fog layer enforces security policies. Devices with high trust scores are allowed to communicate normally, while devices with low trust scores may be restricted or isolated.

The cloud layer performs the general analytics and model optimization. While trust decisions are made at the edge, the cloud environment can periodically update fuzzy rules or membership function parameters using GA or PSO techniques. The updated parameters are then transmitted back to the edge layer.

Depending on a device's current trust score, it may be assigned one of the five states. An IoMT device assigned with a very high trust score is considered to be in a highly trusted state. This means it exhibits a baseline behavior. The gateway routes its traffic to the intended destination, e.g., the local hospital server or remote cloud with prioritized quality of service. An IoMT device assigned with a high trust score is considered to be in a trusted state (reliable). Continuous monitoring persists, ensuring that the device remains within acceptable operational parameters without triggering punitive measures. Traffic is routed with standard priority. An IoMT device assigned with a medium trust score is considered to be in a suspicious state. The gateway executes preventive measures without severing the connection, recognizing that data availability is doubtful. Actions may include limiting the alert generation rate.

An IoMT device assigned with a low trust score is considered to be in a restricted state. This means that when anomalies become more severe, indicating a likely compromise, the device is to be quarantined. Medical telemetry is maintained only if this can be done safely; strict control actions and deep packet inspection are to be enforced. An IoMT device assigned with a very low trust score is considered to be in an isolation state. The gateway performs an immediate and aggressive isolation. Actions can include network segregation or traffic reduction.

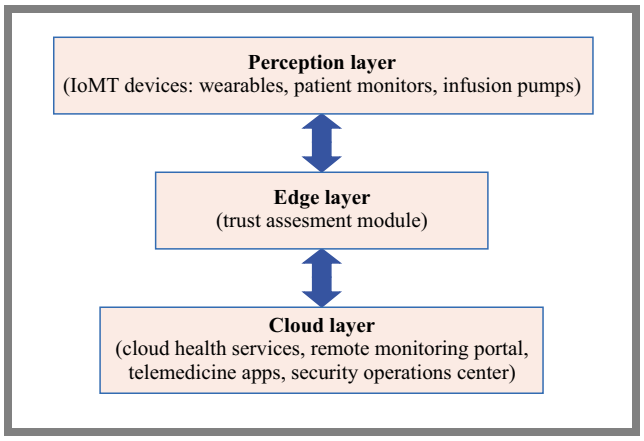


**Fig. 11.** IoMT layered architecture.

As this evaluation occurs directly at the edge gateway, suspicious behavior can be detected quickly without requiring continuous communication with cloud servers.

The developed optimized fuzzy secure scheme for trust assessment in IoMT can be deployed at the edge gateway, such as a smart router, as a JavaScript-based software module. The Node.js environment can be applied due to its open source nature and asynchronous architecture, as it is able to handle many network connections at once without slowing down. This makes it a good option for IoMT conditions as the gateway must constantly manage data streams from many various medical sensors at the same time.

The authors suggest that we divide the software into three parts. The first (feature extractor) unit runs a packet capture tool in Node.js, allowing it to monitor all the traffic flowing through the gateway's ports without interrupting it. It captures the four specific features and sends them to the second unit – the fuzzy inference engine, which is the core component of the JavaScript software module and reproduces the fuzzy inference system structure of the developed during the modeling stage through custom JavaScript functions to yield a trust score. The third (decision) unit processes the obtained trust score value and sends direct commands to the gateway's operating system to apply one of the five security actions.

Such an implementation has several advantages. It supports real-time analysis of device behavior, enables cross-platform deployment, and can be easily integrated with existing network monitoring tools and healthcare management systems. Consequently, this approach provides a practical solution to deploy the optimized fuzzy trust assessment scheme in IoMT networks.

## 8. Conclusions

The proposed fuzzy secure scheme for trust assessment in the IoMT provides an accurate trust evaluation as it produces continuous trust scores, not binary decisions, thus allowing for more flexible security-related decisions, such as partial access rather than complete acceptance or rejection. Furthermore, it ensures low computational complexity, making it suitable for resource-limited medical devices.

