Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.047323

ARTICLE

IoT Smart Devices Risk Assessment Model Using Fuzzy Logic and PSO

Ashraf S. Mashaleh[1,2,*], Noor Farizah Binti Ibrahim[1], Mohammad Alauthman[3], Mohammad Almseidin[4] and Amjad Gawanmeh[5]

[1]School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia

[2]Department Computer Center, Al-Balqa Applied University, Salt, Jordan

[3]Department of Information Security, Faculty of Information Technology, University of Petra, Amman, Jordan

[4]Department of Computer Science, Tafila Technical University, Tafila, Jordan

[5]College of Engineering and IT, University of Dubai, Dubai, United Arab Emirates

*Corresponding Author: Ashraf S. Mashaleh. Email: mashaleh@bau.edu.jo

Received: 02 November 2023 Accepted: 20 December 2023 Published: 27 February 2024

ABSTRACT

Increasing Internet of Things (IoT) device connectivity makes botnet attacks more dangerous, carrying catastrophic hazards. As IoT botnets evolve, their dynamic and multifaceted nature hampers conventional detection methods. This paper proposes a risk assessment framework based on fuzzy logic and Particle Swarm Optimization (PSO) to address the risks associated with IoT botnets. Fuzzy logic addresses IoT threat uncertainties and ambiguities methodically. Fuzzy component settings are optimized using PSO to improve accuracy. The methodology allows for more complex thinking by transitioning from binary to continuous assessment. Instead of expert inputs, PSO data-driven tunes rules and membership functions. This study presents a complete IoT botnet risk assessment system. The methodology helps security teams allocate resources by categorizing threats as high, medium, or low severity. This study shows how CICIoT2023 can assess cyber risks. Our research has implications beyond detection, as it provides a proactive approach to risk management and promotes the development of more secure IoT environments.

KEYWORDS

IoT botnet detection; risk assessment; fuzzy logic; particle swarm optimization (PSO); cybersecurity; interconnected devices

1 Introduction

The IoT has led to significant technological advancements, revolutionizing our interactions and perceptions of our surroundings. The IoT has facilitated significant innovation in various sectors by seamlessly connecting and integrating with everyday objects, resulting in smarter homes, more efficient industrial processes, and improved healthcare systems. The rapid proliferation of IoT devices and their growing incorporation into vital infrastructure has significantly transformed our society, offering exceptional convenience and productivity.

The rapid growth of the IoT has raised significant concerns regarding the security of interconnected devices. With the increasing prevalence of IoT devices, they are also becoming attractive targets for malicious actors aiming to exploit vulnerabilities and compromise network integrity [1]. An alarming menace is the emergence of IoT botnets, which are collections of compromised devices controlled by a single entity. Botnets can initiate extensive cyberattacks, disrupt services, steal sensitive data, and coordinate attacks on vital infrastructure. The importance of detecting IoT botnets is of great significance. Securing and establishing trust in IoT ecosystems is crucial for protecting personal privacy, ensuring critical systems' proper functioning, and maintaining digital infrastructures' stability [2]. Detecting and mitigating IoT botnets is crucial to prevent potentially catastrophic consequences from their misuse.

The IoT has greatly impacted homes, industries, and society by introducing many Internet-connected devices and systems. Approximately 70% of IoT devices are estimated to possess vulnerabilities, rendering them susceptible to cyberattacks. An alarming concern is the rise of IoT botnets, networks of compromised IoT devices that attackers can exploit to launch extensive attacks. In October 2016, the Mirai botnet attack caused significant disruption to the services of Domain Name System (DNS) provider Dyn. This attack involved an overwhelming amount of traffic, estimated to be around 1.2 Tbsp., and affected popular platforms such as Twitter, Netflix, and Spotify, impacting millions of users [3]. The magnitude and consequences of these threats emphasize the necessity for strong security measures.

The rise in IoT devices and the complexity of cyber threats require the creation of efficient methods for detecting IoT botnets and assessing associated risks. This study examines organizations' difficulties when identifying and mitigating cyber risks related to IoT botnets. Engaging in detecting IoT botnets is driven by a sense of social responsibility and a desire to contribute to the greater moral cause. By detecting and assessing the severity of various threats, the detection system can contribute to safeguarding against these threats, enhancing internet security, improving cybersecurity, and providing broader protection against cyber threats. This paper proposes the need for Risk Assessment to aid administrators in monitoring and identifying potential attacks by determining the severity level of each threat and device in the network. The complex and ever-changing nature of IoT ecosystems presents considerable obstacles to traditional botnet detection methods. IoT environments have diverse devices and protocols with different capabilities and limitations. Adversaries consistently adapt their methods to exploit emerging vulnerabilities and avoid being detected. These factors limit the effectiveness of methods that rely on predefined signatures, fixed rules, and binary logic. This paper introduces a new risk assessment framework that integrates fuzzy logic and PSO to overcome the existing limitations.

As the prevalence of IoT devices increases, the frequency of IoT botnet attacks also rises. Therefore, it is crucial to establish a systematic approach for assessing the potential risks associated with these attacks. One solution to mitigate IoT botnet attacks is to develop a risk assessment method that estimates the risk level based on identifying the attack. There is a need for further improvement in the existing attack detection methods. Therefore, a risk assessment technique is needed to accurately identify the attack phase and determine the associated risk severity level, which will enable more effective implementation of mitigation measures, as suggested in this study.

Fuzzy logic is a computing paradigm that emulates human decision-making processes using linguistic variables and rules to manage imprecise and uncertain input [4] effectively. The membership functions of the system ascertain the extent to which input data pertains to distinct linguistic categories, hence enabling the depiction of gradual transitions between these categories. The system's rules are constructed utilizing specialized knowledge and data-driven approaches, resulting in a logical

structure that makes it possible to relate inputs to outputs. Fuzzy logic is a very effective instrument adept at managing scenarios characterized by uncertainty and vagueness [4]. The technology exhibits diverse applications, encompassing control systems, decision support, pattern recognition, and artificial intelligence. Fuzzy logic systems are widely acknowledged as valuable computational tools in contemporary approaches, mostly because of their capacity to represent intricate relationships inside complex domains and successfully manage imprecision. Membership functions play a crucial role in facilitating the effective functioning of a fuzzy logic system [5]. Despite being a traditional method, fuzzy logic provides well-established and optimized tools with linguistic rules that are easy to understand and interpret. In addition, it can effectively model complex system behavior with small training datasets, which can also be efficiently deployed to devices with less computing capacity.

Fuzzy Inference Systems Inference (FIS) is the process of generating logical inferences from known, widely accepted, or partially true assumptions. The method is called approximate reasoning when inferences are drawn from fuzzy linguistic variables using fuzzy set operators (AND, OR NOT). Fuzzy Inference is more informative and efficient than other methods for studying a system's behavior when uncertainties, unanticipated dynamics, and other unknown properties prevent basic mathematical models from determining. FIS are widely used because they can summarize data and focus on decision-relevant information like the human mind [6,7]. The fuzzy inference system has a knowledge base and inference mechanism. Adding and removing noise blocks are needed for FIS clean input and output. Fuzzification makes a precise input value fuzzy, and defuzzification makes a fuzzy output set clear in Fig. 1.

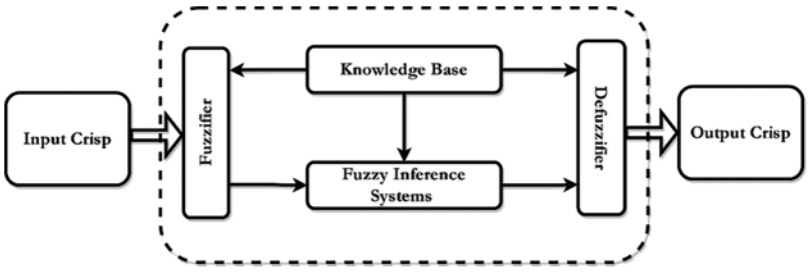

Figure 1: IoT botnet phase detection approach

PSO is a metaheuristic optimization technique that draws inspiration from the collective behavior observed in bird flocking or fish schooling [8]. PSO is a population-based algorithm that is crucial in attaining the objective. The maritime and utilization capabilities of PSO provide it a viable choice for the optimization of diverse components within a fuzzy logic system. The components encompass membership functions, rule weights, and defuzzification techniques [9]. The primary objective of the PSO method is to improve performance and increase accuracy. The combination of PSO and fuzzy logic exhibits the potential to enhance system performance and achieve desired outputs. This integration offers practitioners a valuable approach to enhancing the intricate aspects of fuzzy logic-based models, resulting in improved system behavior and outcomes.

The paper's main contributions can be summarized as follows:

• The system employs a fuzzy logic approach to transition from binary to continuous decision-making, emulating the nuanced nature of human perception, wherein assertions might possess degrees of truth or falsehood.

• The move from discrete to continuous space allows for including varied intensity values, such as 20%, 30%, and 50%. However, this transition introduces complexity.

