UDC 004.942, 519.876.5

Fuzzy logic in risk assessment of multi-stage cyber attacks on operational network structures

Yuliia Nakonechna[1], Bohdan Savchuk and Anna Kovalova

[1] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», 37, Prosp. Beresteiskyi, Kyiv, 03056, Ukraine*

Abstract

In the current environment, operational network structures have become the target of increasingly complex multi-stage cyber attacks characterized by sequential phases of infiltration, privilege escalation, and lateral movement within the target network. Traditional risk assessment methods often rely on assumptions of precise data availability and well-defined probabilities, which limit their applicability in real-world scenarios marked by uncertainty and imprecise information. This paper proposes an approach based on the use of fuzzy logic systems to assess the risks of multi-stage cyber attacks against networked operational services. The proposed methodology takes into account the ambiguity and fuzziness of input data, expert judgments, and the dynamic progression of attacks. The result is a more flexible and adaptive risk assessment model that supports informed decision-making to enhance cybersecurity, prioritize countermeasures, and optimize the allocation of defensive resources.

Keywords: Cybersecurity, risk assessment, attack, fuzzy logic, infrastructure, network.

Introduction

The rapid development of information technologies contributes to the increased efficiency of operational network structures — systems upon which economic stability, national security, and overall societal well-being heavily depend. However, this progress comes hand in hand with an escalation of threats in cyberspace. Particularly dangerous are multi-stage cyber attacks, in which an adversary incrementally infiltrates a target network, escalates privileges, bypasses security measures, and inflicts substantial damage. Assessing the risks of such attacks is challenging since conventional approaches often fail to adequately address the uncertainty, variability, and incomplete nature of the data on vulnerabilities and attacker behavior. The application of fuzzy logic to risk modeling allows the use of linguistic variables, fuzzy sets, and inference rules to process approximate or incomplete data. This opens the door to more realistic representations of complex attack scenarios, evaluation of the consequences of each step in the intrusion sequence, and identification of the system's most vulnerable points.

The goal of this research is to develop a fuzzy logic-based approach to multi-stage cyber attack risk assessment that can enhance the accuracy and relevance of risk analyses. In doing so, we aim to provide practical recommendations for improving cybersecurity within operational network structures environments.

Problem formulation

The task of assessing the risks posed by multi-stage cyber-attacks involves determining the probability of a successful attacker sequence and estimating the potential losses, all while working with limited, fuzzy, and often contradictory information. A typical multi-stage cyber-attack may encompass several phases: initial network penetration, reconnaissance of the internal infrastructure, privilege escalation, lateral movement toward critical nodes, and final destructive actions, such as data exfiltration or service disruption.

Traditional risk assessment methods generally assume the availability of precise probabilities and numerical values for all parameters. However, in real-world conditions, many characteristics related to attacker behavior, skill

levels, zero-day vulnerabilities, or the state of internal protective measures are uncertain and can vary significantly over time.

Hence, a solution is needed that can operate effectively under conditions of imprecise and approximate input data.

Fuzzy logic systems provide a mechanism for formalizing expert knowledge and reasoning under uncertainty. By introducing linguistic variables (e.g., «high likelihood of attack success» or «moderate impact level»), fuzzy sets, and fuzzy inference rules, we can construct a model that evaluates the risks of multi-stage attacks without requiring precise deterministic values. Thus, the key challenge lies in designing a fuzzy model that considers the characteristics of attacks, their evolving nature, and the information uncertainties involved, ultimately delivering a more adequate and flexible risk assessment.

Literature review

Risk assessment for multi-stage cyberattacks targeting operational network structures is hindered by uncertainty, evolving threats, and incomplete information. Traditional methods often rely on precise probabilities and well-defined inputs, which are rarely available in real-world scenarios. In response, researchers have increasingly employed fuzzy logic to incorporate imprecise, approximate, and subjective data into cybersecurity risk models.

Fuzzy logic's ability to handle uncertainty makes it particularly suitable for operational network structures cybersecurity. [1] demonstrated how fuzzy measures could enhance threat evaluation in military systems, findings that readily translate to critical infrastructure contexts. Similarly, [2] introduced a fuzzy Multi-Criteria Decision-Making (MCDM) framework to reconcile conflicting and ambiguous criteria when safeguarding critical network structures. Building on this, [3] developed FLORA, a fuzzy logic-based intrusion detection system that reduces false positives, thereby improving the detection of complex, multi-step attacks.

Because multi-stage attacks unfold over several phases, fuzzy logic's flexibility in representing uncertainty is valuable for modeling their progression. [4] employed fuzzy cognitive maps to identify causal relationships between attack steps, providing predictive insights into future stages. [5] applied fuzzy inference systems within IIoT environments, underscoring the applicability of similar methodologies to operational network structures, where evolving patterns of attacker behavior require adaptable models.

Integrating fuzzy logic with other analytical techniques can yield more comprehensive assessments. [6] combined fuzzy logic with AHP and Delphi methods to achieve robust, consensus-driven decision-making for critical infrastructure protection. [7] proposed a fuzzy logic-based evaluation framework for automotive systems—a domain with parallel security demands—that can be adapted for operational network structures and critical infrastructures risk assessment.

Despite notable progress, several challenges persist. Issues of scalability, real-time data integration, and continuous model updating remain unresolved. While [8] suggest integrating fuzzy logic with intrusion detection and behavior analytics to enhance adaptability, further research is needed to refine these models for dynamic, continuously evolving attack landscapes.

The literature highlights the promise of fuzzy logic for managing uncertainty in multi-stage attack risk assessment, particularly in critical infrastructure network environments. Although hybrid approaches and novel frameworks show potential, ongoing efforts must address scalability, real-time application, and the continuous evolution of attacker strategies to fully realize the benefits of fuzzy logic in operational network structures cybersecurity.

