World Academy of Science, Engineering and Technology
International Journal of Civil and Environmental Engineering
Vol:16, No:09, 2022

Risks beyond Cyber in IoT Infrastructure and Services

Authors : Mattias Bergstrom

Abstract : Significance of the Study: This research will provide new insights into the risks with digital embedded infrastructure. Through this research, we will analyze each risk and its potential negation strategies, especially for AI and autonomous automation. Moreover, the analysis that is presented in this paper will convey valuable information for future research that can create more stable, secure, and efficient autonomous systems. To learn and understand the risks, a large IoT system was envisioned, and risks with hardware, tampering, and cyberattacks were collected, researched, and evaluated to create a comprehensive understanding of the potential risks. Potential solutions have then been evaluated on an open source IoT hardware setup. This list shows the identified passive and active risks evaluated in the research. Passive Risks: (1) Hardware failures- Critical Systems relying on high rate data and data quality are growing; SCADA systems for infrastructure are good examples of such systems. (2) Hardware delivers erroneous data- Sensors break, and when they do so, they don’t always go silent; they can keep going, just that the data they deliver is garbage, and if that data is not filtered out, it becomes disruptive noise in the system. (3) Bad Hardware injection- Erroneous generated sensor data can be pumped into a system by malicious actors with the intent to create disruptive noise in critical systems. (4) Data gravity- The weight of the data collected will affect Data-Mobility. (5) Cost inhibitors- Running services that need huge centralized computing is cost inhibiting. Large complex AI can be extremely expensive to run. Active Risks: Denial of Service- It is one of the most simple attacks, where an attacker just overloads the system with bogus requests so that valid requests disappear in the noise. Malware- Malware can be anything from simple viruses to complex botnets created with specific goals, where the creator is stealing computer power and bandwidth from you to attack someone else. Ransomware- It is a kind of malware, but it is so different in its implementation that it is worth its own mention. The goal with these pieces of software is to encrypt your system so that it can only be unlocked with a key that is held for ransom. DNS spoofing- By spoofing DNS calls, valid requests and data dumps can be sent to bad destinations, where the data can be extracted for extortion or to corrupt and re-inject into a running system creating a data echo noise loop. After testing multiple potential solutions. We found that the most prominent solution to these risks was to use a Peer 2 Peer consensus algorithm over a blockchain to validate the data and behavior of the devices (sensors, storage, and computing) in the system. By the devices autonomously policing themselves for deviant behavior, all risks listed above can be negated. In conclusion, an Internet middleware that provides these features would be an easy and secure solution to any future autonomous IoT deployments. As it provides separation from the open Internet, at the same time, it is accessible over the blockchain keys.

Keywords : IoT, security, infrastructure, SCADA, blockchain, AI
Conference Title : ICHSCIR 2022 : International Conference on Homeland Security and Cyber Infrastructure Resilience
Conference Location : San Francisco, United States
Conference Dates : September 27-28, 2022

Open Science Index, Civil and Environmental Engineering Vol:16, No:09, 2022 publications.waset.org/abstracts/150432.pdf