

Fuzzy Logic for Cybersecurity: Intrusion Detection and Privacy Preservation with Synthetic Data

Marina Soledad Iantorno¹^a and Khalil Beladda²

¹*Campus Founders, Bildung Campus, Heilbronn, Germany*

²*CCT College, Westmorland St, Dublin, Ireland*

Keywords: Cybersecurity, Defuzzification, Fuzzy Logic, Intrusion Detection System, NSL-KDD, Membership Function, Synthetic Data, WGAN.

Abstract: This research explores the use of fuzzy logic in intrusion detection systems (IDS) aiming to improve cybersecurity threat detection. Conventional machine learning models, like Decision Trees and Support Vector Machines, are evaluated against a fuzzy logic model that employs triangle and parallelogram-shaped membership functions to address the uncertainty in network traffic. The fuzzy logic system presented good performance, achieving greater accuracy, precision, and F1-scores than conventional models, particularly when using real network traffic data. Synthetic data produced by Wasserstein Generative Adversarial Networks (WGANs) was also used to evaluate the model's robustness and guarantee privacy protection in future studies. The relevance of this approach lies in its ability to provide more comprehensive threat detection, helping organizations safeguard their systems in environments where strict, rule-based models may fall short. The findings indicate that the fuzzy logic methodology is effective, even when applied to synthetic data, demonstrating its feasible choice for intrusion detection in sensitive contexts. Subsequent research will investigate the incorporation of deep learning methodologies and the modification of the model for distributed systems, focusing on scalability and real-time threat identification.


1 INTRODUCTION

In the contemporary digital era, cybersecurity is critically significant, as organizations encounter increasing dangers from different cyberattacks (CheckPoint, 2024). These attacks, including denial of-service (DoS), remote-to-local (R2L), and user-to root (U2R) incursions, can significantly undermine the integrity, confidentiality, and availability of essential systems. With the growing dependence of organizations on digital infrastructures and online transactions, the security of network environments has emerged as a critical concern (Admass, Munaye, & Diro, 2024). To address this, intrusion detection systems (IDS) are in use to detect anomalous behaviors within network traffic. This paper aims to investigate the use of fuzzy logic in an Intrusion Detection System (IDS) employing the NSL-KDD dataset (DARPA, 2018), which is a common resource for intrusion detection studies, to explain how fuzzy logic can improve the identification of potential cyber

threats while protecting sensitive network information through synthetic data generation.

This analysis has two main goals. Initially, it aims to replicate network traffic and intrusions with the NSL-KDD dataset, distinguishing and categorizing normal traffic from various attack vectors. Secondly, it proposes a fuzzy logic-based methodology for intrusion detection, enabling a more effective modelling and analysis of the inherent ambiguity in network activity. The analysis uses fuzzy logic to enhance the precision of identifying inappropriate network behavior, avoiding dependence on rigid thresholds or binary determinations. Additionally, synthetic data modelling will be utilized to produce realistic, privacy-preserving network traffic, offering enterprises an efficient method to train IDS models while safeguarding the confidentiality of sensitive network data.

In contrast to conventional systems relying on rigid rules or exact thresholds, fuzzy logic allows various levels of truth, thus addressing uncertainty

^a <https://orcid.org/0009-0007-2596-3494>

and ambiguity in network traffic patterns (Masoumi, Deghani, Hossani, & Masoumi, 2020).

Cybersecurity incidents are frequently intricate and unpredictable, complicating the classification of an occurrence as just "safe" or "malicious". Fuzzy logic offers another methodology, enabling the assessment of diverse attack scenarios according to fluctuating probabilities, hence facilitating more adaptable and resilient decision-making processes. As cyber threats become more sophisticated, the integration of fuzzy logic into Intrusion Detection Systems can enhance organizations' ability to identify cyber-attacks more effectively and react to changing threat environments (Keeping Security, 2024).

2 LITERATURE REVIEW

Several researchers have explored the application of fuzzy logic in various fields. Despite being an established technique created by Lotfi Zadeh in the 1960s, fuzzy logic continues to progress as technological improvements and better computer capacity create new opportunities for its use (Perry, 1995). The inherent adaptability of fuzzy logic to address uncertainty and ambiguity makes it a useful instrument for solving complex issues in contemporary industries, including network security, data privacy, and financial audits. Recent advancements in machine learning, artificial intelligence, and big data processing have augmented the capabilities of fuzzy logic, leading to the creation of more sophisticated models that can more efficiently integrate qualitative and quantitative aspects (Castillo & Melin, 2015). Some of the relevant advancements are listed below in chronological order.

