

# Unravelling Network-based Intrusion Detection: A Neutrosophic Rule Mining and Optimization Framework

Tiago Dias, João Vitorino, Tiago Fonseca, Isabel Praça, Eva Maia, Maria João Viamonte

# Outline



# Motivation



The ever-increasing number of cyber-attacks thought the network is a real **concern**. It is of the utmost importance to reliably **detect malicious network traffic**.



**Rule-based** approaches have shown great performance for solving **classification problems**, such as the ones presented in the cybersecurity field.



Knowledge acquisition in cybersecurity can be both **timely** and **cost expensive**.



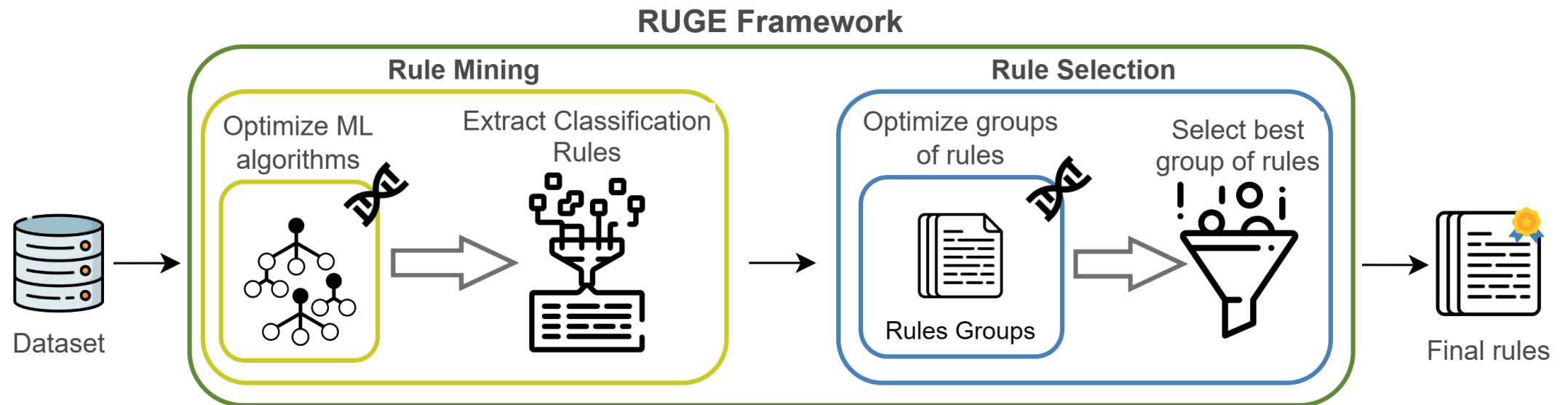
Cybersecurity systems that rely on expert rules are not usually able to **self-update** their knowledge-base.

# Proposed Solution



- **Neutrosophic Rule Mining** and **Optimization** Framework.
- Capable of extracting **interpretable** classification rules.
- Reduces time and effort to obtain **rule-based** knowledge.
- Domain-independent.

# Proposed Solution



# Proposed Solution

Truthness



Indeterminancy



(Cyber-attacks of the same family)