• Avoiding dependence on imprecise rules or membership functions derived from expert knowledge or self-configuration is recommended to address the challenges posed by IoT networks' significant traffic and data volume.

• Utilizes the integration of fuzzy logic and PSO, a metaheuristic approach, for the model.

This work aims to contribute to the ongoing efforts of securing the future of IoT and harnessing its transformative potential without compromising security through a combination of theoretical innovation and practical application. The rest of this paper is organized as follows: Section 2 presents related work on the subject. Section 3 defines the proposed approach involving fuzzy logic and PSO principles. Section 4 discusses results, experimentation, and discussions. Finally, Section 5 concludes the paper with directions for future work.

2 Related Work

Risk assessment techniques analyze the probability and consequences of potential threats to quantify and manage risk. Several risk assessment methods exist, including qualitative and quantitative approaches, Bayesian networks, and machine learning algorithms [10–13]. Qualitative methods rely on expert opinions and subjectivity, whereas quantitative methods utilize objective numerical data. Bayesian networks and machine learning algorithms are probabilistic methods for managing intricate and uncertain data. In recent years, Bayesian networks have been widely employed in diverse safety and risk assessment applications. This increased utilization can be attributed to the intricate nature of installations prevalent in this industry and the inherent capability of Bayesian networks to represent these intricacies effectively, manage uncertainties, and update probabilities of events [Risk assessment of a liquefied natural]. Machine learning algorithms have been employed for risk assessment purposes, including applications in flood susceptibility assessment and risk management [14].

The current literature has examined different techniques for risk assessment, with a predominant reliance on conventional methods such as probabilistic models, Bayesian networks, and traditional machine learning algorithms [15,16]. The methods have limitations when applied to the complex IoT domain, characterized by diverse devices, intricate interconnections, and constantly evolving attacks. Probabilistic models rely on historical data, which may not accurately reflect future attack patterns and vulnerabilities. Bayesian networks face challenges in representing complex relationships and interdependencies within IoT ecosystems.

A fuzzy logic system was designed to assess the risk of IoT networks by using vulnerability, threat, and effect measurements as input variables. The IoT Networks Predictive Risk researchers developed a proactive cybersecurity system for IoT networks. Reference [17] utilized fuzzy logic principles to conduct a real-time evaluation of potential risks and initiate automatic responses accordingly. The risk level was assessed, and automatic reactions were triggered to mitigate the danger using fuzzy logic. A fuzzy logic-based active cyber defense system for IoT networks was developed to do a real-time risk assessment to initiate automatic reactions. The risk level was assessed, and automatic reactions were triggered to mitigate the danger using fuzzy logic.

Reference [18] has presented a novel approach for mitigating IoT security concerns by implementing a cloud-based active defense strategy. There is a growing trend in which Distributed Denial of Service (DDoS) attacks, botnets, and Zero Click exploits are being directed at IoT devices that possess the capability to store confidential information. The defense system known as "CICADA" employs

an edge-based approach, utilizing three simulated deception environments: Honeynet, Pseudocomb, and Honeyclone. These environments are equipped with pretense capabilities based on the CFO triad. The system's efficacy was evaluated within a substantial enterprise IoT network, whereby it successfully detected low-observability threats such as Zero Click with an accuracy rate of 73%. This notable achievement signifies a significant enhancement in the realm of IoT security. A novel approach to mental health evaluation using IoT data was conducted [19] by Intelligent evaluation of Mental presence. The system employs fuzzy logic to compute the membership degree of the risk value and get a precise assessment level. The design system exhibits a remarkable assessment accuracy of up to 99% and achieves a minimal detection time of 5 seconds, thereby significantly enhancing its evaluation performance.

Fuzzy logic reduced erroneous intrusion alarms [20]. They created fuzzy rules to define computer system normality and a fuzzy reasoning engine to detect intrusions. Their thoughts were a set of imprecise rules. Genetic-fuzzy rule mining could identify Intrusion Detection System (IDS). According to [21], DDoS attacks on new technologies, including wireless communication, cloud computing, fog computing, and Software-Defined Networking (SDN), are harmful. The researchers employed fuzzy logic and four sci-kit-learn machine-learning methods to detect DDoS attacks. Use back-propagating Multilayer Perceptron (MLP), K-Nearest Neighbors (K-NN), Support Vector Machines (SVMs), and Multinomial Naive Bayes (MNB).

Moreover, using fuzzy logic enables the incorporation of other attributes into the system, augmenting the traffic dataset. The examination of anomalies inside a network warrants consideration. In this scenario, the derived conclusions and recently acquired fuzzy logic characteristics empower the system to establish connections with its database and autonomously identify botnet activities. Employed fuzzy logic to categorize IoT resources based on their Quality of Service (QoS) attributes to select the most suitable resource for a customer's specific request. The researchers hypothesized that the computational expenses associated with their MCDA algorithms might be reduced by including adaptable logic in the initial resource grouping. Fuzzy logic is employed to effectively manage ambiguity in determining attribute weights. At the same time, the Logistic Model Tree (LMT) machine-learning method is utilized to reclassify resources. The score is calculated using the Simple Additive Weighting (SAW) technique.

Fuzzy and fast fuzzy pattern trees can group IoT malware. Recently developed fuzzy pattern trees are a novel fuzzy system, proven by [22]. This fuzzy top-down induction structure has fuzzy logic arithmetic operators in the center, and input feature predicates at the ends. This fuzzy-based technique uses a tree-like fuzzy top-down induction structure. The leaves are fuzzy input feature predicates, and the inner nodes are fuzzy logic arithmetic operators. Both solutions utilize robust feature extraction and fuzzy classification methodologies to create a more effective way of detecting and classifying malware at the network's edge. As a result of analyzing Vx-Heaven, IoT, Kaggle, and Ransomware datasets, their model achieved outstanding detection accuracy, particularly for the fast-fuzzy pattern trees.

According to [23], using fuzzy logic is associated with the disadvantage of quick expansion of the rule base. The storage of extensive rule bases on sensor nodes can provide challenges due to their limited memory capacity constraints. Various techniques have been devised to mitigate the problem by achieving a reduction of over 70% in the rule-base size while preserving the accuracy of event detection. A further limitation of fuzzy logic is the potential requirement for substantial memory allocation to store the associated rules.

Natural optimization algorithm PSO mimics bird swarming and fish schooling. PSO uses particles to iteratively search the solution space to identify optimal or near-optimal solutions to complicated optimization problems. Many fields use PSO, including medical disease detection. A systematic literature review on using PSO for medical disease detection, conducted by [24], found that PSO has been commonly employed in this field. The review highlights that PSO shows promise in improving the accuracy of disease perception and prediction within the biomedical domain.

PSO has pros and cons compared to other optimization systems. PSO is easy to implement and requires little processing power. Its population-based approach speeds up solution space exploration and helps find global optima. PSO may also solve continuous and discrete optimization problems and integrate them with other optimization methods to improve performance. However, PSO faces obstacles. It may struggle with local optima, slowing global optima finding. Parameter selection can affect convergence and efficacy, especially inertia weight and acceleration coefficients. Due to the curse of dimensionality, PSO may converge slowly or not at all, making it unsuitable for high-dimensional optimization applications. Despite these restrictions, PSO has excelled in medical disease diagnosis, photovoltaic power systems, and engineering optimization. A prudent strategy comprises assessing PSO's pros and cons and alternative optimization methods to make an informed choice that meets unique needs [8].

Numerous research investigations have employed fuzzy logic in the context of security applications, showcasing its efficacy in handling linguistic uncertainties and mimicking human thinking. Reference [15] employed a genetic fuzzy system to enhance IDS detection rates, as outlined in the proposed model for estimating the security level. The detection of network intrusions was performed by employing a methodology based on fuzzy logic within the system. Furthermore, the genetic algorithm was utilized to optimize the parameters of the fuzzy system. The system under consideration was evaluated using the KDD Cup 99 dataset, and the findings indicated that the system exhibited superior performance compared to conventional machine learning techniques. Reference [25] presented a comprehensive methodology that combines fuzzy logic and the Analytic Hierarchy Process (AHP) to develop a risk-based framework for evaluating cybersecurity threats in the IoT context and its associated vectors. The utilization of machine learning algorithms is employed in this technique to augment the precision and efficacy of the evaluation procedure. The Bayesian approach was employed to assess the possible dangers, yielding an estimation of 82%. On the other hand, the CAQ model, utilizing J48, achieved a classification accuracy of 94%. Although the works demonstrate the potential of fuzzy logic, it is important to note that the existing literature needs to provide a comprehensive framework specifically designed to evaluate the intricate hazards associated with IoT botnets. This framework should include both fuzzy logic and computational intelligence.

