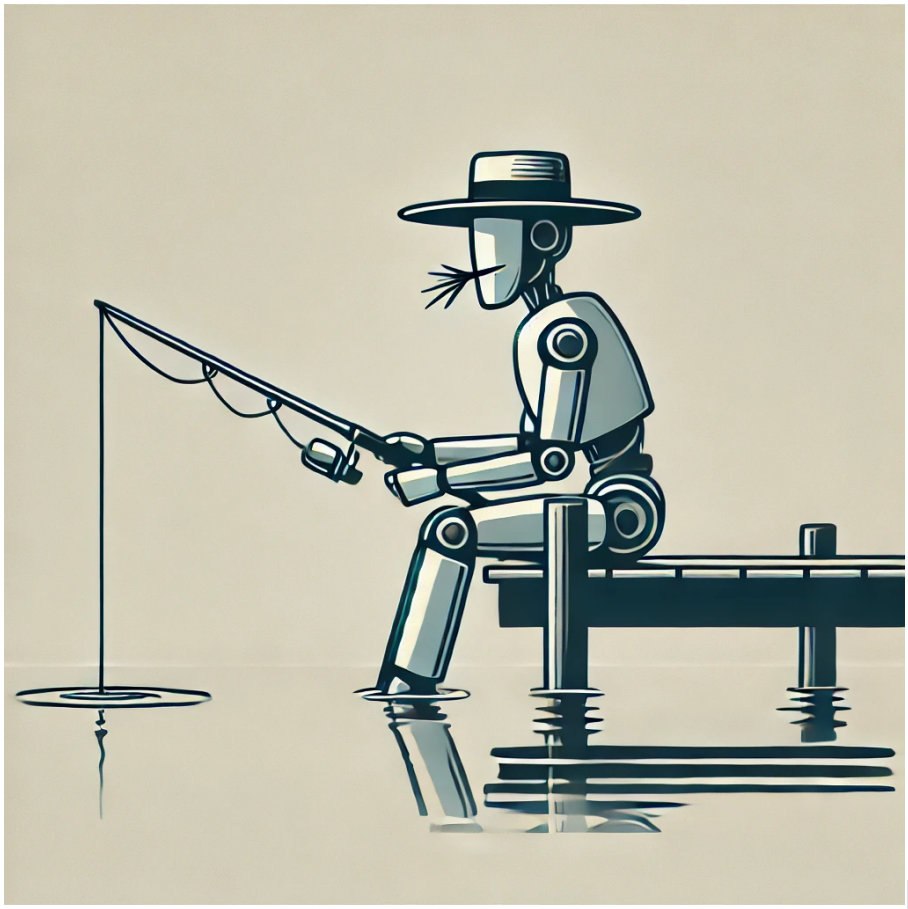
Phishing Detection: A Fuzzy Expert System


[4]

Júlia Amenós
Oriol Miró
Víctor Carballo

December 2024

Planning and Approximate Reasoning (MIA-MESIIA)
Practical Exercise 3: PAR

UNIVERSITAT ROVIRA i VIRGILI
UPC

Contents

1 Introduction

Phishing attacks are a significant threat in the digital world, aiming to deceive users into revealing sensitive information by masquerading as trustworthy entities. These attacks often involve fraudulent websites that mimic legitimate ones to trick users into providing personal data, such as login credentials and financial information.

Detecting phishing websites is crucial for enhancing cybersecurity measures. Traditional detection methods can be bypassed by sophisticated phishing techniques. Therefore, incorporating Artificial Intelligence (AI) methods, particularly fuzzy logic, provides an effective approach to handle the uncertainties and imprecision associated with phishing detection [1, 7, 2].

In this work, we design and implement a fuzzy expert system (FES) to classify websites into four categories based on their phishing risk:

- **Safe**
- **Weakly Suspicious**
- **Strongly Suspicious**
- **Phishing**

Additionally, the system provides a numerical phishing risk score between 0 and 100.

The system utilizes five carefully selected features from the UCI Phishing Websites dataset [6]. The features encompass various aspects of the websites, including URL characteristics, content analysis, and external factors.

2 Definition of Linguistic Variables

In this section, we define the input and output linguistic variables for our fuzzy expert system. Each variable is described with its range, linguistic terms, and corresponding membership functions. The membership functions are designed using triangular and trapezoidal shapes to satisfy the property of fuzzy partition.

2.1 Selection of Features

Based on the features identified in [2], we selected the following five features:

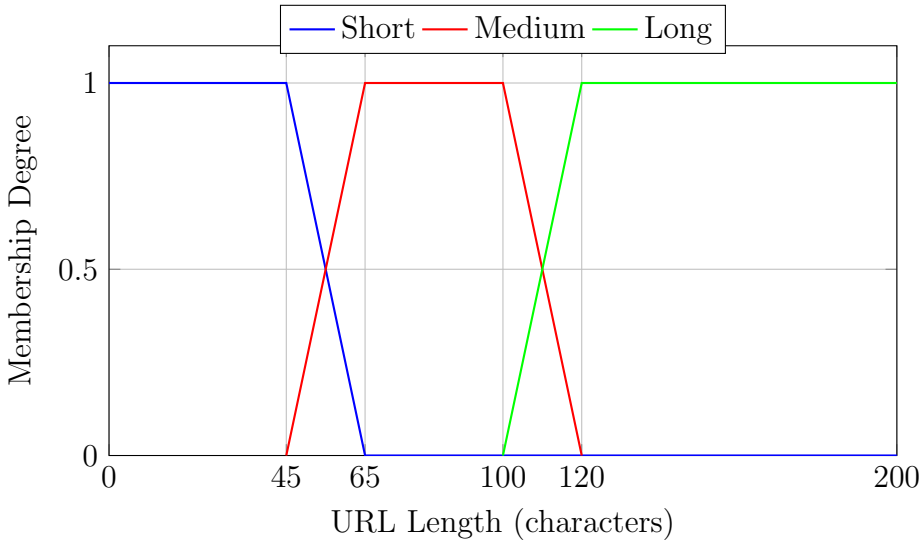
1. **URL Length (Feature 1)**: The total number of characters in the URL. Phishing websites often use long URLs to obscure the actual destination.
2. **Ratio of Digits in URL (Feature 26)**: The proportion of numeric characters in the URL. A high ratio may indicate obfuscation attempts.
3. **Ratio of Internal Hyperlinks (Feature 58)**: The proportion of hyperlinks that are internal (i.e., linking within the same domain). Phishing sites may have fewer internal links.
4. **Domain Age (Feature 83)**: The age of the website's domain in days. Phishing sites are typically newer.
5. **PageRank (Feature 87)**: A measure of the website's importance or popularity. Legitimate sites tend to have higher PageRank values.

2.2 Input Variables

For each input variable, we define the range, linguistic terms, and membership functions. All decisions were derived by analyzing the range of values and identifying common patterns within the dataset [6]. Additionally, insights were gathered from the paper [3].