- 2022. Bambang Leo Handoko and Daniel Marcell examine how understanding audit risk, auditor competency, and fuzzy logic can impact cybersecurity in auditing. The study pushes agency theory and employs a quantitative research approach, using data collected from public accountants in Indonesia. Their results suggest that an auditor's ability to assess risks and competency significantly affects materiality decisions. Moreover, the paper highlights how fuzzy logic can assist in addressing qualitative uncertainties in materiality assessments, such as those related to ambiguity or subjectivity. Fuzzy logic helps auditors to include quantitative and qualitative factors when determining the significance of cybersecurity assessments, particularly helpful for cyber insurance (Handoko & Marcell, 2022).

- 2021. In 2021 researchers from the National Technical University of Ukraine proposed a simulation model for detecting cyberattacks using fuzzy set theory and fuzzy inference. The model includes a functional diagram that processes network traffic telemetry and applies fuzzy logic to detect various types of cyberattacks, such as denial-of-service, remote-to-local, user-to-root, and probes. The authors describe the process of fuzzifying the input parameters—based on linguistic variables and membership functions—and developing fuzzy production rules in a knowledge base. The system was tested with 38 parameters defining network traffic. Their model showed superior performance in detecting polymorphic and traditional attacks compared to other methods, such as neural networks, showing an average accuracy improvement of 10%. The results suggest that the fuzzy logic-based detection system offers a more flexible and effective solution for improving cybersecurity defenses (Subach, Fesokha, Mykytiuk, Kubrak, & Korotayev, 2021).

- 2018. In the paper "Improving risk assessment model of cybersecurity using fuzzy logic inference system" written by researchers from King Saud University in Saudi Arabia and Fordham University in the United States, the authors propose an approach to cybersecurity risk assessment using a Fuzzy Inference System (FIS) based on the Mamdani model. The paper addresses the growing threats of cyberattacks such as DoS, DDoS, malware, and phishing, which needed more advanced risk assessment models. Traditional methods of risk analysis are often limited by the uncertainty and vagueness inherent in assessing cyber risks. To overcome these limitations, the authors suggest incorporating a triangular fuzzy logic, which allows for more flexible and approximate reasoning. Their evaluation shows that the fuzzy-based model can effectively assess risks with a higher degree of accuracy and adaptability, making it a valuable tool in mitigating cyber threats in organizations (Alali, Almogren, Hassan, Rassan, & Bhuiyan, 2018).

These studies highlight how fuzzy logic can be used to improve processes by incorporating uncertainty and vagueness into the analysis. This section has reviewed some key works that have applied fuzzy logic in cybersecurity, risk assessment, and materiality considerations, providing a foundation for understanding how this technique can be further refined and applied in contemporary contexts.

In line with the advancements mentioned above, the authors of this paper aim to use fuzzy logic to

address challenges in cybersecurity, specifically in the context of intrusion detection and data privacy. During their research, they identified several relevant studies that have applied fuzzy logic to similar areas.

3 METHODOLOGY

3.1 Data Gathering

This research uses the NSL-KDD Dataset, an updated version of the KDD Cup 1999 dataset, which is globally recognized for its application in network intrusion detection. The dataset contains labelled instances of both normal network activity and various types of attacks, including DoS, R2L, and U2R attacks. The data holds 41 features, and provides a comprehensive set of attributes, such as protocol type, service, and network bytes, which are instrumental in identifying potential intrusions. The dataset was chosen due to its extensive use in cybersecurity research, making it ideal for testing and comparing different machine learning and fuzzy logic approaches to intrusion detection.

3.2 Data Preparation

Before modelling, data preprocessing was necessary to ensure that the dataset was ready for analysis. The following steps were in place:

- Data cleaning: Removing any duplicates and handling missing values across the dataset.
- Feature encoding: Converting categorical variables such as protocol type and network service into numerical values suitable for machine learning algorithms.
- Normalization: Normalizing the features to bring all the variables to a comparable scale.

Additionally, to preserve data privacy, Wasserstein Generative Adversarial Networks (WGANs) were employed to generate synthetic data that mirrors the patterns found in the original NSLKDD data. This synthetic data was added to test the model's robustness and privacy-preserving capabilities, especially in the context of cybersecurity systems. Words like "is", "or", "then", etc. should not be capitalized unless they are the first word of the title.