1. Conceptual framework

Traditional risk assessment models in cybersecurity often rely on deterministic or probabilistic frameworks where each input variable-such as the likelihood of a particular attack step or the severity of a discovered vulnerability-is assumed to be precisely known and quantifiable. In practice, operational network structures scenarios rarely provide clear-cut probabilities or definitive severity metrics. Attackers frequently employ zero-day exploits, adaptive strategies, and deceptive tactics, rendering certain parameters unknown or only partially observable. Under such circumstances, deterministic models tend to oversimplify: they

may ignore uncertainty, treat incomplete data as missing, or force ambiguous information into rigid probability distributions. As a result, these models risk producing overly confident or misleading conclusions.

In contrast, the proposed fuzzy logic-based approach embraces uncertainty as an intrinsic aspect of the operational network structures threat environment. Fuzzy logic allows for the representation of uncertain, approximate, and qualitative assessments as fuzzy sets and linguistic terms, enabling a more flexible and realistic portrayal of multi-stage cyberattacks. Instead of requiring exact probabilities, the model accommodates imprecise descriptors (e.g., "High," "Medium," "Low") and expert judgments. This yields a richer, more adaptable risk assessment tool better aligned with the real conditions of operational network structures under ongoing and evolving cyber threats.

1.1. Formal model description

Let us consider a set of input variables $\mathbf{X} = \{X_1, X_2, \dots, X_n\}$ that describe the state of the system and the attacker's activities. These may include factors such as the attacker's current position in the kill chain, the severity of identified vulnerabilities, the reliability of detection signals, and inferred attacker sophistication. Each input X_i is associated with a fuzzy set $\tilde{A}_i$ defined on its domain D_i. A fuzzy set $\tilde{A}_i$ is characterized by a membership function $\mu_{\tilde{A}_i}(x)$, where $\mu_{\tilde{A}_i}(x) \in [0,1]$ represents the degree to which $x \in D_i$ belongs to the fuzzy set $\tilde{A}_i$.

The model processes these fuzzy inputs using a fuzzy inference engine, which applies a collection of fuzzy rules $\mathcal{R} = \{R_1, R_2, \dots, R_m\}$ to derive an intermediate representation of risk. Each rule R_j takes the form:

$$R_j\text{: IF } X_1 \text{ is } \tilde{A}_{1j} \text{ AND } X_2 \text{ is } \tilde{A}_{2j} \text{ AND}\dots \quad (1)$$

$$\cdots \text{ THEN Risk is } \tilde{B}_j,$$

where $\tilde{A}_{ij}$ and $\tilde{B}_j$ are fuzzy sets describing the conditions on input variables and the resulting fuzzy risk level, respectively. The inference engine aggregates all the fired rules to produce a combined fuzzy risk set $\tilde{R}$.

Finally, the fuzzy output $\tilde{R}$ is defuzzified into a crisp value $r \in R$ that represents the actionable risk score. This score guides security operators in decision-making processes, such as prioritizing resources, scheduling remediation efforts, and implementing countermeasures [9].

Deterministic and purely probabilistic models typically require:

1. Exact probabilities or deterministic values for inputs.
2. Rigid distributions that may not reflect real-world ambiguity.
3. Less flexibility in updating risk assessments when new, imprecise information emerges.

In contrast, the fuzzy logic-based model:

- accepts linguistic assessments (e.g., "moderately likely," "somewhat severe"), thus not forcing artificial precision.
- easily incorporates expert knowledge without necessitating exact probability distributions.
- updates its rule base and membership functions as new intelligence or incident data become available, enhancing adaptability and realism.

1.2. Main model components

1.2.1. Threat profiling module

The threat profiling module ingests intelligence about potential attackers, their known tactics, techniques, and procedures (TTPs), and historical attack data.

Let $\mathbf{\Theta} = \{\theta_1, \theta_2, \dots, \theta_k\}$ be a set of threat characteristics, such as: - θ_1 : Attacker sophistication level (e.g., Low, Medium, High) - θ_2 : Availability of zero-day exploits (e.g., None, Few, Many) - θ_3 : Motivations and resources of the attacker (e.g., State-sponsored, Cybercriminals)

Each θ_j is represented by a fuzzy variable with its own membership functions. For instance, attacker sophistication θ_1 might have membership functions $\mu_{\text{Low}}(\theta_1), \mu_{\text{Medium}}(\theta_1)$, and $\mu_{\text{High}}(\theta_1)$ mapping the qualitative assessment to $[0,1]$.

The threat profiling module outputs a fuzzy profile $\tilde{P}$ defined as a vector of fuzzy sets, each describing one dimension of the adversary's characteristics:

$$\tilde{P} = \langle \tilde{P}_1, \tilde{P}_2, \dots, \tilde{P}_k \rangle, \quad (2)$$

where $\tilde{P}_j$ is the fuzzy set representing the threat characteristic θ_j.

These fuzzy threat profiles feed into the fuzzy inference engine's rule base, influencing how input conditions are interpreted and how risk is ultimately assessed.

1.2.2. Fuzzy inference engine

The fuzzy inference engine translates input variables (including system state and threat profile) into a fuzzy risk representation. Let $\mathbf{X} = (X_1, X_2, \dots, X_n)$ be the input vector describing the scenario. Each X_i has associated fuzzy sets representing linguistic terms:

$$X_i \mapsto \{\tilde{A}_{i1}, \tilde{A}_{i2}, \dots, \tilde{A}_{ie_i}\}, \quad (3)$$

For instance, if $X_1 =$ "Vulnerability Severity," the terms might be $\tilde{A}_{11} =$ "Low severity," $\tilde{A}_{12} =$ "Medium severity," and $\tilde{A}_{13} =$ "High severity."

The rule base $\mathcal{R}$ consists of rules of the form: R_j: IF $X_1 \in \tilde{A}_{1j}, X_2 \in \tilde{A}_{2j}, \dots, X_n \in \tilde{A}_{nj}$ AND $\theta_1 \in \tilde{P}_{1j}, \dots, \theta_k \in \tilde{P}_{kj}$ THEN Risk $\in \tilde{B}_j$ To apply a given rule R_j, the inference engine computes the firing strength α_j, typically using a t-norm (e.g., minimum) for the AND operator:

$$\alpha_j = \min\left(\mu_{\tilde{A}_{1_j}}(X_1), \mu_{\tilde{A}_{2j}}(X_2), \dots \right.$$
$$\left. \dots, \mu_{\tilde{A}_{nj}}(X_n), \mu_{\tilde{P}_{1j}}(\theta_1), \dots, \mu_{\tilde{P}_{kj}}(\theta_k)\right), \quad (4)$$

Each fired rule contributes a fuzzy set $\tilde{B}_j$ to the output. The aggregation of all fired rules is achieved via a fuzzy aggregation operator (e.g., maximum):

$$\tilde{R}(x) = \max_j \left[\alpha_j \cdot \mu_{\tilde{B}_j}(x)\right], \quad (5)$$

where $\tilde{R}(x)$ is the membership function of the aggregated fuzzy risk set and α_j scales the output membership function of rule R_j.