2.2.1 URL Length

- **Range**: [0, 200] characters
- **Linguistic Terms**: *Short*, *Medium*, *Long*



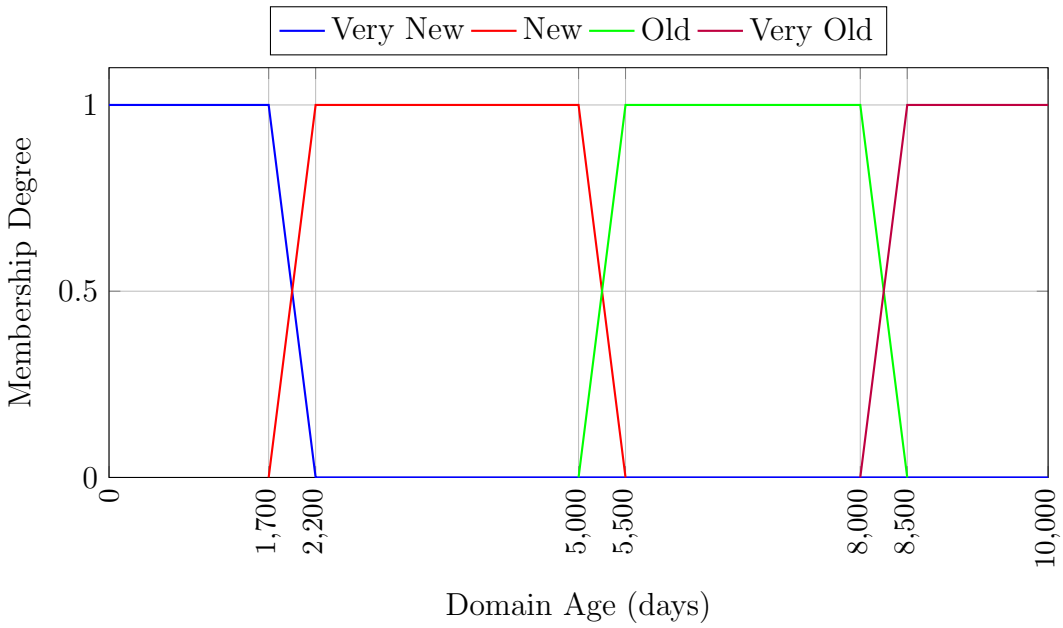
Membership Function Parameters:

- *Short*: Trapezoidal function with parameters (0, 0, 45, 65)
- *Medium*: Trapezoidal function with parameters (45, 65, 100, 120)
- *Long*: Trapezoidal function with parameters (100, 120, 200, 200)

For better visualization of the membership functions, the range was limited to 200. However, note that the dataset includes some urls with larger length. In case of testing samples exceeding 200 characters, assign the upper bound.

2.2.2 Domain Age

- **Range**: [0, 10,000] days
- **Linguistic Terms**: *Very New*, *New*, *Old*, *Very Old*

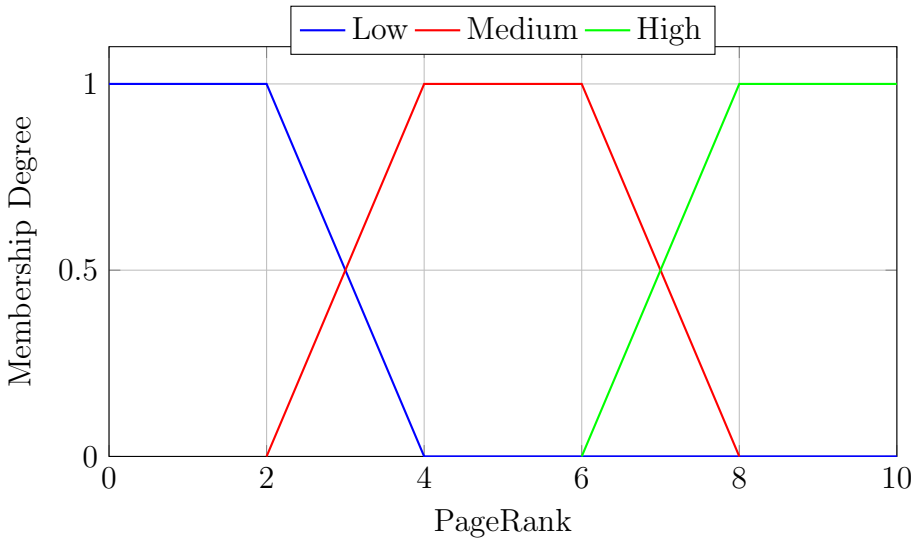


Membership Function Parameters:

- *Very New*: Trapezoidal function with parameters (0, 0, 1700, 2200)
- *New*: Trapezoidal function with parameters (1700, 2200, 5000, 5500)
- *Old*: Trapezoidal function with parameters (5000, 5500, 8000, 8500)
- *Very Old*: Trapezoidal function with parameters (8000, 8500, 10,000, 10,000)

2.2.3 PageRank

- **Range**: [0, 10]
- **Linguistic Terms**: *Low*, *Medium*, *High*

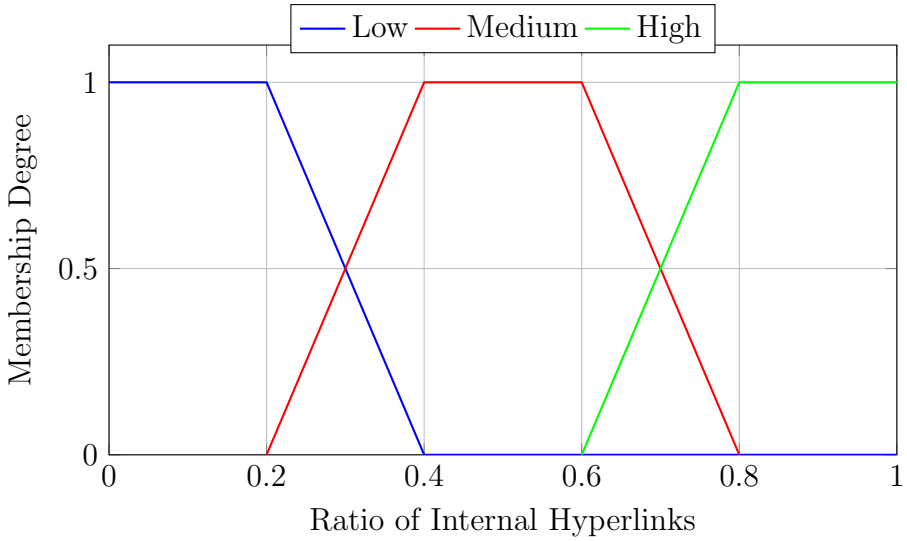


Membership Function Parameters:

- *Low*: Trapezoidal function with parameters (0, 0, 2, 4)
- *Medium*: Trapezoidal function with parameters (2, 4, 6, 8)
- *High*: Trapezoidal function with parameters (6, 8, 10, 10)