3.3 Data Modelling

Several models were created for this study to simulate intrusion detection.

Fuzzy Logic Model: Unlike the research mentioned in chapter II, which predominantly uses

basic fuzzy logic functions, this research adopts innovative membership functions, including triangular and parallelogram-shaped membership functions, to classify network intrusions. These membership functions provide more comprehensive risk evaluations by correlating network characteristics to different levels of risk (e.g., low, medium, high) in a flexible, non-linear manner. By introducing these specific models, the current research aims to enhance the system's ability to adapt to the complexities of modern cyberattacks and provide more precise risk assessments.

Synthetic Data Generation: Using the WGAN model, synthetic data imitating the NSL-KDD dataset was generated. This synthetic data was then integrated with real data to ensure that the intrusion detection system could be tested under realistic conditions while safeguarding sensitive information.

Comparison Models: Several traditional machine learning models were also implemented for comparison, including the Decision Tree Classifier, Support Vector Classifier, and Neural Networks. These models were trained on the NSL-KDD dataset and evaluated for performance using accuracy, precision, recall, and F1-score metrics. This allowed for a detailed comparison between conventional models and the proposed fuzzy logic-based system, highlighting the strengths and weaknesses of each model.

3.4 A Detailed Explanation of the Main Model

Fuzzy Logic is a mathematical methodology used to handle uncertainty and imprecision, which is useful in fields such as cybersecurity, where data is often complex and ambiguous. In fuzzy logic, data is transformed into values that range between 0 and 1, offering a gradient of membership for various categories or conditions, rather than the binary true/false (1/0). This system enables a more flexible way of interpreting and analyzing data, making it ideal for applications such as intrusion detection, where network traffic behavior may not fit neatly into predefined categories (Medium, 2023).

The features of the Fuzzy Logic membership functions are defined as follows:

- **Core:** The core of a membership function for any fuzzy set denotes the area within the universe characterized by total membership in the set. This indicates that components within the core are regarded as entirely belonging to the set (GeeksForGeeks, 2018). In a fuzzy logic model for identifying cyberattacks, if a network's traffic pattern

precisely aligns with the signature of a known attack, it receives a membership value of 1, indicating it is entirely classified as a prospective attack.

- **Support:** The support of a membership function specifies the particular area in the universe where the membership exceeds zero. This includes elements that are partially included in the entire set (TutorialsPoint, 2019). In cybersecurity, the support may include network traffic that displays some, but not all, attributes of an attack. This traffic would have a membership value ranging from 0 to 1, meaning a partial match.

- **Boundary:** The boundary represents the area where membership in the set is non-zero yet incomplete. Elements in the boundary region are ambiguous, exhibiting certain characteristics indicative of belonging to the set (e.g., potential signals of an attack), and they cannot be definitively identified. This component of fuzzy logic is essential for addressing the ambiguous situations in intrusion detection, where an action may not distinctly be classified as malicious or benign (San José State University, 2023).

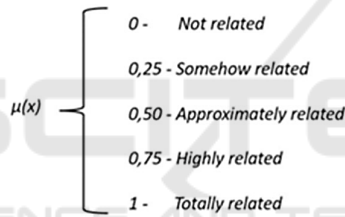


Figure 1: Desirable scale for topic classification.

Fuzzy Logic operates based on probability theory and statistics, although it does not necessitate a strict mathematical model as seen in conventional methods (Gaines, 1978). As it is possible to see in Figure 1, the model will display a series of probabilities of likelihood to find an anomaly behavior. It employs rules and membership functions to assess the extent to which an input is classified inside a particular category, such as "normal" or "intrusion" in the context of cybersecurity. In contrast to conventional classification models that depend on rigid borders, fuzzy logic facilitates a more flexible categorization by assigning items a membership value on a scale ranging from 0 to 1, indicating the probability of an event belonging to a specific category (Ariff, Ariff, Sheikh, & Hussin, 2018).

Table 1: Definition of Fuzzy Rules.

Feature	Membership Function	Fuzzy set
Protocol Type	Triangular	Low/ Medium/High
Service	Parallelogram	Normal/Anomalous
Duration	Triangular	Short/Medium/Long

The fuzzy logic model uses triangular and parallelogram membership functions to classify network traffic into risk categories. Unlike previous work, these shapes provide granular evaluations of ambiguous traffic patterns. The fuzzy rules and sets are explicitly defined in Table 1, ensuring reproducibility.