Network administrators are responsible for monitoring and securing network connections to prevent potential attackers' unauthorized access to sensitive data. The diverse range of IoT devices poses a significant challenge in developing comprehensive security models for each device category. Current research on IoT botnet detection primarily emphasizes botnet detection and identification, with limited attention to risk assessment and mitigation strategies. This study aims to fill the existing gap by presenting a framework to identify IoT botnets, evaluate their associated risks, and offer mitigation strategies. This study aims to develop a risk assessment model to establish an early warning system focused on the risks posed by IoT botnets. The intended outcome is to enhance the security of IoT networks and mitigate the potential harm caused by IoT botnets.

Three Fractional-Order Particle Swarm Optimization (FOPSO) algorithms are proposed and analyzed in the [26]: FOVPSO, FOXPSO, and FOVXPSO. This study focuses on these algorithms'

dynamic representation and stability analysis, assuming weak stagnation. Convergence boundaries are determined for each algorithm. The optimization performance of FOVXPSO is superior to other FOPSO variants, as demonstrated through experiments conducted on benchmark functions and a biological application. The FOPSO algorithm is employed to address the issue of stagnation in the traditional PSO algorithm.

A unique, Improved Fuzzy Particle Swarm Optimization (IFPSO) technique was presented in [27] to support intelligent system identification and control and to preserve the ideal balance between global and local searches. The inertia weight in the Improved Fuzzy Particle Swarm Optimization (IFPSO) algorithm is dynamically adjusted for each particle based on a fuzzy system that considers the particle's personal best fitness, which facilitates global and local search optimization. The IFPSO algorithm is utilized for parameter estimation of a nonlinear dynamic system model and designing a PID controller. Comparative results indicate that IFPSO exhibits superior convergence speed and accuracy compared to other variants of PSO and genetic algorithms. The algorithm is effective for both system identification and optimal controller tuning.

The current IoT botnet detection methods have several limitations. Probabilistic models heavily depend on historical data, which may not accurately represent the rapid evolution of botnet attacks [10]. Bayesian networks face challenges in representing complex IoT ecosystems' intricate relationships and interdependencies [12]. Conventional machine learning models, such as SVMs and neural networks, are often black-box models with limited binary assessment capabilities [15]. Fuzzy logic systems employ interpretable reasoning that mimics human thought processes to manage uncertainty effectively. Many fuzzy approaches rely on complex rules and membership functions that are prone to errors and need more scalability [28–30]. Hybrid models that combine fuzzy methods with nature-inspired optimizations have demonstrated potential [25,31]. However, the existing literature must provide a comprehensive fuzzy-based framework to assess dynamic IoT botnets' risk.

This study's primary objective is to overcome the limitations of existing methods by proposing an adaptive risk assessment approach that utilizes fuzzy logic and PSO. Fuzzy logic offers a structured approach for representing and addressing threats' inherent ambiguities and uncertainties. In the meantime, PSO is employed to optimize the parameters of fuzzy logic components to improve accuracy. The suggested methodology seeks to thoroughly evaluate the risk associated with IoT botnets by using elements of human reasoning with computational swarm intelligence. This technique attempts to provide a resilient, intricate, and all-encompassing assessment. The methodology presents a potentially effective approach to strengthen security tactics and bolster the resilience of future IoT ecosystems in the face of emerging threats. The main objectives of this study include:

- Promote comprehension of the preeminent botnet hazards that an organization is confronted with.
- Prioritize and classify risks according to their severity to facilitate the allocation of mitigation resources.
- Offer cybersecurity teams a dependable and comprehensive approach to evaluate the IoT ecosystem proactively.

This study suggests a unique combination of fuzzy logic and PSO to address previous constraints. Fuzzy logic systematically represents the uncertainties associated with emerging threats in the IoT. PSO optimizes fuzzy rules and memberships to improve accuracy and adaptability in the problem space instead of relying solely on isolated expert inputs. Interpretive modeling enhances security

analytics, while optimization increases resilience to uncertainties. Integrating these techniques results in an intelligent IoT defense system.

3 IoT Botnet Phase Detection

In our study [31], we introduced a framework called the "Malicious Activity Detector Agent" for early detection of IoT botnets and phase detection, as shown in Fig. 2. This component is crucial in the framework as it acts as an alert guardian, protecting the network from potential threats. This design aims to tackle a difficult aspect of IoT security, which involves differentiating between harmless network traffic and malicious activities. It is an intelligent gatekeeper utilizing machine learning to analyze network traffic behavior.

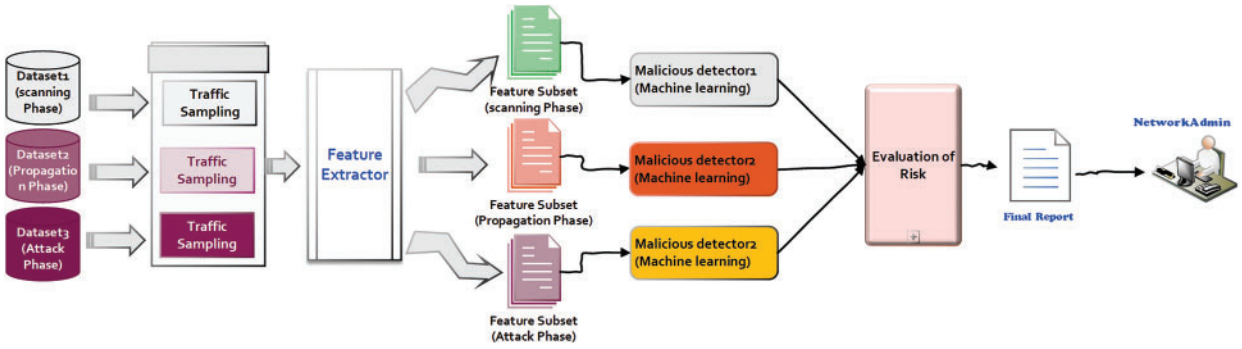

Figure 2: IoT botnet phase detection approach

3.1 Proposed System Architecture

One of the framework's distinguishing characteristics is classifying identified threats into the three phases of the IoT botnet lifecycle: scanning, propagation, and attack. This classification offers a thorough perspective of the risk environment and equips network administrators and security professionals with essential knowledge. Individuals not only develop an awareness of the existence of a possible threat but also acquire a comprehensive comprehension of the current stage and objectives of this threat.

The early detection of these phases fundamentally alters IoT security. The suggested framework offers the capability to identify the presence of botnets during the preliminary scanning phase rather than solely detecting them after they have initiated assaults or infiltrated the network. Implementing this early warning system plays a crucial role in mitigating the advancement of botnet operations towards more detrimental phases, such as DDoS attacks.

An increase in challenges and threats accompanies the expansion of the IoT landscape. The Malicious Activity Detector Agent shows potential for addressing the growing security concerns. This agent effectively safeguards the IoT ecosystem by integrating machine learning, real-time analysis, and comprehensive knowledge of IoT botnet activities. The capability of detecting, categorizing, and issuing early warnings about threats enhances security and encourages a proactive and strategic approach to defending IoT networks. The Malicious Activity Detector Agent is a valuable tool in the current era of connected devices. It provides enhanced security for businesses and consumers, allowing them to fully utilize the IoT while effectively managing and preventing potential threats. The proposed system Architecture is demonstrated in Fig. 2.

3.2 Risk Assessment Model

Fuzzy logic is a mathematical methodology used to handle situations involving uncertainty and imprecision in data. Fuzzy logic is a form of reasoning that permits the consideration of partial truths, allowing objects to possess varying degrees of membership in a set instead of being strictly classified as members or non-members. Fuzzy logic is used in risk assessment to determine and rank risks according to severity levels, occurrence, and detection. Developing a risk assessment model based on fuzzy logic entails the following steps [28–30]:

1. The initial stage in constructing a risk assessment model based on fuzzy logic involves identifying pertinent risk elements. Identifying these factors can be accomplished through the consultation of expert opinions, examination of archive data, or review of pertinent sources.
2. Membership functions are utilized to ascertain the extent of correlation between a risk factor and a particular set. The determination of these functions may rely on the expertise of professionals or historical data.
3. Formulating fuzzy rules is of utmost importance in establishing the correlation between input variables, which represent risk factors, and the output variable, which denotes the level of risk. Expert opinions or historical facts can substantiate the formulation of these guidelines.
4. The fuzzy inference system is crucial in computing the degree of association between input and output variables by utilizing membership functions and fuzzy rules. Utilizing software tools such as MATLAB or Python can greatly aid in implementing this system.
5. Model validation is the conclusive stage of the process, wherein the outcomes of fuzzy logic-based risk assessment are juxtaposed with those derived from alternative risk assessment methodologies or historical data. As mentioned above, the phase holds significant importance in upholding the precision and dependability of the model. PSO, a population-based approach, simulates a swarm of particles moving in a search space to discover the ideal solution [32]. PSO optimizes membership functions and fuzzy rules in a fuzzy logic-based risk assessment model.

The selection of the membership functions and the linguistic variables aimed to balance understandability and accuracy for effective IoT botnet risk evaluation.