Falsehood

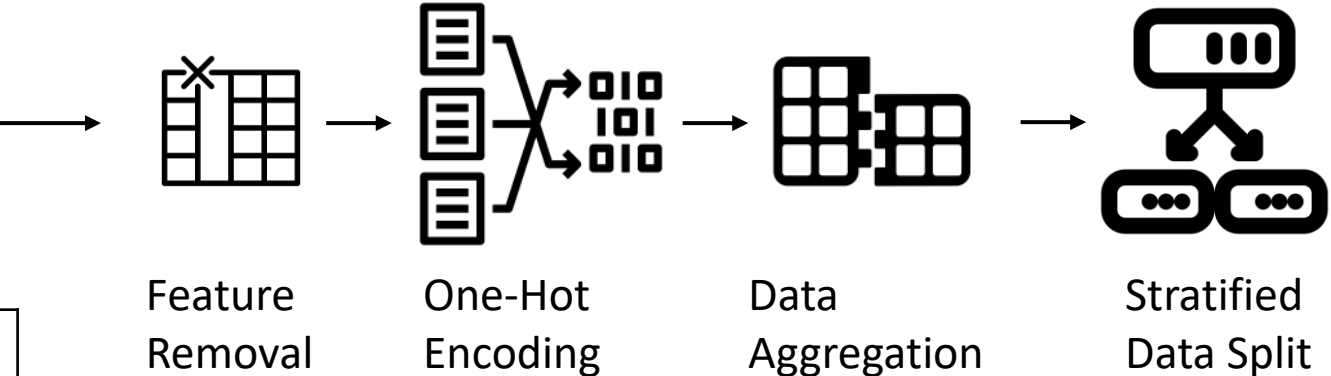


## Single-valued Neutrosophic Cross-Entropy Loss

$$Fitness = \sum_{j=1}^n \left( C_j * \left[ \left[ \log_2 \frac{1}{1+T_j} + \log_2 \frac{1}{1-I_j} + \log_2 \frac{1}{1-F_j} \right] + \left[ T_j \log_2 \frac{T_j}{1+T_j} + (1-T_j) \log_2 \frac{1-T_j}{1+T_j} \right] + \left[ I_j + (1-I_j) \log_2 \frac{1-I_j}{1-I_j} + \left[ F_j + (1-F_j) \log_2 \frac{1-F_j}{1-F_j} \right] \right] \right)$$

Expected \ Predicted	Class 1	Class 2	Class 3
Class 1	T	F	F
Class 2	F	T	I
Class 3	F	I	T

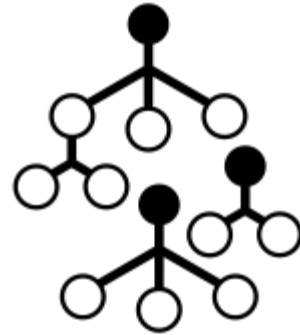
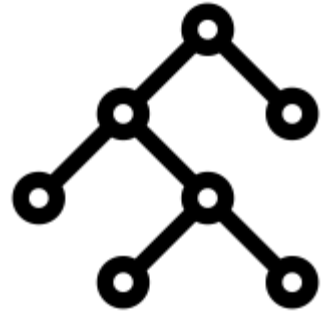
# CICIDS2017 Testbed



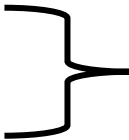
Capture	Attack Type	Attack Class
Tuesday	Brute-force	FTP-Patator; SSH-Patator
Wednesday	Denial-of-Service	GoldenEye; Hulk; Slowhttptest; Slowloris
	Exploit	Heartbleed
Friday	Port Scan	PortScan

Indeterminacy Groups

# CICIDS2017 Testbed



## SKOPE-RULES

- Maximum Depth: 10
  - Minimum samples at leaf: 2
- 
- Avoid oversized rules
  - Rules can be applied to multiple training samples

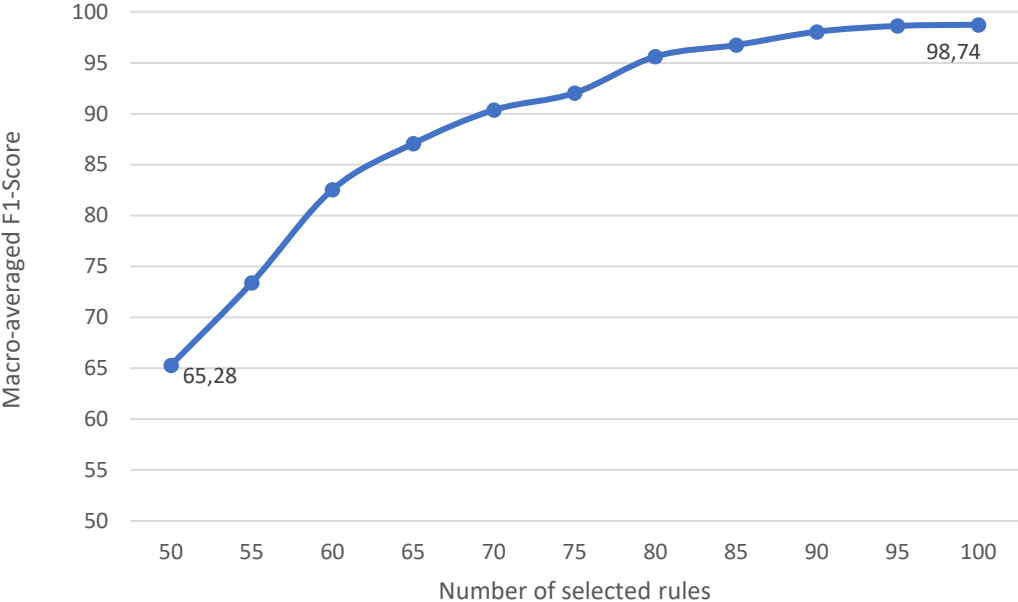
The remaining parameters were optimized by the GA.