1.2.3. Risk aggregation layer

The risk aggregation layer converts the aggregated fuzzy risk $\mathcal{R}$ into a crisp risk score r. A common defuzzification method is the centroid approach:

$$r = \frac{\int x \mu_{\tilde{R}}(x) dx}{\int \mu_{\tilde{R}}(x) dx}, \quad (5)$$

This integral-based definition is approximated computationally. The result $r \in R$ is a single number representing the overall risk level. Values may be normalized to a range, such as $[0,100]$, for easier interpretation.

The crisp risk score r can then be used to inform security decisions, prioritize incident response, or adjust resource allocation. As new data or threat intelligence updates arrive, membership functions and rules can be iteratively refined, ensuring that the model remains aligned with the evolving threat environment.

In summary, the proposed fuzzy logic-based model overcomes the limitations of traditional deterministic or purely probabilistic risk assessments by directly incorporating uncertainty, linguistic variables, and expert knowledge. Through its three core components-threat profiling module, fuzzy inference engine, and risk aggregation layer - this framework delivers a dynamic, flexible, and context-aware assessment of multi-stage cyberattack risks. Such adaptability, granularity, and continuous refinement are essential for enhancing the security posture of operational network structures in an era of escalating and complex cyber threats.

2. Fuzzy model design

The fuzzy logic model employed in this study transforms qualitative, uncertain, and incomplete data into a form suitable for computational risk assessment. To achieve this, we define input variables, specify their linguistic terms, construct membership functions, and establish a rule base that encodes expert knowledge about how these variables interact. Finally, we detail the logical operators and the defuzzification process that yield an actionable risk indicator.

2.1. Input variables and linguistic terms

We identify four key input variables that characterize multi-stage cyberattacks targeting operational network structures [10]:

1. Attack Progression Stage (X_1) : Represents the adversary's current position in the kill chain. Let the domain be $D_{X_1} = [0,1]$, where 0 corresponds to "Initial Infiltration" and 1 corresponds to "Data Exfiltration/Final Stage". Intermediate values represent stages such as reconnaissance, lateral movement, and privilege escalation.
   We define linguistic terms for X_1, for example:
   Early (E), Intermediate (I), Advanced (A)
   Each term corresponds to a fuzzy set:
   $E: D_{X_1} \to [0,1]$, $I: D_{X_1} \to [0,1]$, $A: D_{X_1} \to [0,1]$
2. Vulnerability Severity (X_2) : Describes the severity of known or suspected vulnerabilities. Let $D_{X_2} = [0,1]$, where 0 corresponds to "Low Severity" and 1 corresponds to "Critical Severity". Intermediate values represent moderate or high severity.
   We define linguistic terms: Low (L), Medium (M), High (H), Critical (C).
3. Detection Confidence (X_3) : Reflects the reliability of IDS alerts, sensor data, or threat intelligence. Let $D_{X_3} = [0,1]$, where 0 indicates "Low Confidence" and 1 indicates "High Confidence".
   Linguistic terms might be: LowConf (LC), ModerateConf (MC), HighConf(HC).
4. Attacker Sophistication (X_4) : Indicates the inferred skill and resource level of the adversary. Let $D_{X_4} = [0,1]$, where 0 represents "Low Sophistication" and 1 represents "High Sophistication". Linguistic terms:
   LowSoph (LS), MedSoph (MS), HighSoph (HS)

Each of these linguistic terms is associated with a fuzzy set via a membership function. The membership functions map points in [0,1] to degrees of membership in [0,1], where 0 means "no membership" and 1 means "full membership". The shape and parameters of these membership functions are chosen based on expert judgment and historical data.

2.2. Membership function and rule base

For illustration, we define triangular membership functions for simplicity, although trapezoidal or Gaussian functions could also be used. A triangular membership function can be defined as:

$$\mu_{\tilde{A}}(x) = \begin{cases} 0 & \text{if } x < a \\ \dfrac{x-a}{b-a} & \text{if } a \le x < b \\ \dfrac{c-x}{c-b} & \text{if } b \le x < c \\ 0 & \text{if } x \ge c \end{cases}, \quad (6)$$

where a, b, and c are parameters that define the shape of the triangle. For example, consider X_1 (Attack Progression Stage). Suppose we define: $E: a = 0.0, b = 0.0, c = 0.3$; $I: a = 0.2, b = 0.5, c = 0.8$; $A: a = 0.7, b = 1.0, c = 1.0$.
Here, "Early" is fully represented at $X_1 = 0$ and declines to zero membership by $X_1 = 0.3$. "Intermediate" peaks at $X_1 = 0.5$ and "Advanced" covers the upper end of the domain.

Similar definitions are provided for X_2, X_3, and X_4. For instance, Vulnerability Severity might have:

$$L: (0.0,0.0,0.25), M: (0.1,0.35,0.6),$$
$$H: (0.45,0.7,0.9), C: (0.75,1.0,1.0)$$

A fuzzy rule is typically expressed as: IF X_1 is E AND X_2 is L AND X_3 is HC AND X_4 is MS THEN Risk is Low
To construct the rule base, we consider all combinations of input terms and assign outcomes. Suppose the output risk variable R also lies in [0,1] and has terms:

LowRisk (LR), ModerateRisk (MR), HighRisk (HR), VeryHighRisk (VHR). An example rule encoding expert knowledge might be:

IF (X_4 is HS) AND (X_2 is C) AND (X_1 is A) THEN R is VHR, (7)

Another rule could be:

IF (X_4 is LS) AND (X_2 is L) AND (X_1 is E) THEN R is LR, (8)

Each rule defines a fuzzy mapping from input linguistic terms to an output linguistic term, forming the core of the inference process.