1. Input Variables: The input variables used in this research are scanning, propagation, and attack, which are related to the lifecycle phases of IoT botnets and simulate their behaviors. Moreover, these three parameters provide a comprehensive perspective of the risk.

2. Linguistic Terms: The linguistic terms we chose as inputs are “Low,” “Medium,” and “High,” which are intuitive categories associated with common risk assessment terms.

3. Output Variable: The output classifications of the risk severities are “Low,” “Medium,” “High,” and “Critical” risk align with and facilitate decision-making.

4. Membership Functions: Membership functions help convert exact input data into concepts in language. Different types of membership functions, such as triangular and trapezoidal, can be utilized. In our research, we opted for triangular membership functions due to their simplicity, interpretability, and capacity to facilitate gradual transitions between linguistic terms. Finally, the PSO algorithm was employed for tuning the membership function for each linguistic term.

Fig. 3 shows the integration of the PSO with the fuzzy logic to enhance the precision and effectiveness of the risk assessment model based on fuzzy logic, which is achieved by optimizing the membership functions and fuzzy rules. This approach enhances decision-making by offering a more precise and all-encompassing understanding of the associated risks. Algorithm 1 below shows how the PSO is integrated into the fuzzy logic framework [33,34].

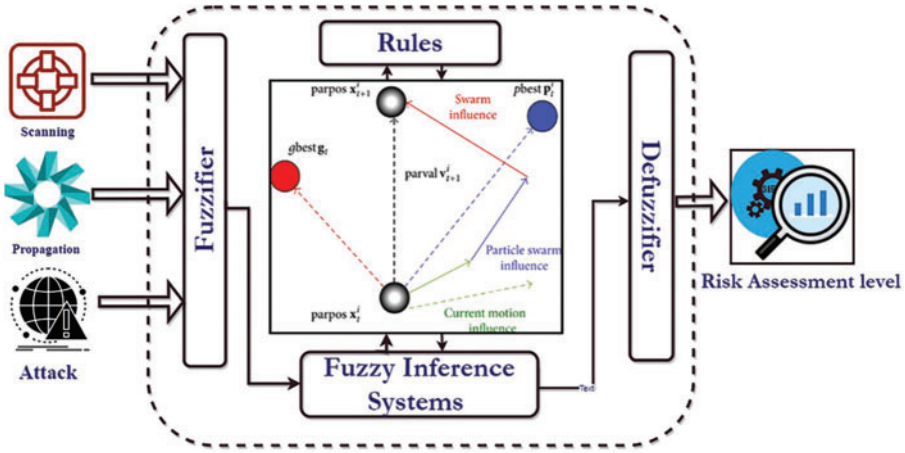

Figure 3: Integration of the PSO with the fuzzy logic

From Algorithm 1, the complexity can be calculated as $O(NM) = NM$, where N is the number of iterations used, and M is the number of swarms. The following metrics were used.

Algorithm 1: PSO for Fuzzy Logic Optimization

```
   Data: input variables, output variable, inertia, c1, c2, max iterations
   Result: Optimal fuzzy logic components
   // Initialize fuzzy logic components
1        Input__variables = [" Scanning," "propagation," Attack"]
2        Output_variable =" Risk_Assessment"
   // Initialize PSO
   // Define fitness function f(x)
   // Initialize swarm with random solutions
3        Swarm_size = M
4        swarm = generate random solutions (swarm size)
   // Set PSO parameters
5        inertia = 0.5
6        c1 = 2.0
7        c2 = 2.0
8        max_iterations = N
   // Evaluate the fitness of each particle
9        for particle in swarm do
10           particle.fitness = fitness_function (particle.solution);
   // While stopping criteria are not met
11           iteration = 0
12       while iteration ≠ max_iterations do
         // For each particle
13       for particle in swarm do
            // Calculate particle velocity
14              update particle_velocity (particle, inertia, c1, c2)
            // Update particle position
```

(Continued)

Algorithm 1 (continued)

```
15              update particle_position(particle)
      // Evaluate new particle fitness values
16        for particle in swarm do
17        particle.fitness = fitness_function(particle.solution)
      // Update personal and global best positions/solutions
18        update best positions(swarm)
19        iteration + = 1
  // Get optimal fuzzy logic components from the best global
PSO solution
20        optimal solution = get global_best_solution(swarm)
21        optimal fuzzy logic components = optimal solution.solution;
  // IoT Botnet Risk Assessment Method
  // Input: Scanning, Propagation, Attack data
22        input data = get input data ().
  // Fuzzify inputs
23        fuzzy inputs = fuzzify inputs (input data, optimal fuzzy_logic components);
  // Apply fuzzy rules to infer risk assessment output
24        inferred output = apply fuzzy rules (fuzzy_inputs, optimal fuzzy_logic components);
  // Defuzzify risk assessment output
25        quantitative_risk_level = defuzzify_output (inferred_output)
  // Output: Quantitative risk level
26        return (quantitative_risk _level)
```

Low: The low function denotes probabilities mostly associated with modest levels of risk. The function $\mu_{\text{Low}}(x)$ assigns the category "Low."

$$\mu_{\text{Low}}(x) = \begin{cases} 1 & \text{if } x \leq 0.01 \\ \dfrac{0.39 - x}{0.39 - 0.01} & \text{if } 0.01 < x < 0.39 \\ 0 & \text{otherwise} \end{cases}$$

Medium: The values ranging from 0.4 to 0.69 are categorized in this set. The function $\mu_{\text{Medium}}(x)$ exhibits a trapezoidal shape.

$$\mu_{\text{Medium}}(x) = \begin{cases} 0 & \text{if } x \leq 0.4 \\ \dfrac{x - 0.4}{0.55 - 0.4} & \text{if } 0.4 < x \leq 0.55 \\ \dfrac{0.69 - x}{0.69 - 0.55} & \text{if } 0.55 < x < 0.69 \\ 0 & \text{otherwise} \end{cases}$$

High: Possibilities within the interval of 0.7 to 0.89 are normally regarded as strong. Furthermore, captured by $\mu_{\text{High}}(x)$.

$$\mu_{\text{High}}(x) = \begin{cases} 0 & \text{if } x \leq 0.7 \\ \dfrac{x - 0.7}{0.8 - 0.7} & \text{if } 0.7 < x \leq 0.8 \\ \dfrac{0.89 - x}{0.89 - 0.8} & \text{if } 0.8 < x < 0.89 \\ 0 & \text{otherwise} \end{cases}$$

Critical: The function $\mu_{\text{Critical}}(x)$ can be described clearly: any values greater than 0.9 are appointed a membership value of 1, indicating their fulfilled inclusion inside the "Critical" set.

$$\mu_{\text{Critical}}(x) = \begin{cases} 0 & \text{if } x < 0.9 \\ 1 & \text{otherwise} \end{cases}$$

The parameters in each function ($\mu_{\text{Low}}(x)$, $\mu_{\text{Medium}}(x)$, $\mu_{\text{High}}(x)$) are selected to create a triangular function considering the peak values of the input and their active range. Finally, the triangular membership functions were selected for several reasons, first due to their simple linear representation requiring only three parameters in implementation while maintaining enough accuracy. Therefore, it allows faster evaluation. In addition, this type of membership function requires simple and easy specification of fuzzy sets. Finally, this modeling allows normalizing member functions to optimize accuracy.

4 Results and Discussion

Through a comprehensive evaluation of every IoT device within the network, valuable insights can be acquired regarding the severity and security associated with each device. An elaborate and all-encompassing technique empowers security professionals to efficiently examine information and mitigate potential risks or vulnerabilities. The earliest actions involved the utilization of a used dataset, the CICIoT2023 [35], presented in Table 1. The outcomes obtained from this dataset are regarded as a representative subset of the outcomes produced by Malicious Activity Detector Agents. They will be utilized by the model to estimate risk probabilities. Moreover, the model employs this knowledge to provide input data for fuzzy logic, which will have a crucial impact on the following calculation of risk severity.