The core component of the scheme – a fuzzy inference system – was developed, analyzed, and validated. The initial stage was to build a mathematical framework for Mamdani-type FIS, its inputs being four network traffic features from the CICIoMT2024 dataset, and its output being a trust score for an IoMT device. The FIS was developed in Matlab. Simulations confirmed the correctness of the developed FIS and its ability to adequately assess trust levels considering the selected traffic features.

However, as its parameters were assigned manually, the developed FIS may not achieve a sufficiently high degree of accuracy. To increase its precision, the FIS was further optimized

and fine tuned using two approaches – genetic algorithms and particle swarm optimization.

Experimental results confirmed that both optimization methods yielded notable improvements in the accuracy of trust estimation. The PSO-optimized FIS produced the most accurate trust predictions. Finally, the comparative analysis of four models – the original Mamdani type FIS, its GA-optimized and PSO-optimized variants, and a weighted sum trust scheme – demonstrated that optimization is essential to maximizing the accuracy of fuzzy trust mechanisms in IoMT.

In general, this study confirms that the application of artificial intelligence techniques significantly improves trust assessment models by increasing the level of accuracy without sacrificing their complexity. The results demonstrate the feasibility of fuzzy logic as an effective approach to trust management in IoMT communications.

## References


[1] N. Khatoon, S. Roy, and P. Pranav, "A Survey on Applications of Internet of Things in Healthcare", in: *Internet of Things and Big Data Applications,* Springer International Publishing, pp. 89–106, 2020 (https://doi.org/10.1007/978-3-030-39119-5_6).

[2] Z. Shouran, A. Ashari, and T. Kuntoro, "Internet of Things (IoT) of Smart Home: Privacy and Security", *International Journal of Computer Applications*, vol. 182, pp. 3–8, 2019 (https://doi.org/10.5120/ijca2019918450).

[3] J.J. Hathaliya and S. Tanwar, "An Exhaustive Survey on Security and Privacy Issues in Healthcare 4.0", *Computer Communications*, vol. 153, pp. 311–335, 2020 (https://doi.org/10.1016/j.comcom.2020.02.018).

[4] W. Najib, S. Sulistyo, and Widyawan, "Survey on Trust Calculation Methods in Internet of Things", *Procedia Computer Science*, vol. 161, pp. 1300–1307, 2019 (https://doi.org/10.1016/j.procs.2019.11.245).

[5] G.J. Blinowski, "Risk-based Decision Making in IoT Systems", *Proc. of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017*, pp. 230–241, 2017 (https://doi.org/10.1007/978-3-319-67220-5_21).

[6] A.M. Konsta, A.L. Lafuente, and N. Dragoni, "A Survey of Trust Management for Internet of Things", *IEEE Access*, vol. 11, pp. 122175–122204, 2023 (https://doi.org/10.1109/access.2023.3327335).

[7] A. Chacko and T. Hayajneh, "Security and Privacy Issues with IoT in Healthcare", *EAI Endorsed Transactions on Pervasive Health and Technology*, vol. 4, art. no. e2, 2018 (https://doi.org/10.4108/eai.13-7-2018.155079).

[8] P.K.D. Pramanik, G. Pareek, and A. Nayyar, "Security and Privacy in Remote Healthcare", *Telemedicine Technologies*, pp. 201–225, 2019 (https://doi.org/10.1016/b978-0-12-816948-3.00014-3).

[9] C. Butpheng, K.-H. Yeh, and H. Xiong, "Security and Privacy in IoT-Cloud-Based e-Health Systems – A Comprehensive Review", *Symmetry*, vol. 12, art. no. 1191, 2020 (https://doi.org/10.3390/sym12071191).

[10] I. Sadek, S.U. Rehman, J. Codjo, and B. Abdulrazak, "Privacy and Security of IoT Based Healthcare Systems: Concerns, Solutions, and Recommendations", *Lecture Notes in Computer Science*, vol. 11862, pp. 3–17, 2019 (https://doi.org/10.1007/978-3-030-32785-9_1).

[11] S. Albishi, B. Soh, A. Ullah, and F. Algarni, "Challenges and Solutions for Applications and Technologies in the Internet of Things", *Procedia Computer Science*, vol. 124, pp. 608–614, 2017 (https://doi.org/10.1016/j.procs.2017.12.196).

