# Iot systems activities in order to take actions

Design, Architecture

ASSIGN BUSTER

IoT environment collect sheer amount of human and systems activities in order to take actions and make human being life easier and productive, huge number of devices are interconnected to each other and to the internet collect information about our activities, dramatically increase of IoT size and the sheer size of data that is gathered by thousands of Internet of things devices could make these devices and data they gathered a very valuable target for intruders, many attacks target these devices, in this paper we will cover most well-known attacks and their countermeasures. 1. IntroductioBillions of intelligent IoT systems connected to internet today, and it is predicted to be 50 billion devices by 20201. these smart, self-decision-making systems control the electricity demands of our cities (smart grid), our home security, transmit our health records to hospitals and receive prescription in order to make human being life easier and productive, Figure 1. Since IoT systems record almost everything around us and collect sheer amount of people and systems activities in addition to the nature of the Internet of things systems that require them to be online almost always, that make the gathered data and systems itself exceptionally important target for attackers and intruders, IoT systems motivate intruders to exploit them to collect data about sensitive environment like Smart Grid or to violate people privacy and committing crimes, exploited IoT systems could be used to lunch attacks against others like DDOS attacks.

To demonstrate the ability of attackers to make the infected IoT devices begin a massive attacks, in 2016, a large attack caused many popular web sites Amazon, BBC, Netflix and others to get down for a while, the attack has then expanded to attack Dyn a DNS solution and Email delivery service making tens of thousands of users unable to access and browse the web, this attack has been lunched using Distributed Denial of Service attack techniques that taking advantage of huge number of infected IoT systems to create a network of botnet and control them to start the attack23, what makes these kinds of attacks risky is that it can be lunched from any system that is connected to the internet which could be for example smart refrigerators, smart TVs part of this type of attacks, other concern of IoT security is the privacy of users, since IoT devices gather information about people activities such as  health information that are gathered by smart wearable devices, forbidden access to these data would be privacy violation, what is more danger is the intruders' ability to tamper with IoT systems to harm people like manipulate medicinal devices to change the victim's receipt.     In this paper we will discuss the different types of attacks that target IoT environment and its countermeasures, section 2 is a general overview of the IoT architecture, section 3 discuss IoT security in general, section 4 lists related work and most well-known attacks against IoT environments, section 5 shows the statement of the problem and challenges, section 6 shown the proposed solution, section 7 is conclusion and future work.     IoT Architecture The IoT infrastructure composed of multiple diverse systems that are connected to each other and exchange information between them. An abstract view of how IoT works is Data is measured by one or more sensors, these measurements are sent the local IoT controller that will do the initial processing and storing, data is then sent through the internet to a cloud service for more processing and for long term storage.

Widely recognizable architecture for IoT environment is to categories devices based on its location and/or based on its function. the three level IoT architecture 4 is a very well-known architecture that split the IoT environment into three layers, application, network and perception figure 3.

. i.

Perceptionlayer: – Inthis layer actions are measured through sensors, these measurements are thensent to IoT controllers which are microcontrollers and embedded boards used toprocess data and store it locally, technologies used in this layer like RFIDand WSN, RFID is stand for Radio-frequency Identification which is thetechnology that used to enable the communication between sensors and themonitored IoT objects through RFID tag, the measured data is sent to thecontroller through wireless network transmission (WSN). devices in this layerhave a limited processing and storing capabilities.