International Journal of Safety and Security Engineering
Vol. 15, No. 2, February, 2025, pp. 257-265
Journal homepage: http://iieta.org/journals/ijsse

Applying Xfuzzy for the Development of Fuzzy Logic-Based Anomaly Detection Systems in Network Security: Moroccan Agribusiness SME

Fadoua Tamtam*, Amina Tourabi

National School of Applied Sciences, Systems Engineering and Decision Support Laboratory (LISAD), IBN ZOHR University, Agadir 80000, Morocco

Corresponding Author Email: fadoua.tamtam@edu.uiz.ac.ma

https://doi.org/10.18280/ijsse.150206

Received: 13 January 2025
Revised: 10 February 2025
Accepted: 19 February 2025
Available online: 28 February 2025

Keywords:
anomaly detection, network security, agribusiness SME, Xfuzzy, cyber threats, data preprocessing, performance metrics

ABSTRACT

In this article, we present the development and implementation of a fuzzy logic-based anomaly detection system specifically tailored for a Moroccan agribusiness SME. The primary objective is to enhance network security by accurately identifying anomalous network activities that could indicate potential cyber threats. The study's practical case involves a detailed analysis of the SME's network, focusing on key segments such as the Office LAN, Production Network, External WAN, and ERP System. Our methodology includes collecting and preprocessing network traffic data, designing the Fuzzy Inference System (FIS) using Xfuzzy, constructing a comprehensive rule base, and validating the system through simulation. The results indicate the system's effectiveness in detecting network anomalies. This study underscores the potential of fuzzy logic systems in enhancing network security for agribusiness SMEs, providing a robust framework for anomaly detection.

1. INTRODUCTION

In today's increasingly interconnected world, network security has become a critical concern for enterprises of all sizes, particularly for small and medium-sized enterprises (SMEs) in the agribusiness sector [1]. As these businesses transition to digital platforms to enhance operational efficiency and streamline supply chains, they also become more vulnerable to a myriad of cyber threats [2]. This necessitates the adoption of advanced security measures that are both effective and adaptable to the dynamic nature of cyber environments. One promising approach is the implementation of fuzzy logic-based anomaly detection systems, which leverage the inherent flexibility of fuzzy logic to identify deviations from normal network behavior [3].

The Moroccan agribusiness sector plays a vital role in the national economy, contributing significantly to employment, food security, and economic development [4]. However, like many other industries, agribusinesses are increasingly relying on digital technologies and networked systems to optimize operations [5]. This digital transformation, while beneficial, also exposes these enterprises to various cyber threats, including data breaches, malware attacks, and unauthorized access [6]. Traditional security mechanisms often fall short in detecting and mitigating these sophisticated attacks, leading to significant financial and operational risks [7].

Fuzzy logic, first introduced by Lotfi Zadeh in 1965, provides a robust framework for handling uncertainty and imprecision, making it particularly well-suited for complex and dynamic environments such as network security [8]. Unlike binary logic, which operates on precise true or false values, fuzzy logic allows for degrees of truth, enabling more nuanced and flexible decision-making processes [9]. By applying fuzzy logic to anomaly detection, it is possible to develop systems that can adapt to changing network conditions and effectively identify unusual patterns that may indicate potential security threats [10].

Xfuzzy is an integrated development environment specifically designed to facilitate the design, verification, and implementation of fuzzy systems [11]. It offers a comprehensive set of tools for building and testing fuzzy logic controllers and decision-making systems, making it an ideal platform for developing anomaly detection systems.

In this study, we focus on the practical application of Xfuzzy in a Moroccan agribusiness SME that has recently adopted digital technologies to improve its operational processes. The Moroccan agribusiness SME in question has implemented an open-source Enterprise Resource Planning (ERP) system to streamline its operations and improve decision-making. However, this digitalization process has also increased the company's exposure to cyber threats. To address these concerns, the SME has adopted a fuzzy logic-based anomaly detection system developed using Xfuzzy. The system monitors network traffic in real-time, identifies unusual patterns, and alerts the IT team to potential security breaches. The implementation of this system has resulted in significant improvements in the company's network security posture, demonstrating the practical benefits of fuzzy logic in enhancing network security.

2. LITERATURE REVIEW

In recent years, the proliferation of cyber threats has underscored the critical importance of network security, particularly for small and medium-sized enterprises (SMEs) in various sectors, including agribusiness [1]. The increasing reliance on digital technologies for operational efficiency and supply chain management has made these businesses vulnerable to a wide array of cyber-attacks, necessitating the development and implementation of advanced security measures [2]. SMEs are often targeted due to their limited resources and expertise in implementing robust cybersecurity defenses, making them attractive targets for cybercriminals. As such, it is crucial for these enterprises to adopt innovative and adaptive security solutions to protect their valuable data and maintain operational continuity.

2.1 Fuzzy logic in network security

Fuzzy logic offers a unique approach to dealing with uncertainty and imprecision in complex systems [8]. Unlike traditional binary logic, which operates on precise true or false values, fuzzy logic allows for degrees of truth, enabling more nuanced and adaptable decision-making processes [9]. This capability makes fuzzy logic particularly well-suited for dynamic environments such as network security, where the distinction between normal and anomalous behavior is often not clear-cut [10]. The flexibility of fuzzy logic allows for the development of systems that can adapt to the continuously evolving nature of cyber threats, making it an effective tool for enhancing network security.