[12] C. Fernandez-Gago, F. Moyano, and J. Lopez, "Modelling Trust Dynamics in the Internet of Things", *Information Sciences*, vol. 396, pp. 72–82, 2017 (https://doi.org/10.1016/j.ins.2017.02.039).

[13] Z. Yan, P. Zhang, and A.V. Vasilakos, "A Survey on Trust Management for Internet of Things", *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014 (https://doi.org/10.1016/j.jnca.2014.01.014).

[14] W. Najib, S. Sulistyo, and Widyawan, "Survey on Trust Calculation Methods in Internet of Things", *Procedia Computer Science*, vol. 161, pp. 1300–1307, 2019 (https://doi.org/10.1016/j.procs.2019.11.245).

[15] A. Rauf, R.A. Shaikh, and A. Shah, "Trust Modelling and Management for IoT Healthcare", *International Journal of Wireless and Microwave Technologies*, vol. 12, pp. 21–35, 2022 (https://doi.org/10.5815/ijwmt.2022.05.03).

[16] L. Gu, J. Wang, and B. Sun, "Trust Management Mechanism for Internet of Things", *China Communications*, vol. 11, pp. 148–156, 2014 (https://doi.org/10.1109/cc.2014.6821746).

[17] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A Survey on the Security of IoT Frameworks", *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018 (https://doi.org/10.1016/j.jisa.2017.11.002).

[18] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things", *IEEE Transactions on Emerging Topics in Computing*, vol. 5, pp. 586–602, 2017 (https://doi.org/10.1109/tetc.2016.2606384).

[19] U. Jayasinghe, N.B. Truong, G.M. Lee, and T.-W. Um, "RpR: A Trust Computation Model for Social Internet of Things", *2016 Int. IEEE Conferences on Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, Tolouse, France, 2016 (https://doi.org/10.1109/uic-atc-scalcom-cbdcom-iop-smartworld.2016.0146).

[20] F. Fei *et al.*, "A K-anonymity Based Schema for Location Privacy Preservation", *IEEE Transactions on Sustainable Computing*, vol. 4, pp. 156–167, 2019 (https://doi.org/10.1109/tsusc.2017.2733018).

[21] F. Jiang *et al.*, "Deep Learning Based Multi-channel Intelligent Attack Detection for Data Security", *IEEE Transactions on Sustainable Computing*, vol. 5, pp. 204–212, 2020 (https://doi.org/10.1109/tsusc.2018.2793284).

[22] I.U. Din *et al.*, "LightTrust: Lightweight Trust Management for Edge Devices in Industrial Internet of Things", *IEEE Internet of Things Journal*, vol. 10, pp. 2776–2783, 2023 (https://doi.org/10.1109/jiot.2021.3081422).

[23] J. Chen *et al.*, "Trust Architecture and Reputation Evaluation for Internet of Things", *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 3099–3107, 2018 (https://doi.org/10.1007/s12652-018-0887-z).

[24] S.W.A. Hamdani *et al.*, "Dynamic Distributed Trust Management Scheme for the Internet of Things", *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 29, pp. 796–815, 2021 (https://doi.org/10.3906/elk-2003-5).

[25] M. Alruwaythi and K.E. Nygard, "Fuzzy Logic Approach Based on User Behavior Trust in Cloud Security", *2019 IEEE International Conference on Electro Information Technology (EIT)*, Brookings, USA, 2019 (https://doi.org/10.1109/eit.2019.8834173).

[26] M.D. Alshehri and F.K. Hussain, "A Fuzzy Security Protocol for Trust Management in the Internet of Things (Fuzzy-IoT)", *Computing*, vol. 101, pp. 791–818, 2018 (https://doi.org/10.1007/s00607-018-0685-7).

[27] P. Singh *et al.*, "Service Versus Protection: A Bayesian Learning Approach for Trust Provisioning in Edge of Things Environment", *IEEE Internet of Things Journal*, vol. 9, pp. 22061–22070, 2022 (https://doi.org/10.1109/jiot.2021.3082272).

[28] U. Jayasinghe, G.M. Lee, T.-W. Um, and Q. Shi, "Machine Learning Based Trust Computational Model for IoT Services", *IEEE Transactions on Sustainable Computing*, vol. 4, pp. 39–52, 2019 (https://doi.org/10.1109/tsusc.2018.2839623).