2.2.4 Ratio of Internal Hyperlinks

- **Range**: [0, 1]
- **Linguistic Terms**: *Low*, *Medium*, *High*

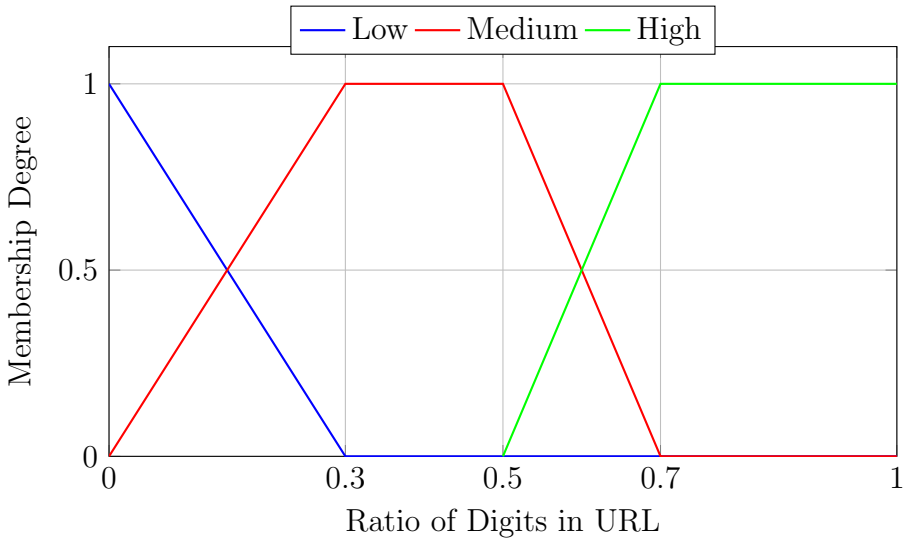


Membership Function Parameters:

- *Low*: Trapezoidal function with parameters (0, 0, 0.2, 0.4)
- *Medium*: Trapezoidal function with parameters (0.2, 0.4, 0.6, 0.8)
- *High*: Trapezoidal function with parameters (0.6, 0.8, 1, 1)

2.2.5 Ratio of Digits in URL

- **Range**: [0, 1]
- **Linguistic Terms**: *Low*, *Medium*, *High*

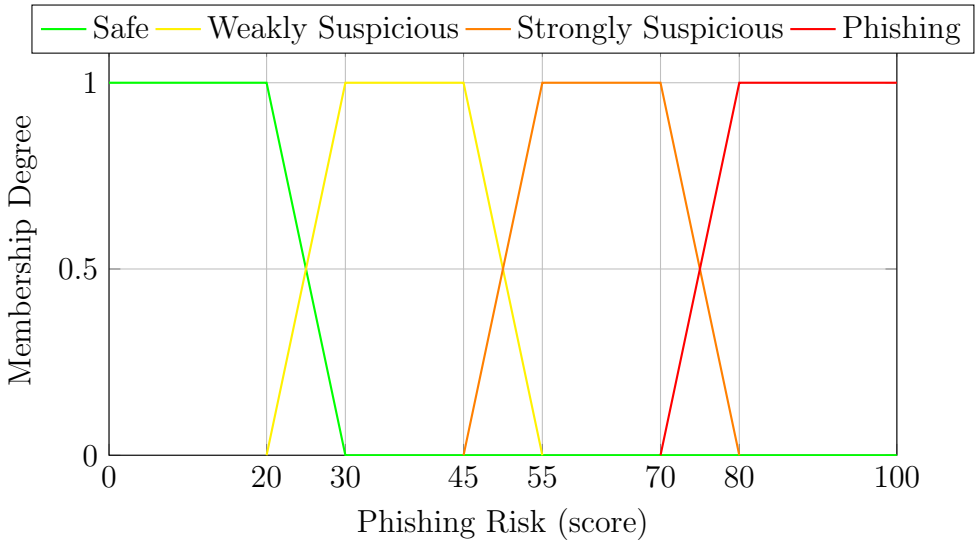


Membership Function Parameters:

- *Low*: Triangular function with parameters (0, 0, 0.3)
- *Medium*: Trapezoidal function with parameters (0, 0.3, 0.5, 0.7)
- *High*: Trapezoidal function with parameters (0.5, 0.7, 1, 1)

2.3 Output Variable

- **Phishing Risk**
- **Range**: [0, 100]
- **Linguistic Terms**: *Safe*, *Weakly Suspicious*, *Strongly Suspicious*, *Phishing*



Membership Function Parameters:

- *Safe*: Trapezoidal function with parameters (0, 0, 20, 30)
- *Weakly Suspicious*: Trapezoidal function with parameters (20, 30, 45, 55)
- *Strongly Suspicious*: Trapezoidal function with parameters (45, 55, 70, 80)
- *Phishing*: Trapezoidal function with parameters (70, 80, 100, 100)

3 Definition of Fuzzy Rules

In this section, we define the fuzzy rules that form the core of our phishing detection expert system. The rules are formulated based on logical relationships between input variables, supported by evidence from the literature [2, 1, 7]. The rules are designed to cover various combinations of input values, focusing on pairs of variables to capture significant interactions while keeping the rule base manageable. Each rule is assigned a weight representing the degree of certainty or importance, reflecting the confidence in the implication.

We have a total of 35 rules, each involving two input variables. The weights assigned to each rule range from 0.7 to 1.0, with higher weights indicating stronger confidence based on the consistency and strength of evidence in the literature. Rules with weights of 1.0 represent well—established relationships, while lower weights account for scenarios with moderate certainty.

3.1 Rules Involving URL Length and Domain Age

These rules assess the phishing risk based on the length of the URL (Input 1) and the age of the domain (Input 2). Phishing websites often have long URLs and recent domain registrations [7, 1].

Table 1: Rules Based on URL Length and Domain Age

Rule	URL Length	Domain Age	Phishing Risk	Weight
1	Short (MF1)	Very Old (MF4)	Safe (MF1)	1.0
2	Large (MF3)	Very New (MF1)	Phishing (MF4)	1.0
3	Large (MF3)	New (MF2)	Strongly Suspicious (MF3)	0.9
4	Medium (MF2)	Old (MF3)	Weakly Suspicious (MF2)	0.8
5	Short (MF1)	Very New (MF1)	Weakly Suspicious (MF2)	0.8
6	Large (MF3)	Very Old (MF4)	Strongly Suspicious (MF3)	0.7
7	Medium (MF2)	Very New (MF1)	Strongly Suspicious (MF3)	0.9

The weights in these rules reflect the degree of association between the URL length and domain age with phishing risk. Rules 1 and 2 have the highest weight (1.0) because they represent clear and strong indicators: a short URL with a very old domain is likely to be safe, while a long URL with a very new domain is strongly associated with phishing. Rules 3 and 7, with weights of 0.9, indicate high suspicion when one feature is at its maximum risk level and the other is moderately risky. Rules 4 and 5, with weights of 0.8, represent moderate suspicion due to mixed indicators. Rule 6 has a lower weight of 0.7 because a long URL with a very old domain is less indicative of phishing but still warrants attention.

3.2 Rules Involving Domain Age and PageRank

These rules involve the domain age (Input 2) and the PageRank (Input 3). Legitimate websites usually have older domains and higher PageRank due to their established presence [2].