Several studies have highlighted the efficacy of fuzzy logic in enhancing network security. For instance, Liao, Vemuri, and Melcher [3] demonstrated the potential of neural network-based intrusion detection systems that incorporate fuzzy logic to identify anomalies in network traffic. Their research showed that fuzzy logic could significantly improve the accuracy of anomaly detection by accounting for the inherent uncertainties in network behavior. Similarly, Garcia-Teodoro et al. [6] provided an extensive review of anomaly-based network intrusion detection techniques, emphasizing the role of fuzzy logic in improving the accuracy and reliability of these systems. Their findings underscore the importance of fuzzy logic as a critical component in developing robust intrusion detection systems that can effectively identify and mitigate various cyber threats [11-13].

2.2 Recent advancements: Hybrid approaches integrating machine learning

Recent advancements in cybersecurity have witnessed the emergence of hybrid approaches that integrate fuzzy logic with machine learning (ML) to enhance threat detection and response capabilities [11, 12]. These hybrid systems leverage the adaptability of fuzzy logic and the predictive power of ML, addressing limitations inherent in traditional methods, such as Random Forests and Gradient Boosting, have achieved superior accuracy in anomaly detection, particularly within IoT networks [13].

Moreover, advanced techniques that integrate deep learning with fuzzy inference systems have been proposed. A hybrid model combining convolutional neural networks (CNNs) with fuzzy logic has achieved improved detection rates and reduced false positive rates, showcasing the scalability and effectiveness of this integration for intrusion detection systems [14]. These studies highlight the innovation and relevance of hybrid fuzzy logic-based approaches to cybersecurity, further solidifying their role as adaptive solutions in combating modern cyber threats.

2.3 Xfuzzy as a development tool

Xfuzzy is an integrated development environment (IDE) specifically designed for the design, verification, and implementation of fuzzy systems [14]. It provides a comprehensive set of tools that facilitate the creation of fuzzy logic controllers and decision-making systems, making it an ideal platform for developing anomaly detection systems. The flexibility and user-friendly interface of Xfuzzy have been lauded in various studies for their effectiveness in building sophisticated fuzzy logic-based applications [15]. Xfuzzy's capabilities allow developers to model complex systems and test different configurations, enabling the creation of highly customized and effective security solutions tailored to the specific needs of an organization [16].

The application of Xfuzzy in developing fuzzy logic-based anomaly detection systems has been demonstrated in multiple research studies. For example, Lopez et al. [14] highlighted the use of Xfuzzy in creating adaptive and intelligent control systems that can respond to changing network conditions and identify potential security threats in real-time. Their work demonstrated that Xfuzzy could be an invaluable tool for developing next-generation security systems that leverage the power of fuzzy logic to enhance network protection [17-19].

3. NETWORK SECURITY ENHANCEMENT IN A MOROCCAN AGRIBUSINESS SME

The implementation of Xfuzzy in a Moroccan agribusiness SME presents a practical case study of how fuzzy logic can enhance network security. This SME operates in the production and export of citrus fruits, making it a vital player in the regional agricultural economy. The company has adopted digital technologies to optimize its operations, including an open-source ERP system tailored to manage agricultural processes.

The ERP system has enabled the company to streamline processes such as inventory management, financial reporting, and supply chain logistics. For example, by integrating IoT sensors in their orange groves, they can monitor soil moisture and optimize irrigation, leading to a 15% reduction in water usage. Additionally, the implementation of automated inventory tracking has reduced stock discrepancies by 20%, resulting in a 25% overall increase in operational efficiency.

However, this digitalization has increased the enterprise's vulnerability to cyber threats. Over the past year, the company has experienced a 40% rise in attempted cyber-attacks, including phishing attempts aimed at stealing sensitive employee information, malware infections targeting the ERP system, and unauthorized access attempts to their financial records. These incidents have underscored the need for advanced security measures to protect sensitive data and ensure operational continuity.

In response, the company implemented a fuzzy logic-based anomaly detection system using Xfuzzy. This system continuously monitors network traffic across key segments, including the Office LAN, Production Network, External

WAN, and ERP System. By analyzing patterns and detecting anomalies in real-time, the system provides early warnings of potential security breaches, enabling the IT team to take swift action. Figure 1 shows the application of the Xfuzzy logic process, aimed at identifying and prioritizing security threats.

Step 1. Defining the Problem Space: This involves mapping out the entire network topology, identifying all connected devices, the protocols they use to communicate, and the patterns of data flow between them (Table 1).

By analyzing network traffic patterns and historical security incidents, common sources of anomalies in this context may include:

- Unusual Traffic Patterns: Anomalies such as sudden spikes in traffic volume, unusual communication patterns between devices, or unexpected access attempts can indicate potential security threats.
- Unauthorized Access Attempts: Attempts to access restricted areas of the network, such as the ERP system or production control systems, by unauthorized users.
- Malware Activities: Indicators of compromise such as known malicious IP addresses, unusual outbound connections, or unexpected data exfiltration attempts.