Table 1: Sample results of the estimation and assessment input values

Time window	IP address	Destination IP	Source port	Destination port	Scanning accuracy	Propagation accuracy	Attack accuracy
1	192.168.137.210	192.168.137.175	443	34981	0.524	0.085	0.952
1	192.168.137.106	192.168.137.139	47850	80	0.380	0.093	0.570
1	192.168.137.38	192.168.137.139	48996	80	0.600	0.133	0.533
1	172.217.13.163	157.249.81.141	55563	80	0.000	0.333	0.653
1	47.88.56.147	192.168.137.41	80	55812	0.520	0.000	0.980
1	51.145.143.28	192.168.137.41	80	56061	0.620	0.000	0.750
1	35.168.43.144	157.249.81.141	57824	80	0.810	0.333	0.667

(Continued)

Table 1 (continued)

Time window	IP address	Destination IP	Source port	Destination port	Scanning accuracy	Propagation accuracy	Attack accuracy
2	54.239.19.122	192.168.137.206	51294	55443	0.571	0.143	0.857
2	142.251.32.74	157.249.81.141	58331	80	0.000	0.333	0.667
2	192.168.137.210	54.230.163.97	43442	443	0.130	0.120	0.934
2	34.158.253.218	13.225.195.54	47088	443	0.800	0.012	0.960
2	192.168.137.253	18.209.215.189	49574	443	0.930	0.294	0.087
2	47.88.56.147	192.168.137.41	80	55812	0.980	0.030	0.497
3	192.168.137.65	192.168.137.206	51294	55443	0.630	0.043	0.960
4	192.168.137.65	192.168.137.206	51294	55443	0.450	0.103	0.500
4	192.168.137.253	192.168.137.41	80	55812	0.148	0.060	0.913
4	192.168.137.106	192.168.137.139	47850	80	0.957	0.120	0.036
5	35.162.13.26	157.249.81.141	58331	80	0.460	0.090	0.948
6	192.168.137.65	18.209.215.189	49574	443	0.412	0.123	0.487
6	192.168.137.253	192.168.137.41	80	55812	0.167	0.089	0.843
6	192.168.137.106	192.168.137.139	47850	80	0.600	0.182	0.230
7	192.168.137.65	192.168.137.206	51294	55443	0.720	0.189	0.420
7	192.168.137.101	13.225.195.54	47088	443	0.831	0.590	0.023
7	192.168.137.228	54.230.163.97	43442	443	0.057	0.690	0.312
7	192.168.137.20	192.168.137.41	80	56061	0.147	0.030	0.981
1	192.168.137.66	192.168.137.139	47850	80	0.206	0.030	0.143
8	192.168.137.20	54.230.163.97	43442	443	0.202	0.006	0.973
9	192.168.137.20	192.168.137.139	47850	80	0.159	0.023	0.896
9	192.168.137.65	192.168.137.206	51294	55443	0.430	0.401	0.530
9	192.168.137.32	54.230.163.97	43442	443	0.418	0.381	0.217
10	192.168.137.20	192.168.137.41	80	56061	0.401	0.401	0.921
10	192.168.137.65	192.168.137.139	47850	80	0.487	0.289	0.333

The convergence properties of the PSO algorithm over a series of 100 iterations were evaluated. The results demonstrated a significant decrease in the optimal cost, with values decreasing from 0.72 to 0.53. The calculation time involved the examination of different dataset sizes, specifically 10 botnets, 100 botnets, and 1000 botnets. The associated computation durations for these dataset sizes were 4.7, 16.2, and 47.3 ms, respectively. The recorded duration aligns with the expected level of complexity, indicating that parallel processing could enhance time efficiency.

The risk estimation method gives the "Attack Accuracy" value (0.5) more importance than the "Scanning Accuracy" value (0.2) and the "Propagation Accuracy" value (0.3), and this means that the algorithm stresses the importance of finding attacks properly and gives IPs with higher attack accuracy higher P(W.atck) values. As shown in Table 2, the risk estimation results let us put Internet Protocol addresses (IP addresses) in order of how likely they are to be involved in different events. IPs with higher P(W.atck) numbers may be more important and need immediate attention to stop possible attacks. In the same way, IPs with high P(W.scan) values may be linked to scanning actions and should be looked into further.

Table 2: Sample results of the estimation and assessment output values

Time window ID	IP Address	P (W.scan)	P (W.prop)	P (W.atck)
1	192.168.137.210	0.172	0.047	0.781
1	192.168.137.106	0.215	0.076	0.708
1	192.168.137.38	0.281	0.094	0.625
1	172.217.13.163	0.000	0.234	0.766
1	47.88.56.147	0.175	0.000	0.825
1	51.145.143.28	0.248	0.000	0.752
1	35.168.43.144	0.272	0.168	0.560
1	192.168.137.66	0.338	0.074	0.588
2	192.168.137.210	0.049	0.068	0.883
2	47.88.56.147	0.431	0.020	0.549
2	54.239.19.122	0.195	0.073	0.732
2	142.251.32.74	0.000	0.231	0.769
2	34.158.253.218	0.249	0.006	0.746
2	192.168.137.253	0.756	0.244	0.000
3	192.168.137.65	0.204	0.021	0.776
4	192.168.137.106	0.780	0.147	0.073
4	192.168.137.253	0.059	0.036	0.906
4	192.168.137.65	0.243	0.832	0.674
5	35.162.13.26	0.155	0.046	0.799
6	192.168.137.106	0.414	0.189	0.397
6	192.168.137.253	0.069	0.055	0.875
6	192.168.137.65	0.227	0.102	0.671
7	192.168.137.65	0.351	0.138	0.511
7	192.168.137.101	0.469	0.499	0.032
7	192.168.137.228	0.030	0.553	0.417
7	192.168.137.20	0.056	0.017	0.927
8	192.168.137.20	0.076	0.004	0.920
9	192.168.137.65	0.182	0.255	0.562
9	192.168.137.20	0.065	0.014	0.920
9	192.168.137.32	0.273	0.373	0.354
10	192.168.137.65	0.278	0.247	0.475
10	192.168.137.20	0.121	0.182	0.697

The analysis of IP addresses 192.168.137.253 and 192.168.137.101 demonstrates a vibrant pattern. The identified IP addresses exhibit a significant propensity for conducting scanning activities (P(W.scan)) and propagating themselves (P(W.prop)), while their inclination towards attacking targets (P(W.atck)) is comparatively lower. Empirical evidence suggests that the likelihood of direct participation in a malicious attack is exceedingly minimal, approaching negligible levels. Based on this discovery,

these IP addresses are likely being utilized for discreet and non-aggressive network reconnaissance rather than overtly hostile activities. Although these IPs do not engage in numerous attacks, their emphasis on scanning behavior suggests their involvement in the initial phases of cyber campaigns. During this stage, they gather information and identify vulnerabilities to exploit in future attacks.

The dataset used in this study is the CICIoT2023 [35], which is presented in Table 1. The algorithm prioritizes the accurate detection of attacks and assigns higher P(W.atck) values to IP addresses with higher attack accuracy. IPs with higher P(W.atck) values should be prioritized for immediate attention to mitigate potential attacks. Similarly, IP addresses with elevated P(W.scan) values may indicate scanning activities and warrant further investigation. The dataset contains labeled instances of botnet samples within network traffic data. The dataset comprises 1000 instances and encompasses a range of attack types observed over a specific time frame. The dataset includes significant features such as source/destination IPs, ports, and packet information, encompassing commonly utilized IoT protocols like Message Queuing Telemetry Transport (MQTT) and DNS traffic. Additionally, it accurately depicts the security vulnerabilities encountered by enterprise IoT networks, including the command and control communication channels.

The simulation methodology employs MATLAB 2021a on a Windows 10 operating system, utilizing an Intel Core i7 CPU with 16 GB of RAM. Utilizing the Fuzzy Logic Toolbox and Global Optimization Toolbox is crucial for the implementation. Utilizing a 10-fold stratified cross-validation technique is a dependable method for assessing the efficacy of a model. In the optimization process, PSO is affected by several parameters, including a swarm size of 25, 100 iterations, an inertia weight of 0.7, and c1/c2 values of 2.0. The experimental framework is improved using optimized triangular/trapezoidal membership functions and key evaluation metrics.

The decision to use fuzzy logic in constructing the model was deliberate, as it can effectively represent intricate relationships and adapt to the dynamic nature of the assessed system. Additionally, the PSO technique enabled the optimization of membership functions, enhancing the model's accuracy. The iterative application of fuzzy logic defines a FIS. The iterative method recognizes the need for a cyclical approach in which designers switch between design, simulation, and revision. The iterative approach is driven by FIS model performance and precision [36]. Simulations and performance reviews inform further adjustments, aligning the FIS with the intended goals as the iterative process progresses. This iterative technique allows designers to increase the FIS's ability to describe complex relationships and adapt to different circumstances, which leads to an effective and durable model for complex and uncertain interactions in control systems, decision-making, and pattern detection.

After creating a FIS in Fuzzy Logic Designer, the user can set input, output, and membership functions. After that, the user can create a fuzzy rule system basis. Each fuzzy if-then rule contains two parts [37]:

- The antecedent refers to the if component of the rule, which delineates the language terms associated with the input variable.
- The consequent refers to the rule component specifying the linguistic terms of the output variable.

When rules are generated for an FIS template structure, the application automatically includes the extracted fuzzy rules for every potential combination. As shown in Fig. 3, the risk assessment Fuzzy Model FIS has three inputs considered for membership functions: scanning propagation and attack. Table 3 shows three membership functions for these three inputs. Figs. 4–6 illustrate the scanning, propaganda, and attack inputs, respectively, while Fig. 7 shows the membership functions for variable output risk assessment.