Table 2: Rules Based on Domain Age and PageRank

Rule	Domain Age	PageRank	Phishing Risk	Weight
8	Very Old (MF4)	High (MF3)	Safe (MF1)	1.0
9	Very New (MF1)	Low (MF1)	Phishing (MF4)	1.0
10	Old (MF3)	Low (MF1)	Strongly Suspicious (MF3)	0.9
11	Old (MF3)	Medium (MF2)	Weakly Suspicious (MF2)	0.8
12	New (MF2)	Low (MF1)	Strongly Suspicious (MF3)	0.9
13	Very Old (MF4)	Low (MF1)	Weakly Suspicious (MF2)	0.7
14	Very New (MF1)	High (MF3)	Weakly Suspicious (MF2)	0.8

In these rules, weights are assigned based on how strongly the combination of domain age and PageRank correlates with phishing risk. Rules 8 and 9 have the highest weight (1.0) because they represent clear—cut cases: a very old domain with high PageRank is likely safe, while a very new domain with low PageRank is a strong phishing indicator. Rules 10 and 12 are weighted at 0.9, reflecting high suspicion when one feature is at high risk. Rules 11 and 14, with weights of 0.8, indicate moderate suspicion due to medium PageRank or a high PageRank for a very new domain. Rule 13 has a lower weight of 0.7, as a very old domain with low PageRank raises some concern but is less definitive.

3.3 Rules Involving URL Length and Ratio of Digits in URL

These rules involve the URL length (Input 1) and the ratio of digits in the URL (Input 5). A long URL with many digits is characteristic of phishing websites attempting to obscure their true destination [7].

Table 3: Rules Based on URL Length and Ratio of Digits

Rule	URL Length	Digits in URL	Phishing Risk	Weight
15	Large (MF3)	High (MF3)	Phishing (MF4)	1.0
16	Short (MF1)	Low (MF1)	Safe (MF1)	1.0
17	Medium (MF2)	High (MF3)	Strongly Suspicious (MF3)	0.9
18	Large (MF3)	Medium (MF2)	Strongly Suspicious (MF3)	0.9
19	Short (MF1)	Medium (MF2)	Weakly Suspicious (MF2)	0.8
20	Medium (MF2)	Low (MF1)	Weakly Suspicious (MF2)	0.7
21	Large (MF3)	Low (MF1)	Weakly Suspicious (MF2)	0.7

The weights assigned to these rules reflect the strength of association between URL characteristics and phishing risk. Rules 15 and 16 have weights of 1.0 because they represent strong indicators—long URLs with many digits are highly suspect, while short URLs with few digits are generally safe. Rules 17 and 18 are weighted at 0.9, indicating high suspicion when one feature is at maximum risk and the other is moderately risky. Rules 19, 20, and 21 have lower weights (0.7 to 0.8) due to mixed indicators, reflecting moderate suspicion.

3.4 Rules Involving PageRank and Ratio of Internal Hyperlinks

These rules consider the PageRank (Input 3) and the ratio of internal hyperlinks (Input 4). Phishing websites may have a low number of internal hyperlinks and low PageRank [1].

Table 4: Rules Based on PageRank and Internal Hyperlinks Ratio

Rule	PageRank	Internal Hyperlinks	Phishing Risk	Weight
22	High (MF3)	High (MF3)	Safe (MF1)	1.0
23	Low (MF1)	Low (MF1)	Phishing (MF4)	1.0
24	Medium (MF2)	Low (MF1)	Strongly Suspicious (MF3)	0.9
25	High (MF3)	Low (MF1)	Weakly Suspicious (MF2)	0.8
26	Low (MF1)	Medium (MF2)	Strongly Suspicious (MF3)	0.9
27	Medium (MF2)	High (MF3)	Weakly Suspicious (MF2)	0.8
28	Low (MF1)	High (MF3)	Weakly Suspicious (MF2)	0.7

The weights reflect how the combination of PageRank and internal hyperlinks ratio influences the phishing risk assessment. Rules 22 and 23 have weights of 1.0 because they reflect strong evidence—high PageRank with many internal links suggests a safe site, while low values for both features are common in phishing sites. Rules 24 and 26 are assigned weights of 0.9 due to high suspicion when one feature is low, indicating risk. Rules 25, 27, and 28 have weights of 0.7 to 0.8, representing moderate suspicion when the indicators are mixed.

3.5 Rules Involving Domain Age and Ratio of Digits in URL

These rules involve the domain age (Input 2) and the ratio of digits in the URL (Input 5). High ratios of digits in the URL combined with recent domain registrations are indicative of phishing attempts [7].

Table 5: Rules Based on Domain Age and Ratio of Digits in URL

Rule	Domain Age	Digits in URL	Phishing Risk	Weight
29	Very Old (MF4)	Low (MF1)	Safe (MF1)	1.0
30	Very New (MF1)	High (MF3)	Phishing (MF4)	1.0
31	Old (MF3)	High (MF3)	Strongly Suspicious (MF3)	0.9
32	Very New (MF1)	Low (MF1)	Weakly Suspicious (MF2)	0.8
33	New (MF2)	Medium (MF2)	Strongly Suspicious (MF3)	0.9
34	Very Old (MF4)	Medium (MF2)	Weakly Suspicious (MF2)	0.7
35	New (MF2)	High (MF3)	Strongly Suspicious (MF3)	0.9

Weights in these rules are assigned based on how strongly the domain age and digit ratio correlate with phishing activity. Rules 29 and 30, with weights of 1.0, represent definitive cases——a very old domain with few digits is safe, while a very new domain with many digits is highly suspicious. Rules 31, 33, and 35 are weighted at 0.9, indicating high suspicion when moderate domain age is combined with high digit ratios. Rule 32 has a weight of 0.8, as a very new domain with a low digit ratio is somewhat suspicious. Rule 34 is weighted at 0.7, since a very old domain with a medium digit ratio presents a lower risk but still requires attention.

4 Implementation in MATLAB

The fuzzy expert system was implemented using MATLAB's Fuzzy Logic Toolbox. The system is a Mamdani-type Fuzzy Inference System (FIS) with the following specifications:

- **Aggregation Method**: Maximum (max)
- **Implication Method**: Minimum (min)
- **Defuzzification Method**: Centroid (Center of Area)

