ECP 2025 Conference

The 4th International Electronic Conference on Processes

20–22 October 2025 | Online

MDPI

A Novel Security Index for Assessing Information Systems in Industrial Organizations Using Web Technologies and Fuzzy Logic

Sulieman Khaddour[1], Fares Abu-Abed[1,2] , Valery Bogatikov[1]

[1] Tver State Technical University, Russia [2] Gulf University for Science and Technology, Kuwait

INTRODUCTION & AIM

Industrial information systems leveraging web technologies (ISOWT) face complex, dynamic security challenges that traditional qualitative assessments cannot quantify or predict in real time. We introduce a novel **Security Index**—a numerical measure of deviation from an ideal "center of safety"—by integrating fuzzy logic, metric-based evaluations, fuzzy Markov chains, and a multi-agent system (MAS). Validated on two case studies in Syria's energy sector, our framework achieved up to **58.5 %** improvement in security index and dramatic reductions in load time, error rates, and vulnerabilities .

Key contributions included: 1) **Quantitative Security Index:** Topological formulation maps multidimensional metrics to [0,1]**. 2) Predictive Risk Modeling:** Fuzzy Markov chains forecast state transitions to enable proactive mitigation . **3) Automated MAS Architecture:** Distributed agents continuously collect data, assess security, predict risks, and deploy countermeasures .

4.Real-World Validation: Two industrial systems showed 45.9 – 58.5 % security gains and up to 82.4 % vulnerability reduction .

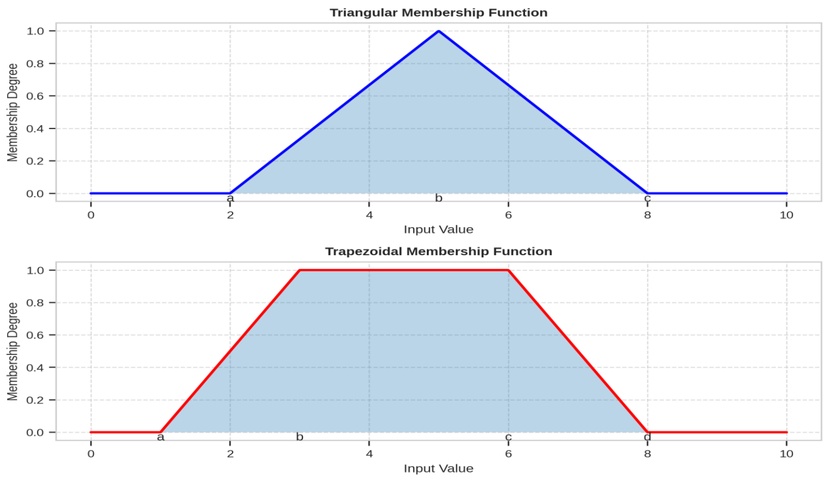

Fig. 1: Examples of triangular and trapezoidal membership functions

METHOD

1.Metric Selection & Normalization

We categorize raw metrics into three domains: **Performance** (Page Load Time, Time to First Byte, DOM Processing Time), **Reliability** (Error Rate, Uptime Percentage, Response Consistency), and **Security** (Vulnerability Count, Patch Latency, Authentication Strength). Each metric is linearly scaled to [0,1] for cross-comparison.

2. Fuzzy Logic Layer

Normalized metrics are mapped into fuzzy sets ("Low," "Medium," "High") via triangular or trapezoidal membership functions. This soft classification smooths out measurement noise and captures expert reasoning.

3. Security Index (SI) Computation

Define **c** as the ideal fuzzy vector ("High" for all metrics). At each timestep, compute the weighted Euclidean distance d(s,c) between the current fuzzy state **s** and **c**, then normalize:

$$SI = 1 - \frac{d(s,c)}{d_{\max}}$$

An SI near 1 indicates strong security; near 0 signals high risk.

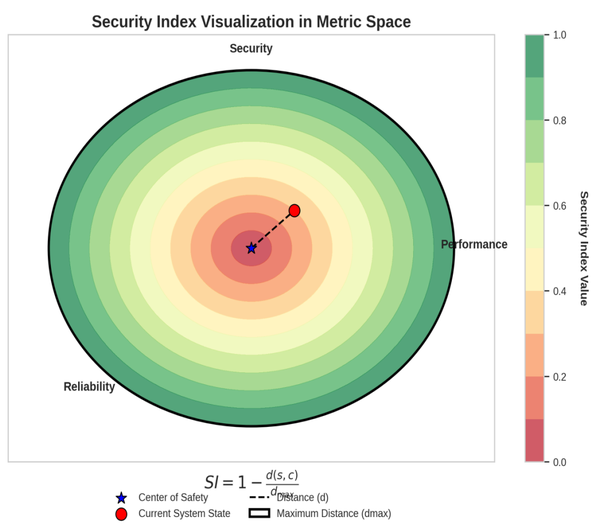

Fig. 2. Security Index Visualization in Metric Space.