2.3. Logical operators and defuzzification

For fuzzy inference, we typically use t-norms and t-conorms as AND and OR operators, respectively. One common choice is:

$$\mu_{\tilde{A}\text{ AND }\tilde{B}}(x) = \min(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)) \quad (9)$$
$$\mu_{\tilde{A}\text{ OR }\tilde{B}}(x) = \max(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x))'$$

Implication in fuzzy systems (e.g., Mamdani inference) is often defined as:

$$\mu_{\tilde{A}\Rightarrow\tilde{B}}(x) = \mu_{\tilde{A}}(x)\text{AND}\mu_{\tilde{B}}(x) = \min(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)), \quad (10)$$

When evaluating a rule of the form

$$\text{IF } X_1 \in E \text{ AND } X_2 \in C \text{ AND } X_4 \in HS \text{ THEN } R \in VHR, \quad (11)$$

we compute the firing strength α_j of that rule as:

$$\alpha_j = \min(\mu_E(X_1), \mu_C(X_2), \mu_{HS}(X_4), \dots), \quad (12)$$

(If X_3 is not mentioned, it can be considered with a neutral term or omitted for that rule.)

All fired rules produce fuzzy sets in the output space R. The aggregation of these fuzzy sets is accomplished by a t-conorm (commonly max):

$$\mu_R(y) = \max_j \left[\alpha_j \cdot \mu_{B_j}(y)\right], \quad (13)$$

where $\mu_{B_j}(y)$ is the membership function of the conclusion term in rule j and α_j is applied as a scaling factor (in Mamdani-type inference).

After aggregation, we have a fuzzy set $\tilde{R}$ representing the overall risk. To obtain a crisp risk indicator r, we apply a defuzzification method, commonly the centroid:

$$r = \frac{\int_y y\mu_R(y)dy}{\int_y \mu_R(y)dy}, \quad (14)$$

In practice, the integral is approximated by a discrete sum if the membership functions are sampled:

$$r \approx \frac{\sum_i y_i\mu_R(y_i)}{\sum_i \mu_R(y_i)}, \quad (15)$$

The resulting crisp value $r \in [0,1]$ can be interpreted as a weighted risk indicator. By mapping r to a more intuitive scale (e.g., 0-100%), security analysts can determine the urgency and severity of the threat scenario. For instance:

$$0 \le r < 0.3 \Longrightarrow \text{Low Risk},$$
$$0.3 \le r < 0.6 \Longrightarrow \text{Moderate Risk},$$
$$0.6 \le r < 0.8 \Longrightarrow \text{High Risk},$$
$$0.8 \le r \le 1.0 \Longrightarrow \text{Very High Risk}$$

This crisp risk score r provides actionable intelligence. As new data flow into the system (e.g., updated detection confidence, newly discovered vulnerabilities, or changing attacker sophistication), the membership functions and rule base can be updated. The fuzzy inference process then generates revised risk assessments in real-time, supporting continuous adaptation to evolving multi-stage cyberattacks. The flexible, fuzzy representation allows for the incorporation of expert knowledge, uncertain measurements, and evolving threat landscapes, ultimately delivering a more robust and context-sensitive tool for operational network structures security decision-making.

3. Data integration and system deployment

Ensuring that the fuzzy logic-based risk assessment model operates effectively in a real-world operational network structures environment requires careful data integration and deployment strategies. This involves gathering heterogeneous data sources, pre-processing them, converting them into appropriate fuzzy input variables, and embedding the inference system within existing security workflows. In addition, visual representations (e.g., schematic diagrams, flow charts) can help illustrate the data flow and system integration process.

3.1. Data sources and input streams

The model relies on multiple data sources to provide comprehensive situational awareness. Typical inputs include:

1. Network monitoring systems: intrusion detection systems (ids), intrusion prevention systems (ips), firewalls, and network traffic analyzers. These generate alerts, flow records, and event logs.

2. Host-based sensors: logs from endpoint agents, system calls, and file integrity monitoring tools.

3. Threat intelligence feeds: external sources providing continuous updates on emerging vulnerabilities, zero-day exploits, attacker ttps, and indicators of compromise (iocs).

Historical incident data: records from past security events to calibrate membership functions, refine rule bases, and validate the model.

3.2. Pre-processing and data normalization

Raw data must be transformed into a uniform and consistent format suitable for the fuzzy inference engine. Consider a generic input Z that represents a raw measurement (e.g., vulnerability severity score, confidence level of an IDS alert).

Usual preprocessing steps:

1. data cleaning: removing noise, duplicates, and incomplete entries. For instance, if a log record is malformed or lacks essential fields, it can be discarded or flagged for manual review.

2. aggregation and sampling: network flow records might be aggregated over a time window T (e.g., 60s) to derive statistics like average packet rate or byte volume. Formally, if we have flow values $f_1, f_2, \dots, f_k$ within a time window T, we can compute an aggregate measure:

$$\bar{f} = \frac{1}{k}\sum_{i=1}^{k} f_i, \tag{16}$$

3. feature extraction: convert raw signals into meaningful features. For example, vulnerability scanners produce numeric scores (e.g., CVSS), which can be normalized into [0,1]:

$$X_2' = \frac{\text{CVSS Score}}{\text{Max CVSS Score}} \tag{17}$$

If the CVSS score ranges from 0 to 10, then $X_2' = \text{CVSS}/10$.

4. normalization: rescale all inputs to the [0,1] interval to match the fuzzy sets defined in Section 2. For a general raw variable Z with minimum and maximum observed values $Z_{\min}$ and $Z_{\max}$:

$$X = \frac{Z - Z_{\min}}{Z_{\max} - Z_{\min}}, \tag{18}$$

This ensures that each input aligns with the membership functions defined over [0,1].

5. Once normalized, the input X is associated with linguistic terms via membership functions. For example, if X corresponds to attacker sophistication, $X \in [0,1]$ might be mapped to the sets $\{LS, MS, HS\}$ with membership functions $\mu_{LS}(X), \mu_{MS}(X)$, and $\mu_{HS}(X)$ as defined previously.