By using fuzzy logic, this research aims to provide a flexible, innovative system for detecting intrusions, allowing cybersecurity systems to handle the inherent uncertainty in network behavior more effectively.

Words like "is", "or", "then", etc. should not be capitalized unless they are the first word of the title.

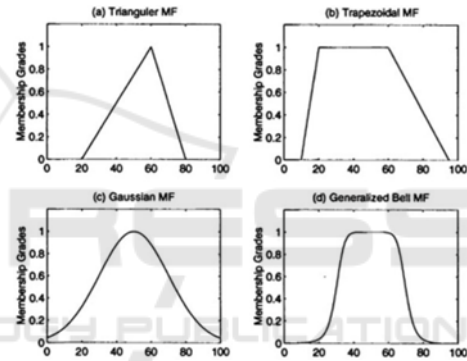


Figure 2: Examples of Fuzzy Logic Membership.

With a clear understanding of how fuzzy logic is applied to handle uncertainties in network intrusion detection, the following section will outline the practical implementation of this methodology.

4 IMPLEMENTATION

The principal dataset utilized was the NSL-KDD dataset, comprising labelled network traffic records for both normal and intrusive behaviors. The implementation phases were categorized into data processing, fuzzy logic system design, and synthetic data production.

The dataset was exposed to an initial preprocessing, which involved normalizing numerical features and transforming categorical variables into numerical formats. Missing data points were addressed through interpolation or removal. Subsequently, feature selection was conducted to

ascertain the most relevant features for intrusion detection.

The fuzzy logic system was then built using the SciKit-Fuzzy library in Python. Membership functions for the relevant features (e.g., duration, protocol type, service) were created, and triangular as well as parallelogram-shaped membership functions were employed to represent the uncertainty in network traffic behavior (Hamarsheh, 2019). Fuzzy rules were defined based on these membership functions to evaluate the likelihood of network traffic being classified as normal or malicious. These rules were based on the characteristics of the network traffic in the NSL-KDD dataset. Once the fuzzy inference system was defined, a defuzzification process was implemented using the centroid method to convert the fuzzy output into a confident decision, determining whether the traffic should be labelled as normal or an intrusion (Science Direct, 2001). The performance of this system was compared to other traditional machine learning models, such as the Decision Tree Classifier and Support Vector Machine, to evaluate the effectiveness of the fuzzy logic model.

For the purpose of data privacy preservation in future cybersecurity training and testing modelling, the synthetic data created was trained to mimic the patterns found in the original NSL-KDD dataset, ensuring that the models could be tested without exposing sensitive information. The generated synthetic data was then fed into the fuzzy logic model and the machine learning models to assess the robustness and accuracy of the system when using synthetic data instead of real data. Finally, the results from the fuzzy logic model and the machine learning models were evaluated using common metrics such as accuracy, precision, recall, and F1-score (Kupchyn, et al., 2022).

The following section will show and discuss the results obtained in the process mentioned above.

5 RESULTS

The table below shows the results obtained in the implementation process.

The results presented in Table 1 show the efficiency of fuzzy logic in intrusion detection. The model report high precision and F1-scores compared to conventional models. The precision and recall metrics also indicate that the fuzzy logic model provides a more balanced performance in detecting true positives and minimizing false positives, particularly in scenarios with real network traffic

data. Moreover, the fuzzy logic model shows competitive performance with synthetic data, highlighting its robustness and adaptability in managing cybersecurity tasks while ensuring data privacy. This, shows once again, that synthetic data could be a possible solution against data privacy scenarios (Riemann, 2024).

Table 2: Comparison Performance.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 - Score (%)
Fuzzy Logic (Real Data)	92.4	93.1	91.8	92.4
Fuzzy Logic (Synthetic Data)	90.1	90.7	89.6	87.6
Decision Tree (Real Data)	87.6	88.3	86.9	84.2
Decision Tree (Synthetic Data)	84.2	84.7	83.9	89.6
SVM (Real Data)	89.7	90.2	89.1	86.3

6 CONCLUSIONS

This study has shown the use of fuzzy logic in cybersecurity, specifically in intrusion detection. The fuzzy logic model, employing the NSL-KDD dataset, outperformed conventional machine learning models like Decision Trees and Support Vector Machines in accuracy, precision, and F1-score, especially with real network traffic data. The implementation of triangle and parallelogram-shaped membership functions facilitated a more detailed assessment of network traffic, providing the system with the capability to categorize ambiguous or uncertain behavioral patterns. This is a significant benefit in cybersecurity, as attacks often show complexity and may not adhere to strict rules or unique parameters (Javaheri, Gorgin, Lee, & Masdari, 2023).