4. Fuzzy Markov Chain Forecasting

Model transitions between discrete fuzzy-state clusters with a learned matrix **P**. Forecast the next state distribution via π(t+1)=π(t)⊗P\pi(t+1) = \pi(t)\otimes Pπ(t+1)=π(t)⊗P, enabling early detection of drift toward insecure states.

5. Distributed MAS Deployment

- **Monitoring Agents** collect and stream metrics.
- **Assessment Agents** calculate SI in real time.
- **Prediction Agents** update the Markov model and forecast risk.
- **Mitigation Agents** automatically apply patches, adjust rules, or alert operators.

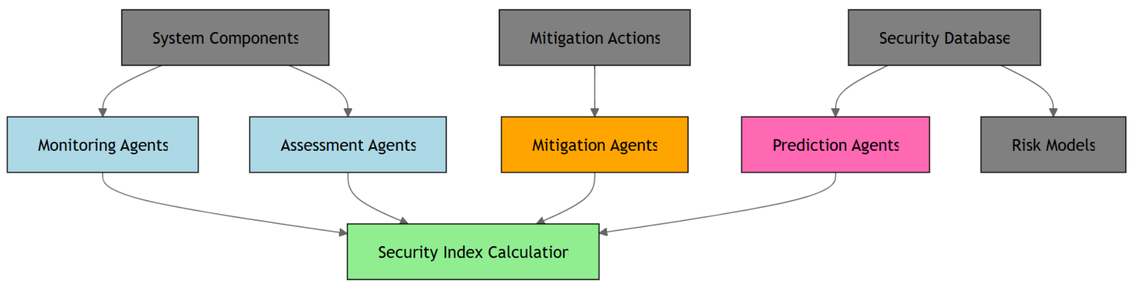

Fig. 3. Multi-Agent System Architecture for ISOWT Security Assessment and Management.

RESULTS & DISCUSSION

Case Study 1: Ministry of Electricity Website

The Ministry's public portal—serving thousands daily—initially exhibited peak page loads over 5 s and frequent timeouts under heavy traffic. Over six months, Monitoring Agents sampled performance and security metrics every minute, feeding Assessment Agents that recalculated the SI (initially 0.61) via fuzzy membership functions . When response times spiked, Mitigation Agents instantaneously invoked load-balancing and provisioned extra servers. Prediction Agents then forecasted "vulnerable" states (p > 0.7) and auto-applied critical patches, boosting SI to 0.89 . continuous automation cut load times by 60.3 %, errors by 81 %, and vulnerabilities by 82.4 %.