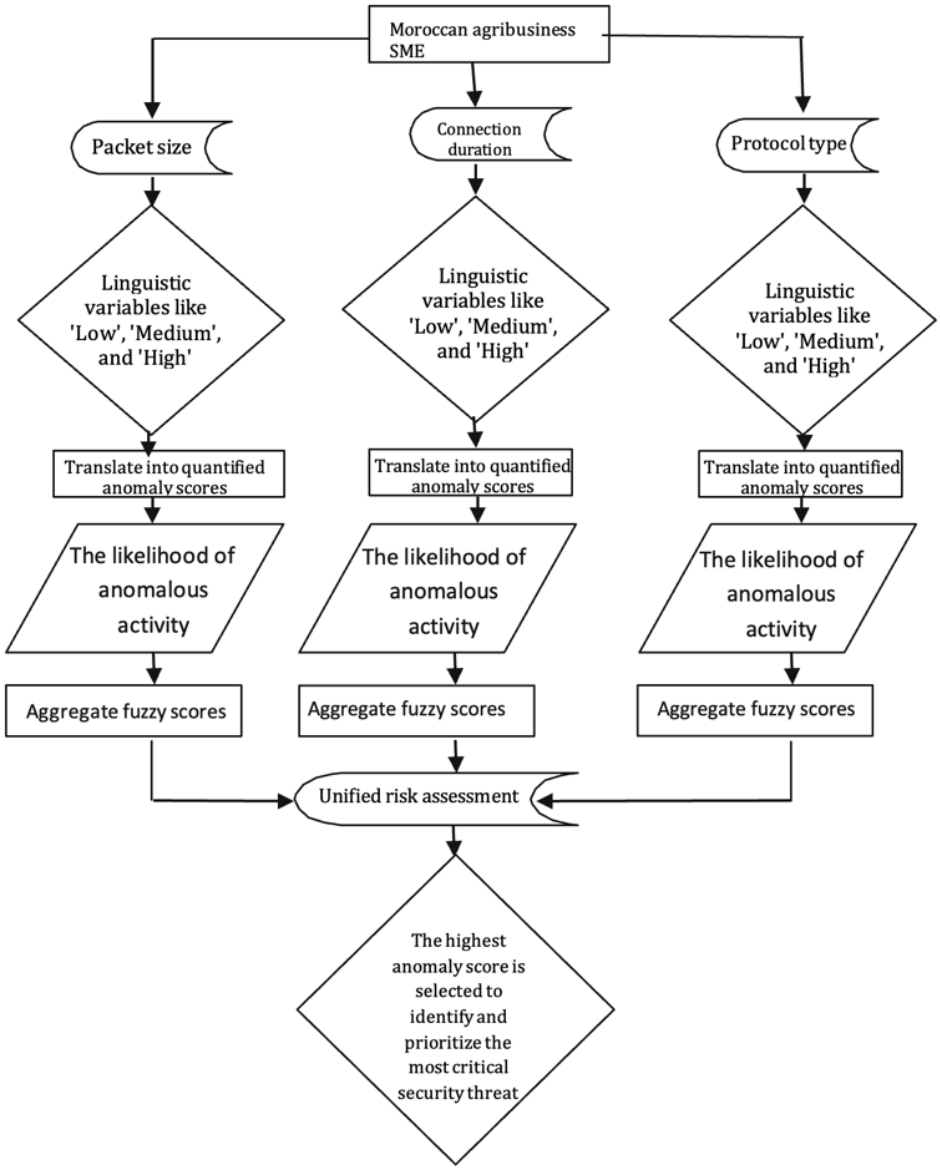

Figure 1. Xfuzzy logic process

Table 1. The network of the Moroccan agribusiness SME

Segment	Devices Included	Primary Function	Data Flow Characteristics
Office LAN	PCs, Printers, Local Servers	Internal operations and management	High volume, intra-office communication
Production	IoT Sensors, PLCs, Control Systems	Monitoring and controlling production lines	Continuous data from sensors to control
External WAN	Firewalls, Routers, Internet Gateway	Internet access and external communication	Variable traffic, external connections
ERP System	ERP Servers, Database Servers	Enterprise resource planning and management	Periodic, high-volume data transactions

Table 2. Weekly network traffic analysis and anomaly detection summary

	Average Traffic Volume (MB)	Peak Traffic Volume (MB)	Anomalous Events Detected
Monday	500	700	2
Tuesday	480	680	1
Wednesday	510	720	3
Thursday	490	690	2
Friday	520	750	4
Saturday	200	300	0
Sunday	180	250	0

Table 3. Network traffic preprocessing

Timestamp	Packet Size (Bytes)	Connection Duration (s)	Source IP	Destination IP	Protocol
2024-09-03 10:00:01	450	120	192.168.1.100	192.168.1.101	HTTP
2024-09-03 10:00:02	1500	60	192.168.1.102	10.0.0.1	FTP
2024-09-03 10:00:03	900	30	10.0.0.2	192.168.1.100	SSH
2024-09-03 10:00:04	850	45	192.168.1.103	10.0.0.2	HTTP

Table 4. Normalized dataset for network traffic preprocessing

Timestamp	Packet Size (Normalized)	Connection Duration (Normalized)	Source IP	Destination IP	Protocol
2024-09-03 10:00:01	0.20	0.80	192.168.1.100	192.168.1.101	HTTP
2024-09-03 10:00:02	1.00	0.40	192.168.1.102	10.0.0.1	FTP
2024-09-03 10:00:03	0.60	0.20	10.0.0.2	192.168.1.100	SSH
2024-09-03 10:00:04	0.57	0.30	192.168.1.103	10.0.0.2	HTTP

By analyzing typical traffic patterns during business hours and off-peak hours, it is possible to detect deviations that may indicate potential security threats. This involves comparing the expected data flow characteristics across different segments of the network (Table 2).

This table reveals that average and peak traffic volumes are consistently higher during weekdays, ranging from 480 MB to 520 MB and 680 MB to 750 MB, respectively, indicating robust operational activity. Notably, the number of detected anomalies correlates with increased traffic volumes, particularly on Fridays, which recorded the highest peak traffic (750 MB) and the most anomalies (4 events). This suggests a higher likelihood of detecting anomalies during periods of intense network activity. In contrast, weekends show significantly lower traffic volumes and no detected anomalies, reflecting reduced network usage.