[29] K. Prathapchandran and T. Janani, "A Trust-based Security Model to Detect Misbehaving Nodes in Internet of Things (IoT) Environment using Logistic Regression", *Journal of Physics: Conference Series*, vol. 1850, art. no. 012031, 2021 (https://doi.org/10.1088/1742-6596/1850/1/012031).

[30] P. Kannimuthu and J. Thangamuthu, "Decision Tree Trust (DTTrust)-based Authentication Mechanism to Secure RPL Routing Protocol on Internet of Battlefield Thing (IoBT)", *International Journal of Business Data Communications and Networking*, vol. 17, pp. 1–24, 2021 (https://doi.org/10.4018/ijbdcn.2021010101).

[31] L. Liu *et al.*, "A Detection Framework Against CPMA Attack Based on Trust Evaluation and Machine Learning in IoT Network", *IEEE Internet of Things Journal*, vol. 8, pp. 15249–15258, 2021 (https://doi.org/10.1109/jiot.2020.3047642).

[32] M.M. Hassan *et al.*, "A Robust Deep-learning-enabled Trust-boundary Protection for Adversarial Industrial IoT Environment", *IEEE Internet of Things Journal*, vol. 8, pp. 9611–9621, 2021 (https://doi.org/10.1109/jiot.2020.3019225).

[33] Y. Alghofaili and M.A. Rassam, "A Trust Management Model for IoT Devices and Services Based on the Multi-criteria Decision-making Approach and Deep Long Short-term Memory Technique", *Sensors*, vol. 22, art. no. 634, 2022 (https://doi.org/10.3390/s22020634).

[34] N.A. Azeez and C.V. der Vyver, "Security and Privacy Issues in e-health Cloud-based System: A Comprehensive Content Analysis", *Egyptian Informatics Journal*, vol. 20, pp. 97–108, 2019 (https://doi.org/10.1016/j.eij.2018.12.001).

[35] A. Almogren *et al.*, "FTM-IoMT: Fuzzy-based Trust Management for Preventing Sybil Attacks in Internet of Medical Things", *IEEE Internet of Things Journal*, vol. 8, pp. 4485–4497, 2021 (https://doi.org/10.1109/jiot.2020.3027440).

[36] S.E. Ali *et al.*, "BFT-IoMT: A Blockchain-based Trust Mechanism to Mitigate Sybil Attack Using Fuzzy Logic in the Internet of Medical Things", *Sensors*, vol. 23, art. no. 4265, 2023 (https://doi.org/10.3390/s23094265).

[37] L. Yang *et al.*, "An Intelligent Trust Cloud Management Method for Secure Clustering in 5G Enabled Internet of Medical Things", *arXiv*, 2022 (https://doi.org/10.48550/ARXIV.2207.09057).

[38] S. Dadkhah *et al.*, "CICIoMT2024: A Benchmark Dataset for Multi-protocol Security Assessment in IoMT", *Internet of Things*, vol. 28, art. no. 101351, 2024 (https://doi.org/10.1016/j.iot.2024.101351).

**Olena Semenova, Ph.D.**
Department of Infocommunication Systems and Technologies
https://orcid.org/0000-0001-5312-9148
E-mail: semenova.o.o@vntu.edu.ua
Vinnytsia National Technical University, Vinnytsia, Ukraine
https://vntu.edu.ua

**Olha Voitsekhovska, Ph.D.**
Department of System Analysis and Information Technologies
https://orcid.org/0000-0001-8504-1204
E-mail: o_voytsekhovska@vntu.edu.ua
Vinnytsia National Technical University, Vinnytsia, Ukraine
https://vntu.edu.ua

**Andrii Dzhus, M.Sc.**
Department of Infocommunication Systems and Technologies
https://orcid.org/0009-0005-3583-5766
E-mail: dzhuz1988@gmail.com
Vinnytsia National Technical University, Vinnytsia, Ukraine
https://vntu.edu.ua

**Vladyslav Kuzniak, M.Sc.**
Department of Information Radioelectronic Technologies and Systems
https://orcid.org/0009-0001-1775-420X
E-mail: kuzniakvl@gmail.com
Vinnytsia National Technical University, Vinnytsia, Ukraine
https://vntu.edu.ua