Table 3: Membership functions for the three inputs

Scanning		Optimized values
Low	Triangular	[0.227456 0.362587 0.522341]
Med	Triangular	[0.127363 0.285655 0.294206]
High	Triangular	[0.166578 0.560892 0.578212]
Propagation		
Low	Triangular	[-0.416667 0 0.416667]
Med	Triangular	[0.0833333 0.5 0.916667]
High	Triangular	[0.583333 1 1.41667]
Attack		
Low	Triangular	[0.0564133 0.294593 0.301042]
Med	Triangular	[0.08343 0.5 0.9166]
High	Triangular	[0.5834 1 1.417]

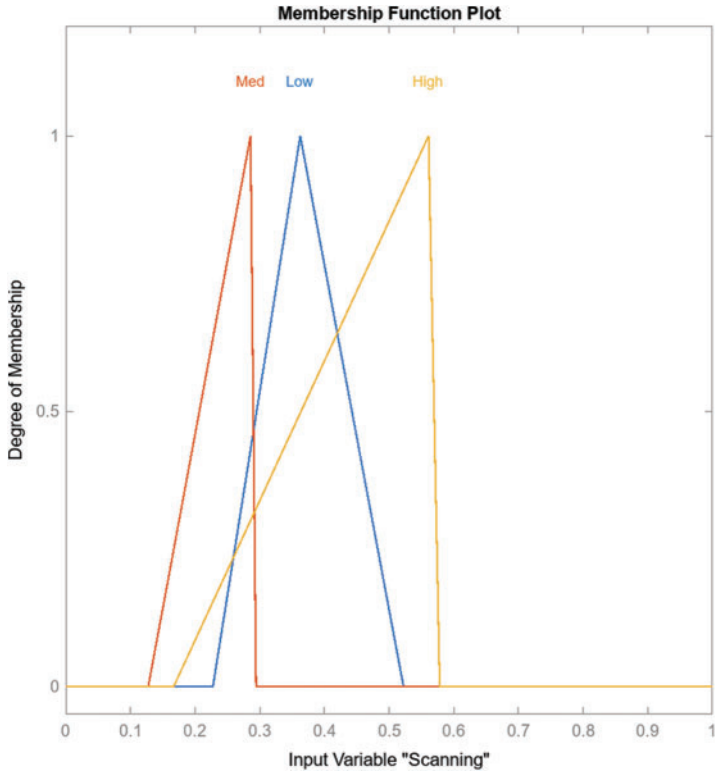

Figure 4: Membership functions for variable scanning

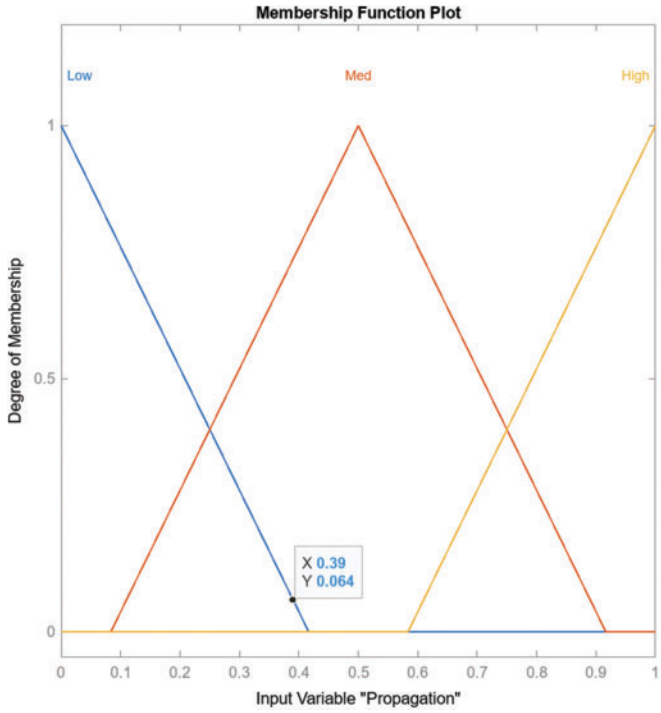

Figure 5: Membership functions for variable inputs propagation

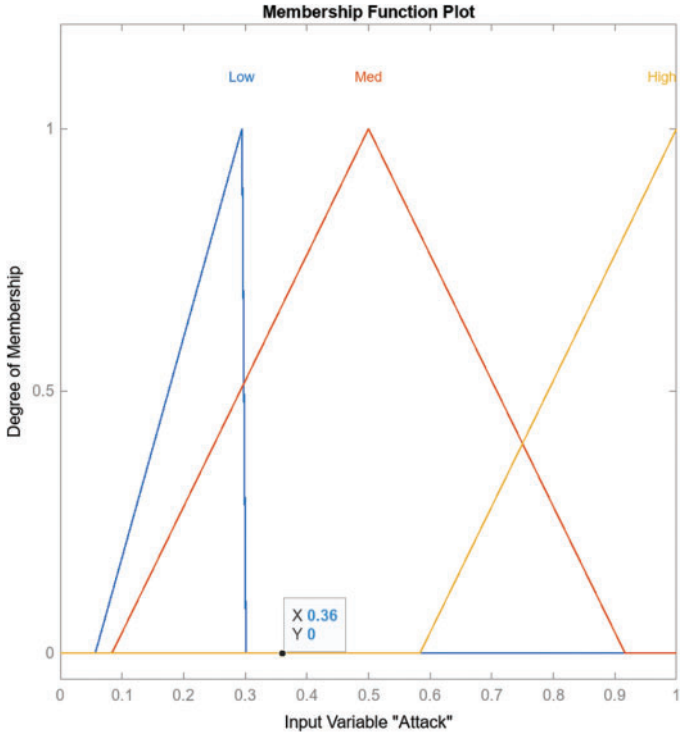

Figure 6: Membership functions for variable inputs attack

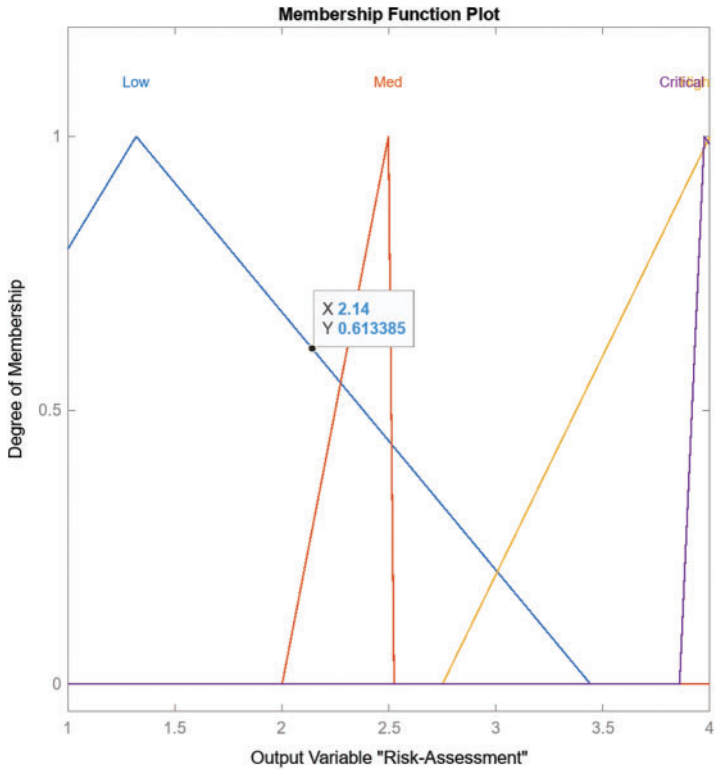

Figure 7: Membership functions for variable output risk assessment

The method presented in this work for enhancing IoT device security has several advantages. The main one is providing a significant understanding and evaluation of the risk and security associated with each IoT device. Hence, it helps identify vulnerabilities in the network. On the other hand, the CICIoT2023 dataset is considered representative of several network security vulnerabilities and risks, and it demonstrated the ability of the proposed model to function with real data for risk and security assessment. Furthermore, using fuzzy logic in risk and security assessment improved the accuracy measurement of intended parameters, such as attack, scanning, and propagation. Finally, the proposed method provides a mechanism to investigate and observe risk associated with specific IP addresses, for instance, 192.168.137.253 and 192.168.137.101, which can outline specific patterns where these addresses are used for scanning and propagation activities, which provides tools to highlight suspicious network behavior.

The novelty of the proposed risk assessment model lies in its integration of fuzzy logic and PSO to address the risks of IoT botnets. Fuzzy logic enables a systematic method for representing and managing the inherent ambiguities and uncertainties related to IoT botnet risks. Simultaneously, PSO improves the risk assessment model's precision and efficiency by optimizing parameters in botnet detection algorithms. The model categorizes risk levels into four distinct categories: Low, Medium, High, and Critical. This classification system offers a clear and practical means of categorizing risks based on their severity and impact. The risk assessment model facilitates proactive risk management, allowing security teams to allocate resources efficiently and mitigate risks in IoT ecosystems, thereby enhancing cybersecurity. Finally, the approach can be enhanced by considering new ransomware and spam attacks, and that evolve continuously [38,39].