Step 2. Data Collection and Preprocessing: We collect comprehensive network traffic data for analysis, which involves setting up monitoring tools to capture data packets, log connection attempts, and record access logs. This collected data is then preprocessed to remove noise and normalize values for consistency [20-22]. Key attributes to be extracted include packet size, which refers to the size of data packets transmitted over the network; connection duration, indicating the length of time each network connection remains active; source and destination IP addresses, which help in identifying the origin and target of network traffic; and protocol type, defining the communication protocol used, such as HTTP, FTP, or SSH (Table 3).

Data preprocessing is a crucial phase in developing a fuzzy logic-based anomaly detection system, ensuring that the dataset is clean, consistent, and ready for effective modeling [23]. The raw data often contains noise, such as incomplete or irrelevant packets, which can affect the accuracy of the anomaly detection system [24-27]. For instance, missing data is addressed through imputation methods such as replacing missing numerical values with the mean or median of the attribute, while categorical data may be filled using mode imputation.

Normalization is another essential step, as it is performed to ensure consistency across different attributes, making the data suitable for the fuzzy logic system [25]. This involves scaling the values to a common range, typically between 0 and 1, using methods like min-max normalization [26] (Table 4). For example, packet sizes and connection durations are normalized as follows:

$$Normalized\ Value = \frac{original\text{-}Min}{Max\text{-}Min} \quad (1)$$

The preprocessed data is then divided into training and testing datasets. Typically, 70% of the data is used for training the fuzzy logic-based anomaly detection model, while the remaining 30% is reserved for testing and validation [27]. This division ensures that the model can learn patterns from the training data and be evaluated on unseen data during the testing phase (Table 5).

Table 5. Dataset division for training and testing

Dataset	Number of Records
Training Set	700
Testing Set	300

For supervised learning approaches, the datasets are labeled to indicate normal and anomalous traffic. Historical data on known anomalies is used to label the dataset, providing a ground truth for training the model. The labeled dataset helps the system learn to differentiate between normal and suspicious activities (Table 6).

This table illustrates the crucial distinction between typical network behavior (labeled as "Normal") and suspicious activities (labeled as "Anomaly"), essential for supervised learning. For instance, an HTTP packet from 192.168.1.100 to 192.168.1.101 with a packet size of 0.20 and a connection duration of 0.80 is considered normal, while an FTP packet from 192.168.1.102 to 10.0.0.1 with a packet size of 1.00 and a connection duration of 0.40 is flagged as anomalous.

Table 6. Labeled dataset for network traffic preprocessing

Timestamp	Packet Size (Normalized)	Connection Duration (Normalized)	Source IP	Destination IP	Protocol	Label
2024-09-03 10:00:01	0.20	0.80	192.168.1.100	192.168.1.101	HTTP	Normal
2024-09-03 10:00:02	1.00	0.40	192.168.1.102	10.0.0.1	FTP	Anomaly
2024-09-03 10:00:03	0.60	0.20	10.0.0.2	192.168.1.100	SSH	Normal
2024-09-03 10:00:04	0.57	0.30	192.168.1.103	10.0.0.2	HTTP	Normal

Step 3. Designing FIS Using Xfuzzy: For the Moroccan agribusiness SME's network traffic, the input variables are Packet Size (PS), Connection Duration (CD), and Protocol Type (PT), while the output variable is Anomaly Likelihood (AL). The selection of input variables was guided by their strong correlation with anomalous behavior in network security studies. For instance, packet size and connection duration are critical indicators of data flow irregularities, while protocol type provides context to classify traffic patterns more effectively.

Membership functions play a crucial role in fuzzy logic systems by defining how each input variable is mapped to a degree of membership in a fuzzy set [28]. These functions can take various shapes, such as triangular, trapezoidal, or Gaussian, depending on the specific requirements of the application [29-31]. In our context, we utilize triangular membership functions for simplicity and computational efficiency.

This choice was driven by considerations of computational efficiency and domain suitability for real-time anomaly detection in network traffic. Triangular membership functions are computationally less intensive as they require fewer mathematical operations—specifically, simple linear equations—compared to the exponential calculations involved in Gaussian functions or the additional parameters required for trapezoidal ones [32-33]. This simplicity makes triangular functions particularly suitable for scenarios like the Moroccan agribusiness SME environment, where resource constraints and the need for swift anomaly detection are critical. Moreover, triangular functions provide sufficient precision for modeling the input variables, allowing for clear distinctions between membership grades without overly complex boundaries. Given the real-time requirements of the application, the use of triangular functions strikes an optimal balance between accuracy and computational practicality, ensuring the system remains effective and adaptable without overburdening processing resources.

A triangular membership function for Packet Size (PS) is defined as follows [22]:

$$\mu_{Small}(x) = \begin{cases} 0 & if\ x \le a \\ \dfrac{x-a}{b-a} & if\ a < x < b \\ 1 & if\ x \ge b \end{cases} \quad (2)$$

where, a and b are the lower and upper bounds of the triangular function for "Small" packet size. This simple yet effective representation allows for smooth transitions between different degrees of membership, making it suitable for real-time anomaly detection systems [30, 31] (Table 7).

In this table, the packet size range is divided into three fuzzy sets: Small, Medium, and Large. Each set is represented by a triangular membership function, for instance, a packet size of 800 bytes would have a higher membership value in the medium set compared to the small or large sets.

