A Comprehensive IoT Security Attacks and Defenses at Sensing Layer: A Survey

Pavithra M, Velivela Gopinath, Chithralekha T

Department of Computer Science, Pondicherry University, Puducherry

ABSTRACT

Internet of Things (IoT) is the evolutionary technology which enforces the smart work force with combination of various technologies like communication technology, information technology, data computing and analysis, embedded systems, sensors and actuators, and other advanced technologies. These technologies are integrated to increase the efficiency and comfort level for the users. But, the evolution of these technologies leads to progress of cybercrime. It develops various attacks, tools and techniques which allow adversary to penetrate into complex and controlled environment. It produces physical and logical damage which may remain untraceable. This work discusses about the attacks at all the layers such as sensing, network and application layers. We have discussed about the importance of security and attacks at the sensing layer in IoT. Based on the analysis, we have proposed a security model using hummingbird encryption incorporated in FPGA which is a resource constrained device. Hummingbird encryption algorithm is a lightweight cryptography which acts as a resistant to attacks in IoT sensing layer. By providing this model, the attacks like node capturing attack, replay attack, eavesdropping attack, sleep deprivation attack, false data injection attack, side channel attack and booting attack are avoided. We can control the attack which happens in other IoT layers to the greater extend.

 Series: AIJR Abstracts; ISBN: 978-81-942709-3-5 (eBook); DOI: 10.21467/abstracts.90