AI-Driven Secure Networked Control and Fault Detection in Three-Tank Systems Using Fuzzy Logic and Secret Sharing

U. Fatima[(1)] and T. Ahsan[(2)]

[(1)] NED University of Engineering and Technology, Karachi, Pakistan [(2)] (RPTU) Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau Kaiserslautern, Germany

The integration of cloud-based monitoring in cyber-physical systems raises concerns regarding data privacy, security, and robustness against faults. Ensuring secure and reliable fault detection while maintaining control performance remains a key challenge in industrial applications. This work presents an AI-driven and fuzzy logic-based framework for secure networked control and fault detection in a benchmark three-tank system [1] using secret sharing [2].

The system is modeled as a networked control architecture with distributed computation. Sensor outputs and control inputs are partitioned via secret sharing and processed across multiple nodes, ensuring that no single entity accesses complete system information. A residual-based fault detection scheme is employed, where partial residuals are fused to obtain a global residual signal. To improve robustness under uncertainty, a fuzzy logic-based decision mechanism is integrated for adaptive fault evaluation.

System stability is ensured through observer-based design, with eigenvalues placed to guarantee convergence of estimation error in fault-free conditions. Simulation results demonstrate accurate and timely fault detection, while maintaining robustness against disturbances and preventing leakage of sensitive information.

The proposed framework (Figure 1) provides a secure and intelligent control architecture suitable for modern cyber-physical systems, highlighting the integration of fuzzy reasoning and cryptographic techniques for reliable fault detection.

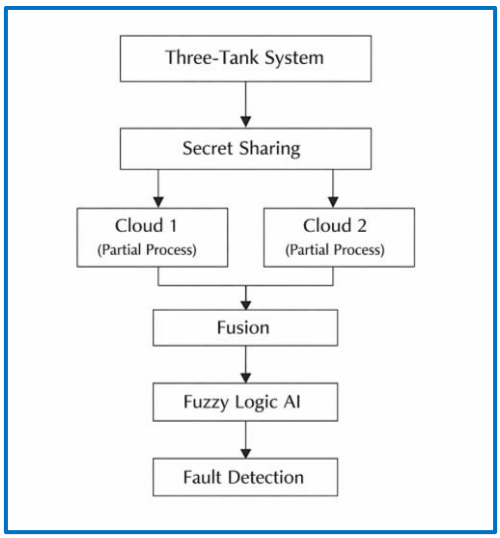

Figure 1: Proposed secure networked control framework

[1] S. Yu et al., Int. J. Control Autom. Syst., 18, 2630–2640, 2020.

[2] J. Sun et al., IFAC, 58(4), 252–257, 2024.