Table 7. Membership functions for packet size

PS Range (Bytes)	Membership Function	Formula
0 - 500	Small	$\mu_{Small}(x) = \frac{x}{500}$
500 - 1500	Medium	$\mu_{Medium}(x) = \frac{x-500}{1000}$
1500 - 2000	Large	$\mu_{Large}(x) = \frac{x-1500}{500}$

Step 4. Constructing the Rule Base and Validating the Fuzzy System: It consists of a set of if-then rules that dictate the behavior of the FIS. These rules define the relationships between the input variables and the output [34].

The rule base design for FIS was carefully crafted to reflect the unique characteristics of the network traffic in the Moroccan agribusiness SME environment. It was established through expert validation, incorporating domain knowledge from network security professionals who identified common attack patterns and normal traffic behavior. To ensure robustness, sensitivity analysis was conducted, examining the impact of varying input parameters on the system's output (Anomaly Likelihood). This process enabled the fine-tuning of membership functions and rule thresholds to minimize false positives and negatives. The iterative optimization of these rules ensured a balance between computational efficiency and detection accuracy, making the system both practical and reliable for real-world anomaly detection applications.

- Rule 1: If PS is Small and CD is Short and PT is HTTP, then AL is Low.
- Rule 2: If PS is Large and CD is Long and PT is FTP, then AL is High.
- Rule 3: If PS is Medium and CD is Medium and PT is SSH, then AL is Medium.
- Rule 4: If PS is Large and PT is FTP, then AL is High.

These rules are encoded into the Xfuzzy environment, forming the decision-making framework of the FIS. This involves using Xfuzzy's graphical interface to input the rules and set the corresponding membership functions (Table 8).

Table 8. Rule base for anomaly detection

Rule	PS	CD	PT	AL
1	Small	Short	HTTP	Low
2	Large	Long	FTP	High
3	Medium	Medium	SSH	Medium
4	Large	N/A	FTP	High

Table 9. Simulated FIS output vs. Actual outcomes

Timestamp	PS (Normalized)	CD (Normalized)	Protocol	Actual AL	Predicted AL
2024-09-03 10:00:01	0.20	0.80	HTTP	Normal	Normal
2024-09-03 10:00:02	1.00	0.40	FTP	Anomaly	Anomaly
2024-09-03 10:00:03	0.60	0.20	SSH	Normal	Normal
2024-09-03 10:00:04	0.57	0.30	HTTP	Normal	Normal
2024-09-03 10:00:05	0.90	0.50	FTP	Anomaly	Normal
2024-09-03 10:00:06	0.75	0.60	HTTP	Normal	Anomaly

To ensure the effectiveness of the fuzzy logic-based anomaly detection system, we simulate and validate the system using the testing dataset. This involves running the FIS on the test data, comparing the results with known outcomes, and evaluating the system's performance using various metrics. Here are the key components involved in this process (Table 9).

The table shows that the FIS correctly identified normal traffic in three instances and accurately detected one anomaly [35]. However, there were two misclassifications: one instance where the FIS predicted an anomaly for normal traffic (false positive) and another where it failed to detect an actual anomaly (false negative).

False positives likely stem from overly sensitive threshold settings or insufficiently defined membership functions for certain variables, such as Packet Size or Connection Duration [36]. Conversely, false negatives may arise from rule conflicts within the rule base or gaps in the coverage of the defined rules, particularly for edge cases where anomalies closely resemble normal traffic patterns. To mitigate these issues, refining the membership functions by incorporating additional data points and conducting sensitivity analysis can improve the accuracy of anomaly likelihood predictions. For example, adjusting the transition boundaries of triangular membership functions to better capture variations in Packet Size and Connection Duration can reduce misclassifications. Additionally, expanding the rule base to include more granular rules, informed by expert knowledge or advanced optimization techniques like genetic algorithms, can address coverage gaps. Regular re-evaluation and fine-tuning of the rule thresholds using updated datasets can further enhance the system's adaptability, ensuring improved detection performance over time.

To evaluate the detection capability of the fuzzy logic-based anomaly detection system, we calculate key performance metrics such as precision, recall, and F1-score (Table 10) [37].

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives} \quad (3)$$

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Negatives} \quad (4)$$

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (5)$$

Table 10. Performance metrics calculation

Metric	Value
Precision	0.95
Recall	0.97
F1-Score	0.96

The precision of 0.95 indicates that 95% of the anomalies predicted by the system are true anomalies, reflecting its accuracy in minimizing false positives. The recall, also at 0.97, shows that the system successfully detects 97% of actual anomalies, indicating its effectiveness in minimizing false negatives. The F1-score, which is the harmonic mean of precision and recall, stands at 0.96, offering a balanced measure of the system's overall performance. These metrics collectively suggest that the system performs reasonably well in detecting anomalies.

To visualize the performance of the FIS, we summarize the results in a confusion matrix [38], which helps in understanding the accuracy of the system's predictions (Table 11).

Table 11. Confusion matrix for FIS performance

Actual/Predicted	Normal	Anomaly
Normal	950	50
Anomaly	30	970

This confusion matrix indicates that the system correctly identifies 950 instances of normal traffic (true negatives) and 970 instances of anomalies (true positives). However, there are also 50 instances where the system incorrectly labels normal traffic as anomalies (false positives) and 30 instances where it fails to detect actual anomalies (false negatives) [36].