4.1 FIS Structure

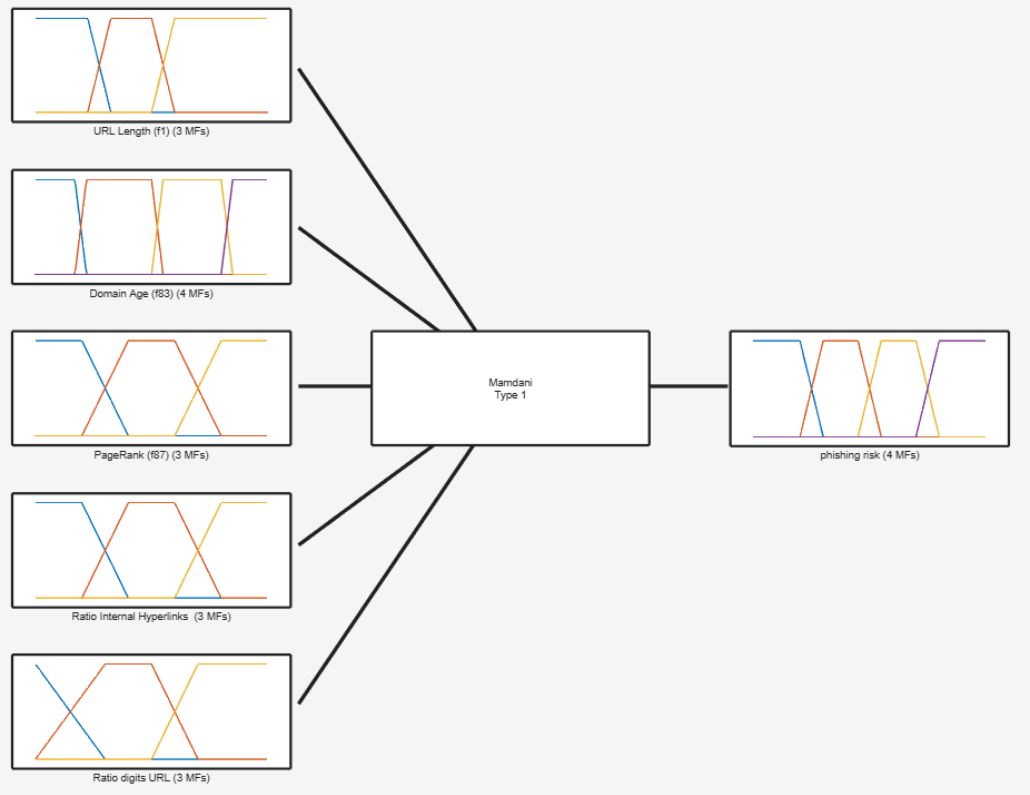


Figure 1: FIS Structure in MATLAB

4.2 Validation of the System

To validate the system, 3D surface plots were generated for different combinations of input variables. These plots help visualize how the inputs affect the output phishing risk.

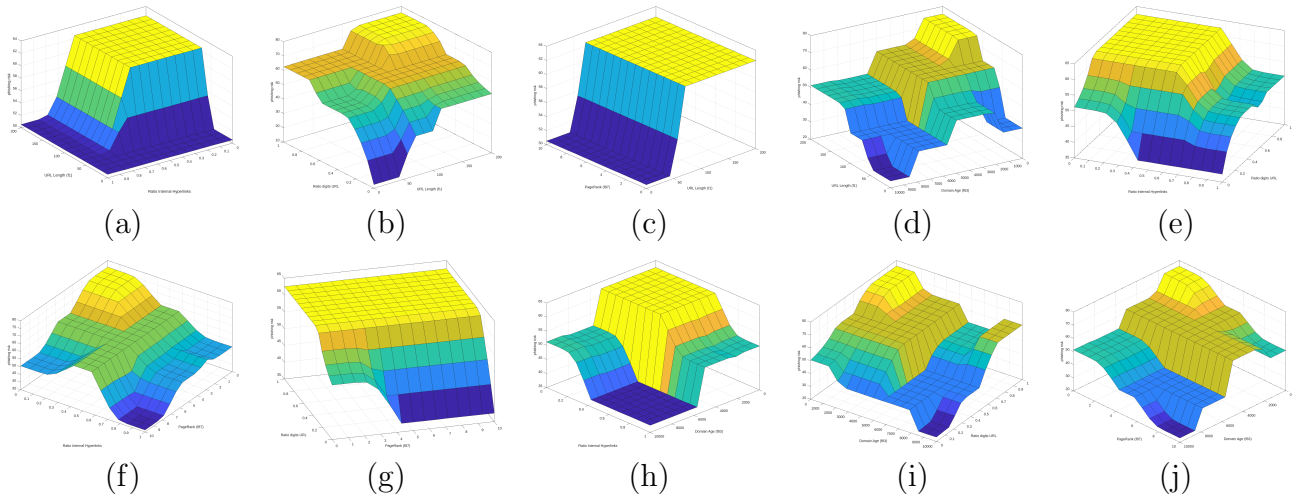


Figure 2: 3D Surface Plots of Phishing Risk for Different Feature Combinations

Descriptions of the subplots:

- (a) URL Length vs. Ratio of Internal Hyperlinks
- (b) URL Length vs. Ratio of Digits in URL

- (c) URL Length vs. PageRank
- (d) URL Length vs. Domain Age
- (e) Ratio of Internal Hyperlinks vs. Ratio of Digits in URL
- (f) PageRank vs. Ratio of Internal Hyperlinks
- (g) PageRank vs. Ratio of Digits in URL
- (h) Domain Age vs. Ratio of Internal Hyperlinks
- (i) Domain Age vs. Ratio of Digits in URL
- (j) Domain Age vs. PageRank

Several subplots demonstrate smooth and gradual transitions, which are desirable for interpretability. Non-linear behaviours, seen in plots like (b), (d) and (j) indicate that the system accounts for complex interactions between variables.

There are also some steep transitions in some subplots (e.g. (a) or (c)), indicating overly sharp rule definitions. Including additional rules could help smoothing the sharp changes and improve the system's generalizability. However, this would significantly increase the complexity of the rule set, which falls beyond the scope of this assignment.

5 Task 4: Testing the System

We tested the fuzzy expert system with four different websites, extracted from the dataset [6]. The urls are classified as legitimate or phishing. Each case represent different scenarios, based on the input variables.

5.1 Test Case 1: Safe Website

URL: `https://www.facebook.com/thekeyboardcat`

True label: Legitimate

Input Variables:

- URL Length: 39 (short)
- Domain Age: 8516 days (very old)
- PageRank: 10 (high)
- Ratio of Internal Hyperlinks: 0.32 (low/medium)
- Ratio of Digits in URL: 0.0 (low)

Output: The phishing risk score was 19.2/100

Activated rules:

- Rule 1: If URL Length (f1) is short and Domain Age (f83) is very old then phishing risk is safe

- Rule 8: If Domain Age (f83) is very old and PageRank (f87) is high then phishing risk is safe
- Rule 16: If URL Length (f1) is short and Ratio digits URL (f26) is low then phishing risk is safe
- Rule 25: If PageRank (f87) is high and Ratio Internal Hyperlinks (f58) is low then phishing risk is weakly suspicious

The system correctly identifies the website as legitimate, giving a low phishing risk score of 19.2. The activated rules highlight strong legitimacy indicators such as short URL legnth, very old domain, high PageRank and outweighing minor suspicion from the low ratio of internal hyperlinks.