# Obtained Results

983 -> 99.92% | 100 -> 98.74%

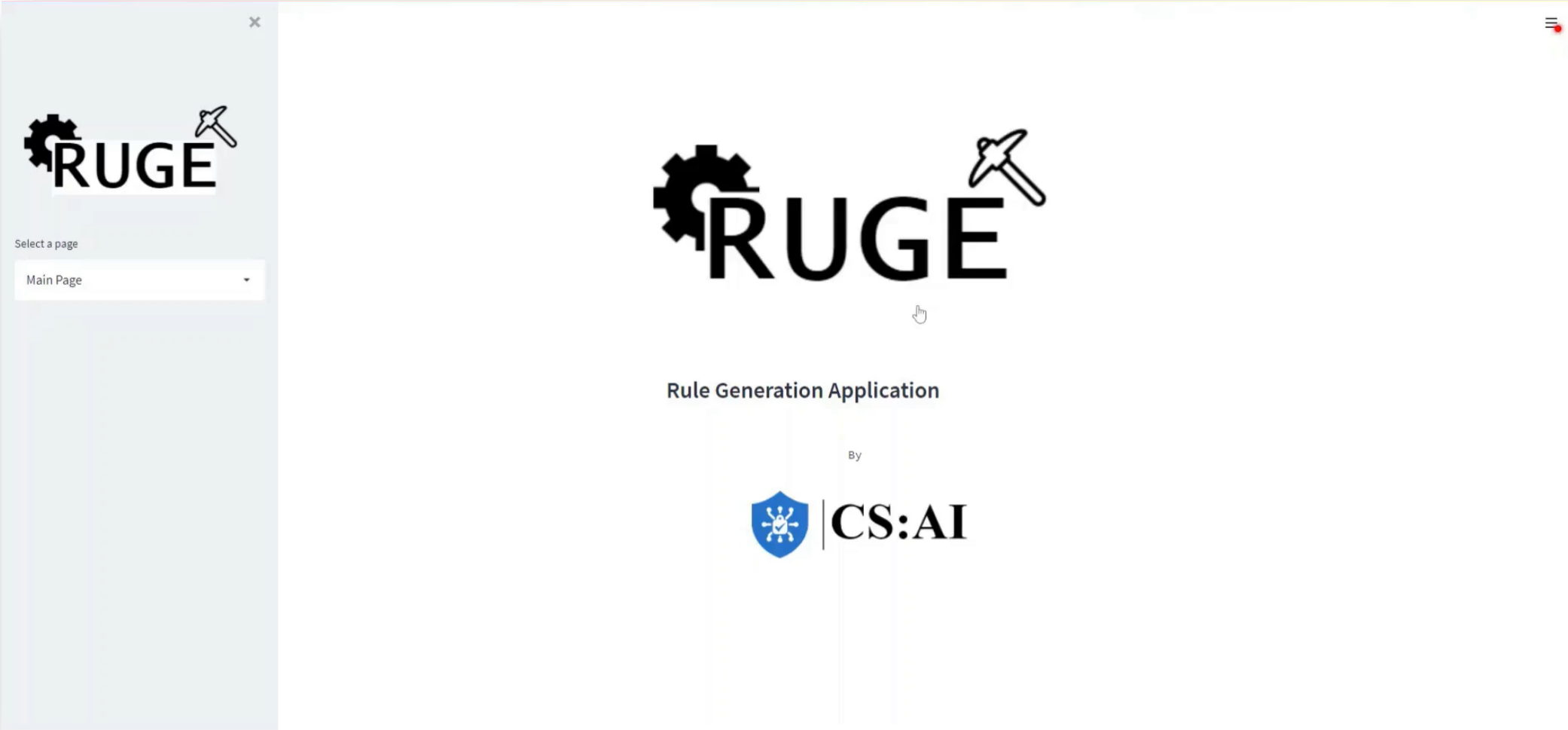
Packet size and communication specificities were the most relevant features



```
If
  bwd_packet_length_std > 1494.157 AND
  fwd_packet_length_max <= 422.5 AND
  total_length_of_bwd_packets <= 11605.0 AND
  total_length_of_bwd_packets > 11565.5
Then
  DoS_Hulk
```



# Demonstration



# Conclusions

- ➕ RUGE was capable of summarizing a great amount of attack signatures into a small and concise set of explainable and well-performing rules.
- ➕ The tool was also able to deal with fuzzy knowledge, by relying on a neutrosophic operator to calculate the fitness of the rules.
- ✓ Increased knowledge acquisition efficiency and efficacy.
- ★ The future work includes the addition of more complex algorithms, experimentation with more datasets and the application of the tool to a real context to assess its suitability.



Thank you