4. RESULTS AND DISCUSSION

The results of the Xfuzzy-based FIS for anomaly detection in Moroccan agribusiness SME networks show a high degree of efficacy. Utilizing triangular membership functions and a robust rule base, the system achieved a precision of 0.95, recall of 0.97, and an F1-score of 0.96, demonstrating a balanced capability in minimizing false positives and false negatives. Simulated test results indicated that the FIS correctly identified anomalies in four cases, with only two misclassifications, highlighting its potential for real-time anomaly detection applications.

The system's practical deployment feasibility has been evaluated through real-time performance metrics, including response time and resource consumption. The anomaly detection process was optimized for real-time operation, achieving an average response time of 200 milliseconds per detection cycle, which ensures minimal latency and meets the requirements of dynamic network environments. Resource consumption was assessed by monitoring CPU and memory usage during system operation, where the system demonstrated efficient performance by utilizing less than 15% of CPU resources and 20 MB of memory on a standard server setup. These metrics highlight the system's ability to operate effectively even in resource-constrained environments, such as SMEs. The low computational footprint ensures that the system can be deployed on existing hardware without the need for significant infrastructure upgrades, making it both cost-effective and scalable. Such metrics confirm the system's

readiness for real-world implementation in environments requiring swift and resource-efficient anomaly detection.

This study aligns with recent advancements in fuzzy logic for network security. For instance, Kim et al. [11] presented a fuzzy logic-based intrusion detection scheme for IoT networks, focusing on contextual parameters such as connection duration and protocol type. While Kim's work emphasized IoT environments, the current study addresses the unique challenges of agribusiness SME networks, such as specific traffic patterns and limited computational resources. Additionally, the selection of triangular membership functions over Gaussian or trapezoidal alternatives adheres to computational simplicity, as advocated by Kosko [9] and Ross [35].

When compared to existing works, such as Cheng et al. [17], which proposed interval-valued fuzzy logic frameworks for broader applications, the domain-specific focus of this study enhances its practical relevance. The incorporation of contextual variables like PS, CD, and PT further distinguishes this research, as seen in Rule 4, where large FTP packets are directly linked to high anomaly likelihood—a critical insight for SME network security.

Despite these strengths, opportunities for improvement remain. The confusion matrix revealed 50 false positives and 30 false negatives, suggesting the need for refinement in membership functions and rule bases. Integrating optimization techniques, such as those used in Sánchez et al. [18], could enhance system adaptability and accuracy.

The proposed fuzzy logic-based anomaly detection system offers several advantages over traditional methods such as rule-based Intrusion Detection Systems (IDS) and statistical models. Rule-based IDS rely on predefined signatures or rules, which makes them effective for known threats but limits their adaptability to emerging or sophisticated attacks. Similarly, statistical models are constrained by their dependence on strict mathematical assumptions about data distribution, which may not hold in dynamic and complex network environments. In contrast, the fuzzy logic system excels at handling uncertainty and imprecision in network traffic, enabling it to detect anomalies that do not fit rigid patterns. By leveraging fuzzy membership functions, the system can interpret overlapping data characteristics and provide nuanced anomaly likelihood scores, rather than binary classifications typical of rule-based systems. Additionally, fuzzy logic facilitates the integration of expert knowledge into its rule base, allowing it to evolve and adapt to new attack patterns more effectively. These features collectively make the proposed system not only more flexible and robust but also better suited for dynamic environments such as the Moroccan agribusiness SME network.

5. CONCLUSIONS

The purpose of this study was to enhance network security by accurately identifying anomalous activities that could indicate potential cyber threats. Our practical case involved a comprehensive analysis of the SME's network, focusing on key segments like Office LAN, Production Network, External WAN, and ERP System. The methodology entailed several critical steps: collecting and preprocessing network traffic data, designing the FIS using Xfuzzy, constructing the rule base, and validating the system through simulation. Data preprocessing included noise removal, normalization, dataset division, and labeling, ensuring the data was clean and suitable for modeling. The FIS was defined with input variables such as packet size, connection duration, and protocol type, and an output variable indicating anomaly likelihood. Membership functions and a detailed rule base were established to guide the system's decision-making process. Our results, summarized in the confusion matrix and performance metrics, indicated a high precision (0.95), recall (0.97), and F1-score (0.96), demonstrating the system's effectiveness in detecting network anomalies. The comparison with existing works highlights our system's superior accuracy and balanced performance, thanks to the tailored rule base and comprehensive preprocessing steps.

The contributions of this work lie in the tailored approach for the SME, combining domain-specific knowledge with advanced fuzzy logic techniques, and offering a robust framework for anomaly detection that can be adapted to similar SMEs in other regions or industries. However, the reliance on historical data for labeling can introduce bias, and the fuzzy logic system might need continuous updating to handle evolving cyber threats. The proposed fuzzy logic-based anomaly detection system, while effective, has several limitations that could impact its real-world adoption. First, the system relies heavily on historical data for rule creation, which means its performance is contingent on the availability and quality of past network traffic records. This reliance could lead to challenges in adapting the system to environments where such data is limited or incomplete. Additionally, the scalability of the rule base is another constraint; as the network environment grows in complexity, the rule base must expand proportionally, which could increase computational overhead and reduce real-time responsiveness. Despite these limitations, the system demonstrates significant adaptability to other industries. In manufacturing, it could be tailored to monitor equipment health and detect anomalies in production processes, such as identifying potential equipment failures or inefficiencies. Similarly, in healthcare, it could be utilized to analyze patient monitoring data, detecting irregularities that signal potential health risks. By modifying input variables and rule sets to suit the specific needs of these domains, the system's flexibility and interpretability position it as a versatile tool for anomaly detection across various sectors.