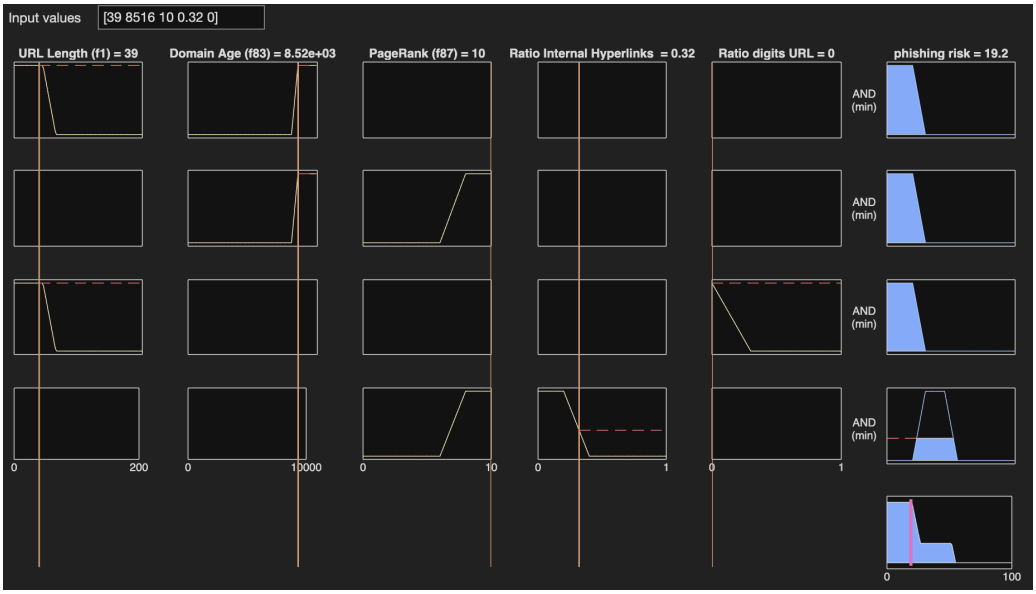


Figure 3: Rule inference for test 1 (showing only active rules)

5.2 Test Case 2: Weakly suspicious Website

URL: `http://dic.academic.ru/dic.nsf/ruwiki/1425594`

True label: Legitimate

Input Variables:

- URL Length: 45 (short)
- Domain Age: 7156 days (old)
- PageRank: 3 (low/medium)
- Ratio of Internal Hyperlinks: 0.93 (high)
- Ratio of Digits in URL: 0.15 (low)

Output: The phishing risk score was 38.2/100

Activated rules:

- Rule 10: If Domain Age (f83) is old and PageRank (f87) is low then phishing risk is strongly suspicions
- Rule 11: If Domain Age (f83) is old and PageRank (f87) is medium then phishing risk is weakly suspicious
- Rule 16: If URL Length (f1) is short and Ratio digits URL (f26) is low then phishing risk is safe
- Rule 19: If URL Length (f1) is short and Ratio digits URL (f26) is medium then phishing risk is weakly suspicious
- Rule 27: If PageRank (f87) is medium and Ratio Internal Hyperlinks (f58) is high then phishing risk is weakly suspicious
- Rule 28: If PageRank (f87) is low and Ratio Internal Hyperlinks (f58) is high then phishing risk is weakly suspicious

The system associates the website with a phishing risk score of 38.2/100. The system's assessment is influenced by the low/medium PageRank, increasing the score. However, the other indicators are consistent with legitimate websites: short URL length, old domain age, low ratio of digits in URL and high ratio of internal hyperlinks.

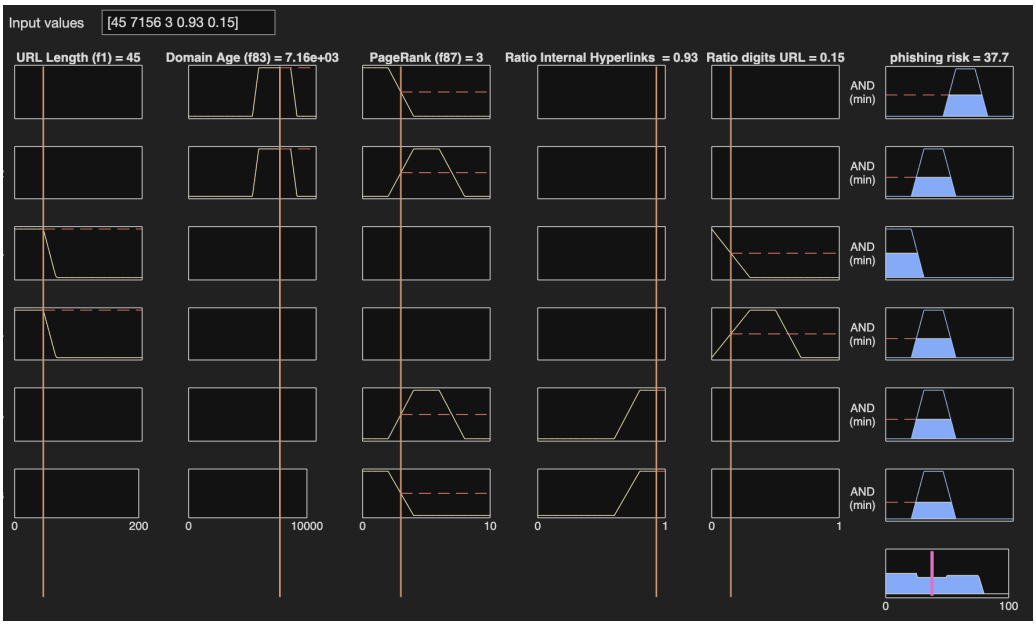


Figure 4: Rule inference for test 2 (showing only active rules)

5.3 Test Case 3: Strongly Suspicious Website

URL: `https://sure.eligulinsaat.com/tz?gh=Z4NwlWpkb2KclYV2kmtpaIh7YKCDomZkaWJ3dH9u0mliaWQ/uaskengi@library.usask.ca`

True label: Phishing

Input Variables:

- URL Length: 109 (medium/large)

- Domain Age: 14 (very new)
- PageRank: 0 (low)
- Ratio of Internal Hyperlinks: 0.46 (medium)
- Ratio of Digits in URL: 0.06 (low)

Output: The phishing risk score was 62.5/100

Activated rules:

- Rule 2: If URL Length (f1) is large and Domain Age (f83) is very new then phishing risk is phishing
- Rule 7: If URL Length (f1) is medium and Domain Age (f83) is very new then phishing risk is strongly suspicions
- Rule 9: If Domain Age (f83) is very new and PageRank (f87) is low then phishing risk is phishing
- Rule 18: If URL Length (f1) is large and Ratio digits URL (f26) is medium then phishing risk is strongly suspicions
- Rule 20: If URL Length (f1) is medium and Ratio digits URL (f26) is low then phishing risk is weakly suspicious
- Rule 21: If URL Length (f1) is large and Ratio digits URL f26 is low then phishing risk is weakly suspicious
- Rule 26: If PageRank (f87) is low and Ratio Internal Hyperlinks (f58) is medium then phishing risk is strongly suspicions
- Rule 32: If Domain Age (f83) is very new and Ratio digits URL (f26) is low then phishing risk is weakly suspicious

The system considers a phishing risk score of 62.5/100. The key indicators contributing to this outcome include the large URL length, very new domain age and low PageRank, both strong indicators of phishing activity. While medium ratio of hyperlinks and low ratio of digits reduce the severity of suspicion, activated rules highlight potential risk.