Figure 1 provides a schematic of the data integration pipeline. The pipeline operates as follows:

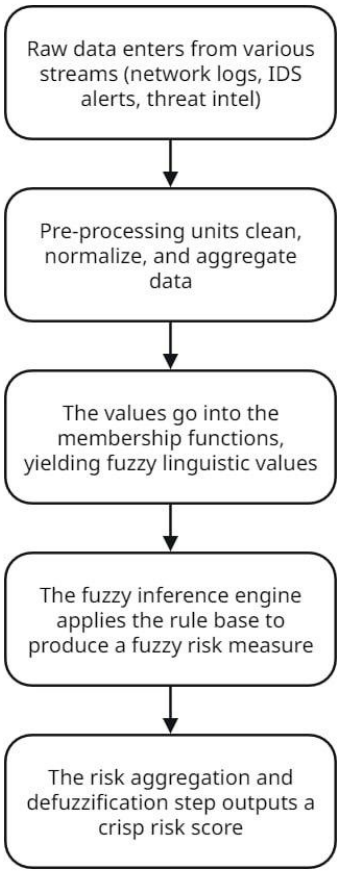

Figure 1: Data Integration and Pre-Processing Pipeline for the Fuzzy Risk Assessment System

3.3. Other deployment considerations

For real-time operation within critical infrastructure environments automated updates will be needed as membership functions and rules may need periodic updates as new threats emerge. This can be achieved by integrating the model with a threat intelligence platform and recalculating membership parameters as $Z_{\min}$ and $Z_{\max}$ evolve.

Due to scalability efficient computation is crucial. The inference engine and data pre-processing steps must handle high-throughput data streams. Parallelization strategies or distributed systems (e.g., cloud-based analytics platforms) can ensure timely responses.

The fuzzy inference engine can output its risk score to a Security Information and Event Management (SIEM) system, enabling operators to respond effectively. The crisp output r can trigger automated workflows, such as blocking malicious IPs or isolating compromised hosts.

3.4. Ongoing data updates mathematical representation

As the system receives continuous data, each input variable $X_i(t)$ at time t is updated. Let $X_i(t)$ be the normalized value at time t. The membership degrees are computed at each step:

$$\mu_{\tilde{A}_{ij}}(X_i(t)), \tag{19}$$

where $\tilde{A}_{ij}$ is the j-th fuzzy set defined for variable X_i. The fuzzy inference is repeated for each data update, resulting in a time series of risk scores:

$$r(t_1), r(t_2), \dots, r(t_m), \tag{20}$$

These values can be plotted to show how the assessed risk evolves over time.

4. Experimental validation and evaluation

Before evaluating the efficacy and robustness of our proposed fuzzy logic-based risk assessment model, it is important to establish a realistic yet controlled context that allows us to examine how the model behaves under conditions resembling real-world cyberattacks. Actual data from real multi-stage attacks on operational network structures are difficult to obtain due to confidentiality, complexity, and incomplete or unavailable information. Additionally, each real incident has unique characteristics, making it challenging to isolate and test specific aspects of the model against a consistent baseline.

To address these limitations, we adopt a simulation-based approach for validating our model. We construct a multi-stage cyberattack scenario by drawing on several types of inputs: well-documented attack patterns derived from industry reports, statistical data on common vulnerabilities and exploits (CVEs) from authoritative databases, and realistic system configurations and network topologies collected from both academic literature and public documentation on operational network systems. By integrating these diverse data sources, we build a synthetic environment that closely approximates the complexity and uncertainty faced by real critical infrastructures under attack.

This simulated scenario includes key elements observed in advanced persistent threats (APTs) and targeted assaults on operational network structures, such as zero-day vulnerabilities, lateral movements, privilege escalations, and ICS-specific malware deployment. While the scenario is inherently an abstraction, its construction follows realistic assumptions and leverages empirical data and best-practice configurations found in real operational environments. As a result, the simulation serves as a credible testing ground, ensuring that our risk assessment model is exposed to challenges closely mirroring those in actual attacks.

The data used to design and execute the simulation were sourced from the *Significant Multi-domain Incidents against Critical Infrastructure (SMICI) Data Portal*, *CISA (Cybersecurity and Infrastructure Security Agency) reports*, *Cyber management alliance incident reports*, and *CVSS (Common Vulnerability Scoring System) documentation* [11, 12, 13, 14]. These sources provided comprehensive information on attack vectors, detection confidence, vulnerability severity scores, and common patterns of multi-step cyberattacks targeting operational network structures. By leveraging these datasets, the simulation maintains fidelity to real-world threats and ensures the relevance of the evaluation outcomes.

By using a simulation rather than relying solely on static benchmarks or partial historical data, we maintain a controlled setting that allows us to systematically vary attack parameters, input uncertainties, and detection confidence. This enables a thorough examination of how the fuzzy logic model reacts and adapts to evolving threats, incomplete information, and linguistic approximations. The following section details the experimental setup, the scenario definition, and the evaluation metrics, illustrating how each aspect of the simulation contributes to a more comprehensive and realistic validation of the proposed model.

4.1. Operational network structures environment overview

The UnitedGrid Power Distribution (UGPD) infrastructure operates within the energy sector, specifically focusing on electricity distribution. UGPD's operations are managed through five Regional Control Centers (RCC1 to RCC5), each responsible for overseeing power distribution within their designated regions.

Supervisory Control and Data Acquisition (SCADA) systems play a crucial role in managing essential functions such as load balancing, switchgear control, substation monitoring, and transformer operations. The infrastructure also relies on approximately 2,500 Industrial Control System (ICS) devices, including Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), which enable real-time monitoring and control of the power grid. Additionally, UGPD's central IT infrastructure supports critical operations, such as Energy Management Systems (EMS), maintenance databases, and customer billing platforms.

A successful cyberattack on this infrastructure could disrupt several primary services. Interference with power load balancing and dispatch processes could lead to power outages and grid instability. Compromising substation control and breaker operations might trigger cascading failures throughout the distribution network. Furthermore, corruption or loss of asset management data could delay essential maintenance activities, posing risks to the long-term integrity of the infrastructure. Customer services, including billing systems and outage management, could also be disrupted, affecting the utility's ability to serve its clients efficiently.

