UR-31 An Empirical Study of Thermal Attacks on Edge Platforms

INTRO/ABSTRACT

Cloud-edge systems are vulnerable to thermal attacks as the increased energy consumption may remain undetected, while occurring alongside normal, CPU-intensive applications. The purpose of our research is to study thermal effects on modern edge systems. We also analyze how performance is affected from the increased heat and identify preventative measures. We speculate that due to the technology being a recent innovation, research on cloud-edge devices and thermal attacks is scarce. Other research focuses on server systems rather than edge platforms. In our paper, we use a Raspberry Pi 4 and a CPU-intensive application to represent thermal attacks on cloud-edge systems. We performed several experiments with the Raspberry Pi 4 and used stress-ng, a benchmarking tool available on Linux distributions, to simulate the attacks. The resulting effects displayed drastic increases in the temperature and power consumption. The key impact of our research is to highlight the following risks and mitigation plans: the vulnerability of cloud-edge systems from thermal attacks, the capability for the attacks to go unnoticed, to further the understanding of edge devices as well as the prevention of these attacks.

METHODS

The experiments consisted of executing stress tests on edge devices while recording resource consumption before, during, and after the stress tests. We performed four experiments: comparison of cooling configurations (CPU temperatures), power consumption and temperatures with thermal attacks, temperatures during throttling at various maximum frequencies, CPU frequency and temperature with an AI Benchmark. The tools we used are: Raspberry PI 4B, USB voltage tester, stress-ng (stress test), AI-Benchmark, CPU cooling fan, Raspberry Pi heat sinks, Google Coral, and NVIDIA Jetson TX2

RESULTS

Our research and experiments concluded during throttling edge device performance is negatively affected with the least performance decrease with the lowest maximum frequencies. Power consumption and temperatures increased by 105% and 70% respectively during simulated thermal attacks. Compute-intensive workloads such as the AI Benchmark display a negative correlation between CPU frequency and CPU temperature. After the tests concluded the thermal attack effects were still visible with the device remaining overheated and requiring 240 seconds to return to its normal temperatures.

How well do edge devices perform when they experience excessive temperatures?

Figure 1: Raspberry Pi 4 CPU Throttled Temperatures

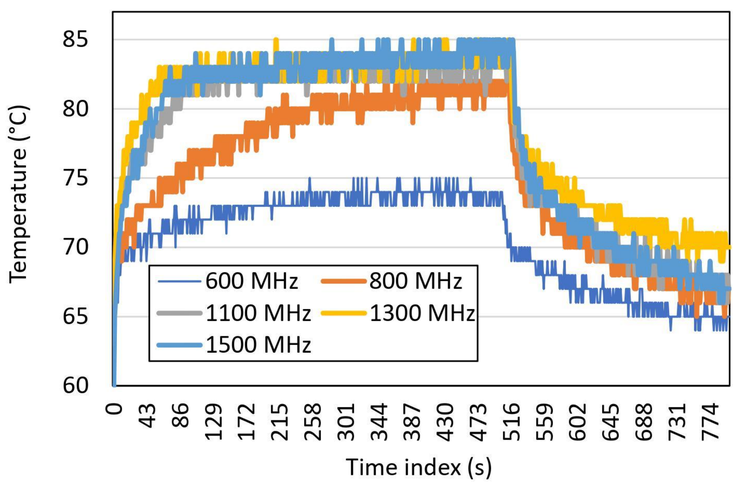

Figure 2: Cooling Strategies Comparison

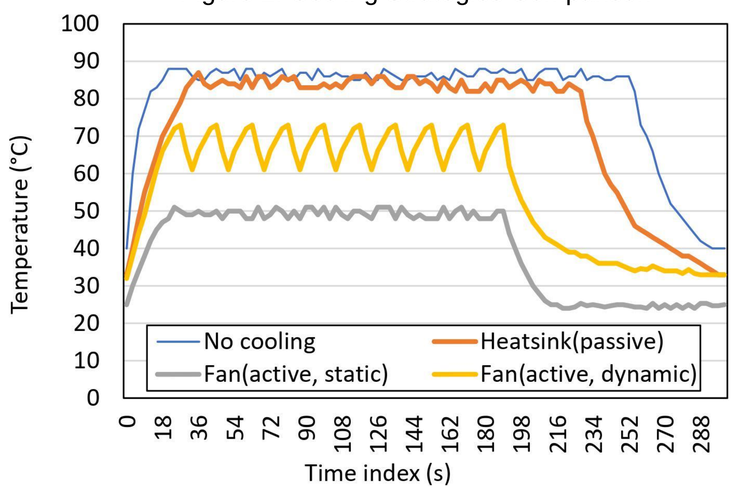

Figure 3: Power and Temperature Trace During Thermal Attack

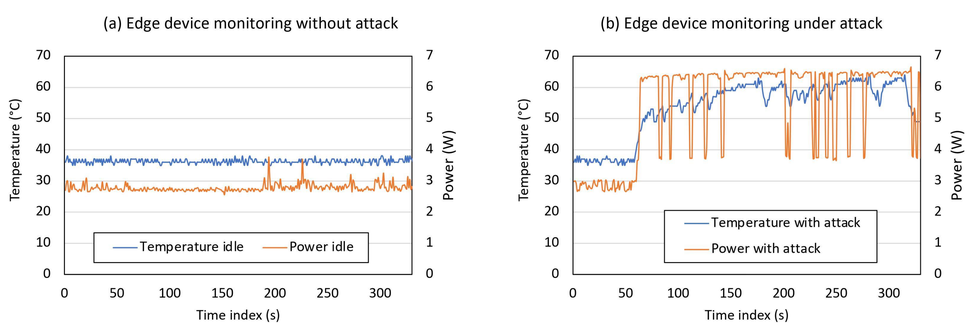

Figure 4: CPU Frequency and Temperature with AI Benchmark

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Author(s): Justin Duchatellier and Tyler Holmes
Advisors(s): Professor Kun Suo