In a similar vein, the integration of synthetic data produced by the WGAN technique provided additional insights into the possibility of using artificial data to safeguard privacy while preserving detection efficacy. This is an ongoing discussion at the moment in industry and academia, and this research shows that the fuzzy logic model maintained competitive performance when trained on synthetic data, which indicates that privacy-preserving techniques can be effectively incorporated without substantially compromising model accuracy

(International Association of Privacy Professionals, 2023). This finding is particularly significant in domains involving sensitive data, such as network security.

Further studies conducted by the authors of this research may investigate the augmentation of this model by integrating more sophisticated membership functions or combining fuzzy logic with additional machine learning methodologies to further improve performance. Furthermore, using this methodology to other cybersecurity datasets, such as real-time network traffic data, may lead to a deeper understanding of the system's performance in dynamic contexts (Pancardo, Hernandez-Nolasco, Wister, & Garcia-Constantino, 2021). Moreover, adding explainable AI methodologies to clarify the reasoning behind the fuzzy logic model's conclusions could also enhance transparency and fostering trust among cybersecurity professionals using this system (Cao, et al., 2024).

The fuzzy logic model could also benefit from the integration of deep learning techniques to enhance its ability to detect more sophisticated and emerging threats, such as zero-day attacks (Han, 2024). This is an area that has not yet been explored.

Another promising direction for future work could be to adapt the model for use in distributed or cloud-based environments, where cybersecurity challenges differ due to the decentralized nature of these systems (Prasath, Bharathan, Lakshmi, & Nathiya, 2023). This would involve testing the model's scalability and resilience in managing largescale network data. Exploring real-time deployment and optimization for faster threat detection could also lead to practical implementations in live cybersecurity systems, further proving the value of fuzzy logic in modern threat landscapes.

REFERENCES

- A. Kupchyn, Komarov, V., I. Borokhvostov, M. Bilokur, A. Kuprinenko, Y. Mishchenko, V. Bohdanovych, & O. Kononov. (2022). Determining the Accuracy for Fuzzy Logic Technology Foresight Model. *Cybernetics and Systems Analysis*, 58(3), 382–391. <https://doi.org/10.1007/s10559-022-00470-1>
- 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>
- Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*, 74(74), 323–339. <https://doi.org/10.1016/j.cose.2017.09.011>
- Ariff, A., Ariff, A., Sheikh, S., & Hussin, M. (2018). ConBEE Green envelope as an architectural strategy for energy efficiency in a library building. *MATEC Web of Conferences*. <https://doi.org/10.1051/mateconf/20191145/3556089.3556107>
- Bambang Leo Handoko, & Marcell, D. (2022). The Impact of Understanding Audit Risk, Auditor's Competency, and Fuzzy Logic Analysis to Materiality Level Consideration. *ICEME '22: Proceedings of the 2022 13th International Conference on E-Business, Management and Economics*, 211, 500–506. <https://doi.org/10.1145/3556089.3556107>
- CAO, J., Zhou, T., Zhi, S., Lam, S., REN, G., ZHANG, Y., Wang, Y., Dong, Y., & Cai, J. (2024). Fuzzy Inference System with Interpretable Fuzzy Rules: Advancing Explainable Artificial Intelligence for Disease Diagnosis—A Comprehensive Review. *Information Sciences*, 120212–120212. <https://doi.org/10.1016/j.ins.2024.120212>
- Castillo, O., & Melin, P. (2014). Fuzzy Logic Augmentation of Nature-Inspired Optimization Metaheuristics. In *Studies in computational intelligence*. Springer Nature. <https://doi.org/10.1007/978-3-319-10960-2>
- CheckPoint. (2024, July 16). Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks. Check Point Blog. <https://blog.checkpoint.com/research/check-pointresearch-reports-highest-increase-of-global-cyberattacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/darpa>
- DARPA. (2018). NSL-KDD. www.kaggle.com/datasets/hassan06/nslkdd
- Gaines, B. R. (1978). Fuzzy and probability uncertainty logics. *Information and Control*, 38(2), 154–169. [https://doi.org/10.1016/s0019-9958\(78\)90165-1](https://doi.org/10.1016/s0019-9958(78)90165-1)
- GeeksforGeeks. (2018, April 10). Fuzzy Logic | Introduction. [GeeksforGeeks. https://www.geeksforgeeks.org/fuzzy-logicintroduction/](https://www.geeksforgeeks.org/fuzzy-logicintroduction/)
- Hamarsheh, Q. (2019). Different Types of Membership Functions. https://www.philadelphia.edu.jo/academics/qhamarsheh/uploads/Lecture%2018_Different%20Types%20of%20Membership%20Functions%201.pdf
- Han, X. (2024). Analyzing the impact of deep learning algorithms and fuzzy logic approach for remote English translation. *Scientific Reports*, 14(1). <https://doi.org/10.1038/s41598-024-64831-w>
- International Association of Privacy Professionals. (2023, December 12). IAPP. [iapp.org. https://iapp.org/news/a/synthetic-data-whatoperational-privacy-professionals-need-to-know](https://iapp.org/news/a/synthetic-data-whatoperational-privacy-professionals-need-to-know)
- Javaheri, D., Gorgin, S., Lee, J.-A., & Masdari, M. (2023). Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives. *Information Sciences*, 626, 315–338. <https://doi.org/10.1016/j.ins.2023.01.067>
- Masoumi, M., Dehghani, F., Hossani, S., & Masoumi, A. (2020, May). (PDF) THE CHALLENGES AND ADVANTAGES OF FUZZY SYSTEMS