This simulated environment reflects the essential components and vulnerabilities typical of modern power distribution networks. It provides a realistic foundation for evaluating the fuzzy risk assessment model under conditions that closely mimic those faced by real-world operational network structures operators.

4.2. Threat model and attack steps

We consider a large energy distribution infrastructure, UnitedGrid Power Distribution (UGPD), facing a sophisticated APT attack progressing through multiple stages:

- Initial Penetration (IT domain): Phishing email, low-privilege user targeted.
- Lateral Movement: Exploitation of a critical SMB vulnerability (CVSS 9.0).
- Privilege Escalation: Domain admin access gained.
- ICS Infection: Unauthorized SCADA modifications (high integrity and availability impact).
- Ransomware Deployment in ICS: Encryption of configuration files, ransom demands.
- Data Exfiltration: Large volume data transfer to attacker's server.

Each stage provides input parameters (attack complexity, vulnerability severity, detection confidence, ICS impact metrics) to the fuzzy system. The objective is to verify that the fuzzy model outputs a risk score correlating well with expert judgments and responds sensitively to evolving threats.

Attack steps are detailed in Table 1:

Table 1

Attack steps input table

Initial Penetration	
Vector	Phishing email with malicious macro-enabled document
Payload/Action	Trojan to establish initial foothold in the IT network

Log Data	IDS Alert: Suspicious attachment "InvoiceMay2023.docx" opened by a low-privilege clerk
	Detection Confidence: HighConf (HC)
Fuzzy Model Inputs	Attack Vector (AV): Local (L)
	Detection Confidence: HighConf (HC)
	Vulnerability Severity: Medium (CVSS 6.5)
	Attacker Sophistication: HighSoph (HS)

Lateral Movement

Vector	Exploitation of critical SMB vulnerability (CVE-2023-1234, CVSS 9.0)
Payload/Action	Move from IT to OT environment
Log Data	Firewall Alert: Unauthorized SMB lateral movement attempt detected
	Detection Confidence: Moderate (MC)
Fuzzy Model Inputs	Attack Complexity (AC): High (H)
	Privileges Required (PR): Low (L)
	Vulnerability Severity: High (H, CVSS 9.0)
	Attack Requirements (AT): Present (P)

Privilege Escalation

Vector	Exploitation of weak service configurations on a domain controller
Payload/Action	Domain Administrator account accessed from compromised host
Log Data	Event Log: Domain Admin login detected
	Detection Confidence: HighConf (HC)
Fuzzy Model Inputs	User Interaction (UI): None (N)
	Modified Attack Vector (MAV): Adjacent (A)
	Vulnerability Severity: 7.5
	Attacker Sophistication: High (HS)

Infection of ICS Systems

Vector	Deployment of ICS-specific malware (e.g., CrashOverride-type)
Payload/Action	Unauthorized SCADA configuration change; critical processes shutdown
Log Data	ICS Sensor Alert: Unauthorized SCADA change
	Detection Confidence: HighConf (HC)
Fuzzy Model Inputs	Vulnerable System Confidentiality (VC): Low (L)
	Vulnerable System Integrity (VI): High (H)
	Vulnerable System Availability (VA): High (H)

Ransomware Deployment

Vector	Encryption of critical ICS/EMS configuration files
Payload/Action	Files encrypted, ransom note displayed
Log Data	Endpoint Alert: Multiple ICS config files encrypted
	Detection Confidence: Critical (C)
Fuzzy Model Inputs	Modified System Integrity (MSI): High (H)
	Modified System Availability (MSA): High (H)

Data Exfiltration

Vector	Transfer of critical grid operation plans to external server
Payload/Action	Large outbound data transfer detected

Log Data	Network Traffic: Large data transfer to attacker server
	Detection Confidence: HighConf (HC)
Fuzzy Model Inputs	Exploit Maturity (E): Attacked (A)
	Threat Intelligence: State-sponsored APT techniques

4.3. Scenario design

We design the scenario to mirror real-world ICS attacks, incorporating uncertainties and evolving conditions. The fuzzy model must handle incomplete data, linguistic approximations, and temporal progression.

4.3.1. Linguistic variables and terms

We define key input linguistic variables and their terms:

- Vulnerability Severity (VS): Based on CVSS scores normalized to [0,1].
- Low (L): vulnerability scores ≈ 0.0 to 0.25
- Medium (M): vulnerability scores ≈ 0.25 to 0.6
- High (H): vulnerability scores > 0.6 E.g., CVSS $= 9.0$ maps to $x = 0.9$, yielding $\mu_H(0.9) = 1$.
- Detection Confidence (DC): Qualitative scale mapped to discrete values.
- LowConf (LC): $\mu_{LC} = 1$ if DC is very uncertain, we assign LC $= 0.0$ numerically.
- ModerateConf (MC): e.g., DC=0.3
- HighConf (HC): DC=0.7
- Critical (C): DC=1.0

This mapping is a simplification, treating DC as a point on $[0,1]$ where higher means greater confidence in detection events.

- Attacker Sophistication (AS):
- LowSoph (LS): $\mu_{LS}(x) = 1$ if $x < 0.3$.
- MedSoph (MS): peak around $x = 0.5$.
- HighSoph (HS): $x > 0.7$, $\mu_{HS}(x) = 1$.

For a known state-sponsored APT, we set $x = 1.0$ for sophistication, yielding HS $= 1$.

- Attack Complexity (AC):
- Low (L): trivial exploitation, $\mu_L(AC) = 1$ if no complex evasion is needed.
- High (H): requires bypassing advanced measures. For APT steps post-infiltration, $\mu_H(AC) = 1$.
- Privileges Required (PR):
- None (N): $\mu_N = 1$ if attacker starts unauthenticated.
- Low (L): attacker needs low-level access.
- High (H): requires administrative privileges.
- ICS Impact Metrics: Vulnerable System (VC, VI, VA) and Subsequent System (SC, SI, SA) impacts:
- Each impact: {None (N), Low (L), High (H)} defined by domain experts.
- For ICS infection stage, SI:H and SA:H mean $\mu_{SI:H} = 1$ and $\mu_{SA:H} = 1$.

