RADemics

Fuzzy Logic and Evolutionary Computation for Adaptive Cyber Risk Management in Dynamic Cloud Environments

Nivedhitha M, Sumitha Manoj, R. Sambath Kumar
SRM, ACS COLLEGE OF ENGINEERING, MANAKULA VINAYAGAR INSTITUTE OF TECHNOLOGY.

Fuzzy Logic and Evolutionary Computation for Adaptive Cyber Risk Management in Dynamic Cloud Environments

[1]Nivedhitha M, Assistant professor, Networking and Communication, SRM, kattankulthur, nivedhim1@srmist.edu.in

[2]Sumitha Manoj, Professor, ECE, ACS college of Engineering Bangalore 560079, sumithamanoj2012@gmail.com

[3]R. Sambath Kumar, Assistant professor, ECE, Manakula vinayagar Institute of Technology, Puducherry, Sambath15031991@gmail.com

Abstract

The increasing complexity and dynamism of cloud environments have introduced significant cybersecurity challenges, necessitating advanced risk assessment methodologies capable of handling uncertainty and evolving threats. Traditional risk management frameworks often rely on static and rule-based mechanisms, which lack adaptability in dynamic cloud ecosystems. To address these limitations, this chapter explores the integration of fuzzy logic and evolutionary computation for adaptive cyber risk management in cloud environments. Fuzzy logic provides a powerful framework for modeling imprecise security parameters and uncertainty in threat landscapes, enabling more flexible and context-aware risk assessment. Meanwhile, evolutionary computation offers an adaptive mechanism to optimize cybersecurity strategies through heuristic learning and intelligent decision-making. The chapter presents a hybrid risk assessment framework that leverages fuzzy inference systems to quantify risk levels and evolutionary algorithms to dynamically optimize security controls, it examines the scalability of fuzzy-evolutionary approaches in large-scale cloud infrastructures and their effectiveness in mitigating real-time cyber threats, such as zero-day attacks, insider threats, and advanced persistent threats. The potential integration of explainable AI (XAI), deep learning, and quantum computing in enhancing fuzzy-based risk assessment models is also discussed. This research contributes to the advancement of self-learning, adaptive cyber defense mechanisms capable of proactively mitigating risks in multi-cloud and hybrid-cloud environments. The proposed framework ensures improved threat intelligence, automated risk prioritization, and enhanced decision transparency, offering a robust solution for next-generation cloud security.

Keywords: Fuzzy Logic, Evolutionary Computation, Cyber Risk Assessment, Adaptive Security, Cloud Computing, Explainable AI

Introduction

The rapid evolution of cloud computing has revolutionized modern digital infrastructures, offering on-demand scalability, cost efficiency, and enhanced computational power. However, the increasing adoption of cloud environments has also introduced significant cybersecurity risks, as dynamic cloud ecosystems are inherently vulnerable to data breaches, insider threats, and

advanced cyberattacks. Traditional risk management frameworks, which rely on predefined security policies and static rule-based approaches, struggle to adapt to the ever-changing nature of cloud threats. The complexity of multi-cloud and hybrid-cloud environments further amplifies security challenges, as organizations must navigate heterogeneous infrastructures with varying security postures. Addressing these limitations requires an adaptive and intelligent cybersecurity framework capable of handling real-time risk assessment and threat mitigation.

Fuzzy logic, a powerful mathematical approach for dealing with uncertainty and imprecise data, offers a promising solution for cyber risk assessment in cloud environments. Unlike binary decision-making models, fuzzy logic enables a gradual and context-aware evaluation of cyber risks, allowing for flexible and adaptive security assessments. By defining security parameters in linguistic terms rather than rigid numerical values, fuzzy logic provides an intuitive framework for quantifying risk severity, threat probabilities, and mitigation priorities. This adaptability is crucial in cloud security, where threat landscapes are constantly evolving, and conventional risk assessment models fail to capture uncertainty and incomplete information. Despite its advantages, standalone fuzzy logic models have limitations in optimization and computational efficiency, making it essential to integrate them with evolutionary computation techniques to enhance their adaptability and performance.

Evolutionary computation, inspired by biological processes such as natural selection and genetic evolution, provides a robust optimization mechanism for cybersecurity strategies. Techniques such as genetic algorithms (GA), particle swarm optimization (PSO), and differential evolution (DE) enable security models to continuously adapt by learning from historical attack patterns and real-time threat intelligence. These algorithms iteratively refine security controls, ensuring that risk mitigation strategies evolve dynamically based on emerging cyber threats. When combined with fuzzy logic, evolutionary computation enhances decision-making efficiency by automatically optimizing fuzzy rule sets and adapting security parameters based on changing attack patterns. The hybridization of fuzzy logic and evolutionary computation creates an intelligent, self-learning cybersecurity framework capable of real-time threat detection, risk quantification, and adaptive response mechanisms in cloud environments.