World Academy of Science, Engineering and Technology
International Journal of Civil and Architectural Engineering
Vol:17, No:11, 2023

An Analytical Metric and Process for Critical Infrastructure Architecture System Availability Determination in Distributed Computing Environments under Infrastructure Attack

Authors : Vincent Andrew Cappellano

Abstract : In the early phases of critical infrastructure system design, translating distributed computing requirements to an architecture has risk given the multitude of approaches (e.g., cloud, edge, fog). In many systems, a single requirement for system uptime / availability is used to encompass the system's intended operations. However, when architected systems may perform to those availability requirements only during normal operations and not during component failure, or during outages caused by adversary attacks on critical infrastructure (e.g., physical, cyber). System designers lack a structured method to evaluate availability requirements against candidate system architectures through deep degradation scenarios (i.e., normal ops all the way down to significant damage of communications or physical nodes). This increases risk of poor selection of a candidate architecture due to the absence of insight into true performance for systems that must operate as a piece of critical infrastructure. This research effort proposes a process to analyze critical infrastructure system availability requirements and a candidate set of systems architectures, producing a metric assessing these architectures over a spectrum of degradations to aid in selecting appropriate resilient architectures. To accomplish this effort, a set of simulation and evaluation efforts are undertaken that will process, in an automated way, a set of sample requirements into a set of potential architectures where system functions and capabilities are distributed across nodes. Nodes and links will have specific characteristics and based on sampled requirements, contribute to the overall system functionality, such that as they are impacted/degraded, the impacted functional availability of a system can be determined. A machine learning reinforcement-based agent will structurally impact the nodes, links, and characteristics (e.g., bandwidth, latency) of a given architecture to provide an assessment of system functional uptime/availability under these scenarios. By varying the intensity of the attack and related aspects, we can create a structured method of evaluating the performance of candidate architectures against each other to create a metric rating its resilience to these attack types/strategies. Through multiple simulation iterations, sufficient data will exist to compare this availability metric, and an architectural recommendation against the baseline requirements, in comparison to existing multi-factor computing architectural selection processes. It is intended that this additional data will create an improvement in the matching of resilient critical infrastructure system requirements to the correct architectures and implementations that will support improved operation during times of system degradation due to failures and infrastructure attacks.

Keywords : architecture, resiliency, availability, cyber-attack
Conference Title : ICCISE 2023 : International Conference on Critical Infrastructure Systems Engineering
Conference Location : San Francisco, United States
Conference Dates : November 06-07, 2023