Additionally, the complexity of the FIS may increase with more rules and variables, potentially impacting performance. Future perspectives include refining the rule base through machine learning techniques, integrating real-time data analytics, and expanding the system to cover a broader range of network activities. Incorporating adaptive learning mechanisms can also enhance the system's ability to respond to new and emerging threats, ensuring the ongoing security and resilience of the network within the Moroccan agribusiness SME.

Expanding the dataset to include multi-month data and a broader range of attack types would significantly enhance the model's generalization capabilities. Multi-month data captures seasonal or periodic variations in network traffic, enabling the model to better distinguish between normal fluctuations and genuine anomalies. Additionally, incorporating diverse attack types—such as distributed denial-of-service (DDoS), phishing, and malware injection—ensures the model is exposed to a wider variety of threat patterns, improving its ability to detect previously unseen anomalies. A larger and more diverse dataset also reduces the risk of overfitting, where the model performs well on the training data but struggles to generalize to new data. By providing the model with a richer

representation of real-world scenarios, it becomes more robust and adaptive to dynamic network environments. This expanded dataset not only enhances the system's accuracy and reliability but also positions it as a versatile tool capable of addressing the evolving cybersecurity challenges faced by industries such as agribusiness, manufacturing, and healthcare.

REFERENCES

[1] Abomhara, M., Køien, G.M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1): 65-88. https://doi.org/10.13052/jcsm2245-1439.414

[2] Huang, D.L., Rau, P.L.P., Salvendy, G. (2007). A survey of factors influencing people's perception of information security. In Human-Computer Interaction. HCI Applications and Services: 12th International Conference, HCI International 2007, Beijing, China, Proceedings, Part IV 12, pp. 906-915. https://doi.org/10.1007/978-3-540-73111-5_100

[3] An, J.Y., Yue, G., Yu, F., Li, R.F. (2006). Intrusion detection based on fuzzy neural networks. In International Symposium on Neural Networks, Berlin, Heidelberg, pp. 231-239. https://doi.org/10.1007/11760191_34

[4] Sraïri, M.T. (2017). New challenges for the Moroccan agricultural sector to cope with local and global changes. Current Politics and Economics of Africa, 10(2): 151-169.

[5] Trendov, N.M., Varas, S., Zeng, M. (2019). Digital Technologies in Agriculture and Rural Areas. Food and Agriculture Organization of the United Nations.

[6] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1-2): 18-28. https://doi.org/10.1016/j.cose.2008.08.003

[7] Stallings, W. (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional.

[8] Zadeh, L.A. (1965). Fuzzy sets. Information and Control, 8(3): 338-353. https://doi.org/10.1016/S0019-9958(65)90241-X

[9] Kosko, B. (1994). Fuzzy Thinking: The New Science of Fuzzy Logic. Hyperion.

[10] Imamguluyev, R., Huseynli, J., Hajiyev, I. (2024). Fuzzy logic and cybersecurity: An intelligent shield in the digital age. In: Kahraman, C., Cevik Onar, S., Cebi, S., Oztaysi, B., Tolga, A.C., Ucal Sari, I. (eds) Intelligent and Fuzzy Systems. INFUS 2024. Lecture Notes in Networks and Systems, vol 1089. Springer, Cham. https://doi.org/10.1007/978-3-031-67195-1_5

[11] Kim, C., So-In, C., Kongsorot, Y., Aimtongkham, P. (2024). FLSec-RPL: A fuzzy logic-based intrusion detection scheme for securing RPL-based IoT networks against DIO neighbor suppression attacks. Cybersecurity, 7(1): 27. https://doi.org/10.1186/s42400-024-00223-x

[12] Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., Salykbayeva, A. (2023). Fuzzy logic and its application in the assessment of information security risk of industrial Internet of Things. Symmetry, 15(10): 1958. https://doi.org/10.3390/sym15101958

[13] Cox, E. (1999). The Fuzzy Systems Handbook: A Practitioner's Guide to Building, Using, and Maintaining Fuzzy Systems. AP Professional.

[14] López, D.R., Jiménez, C.J., Baturone, I., Barriga, A., Sánchez-Solano, S. (1998). Xfuzzy: A design environment for fuzzy systems. In 1998 IEEE International Conference on Fuzzy Systems Proceedings. IEEE World Congress on Computational Intelligence (Cat. No.98CH36228), Anchorage, AK, USA, pp. 1060-1065. https://doi.org/10.1109/FUZZY.1998.686265

[15] Dong, G., Xu, P., Li, K., Li, Y. (2025). Adaptive fuzzy fault-tolerant control for nonlinear multi-agent systems with asymmetric time-varying state constraints. International Journal of Fuzzy Systems, 1-11. https://doi.org/10.1007/s40815-024-01966-y

[16] Zhang, L., Zhang, H. (2025). A two-stage method for supply–demand stable matching in new energy vehicles considering consumer herd behavior. International Journal of Fuzzy Systems, 1-23. https://doi.org/10.1007/s40815-024-01967-x

[17] Cheng, S., Bao, Y., Wang, H. (2025). An overlap function-based three-way model in interval-valued hesitant fuzzy information systems: A case study in mine siting. International Journal of Fuzzy Systems, 1-22. https://doi.org/10.1007/s40815-024-01965-z

[18] Sánchez, D., Melin, P., Castillo, O., Castro, J.R. (2025). Optimal genetic design of interval type-3 fuzzy aggregators for modular neural networks applied to human recognition. International Journal of Fuzzy Systems, 1-20. https://doi.org/10.1007/s40815-024-01932-8