The system's scalability is proportional to the number of rules and membership function parameters that must be stored. This characteristic allows the system to be optimized based on specific application limitations. Hence, the scalability of the proposed method can be achieved by employing a distributed computing approach, where the proposed method can scale and support extensive IoT networks comprising numerous devices. Using fuzzy logic controllers integrated into IoT devices boosts intelligence at the edge level, reducing potential bottlenecks and facilitating decentralized analysis. PSO is known for achieving rapid convergence in typical settings. However, it may require some tweaks to ensure convergence in bigger search areas.

Although the proposed IoT botnet risk assessment method, which combines fuzzy logic and PSO, shows promise, it has limitations. These limitations emphasize the importance of thoughtful deliberation and effective management. PSO optimization adds a pseudopolynomial element to computational complexity. Large-scale applications may need advanced hardware or approximations to run efficiently. Also, the model's interpretability and accuracy are tradeoffs. A higher number of rules and membership functions improves accuracy but reduces interpretability. Optimizing equilibrium is key. In addition, optimization of fuzzy rules requires iterative adjustment and analysis. Suboptimal rules can severely affect risk assessment reliability and validity.

5 Conclusions

This paper introduces a comprehensive fuzzy logic-based system incorporating three input parameters: scanning, attack, and propagation. Each input parameter is defined by three membership functions: "low," "mid," and "high." Furthermore, it is represented as triangular membership functions for simplicity. Using triangular membership functions facilitates representing these parameters' gradual and intuitive characteristics. The PSO technique was employed to optimize the membership functions, hence refining the parameters of the membership function to enhance accuracy and performance. Also, the system has been optimized using PSO to fine-tune membership functions and derive rules, resulting in an optimal representation of the risk assessment factors. The output parameter "risk assessment" comprises three membership functions: "low," "mid," and "critical." This system's use of triangular membership functions improves the interpretation of risk assessment outcomes, thereby increasing its reliability and precision for evaluating security-related scenarios.

An IoT botnet risk assessment model was developed by integrating fuzzy logic with PSO. The framework demonstrates a significant accuracy enhancement of 12% and 6.5% compared to baseline machine learning models and standard fuzzy systems. The optimized fuzzy approach achieves effective botnet detection with a precision rate exceeding 80% across various attack vectors. The proposed approach utilizes a structured fuzzy logic framework enhanced by swarm intelligence to improve resilience in the face of uncertainties. The system enhances security teams' capabilities by quantifying the severity of attacks and conducting proactive risk assessments. Additional enhancements can be achieved by investigating ensemble models that combine fuzzy outputs with other techniques, thus presenting a valuable avenue for exploration. Implementing edge-level analytics with fuzzy logic microcontrollers can enhance scalability.

The proposed method utilized the fuzzy logic system, facilitating the shift from binary decision-making to a continuous spatial framework. Fuzzy logic is a reasoning methodology that exhibits similarities to human perception, enabling the consideration of partial truths. This approach allows for evaluating statements with degrees of truthfulness or falsity rather than being strictly binary. Despite the ability of our methodology to offer a range of intensity levels, such as 20%, 30%, and 50%, the process of transitioning from a discrete to a continuous area presents significant complexities.

However, the decision was made to avoid using fuzzy rules or membership function factors derived from expert knowledge or self-configuration due to IoT networks' large traffic and data volume.

In contrast, the methodology used involved the utilization of fuzzy logic to get the optimum values for the fuzzy rules and membership functions by applying PSO, a metaheuristic optimization technique. PSO, or Particle Swarm Optimization, is a stochastic optimization technique that demonstrates efficacy in exploring vast solution spaces by using swarms' collective behavior and intelligence. Risk levels are classified into four categories: Low, Medium, High, and Critical. The determination of these levels is achieved through the evaluation of input probabilities utilizing maximum and minimum operators. The investigation identified 36 optimal fuzzy rules that describe the behavior of IoT botnets, with a specific focus on scanning, propagation, and the severity of attacks. These regulations facilitate assessing the risk level associated with individual IP addresses, specifically individual devices. The experiment employs control surfaces to transform imprecise output data into actionable control actions, as shown in Fig. 8. The implementation of these control mechanisms is necessary to address possible hazards adequately. This study presents a fundamental component in addressing computerized risk assessment, a critical task for security teams in effectively allocating resources and proactively mitigating risks.

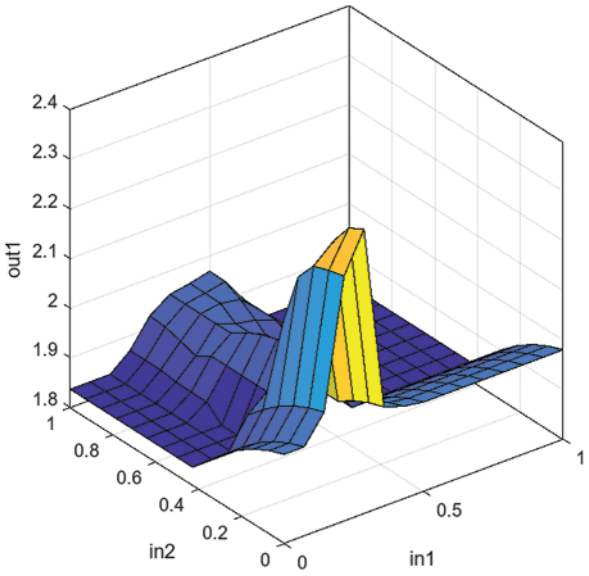

Figure 8: Control surface for output *vs.* inputs

The approach's limitations include reliance on one dataset (CICIoT2023) and having a fixed value in risk calculation. As a future work, we intend to further refine the fuzzy logic-based model by introducing more input variables and rules that capture more detailed risk assessment parameters, and this can be network traffic patterns, device behavior history, static or dynamic geographical location, authentication status, device vulnerability status, to list some. Incorporating such parameters into the model can provide new insights about risk assessment. In addition, we intend to conduct a pilot study to evaluate the system in a live IoT network in real-time operation.

Acknowledgement: The authors are grateful to the Deanship of Scientific Studies at the University of Dubai, UAE, for funding this research.

Funding Statement: No research fund was used to conduct this research. The University of Dubai will provide an APC charge.

Author Contributions: A.S.M. formulated the research approach, conducted algorithm design and implementation, performed simulations, analyzed literature for the review, scrutinized outcomes, and composed the initial draft of the publication. The research work was supervised by N.F.B.I. and M.A., who also read and edited the article. N.F.B.I. contributed to algorithm design and participated in the paper review. M.A. played a role in the algorithm design analysis of literature for the review and contributed to the paper review analysis. M.A.A. contributed to the literature review, conducted algorithm analysis, and participated in the review process. A.G. contributed to data visualization, conducted research, provided valuable input in reviewing and editing the text, played a key role in paper writing, and contributed to the algorithm complexity analysis and literature review analysis. The final manuscript was read and approved by all authors.

Availability of Data and Materials: The dataset used in this study was obtained from the publication titled "E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani (2023): "CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment". The dataset is publicly accessible. The supplementary datasets utilized or examined in this research can be acquired by contacting the corresponding author.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] T. N. Nguyen, Q. D. Ngo, H. T. Nguyen, and G. L. Nguyen, "An advanced computing approach for IoT-botnet detection in industrial internet of things," *IEEE Trans. Industr. Inform*, vol. 18, pp. 8298–8306, 2022. doi: 10.1109/TII.2022.3152814.

[2] M. Al-Kasassbeh, M. Almseidin, K. Alrfou, and S. Kovacs, "Detection of IoT-botnet attacks using fuzzy rule interpolation," *J. Intell. Fuzzy. Syst.*, vol. 39, no. 1, pp. 421–431, Jan. 2020. doi: 10.3233/JIFS-191432.

[3] J. A. Jerkins, "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code," in *2017 IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, 2017, pp. 1–5.

[4] Y. Liu, "Design and construction of personalized recommendation teaching system under artificial intelligence background," in *2023 4th International Conference on Education, Knowledge and Information Management (ICEKIM 2023)*, pp. 1601–1605, 2023. doi: 10.2991/978-94-6463-172-2_177.

[5] J. M. Belman-Flores, D. A. Rodríguez-Valderrama, S. Ledesma, J. J. García-Pabón, D. Hernández and D. Pardo-Cely, "A review on applications of fuzzy logic control for refrigeration systems," *Appl. Sci.*, vol. 12, no. 3, pp. 1302, 2022. doi: 10.3390/app12031302.

[6] C. C. Lee, "Fuzzy logic in control systems: Fuzzy logic controller—Part I," *IEEE Trans. Syst. Man Cybern.*, vol. 20, no. 2, pp. 404–418, 1990. doi: 10.1109/21.52551.