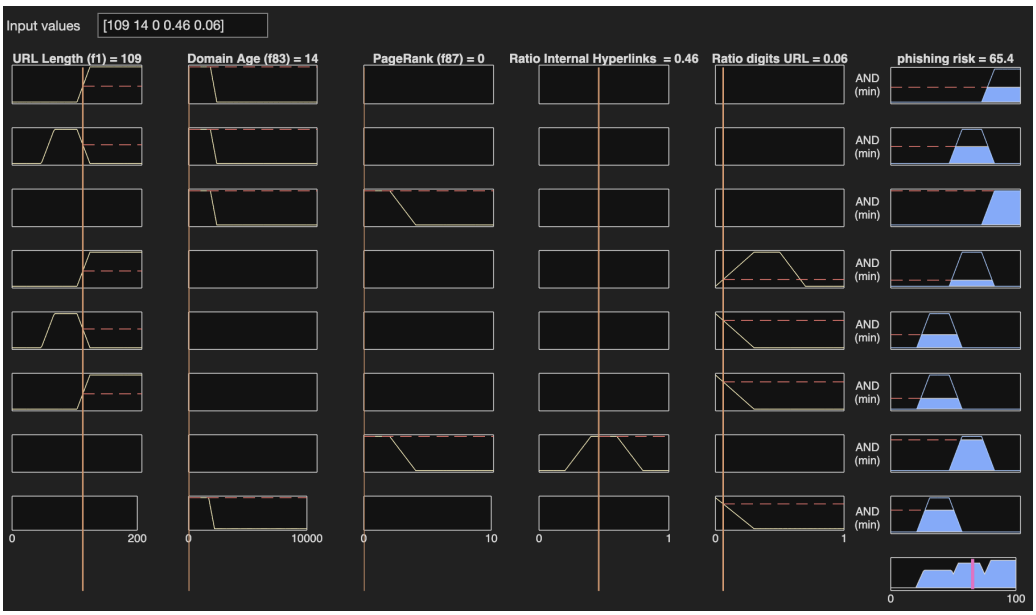


Figure 5: Rule inference for test 3 (showing only active rules)

5.4 Test Case 4: Phishing Website

URL `https://fairilyused.com/wp-content/upgrade/en/ky-1/1/index.html?7777772e66616972696c79757365642e636f6d-7777772e66616972696c79757365642e636f6d-7777772e66616972696c79757365642e636f6d7777772e66616972696c79757365642e636f6d7777772e66616972696c79757365642e636f6d`

True label: Phishing

Input Variables:

- URL Length: 200 (long)
- Domain Age: 1109 (very new)
- PageRank: 0 (low)
- Ratio of Internal Hyperlinks: 0.08 (low)
- Ratio of Digits in URL: 0.65 (medium/high)

Output: The phishing risk score was 82.4/100

Activated rules:

- Rule 2: If URL Length (f1) is large and Domain Age (f83) is very new then phishing risk is phishing
- Rule 9: If Domain Age (f83) is very new and PageRank (f87) is low then phishing risk is phishing
- Rule 15: If URL Length (f1) is large and Ratio digits URL (f26) is high then phishing risk is phishing
- Rule 18: If URL Length (f1) is large and Ratio digits URL (f26) is medium then phishing risk is strongly suspicions

- Rule 23: If PageRank (f87) is low and Ratio Internal Hyperlinks (f58) is low then phishing risk is phishing
- Rule 30: If Domain Age (f83) is very new and Ratio digits URL (f26) is high then phishing risk is phishing

The system correctly associates the website with a high risk of phishing, with a score of 82.4/100. The system appropriately captures key phishing indicators such as the very long URL length, very new domain age, low PageRank, low ratio of internal hyperlinks and high ratio of digits in the URL. The activated rules recognize these suspicious patterns effectively.

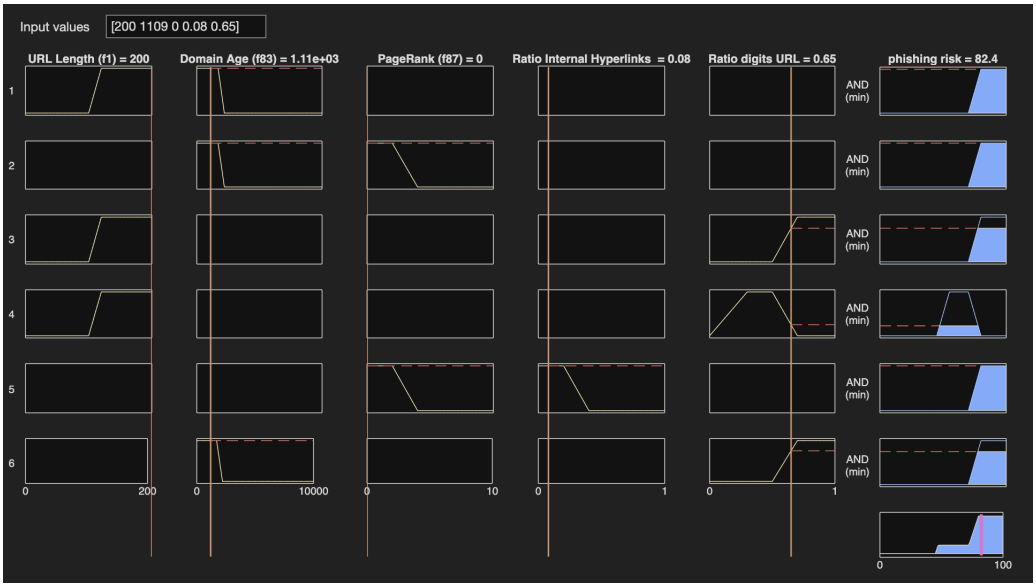


Figure 6: Rule inference for test 4 (showing only active rules)

6 Design of a More Complete Fuzzy Expert System

To enhance the effectiveness of phishing detection, we propose designing a more comprehensive fuzzy expert system that incorporates additional features and a hierarchical structure. This section outlines the design of this advanced system, grounded in literature and best practices in the field.

6.1 Incorporating Additional Features

Expanding the feature set used in phishing detection can significantly enhance the accuracy and robustness of the system [7, 1]. Based on insights from recent surveys and studies, we propose including the following additional features:

- **HTTPS Usage**: Evaluating whether the website employs HTTPS and possesses valid SSL certificates. Phishing sites often lack proper SSL implementation, making this a critical indicator [7].
- **Abnormal URL Features**: Detecting anomalies in URLs, such as the presence of IP addresses instead of domain names, excessive use of subdomains, or inclusion of suspicious special characters [3].
- **Web Traffic Rank**: Assessing the web traffic rank of a site, as legitimate websites typically have higher traffic compared to phishing sites, which are relatively obscure [1].