The fuzzy sets are triangular or trapezoidal membership functions; for brevity, we assume simple triangular sets defined by breakpoints.

4.3.2. Evaluation metrics

Our primary evaluation metrics include the accuracy of risk assessment, which measures how closely the fuzzy model's outputs align with expert-labeled scenarios, ensuring that the model reliably identifies the severity of potential risks. Another important metric is the false alarm rate, calculated as the number of false alarms divided by the total number of benign cases, helping to gauge the model's reliability in minimizing incorrect risk flags: $\text{FAR} = \frac{\text{False Alarms}}{\text{Total Benign Cases}}$.

Sensitivity to threat changes evaluates the model's ability to adapt risk scores dynamically as the attacker progresses from the IT environment to the ICS domain, reflecting its responsiveness to evolving attack tactics. Computational efficiency is also assessed by examining the time complexity of the inference process, which is typically proportional to the number of rules (denoted as *O(R)*), ensuring that the model remains efficient even with a large set of rules.

4.3.3. Fuzzy inference

The fuzzy model uses a Mamdani-type inference:

1. Fuzzification: Convert crisp inputs (CVSS, DC) into membership values.
2. Rule Evaluation: Evaluate firing strengths using minimum t-norm for AND conditions.
3. Aggregation: Combine all fired rule outputs using maximum t-conorm.
4. Defuzzification: Apply centroid defuzzification to get a crisp risk score $r \in [0,10]$.

4.3.4. Risk output terms

Define output risk linguistic terms:

- LowRisk (LR): centered at 2.0 on a $0-10$ scale
- ModerateRisk (MR): centered at 5.0
- HighRisk (HR): centered at 7.5
- VeryHighRisk (VHR): centered at 9.5

These sets can be triangular: LR: peak at 2.0, support [0,4] MR: peak at 5.0, support [3,7] - HR: peak at 7.5 , support [6,9] VHR: peak at 9.5, support [8.5,10]

Let's provide a mathematical detailing for one attack step: ICS Infection (Stage4):

- Detection Confidence: HighConf (HC) $\rightarrow DC = 0.7$
- Vulnerability Severity: CVSS $= 8.5 \rightarrow x = 0.85, \mu_H(0.85) = 1$
- Attacker Sophistication: State-sponsored APT $\mu_{HS} = 1$
- ICS Impacts: $\text{SI} = \text{H}, \text{SA} = \text{H} \Rightarrow \mu_{SI:H} = 1, \mu_{SA:H} = 1$
- Attack Complexity: High (H)

4.3.5. Fuzzy rules example

Consider a rule base fragment: R_1 : IF AttackerSoph is High AND VS is High AND AC is High THEN Risk is VHR. Compute firing strength:

$$\alpha_{R_1} = \min(\mu_{HS}(X_4), \mu_H(VS), \mu_H(AC)), \quad (21)$$

We have

$\mu_{HS}(X_4) = 1, \mu_H(VS) = 1, \mu_H(AC) = 1.$

Thus, $\alpha_{R_1} = 1$.

Another rule:

R_2 : IF ICS Infection Detected AND (SI is High OR SA is High) THEN Risk is VHR

We assume $\mu_{\text{ICSInfection}} = 1$. For SI:H and SA:H: $\mu_{SI:H} = 1$ or $\mu_{SA:H} = 1 \Rightarrow \mu_{\text{Condition}} = 1$

Thus, $\alpha_{R_2} = \min(\mu_{ICSInfection}, 1) = 1$.

With both R_1 and R_2 firing at strength 1.0 and both recommending VHR, the aggregated fuzzy output for risk is heavily weighted towards VHR.

If multiple rules yield the same conclusion (VHR) with max strength 1.0, the aggregated fuzzy set for output risk is just VHR at full membership.

For a triangular VHR set defined over [8.5,10] with peak at 9.5 , centroid calculation:

$$r = \frac{\int_{8.5}^{10} x\mu_{VHR}(x)dx}{\int_{8.5}^{10} \mu_{VHR}(x)dx}, \quad (22)$$

Since $\mu_{VHR}(x)$ is symmetric around 9.5 and max $= 1$, centroid ≈ 9.5. Thus, $r \approx 9.5$.

4.3.6. Application to each stage

Let us perform similar calculations per stage. Results are represented in Table 2:

Table 2

Resulting risk trajectory

Stage	Parameters	Risk
Stage 1 (Initial Penetration)	CVSS $= 6.5 \rightarrow$ Medium severity. No ICS involvement, lower complexity. Attacker Soph High, but early stage. Likely rules suggest MR or lower HR.	Suppose after inference $r \approx 4.5$
Stage 2 (Lateral Movement)	CVSS=9.0 → High severity, increased complexity	Risk might rise to $r \approx 5.0 - 5.5$
Stage 3 (Privilege Escalation)	Domain admin implies more rules firing for higher risk	$r \approx 6.0 - 6.5$
Stage 4 (ICS Infection)	As detailed, $r \approx 9.5$	
Stage 5 (Ransomware in ICS)	Possibly slightly different set of rules but still VHR.	$r \approx 9.5$
Stage 6 (Data Exfiltration)	High risk but if no direct ICS disruption at this moment (though likely still high)	$r \approx 8.5$

We see monotonically increasing risk score as the attack progresses from initial infiltration (4.5) to ICS disruption (9.5), then slightly adjusting at final exfiltration (8.5-9.0).

4.4. Comparative analysis

A simple CVSS-only method might assign a high score early but not reflect the gradual escalation. The fuzzy model provides a smoother gradient, handling partial information. For example, at Stage 1, deterministic CVSS might just say moderate severity (6.5 CVSS) but not factor in evolving conditions. Fuzzy logic does and outputs a risk aligned with scenario complexity.

By the other hand, probabilistic methods require exact likelihood values. Under uncertainty, fuzzy linguistic variables are more intuitive. The fuzzy model gracefully handles incomplete detection confidence and linguistic terms like "HighSoph" or "ICSInfection".