[7] A. Jain and A. Sharma, "Membership function formulation methods for fuzzy logic systems: A comprehensive review," *J. Crit. Rev*, vol. 7, no. 19, pp. 8717–8733, 2020.

[8] F. Marini and B. Walczak, "Particle swarm optimization (PSO). A tutorial," *Chemom. Intell. Lab. Syst.*, vol. 149, pp. 153–165, 2015. doi: 10.1016/j.chemolab.2015.08.020.

[9] N. Delgarm, B. Sajadi, F. Kowsary, and S. Delgarm, "Multi-objective optimization of the building energy performance: A simulation-based approach by means of particle swarm optimization (PSO)," *Appl. Energy*, vol. 170, pp. 293–303, 2016. doi: 10.1016/j.apenergy.2016.02.141.

[10] R. A. Smirnov and S. N. Novikov, "Research on information security risk assessment techniques," *Interexpo GEO–Siberia*, vol. 6, pp. 250–257, 2022. doi: 10.33764/2618-981x-2022-6-250-257.

[11] J. Mallick *et al.,* "Risk assessment of resources exposed to rainfall induced landslide with the development of GIS and RS based ensemble metaheuristic machine learning algorithms," *Sustain.*, vol. 13, no. 2, pp. 457, 2021. doi: 10.3390/su13020457.
[12] H. Zerrouki, "Risk assessment of a liquefied natural gas process facility using bow-tie and Bayesian networks," *Process. Saf. Prog.*, vol. 41, pp. 480–491, 2022. doi: 10.1108/IJQRM-11-2022-0336.
[13] K. Biron, W. Bazzaza, K. Yaqoob, A. Gawanmeh, and C. Fachkha, "A big data fusion to profile CPS security threats against operational technology," in *2020 IEEE 21st International Symposium on A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, IEEE, 2020, pp. 397–402. doi: 10.1109/WoWMoM49955.2020.00073.
[14] R. Madhuri, S. Sistla, and K. S. Raju, "Application of machine learning algorithms for flood susceptibility assessment and risk management," *J. Water. Clim. Change*, vol. 12, no. 6, pp. 2608–2623, 2021. doi: 10.2166/wcc.2021.051.
[15] O. Yanholenko, O. Cherednichenko, O. Yakovleva, and D. Arkatov, "A model for estimating the security level of mobile applications: A fuzzy logic approach," in *Int. Workshop Intell. Inf. Technol. Syst. Inf. Secur.*, 2020.
[16] S. Ksibi, F. Jaïdi, and A. Bouhoula, "IoMT security model based on machine learning and risk assessment techniques," in *Int. Wirel. Commun. Mob. Comput. (IWCMC)*, 2023, pp. 614–619.
[17] A. A. Bolgov, S. A. Ermakov, L. Parinova, and V. N. Kostrova, "Internet of Things networks predictive risk assessment method and security management," *IOP Conf. Ser. Mater. Sci. Eng.*, IOP Publishing, vol. 862, no. 5, pp. 052035, 2020. doi: 10.1088/1757-899X/862/5/052035.
[18] R. L. Neupane *et al.*, "CICADA: Cloud-based intelligent classification and active defense approach for IoT security," in *IEEE INFOCOM, 2023—IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2023, pp. 1–6.
[19] H. Luo, "Intelligent assessment of mental health based on IoT data," *Secur. Commun. Netw.*, vol. 2023, pp. 9758342, 2023. doi: 10.1155/2023/9758342.
[20] S. Elhag, A. Fernández, A. Bawakid, S. Alshomrani, and F. Herrera, "On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems," *Expert. Syst. Appl.*, vol. 42, pp. 193–202, Dec. 2015. doi: 10.1016/j.eswa.2014.08.002.
[21] A. Bajpai and V. S. Kushwah, "Importance of fuzzy logic and application areas in engineering research," *Int. J. Recent Technol. Eng. (IJRTE)*, vol. 7, pp. 1467–1471, 2019.
[22] E. M. Dovom, A. Azmoodeh, A. Dehghantanha, D. E. Newton, R. M. Parizi, and H. Karimipour, "Fuzzy pattern tree for edge malware detection and categorization in IoT," *J. Syst. Architect.*, vol. 97, pp. 1–7, 2019. doi: 10.1016/j.sysarc.2019.01.017.
[23] K. Kapitanova, S. H. Son, and K. D. Kang, "Using fuzzy logic for robust event detection in wireless sensor networks," *Ad. Hoc. Netw.*, vol. 10, no. 4, pp. 709–722, 2012. doi: 10.1016/j.adhoc.2011.06.008.
[24] S. Pervaiz, Z. Ul-Qayyum, W. H. Bangyal, L. Gao, and J. Ahmad, "A systematic literature review on particle swarm optimization techniques for medical diseases detection," *Comput. Math. Methods. Med.*, vol. 2021, pp. 5990999, 2021. doi: 10.1155/2021/5990999.
[25] R. Kumar, A. I. Khan, Y. B. Abushark, Md. M. Alam, A. Agrawal, and R. Ahmad Khan, "An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications," *IEEE Access*, vol. 8, pp. 50944–50957, 2020. doi: 10.1109/ACCESS.2020.2970245.
[26] A. Alfi and M. M. Fateh, "Intelligent identification and control using improved fuzzy particle swarm optimization," *Expert Syst. Appl.*, vol. 38, no. 10, pp. 12312–12317, 2011. doi: 10.1016/j.eswa.2011.04.009.
[27] S. M. A. Pahnehkolaei, A. Alfi, and J. A. T. Machado, "Analytical stability analysis of the fractional-order particle swarm optimization algorithm," *Chaos Solit. Fractals*, vol. 155, pp. 111658, 2022. doi: 10.1016/j.chaos.2021.111658.
[28] C. Karahan, E. A. Güzeldereli, and A. Tüfekci, "Fuzzy logic approach in risk assessment," in *Encyclopedia of Information Science and Technology, Fourth Edition*, IGI Global, pp. 6789–6805, 2018. doi: 10.4018/978-1-5225-2255-3.ch588.

[29] Sankar, S. Divya, K Shashikanth, A. Bhaumik, and A. Pawar, "Fuzzy inference system based risk management in complex civil engineering projects," *Neuroquantology*, vol. 20, no. 10, p. 11334–11342, 2022. doi: 10.14704/nq.2022.20.10.NQ551098.

[30] S. Sharma and P. K. Goyal, "Fuzzy logic: An appropriate technique for effective risk analysis and decision making for construction projects," *International Journal of Emerging Technology and Advanced Engineering*, vol. 5, no. 12, pp. 71–77, 2015.

[31] A. S. Mashaleh, N. F. B. Ibrahim, M. Alauthman, and A. Almomani, "A proposed framework for early detection IoT botnet," in *2022 Int. Arab Conf. Inf. Technol. (ACIT)*, 2022, pp. 1–7.

[32] F. Zakeri, M. Golsorkhtabaramiri, and M. Hosseinzadeh, "Optimizing radio frequency identification networks planning by using particle swarm optimization algorithm with fuzzy logic controller and mutation," *IETE J. Res.*, vol. 63, pp. 728–735, 2017. doi: 10.1080/03772063.2015.1083905.

[33] N. Roy, C. Beauthier, and A. Mayer, "Setup of a new adaptive fuzzy particle swarm optimization algorithm," in *2022 IEEE Congress Evol. Comput. (CEC)*, 2022, pp. 1–8.

[34] I. Z. M. Darus and M. H. A. Talib, "Development of fuzzy logic controller by particle swarm optimization algorithm for semi-active suspension system using magneto-rheological damper," *WSEAS Trans. Syst. Control Archive*, vol. 9, pp. 77–85, 2014.

[35] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu and A. A. Ghorbani, "CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment," *Sensors*, vol. 23, no. 13, pp. 5941, 2023. doi: 10.3390/s23135941.

[36] I. P. Seletkov, "Application of matrix approach of fuzzy logic for decision support in oil mining equipment service," *Appl. Math. Control Sci.*, no. 4, pp. 65–88, 2020. doi: 10.15593/2499-9873/2020.4.05.

[37] P. L. C. van Geert, "Dynamic systems, process and development," *Hum. Dev.*, vol. 63, no. 3–4, pp. 153–179, 2020. doi: 10.1159/000503825.

[38] S. Razaulla *et al.,* "The age of ransomware: A survey on the evolution, taxonomy, and research directions," *IEEE Access*, vol. 11, pp. 40698–40723, Dec. 2023. doi: 10.1109/ACCESS.2023.3268535.

[39] A. S. Mashaleh, N. F. Binti Ibrahim, M. A. Al-Betar, H. M. J. Mustafa, and Q. M. Yaseen, "Detecting spam email with machine learning optimized with harris hawks optimizer (HHO) algorithm," *Procedia Comput. Sci.*, vol. 201, pp. 659–664, 2022. doi: 10.1016/j.procs.2022.03.087.