- APPLICATIONS A PREPRINT. ResearchGate. https://www.researchgate.net/publication/341426529_THE_CHALLENGES_AND_ADVANTAGES_OF_FUZZY_SYSTEMS_APPLICATIONS_A_PREPRINT
- Medium. (2023, July 15). Exploring GANs to Generate Synthetic Data. The Research Nest. <https://medium.com/the-research-nest/exploring-gansto-generate-synthetic-data-ca48f8a4b518>
- Pancardo, P., Hernandez-Nolasco, J. A., Wister, M. A., & Garcia-Constantino, M. (2021). Dynamic Membership Functions for Context-Based Fuzzy Systems. *IEEE Access*, 9, 29665–29676. <https://doi.org/10.1109/access.2021.3058943>
- Perry, T. (1995, June 1). Lotfi Zadeh and the Birth of Fuzzy Logic - IEEE Spectrum. [Spectrum.ieee.org](https://spectrum.ieee.org/lotfi-zadeh)
- Prasath, V., Bharathan, N., Lakshmi, N., & Nathiya, M. (2023). Fuzzy Logic In Cloud Computing. <https://www.ijert.org/research/fuzzy-logic-in-cloudcomputing-IJERTV2IS3439.pdf>
- Riemann, R. (2024, May 9). Synthetic Data | European Data Protection Supervisor. [Www.edps.europa.eu](https://www.edps.europa.eu/presspublications/publications/techsonar/synthetic-data_en)
- San José State University. (2023, January). Fuzzy Logic: The Logic of Fuzzy Sets. [Sjsu.edu](https://www.sjsu.edu/faculty/watkins/fuzzysets.htm)
- Science Direct. (2001). Defuzzification - an overview | ScienceDirect Topics. [Www.sciencedirect.com](https://www.sciencedirect.com/topics/engineering/defuzzification)
- Security, K. (2024, March 26). Cyber Attacks Are More Sophisticated Than Ever, With AI-Powered Attacks Posing the Greatest Risk. [Www.prnewswire.com](https://www.prnewswire.com/news-releases/cyberattacks-are-more-sophisticated-than-ever-with-ai-powered-attacks-posing-the-greatest-risk-302098797.html)
- Subach, I., Fesokha, V., Mykytiuk, A., Kubrak, V., & Korotayev, S. (2021). Simulation Model of a Fuzzy Cyber Attack Detection System. <https://ceurws.org/Vol-3241/paper9.pdf>
- TutorialsPoint. (2019). Fuzzy Logic - Membership Function - Tutorialspoint. [Www.tutorialspoint.com](https://www.tutorialspoint.com/fuzzy_logic/fuzzy_logic_membership_function.htm)