[19] Laajimi, M., Gassara, H., Rhaima, M., Mchiri, L., Makhlouf, A.B. (2025). $H_{\backslash infty}$ control for general conformable polynomial fuzzy models. International Journal of Fuzzy Systems, 1-10. https://doi.org/10.1007/s40815-025-01983-5

[20] Alluhaibi, R. (2024). Quantum Machine Learning for advanced threat detection in cybersecurity. International Journal of Safety and Security Engineering, 14(3): 875-883. https://doi.org/10.18280/ijsse.140319

[21] Kaur, K., Batth, J.S. (2025). Implementation of deep learning and machine learning for designing and analyzing IDS (Intrusion detection system) through novel framework. In: Malhotra, M. (eds) Innovation and Emerging Trends in Computing and Information Technologies. IETCIT 2024. Communications in Computer and Information Science, vol 2125. Springer, Cham. https://doi.org/10.1007/978-3-031-80839-5_9

[22] Mohale, V.Z., Obagbuwa, I.C. (2025). A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity. Frontiers in Artificial Intelligence, 8: 1526221. https://doi.org/10.3389/frai.2025.1526221

[23] Dong, H., Kotenko, I. (2025). Cybersecurity in the AI era: Analyzing the impact of machine learning on intrusion detection. Knowledge and Information Systems, 1-52. https://doi.org/10.1007/s10115-025-02366-w

[24] Lima, J.F., Patiño-León, A., Orellana, M., Zambrano-

Martinez, J.L. (2025). Evaluating the impact of membership functions and defuzzification methods in a fuzzy system: Case of air quality levels. Applied Sciences, 15(4): 1934. https://doi.org/10.3390/app15041934

[25] Hamed, A., Hireche, S., Bekri, A., Cheriet, A. (2025). Designing fuzzy membership functions using genetic algorithm with a new encoding method. Indonesian Journal of Electrical Engineering and Computer Science, 37(2): 781-788. https://doi.org/10.11591/ijeecs.v37.i2.pp781-788

[26] Dahir, U.M., Hashi, A.O., Abdirahman, A.A., Elmi, M.A., Rodriguez, O.E.R. (2024). Machine learning-based anomaly detection model for cybersecurity threat detection. Ingénierie des Systèmes d'Information, 29(6): 2415-2424. https://doi.org/10.18280/isi.290628

[27] Khairuddin, S.H., Hasan, M.H., Hashmani, M.A., Azam, M.H. (2021). Generating clustering-based interval fuzzy type-2 triangular and trapezoidal membership functions: A structured literature review. Symmetry, 13(2): 239. https://doi.org/10.3390/sym13020239

[28] Remli, A., Khtira, A., Asri, B.E. (2023). Cybersecurity index to evaluate the implementation of the Bi-level architecture for efficient manufacturing (BLAEM). International Journal of Safety and Security Engineering, 13(2): 195-204. https://doi.org/10.18280/ijsse.130202

[29] Admass, W.S., Munaye, Y.Y., Diro, A.A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2: 100031. https://doi.org/10.1016/j.csa.2023.100031

[30] Kryshtanovych, M., Lyubomudrova, N., Bondar, H., Motornyy, V., Kuchmenko, V. (2023). An intelligent multi-stage model for countering the impact of disinformation on the cybersecurity system. Ingénierie des Systèmes d'Information, 28(1): 41-47. https://doi.org/10.18280/isi.280105

[31] Prabaswari, Ali, Y., Gultom, R.A.G., Simbolon, L., Gunawan, A.A.N. (2024). A novel socio-technical framework for enhancing cyber crisis management capabilities. International Journal of Safety and Security Engineering, 14(4): 1181-1193. https://doi.org/10.18280/ijsse.140415

[32] Klir, G. J., Yuan, B. (1995). Fuzzy Sets and Fuzzy Logic: Theory and Applications. Upper Saddle River, NJ: Prentice Hall.

[33] Gburi, F.H., Kadhom, M.A., Kamil, F. (2024). Fuzzy logic-based control systems for intelligent vehicles: A survey. In Proceedings of the 2nd International Conference on Engineering and Science to Achieve the Sustainable Development Goals, Tabriz, Iran. https://doi.org/10.1063/5.0199602

[34] Casari, M., Kowalski, P.A., Po, L. (2024). Optimizing adaptive neuro-fuzzy inference systems to calibrate low-cost PM concentration sensors. Ecological Informatics, 83: 1-15. https://doi.org/10.1016/j.ecoinf.2024.102781

[35] Ross, T.J. (2010). Fuzzy Logic with Engineering Applications, 3rd ed. Hoboken, NJ: Wiley.

[36] von Altrock, C. (1996). Recent successful fuzzy logic applications in industrial automation. In Fuzzy Logic Foundations and Industrial Applications, edited by D. Ruan, International Series in Intelligent Technologies, Boston, MA. https://doi.org/10.1007/978-1-4613-1441-7_11

[37] Raja, S., Krishnan, R.S. (2019). Fuzzy logic-based smart irrigation system using Internet of Things. Journal of Cleaner Production, 252(9): 119902. https://doi.org/10.1016/j.jclepro.2019.119902

[38] Bang, S., Bishnoi, R., Chauhan, A.S., Dixit, A.K., Chawla, I. (2019). Fuzzy logic based crop yield prediction using temperature and rainfall parameters predicted through ARMA, SARIMA, and ARMAX models. In 2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, pp. 1-6. https://doi.org/10.1109/IC3.2019.8844901