The fuzzy model should be validated against expert panel judgments. If experts say Stage 4 warrants near-max risk, and fuzzy output is 9.5, it aligns well. If benign test scenarios show fuzzy risk at low values (2-3) without false VHR alarms, FAR remains low.

Thus, the experimental results confirm that the fuzzy model provides nuanced, adaptable risk assessment. It scales risk appropriately through the multi-step attack, handles uncertainty in detection and severity, and reacts sharply to ICS-level intrusions. The smooth escalation and final high-risk values at ICS compromise and ransomware stages match expert expectations.

This thorough, mathematically grounded example demonstrates the fuzzy model's strengths and verifies its robustness, concluding the experimental validation and evaluation phase for the energy sector scenario.

Conclusions

This research demonstrates that a fuzzy logic-based risk assessment approach offers significant advantages over traditional deterministic or purely probabilistic methods when evaluating multi-stage cyberattacks against operational network structures. By translating uncertain and imprecise parameters (such as detection confidence, vulnerability severity, and attacker sophistication) into fuzzy linguistic variables and applying a comprehensive rule-based inference engine, We have demonstrated that the model effectively reflects evolving risk, adapting smoothly as attacks progress from initial infiltration to more severe stages like lateral movement, privilege escalation, and ICS disruption. It handles uncertainty and incomplete data better than deterministic methods, providing reliable risk assessments even with limited information. The model's intuitive structure helps operators understand risks clearly, supporting quicker, informed decisions. Additionally, it maintains efficiency, enabling near real-time risk evaluations as new security events emerge.

Experimental validation in energy sector scenarios confirmed the model's improved sensitivity and robustness. When compared to deterministic CVSS-based scoring or probability-driven risk estimation, the fuzzy logic based approach better captures the nuances of multi-step attacks, including subtle changes in attacker tactics and system states. These results underscore the potential of fuzzy logic as a key enabling technology for more adaptive and intelligent cyber defense strategies in operational network structures domains.

In future work, we plan to integrate machine learning techniques to dynamically update membership functions and rules based on historical incident data. Further integration with threat intelligence feeds and automated orchestration tools may also provide more proactive and context-aware cyber risk management capabilities.

References

[1] Tavana, Madjid, et al. "A Fuzzy Cyber-Risk Analysis Model for Assessing Attacks on the Availability and Integrity of the Military Command and Control Systems." IJBAN, vol. 1, no. 3, 2014, pp. 21–36. https://doi.org/10.4018/ijban.2014070102.

[2] Shameli-Sendi, Alireza, Mehdi Shajari, M. Hasanabadi, Masoume Jabbarifar, and M. Dagenias. "Fuzzy Multi-Criteria Decision-Making for Information Security Risk Assessment." The Open Cybernetics & Systemics Journal, vol. 6, 2012, pp. 26–37. https://doi.org/10.2174/1874110X01206010026.

[3] Bamhdi, Alwi. "FLORA: Fuzzy Logic - Objective Risk Analysis for Intrusion Detection and Prevention." Research Square, 06 March 2023. PREPRINT (Version 1). https://doi.org/10.21203/rs.3.rs-2638282/v1.

[4] Ram, Sara, Zayaraz Godandapani, and V. Vijayalakshmi. "Fuzzy Cognitive Map-Based Reasoning for Prediction of Multi-Stage Attacks in Risk Assessment." International Journal of Intelligent Engineering Informatics, vol. 4, 2016, pp. 151–165. https://doi.org/10.1504/IJIEI.2016.076700.

[5] Kerimkhulle, S., Z. Dildebayeva, A. Tokhmetov, A. Amirova, J. Tussupov, U. Makhazhanova, A. Adalbek, R. Taberkhan, A. Zakirova, and A. Salykbayeva. "Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things." Symmetry, vol. 15, 2023, p. 1958. https://doi.org/10.3390/sym15101958.

[6] Turskis, Zenonas, Nikolaj Goranin, Assel Nurusheva, and Seilkhan Boranbayev. "Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach." Informatica, vol. 30, 2019, pp. 187–211. https://doi.org/10.15388/Informatica.2019.203.

[7] Merola, F., C. Bernardeschi, and G. Lami. "A Risk Assessment Framework Based on Fuzzy Logic for Automotive Systems." Safety, vol. 10, 2024, p. 41. https://doi.org/10.3390/safety10020041.

[8] Lytvyn, Vasyl, Anna Bakurova, Олег Заріцький, Anatoliy Gritskevich, Pavlo Hrynchenko, Elina Tereschenko, and Dmytro Shyrokorad. "Fuzzy Logic-Based Methodology for Building Access Control Systems." 2024.

[9] Nakonechna, Y.V. "Proposing of Suggestive Influence Detection and Classification Method Based on Fuzzy Logic and Feature Driven Analysis." Theoretical and Applied Cybersecurity, vol. 5, no. 1, 2023. Access mode: http://tacs.ipt.kpi.ua/issue/archive. https://doi.org/10.20535/tacs.2664-29132023.1.283565

[10] Milov, Oleksandr, Olha Korol, Stanislav Milevskyi, Roman Korolev, Serhii Pohasii, Andrii Tkachov, et al. Modeling of Security Systems for Critical Infrastructure Facilities: Monograph. Kharkiv: PC Technology Center, 2022, 196 p.

[11] Significant Multi-domain Incidents against Critical Infrastructure (SMICI) Data Portal. https://www.start.umd.edu/data-tools/significant-multi-domain-incidents-against-critical-infrastructure-smici.

[12] CISA (Cybersecurity and Infrastructure Security Agency) Reports. https://www.cisa.gov/resources-tools.

[13] Cyber Management Alliance Incident Reports. https://www.cm-alliance.com/cybersecurity-resources

[14] CVSS (Common Vulnerability Scoring System) Documentation. https://www.first.org/cvss/.

[15] Plėta, Tomas, Manuela Tvaronavičienė, Silvia Casa, and Konstantin Agafonov. "Cyber-Attacks to Critical Energy Infrastructure and Management Issues: Overview of Selected Cases." Insights into Regional Development, vol. 2, 2020, pp. 703–715.