- **DNS Record Validity**: Verifying the validity of DNS records, including the existence of MX records and consistency in WHOIS data, which can reveal discrepancies common in phishing domains [7].
- **URL Shortening Services**: Identifying the use of URL shortening services that may conceal the true destination of a link, a tactic often used by phishers [3].
- **Content Features**: Analyzing webpage content for elements such as login forms placed on unsecure pages, mismatched URLs in anchor tags, or counterfeit security seals and certifications [1].
- **Third-Party Domain Requests**: Examining the number and nature of requests made to external domains, which may indicate potential data exfiltration or redirection to malicious sites [7].

6.2 Hierarchical Fuzzy Inference System

To manage the increased complexity due to additional features, we propose structuring the fuzzy expert system hierarchically, as suggested in the literature [5]. This structure divides the system into multiple layers or modules, each focusing on different categories of features.

6.2.1 System Architecture

The proposed system consists of the following modules:

1. **URL-based Feature Module**: Processes features related to the URL, such as length, presence of IP addresses, and abnormal characters.
2. **Domain-based Feature Module**: Analyzes domain-related features, including domain age, DNS records, and web traffic rank.
3. **Content-based Feature Module**: Examines the content of the webpage, like the presence of forms, scripts, and mismatched URLs.
4. **HTTPS and Security Module**: Evaluates the usage of HTTPS, SSL certificates, and security seals.
5. **External Links Module**: Assesses the number and nature of external links and requests.

Each module produces an intermediate risk assessment based on its specific features. These intermediate outputs are then combined in a higher-level fuzzy inference system to compute the overall phishing risk.

6.3 Proposed System Diagram

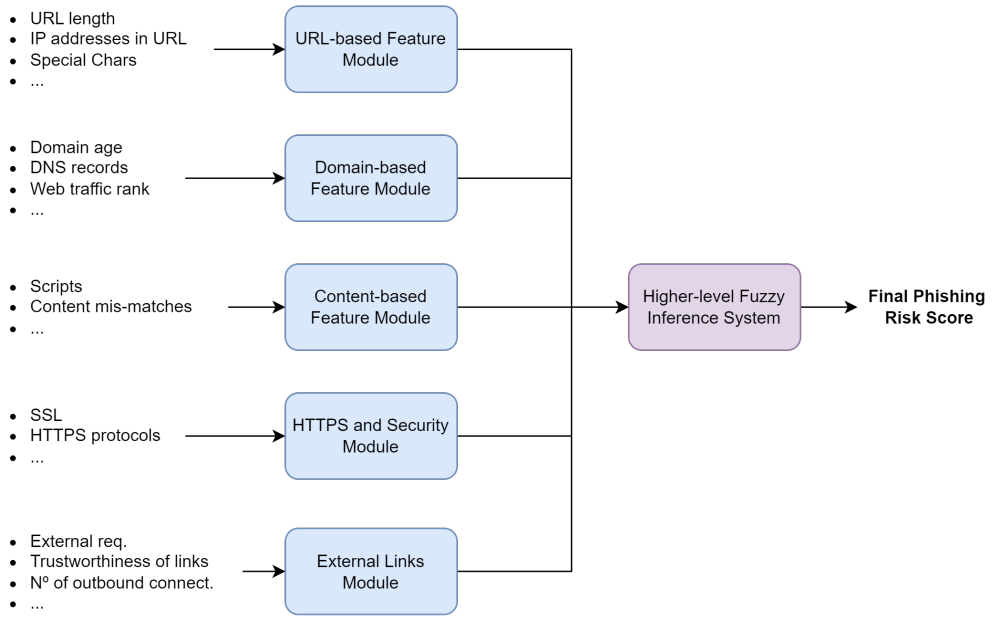


Figure 7: Proposed hierarchical fuzzy expert system architecture for phishing detection.

6.4 Rule Blocks

In the hierarchical fuzzy inference system, each module is associated with a corresponding rule block within the rule base. Each rule block encapsulates a set of fuzzy rules tailored to the specific features and risk indicators pertinent to that module. While the modules were previously introduced in the System Architecture subsection, presenting them again in terms of their rule blocks serves to highlight the direct linkage between system components and their underlying inference logic.

- **URL Module Rule Block**: Contains rules related to URL length, the presence of IP addresses in the URL, the use of special characters or suspicious subdomains, and other URL-based indicators.
- **Domain Module Rule Block**: Contains rules concerning domain-centric features, such as domain age, DNS record validity, WHOIS data consistency, and web traffic rank.
- **Content Module Rule Block**: Contains rules that evaluate the nature of webpage elements. These may include the presence and suspicious placement of login forms, scripts, mismatched anchors, or deceptive content features.
- **HTTPS Module Rule Block**: Contains rules evaluating the security status of the site, considering factors like the presence and validity of SSL certificates, enforcement of HTTPS protocols, and whether security seals are legitimate.
- **External Links Module Rule Block**: Contains rules assessing the extent and legitimacy of external requests, the trustworthiness of linked domains, and the number of outbound connections, which may suggest data leakage or redirection to malicious sites.

Each rule block processes its inputs and outputs a risk score or classification. The higher-level fuzzy inference system then combines these intermediate assessments to produce the final phishing risk score.

7 Conclusion

In this work, we successfully designed and implemented a fuzzy expert system to detect phishing in websites using five input features. The system classifies websites into four categories and provides a numerical phishing risk score. We defined linguistic variables and membership functions for each feature, formulated 35 fuzzy rules based on logical relationships and literature insights, and implemented the system using MATLAB's Fuzzy Logic Toolbox.

Testing the system with real-world examples demonstrated its effectiveness in capturing critical phishing indicators and providing accurate risk assessments. The system appropriately classified websites into risk categories ranging from safe to phishing.

To enhance detection accuracy and address limitations due to the limited feature set and rule simplicity, we proposed a more comprehensive fuzzy expert system incorporating additional features and a hierarchical structure to manage complexity. This advanced system aims to improve robustness against sophisticated phishing techniques, representing a direction for future work.

References

[1] Z. Dou et al. A systematic review of software-based web phishing detection. *IEEE Communications Surveys & Tutorials*, 19(4):2797–2819, 2017.

[2] A. Hannousse and S. Yahiouche. Towards benchmark datasets for machine learning based website phishing detection: An experimental study. *Engineering Applications of Artificial Intelligence*, 104, 2021.

[3] R. M. Mohammad, F. Thabtah, and L. McCluskey. Phishing websites features. Technical report, School of Computing and Engineering, University of Huddersfield, 2015.

[4] OpenAI. This image was created with the assistance of dall·e 2. `https://openai.com/dall-e-2`, 2024. Accessed: 12-10-2024.

[5] Radek Sindelar. Hierarchical fuzzy logic systems. *Journal of Engineering*, 10(4):123–134, 2022.

[6] UCI Machine Learning Repository. Phishing websites data set. `https://archive.ics.uci.edu/ml/datasets/Phishing+Websites`. Accessed: 2024-06-17.

[7] R. Zieni, L. Massari, and M. C. Calzarossa. Phishing or not phishing? a survey on the detection of phishing websites. *IEEE Access*, 11:18499–18519, 2023.