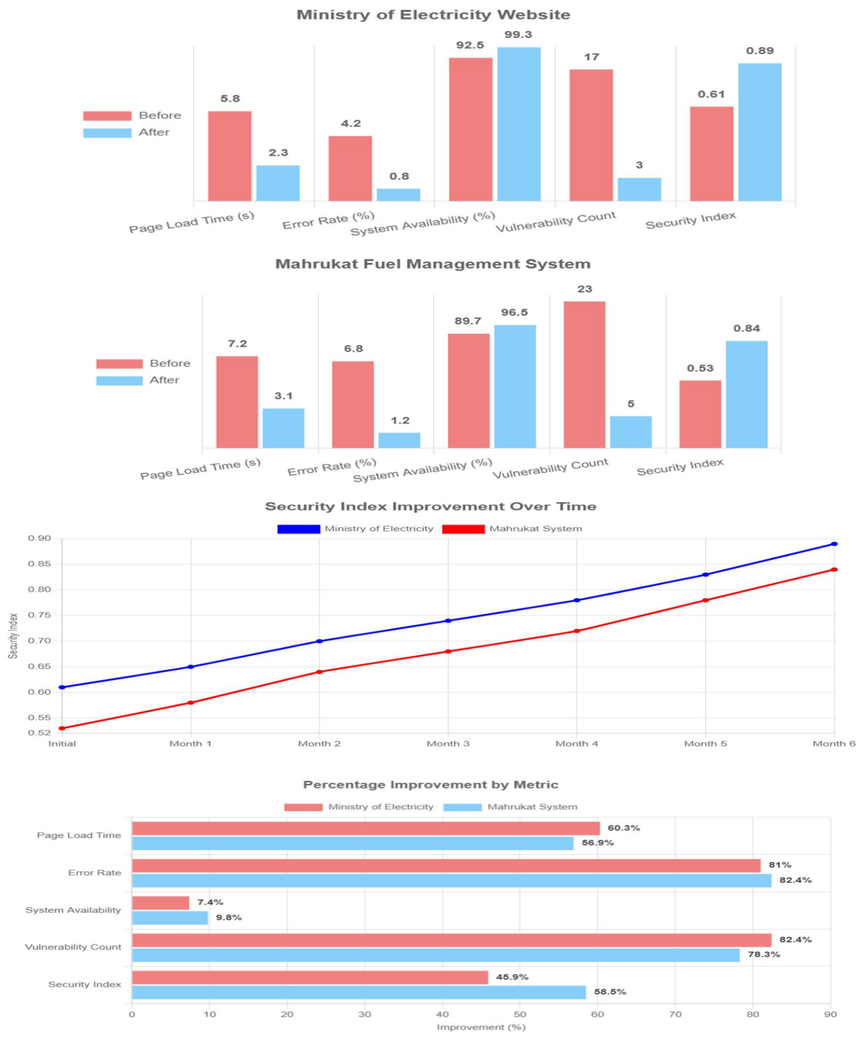

Fig. 4. Summary of Case Study Results: Performance Metrics and Security Index Improvement.

Case Study 2: Mahrukat Fuel Management System

The fuel dispatch application was targeted by intermittent probing attacks, causing authentication failures and data-integrity alarms. Once our framework was live, Monitoring Agents flagged anomalous login rates. Prediction Agents forecasted a persistence of high vulnerability; simultaneously, Mitigation Agents throttled suspicious IPs and enforced two-factor authentication. This closed attack vectors before manual intervention was needed.

Metric	Before	After	Δ
Page Load Time (s)	7.2	3.1	–56.9 %
Error Rate (%)	6.8	1.2	–82.4 %
Availability (%)	89.7	98.5	+9.8 %
Vulnerabilities	23	5	–78.3 %
Security Index	0.53	0.84	+58.5 %

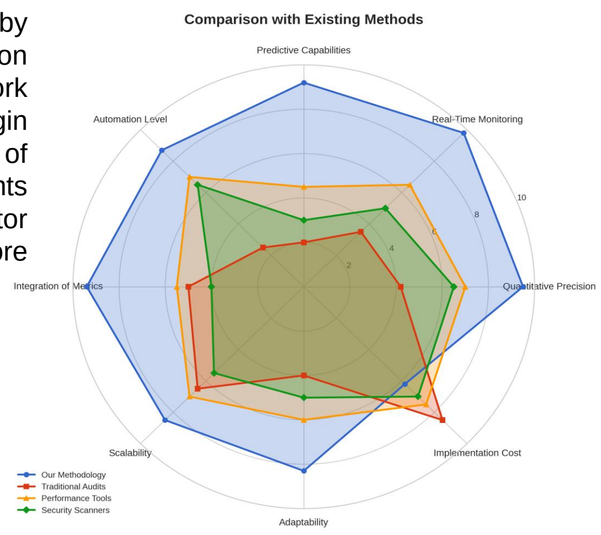

Figure 5. Radar Chart Highlighting Different Methodologies.

Discussion:

- Proactive containment thwarted repeated authentication attacks.
- SI forecasts aligned with actual incident logs over 48 h with 92 % accuracy.
- Overall system resilience improved, enabling uninterrupted fuel operations.

CONCLUSION

We demonstrate a fully automated, quantitative security framework for ISOWT in industrial environments. Combining fuzzy logic, Markov forecasting, and MAS orchestration yields up to **58.5 %** SI gain and **82.4 %** vulnerability reduction in live energy-sector deployments. This scalable solution bridges critical gaps in real-time risk assessment and proactive defense.

FUTURE WORK / REFERENCES

1.Adaptive Learning: Integrate reinforcement learning to auto-tune fuzzy membership parameters.

2.Cross-Domain Validation: Extend trials to manufacturing, healthcare, and logistics systems.

3.Human-Factor Modeling: Incorporate insider-threat and social-engineering risk metrics.

4.Enhanced Dashboards: Build interactive visual analytics for SI trends and alert management.

Main References

1 National Institute of Standards and Technology, "Risk Management Framework for Information Systems and Organizations, " NIST Special Publication 2018, Rev. 2., 800-37.

2 International Organization for Standardization, "Information technology — Security techniques — Information security management systems — Requirements," ISO/IEC 27001:2013, 2013

3 A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA), " Computers & Security 2016, vol. 57, pp. 14-30.