POSTER: A SURVEY OF SECURITY ISSUES FOR IOT INTELLIGENT SYSTEMS

[1]QUENTIN GOSS, [2]KARIM ELISH

Florida Polytechnic University, Lakeland, FL 33805
E-mail: kelish09@gmail.com

Over the course of the last few decades came many innovations in technology that would shape the world as we know it. At first there were computers that were connected only by long cords and the limits of their connection were whatever length of cord the hardware store had at the time. Then, in the 1990's enters the World Wide Web, which kicked off the age of information, where anyone could connect with anyone else – however grand though the early internet was, we lacked necessary computation power and network infrastructure which would eventually be created by the entrepreneurs of the following decades. Nowadays, we are in a time with server farms collecting and processing big data and one can purchase a seemingly infitesimal amount of computational power or storage to access from anywhere. Grand and amazing this cloud computing technology, connecting things that have never been connected before; our air conditioners to our refrigerators, our smart phones to our cars, smart cities where the cars talk to the traffic lights which talk to the electrical grid, where everything forms the Internet of Things. Although, our never-ending quest to connect anything and everything surpasses our readiness to support the infrastructure we create – to retain the perfect balance of availability, integrity, and confidentiality. The goal of this poster is to survey the security considerations for the internet of things intelligent systems by examining existing works and to discuss potential threats and solutions for some issues such as secure communications, identifying sensitive data, identifying "things", and malicious "things".