IoT Wireless Network Security Issues

Abstract

IoT is a newer concept, which also identifies as the internet of things .where the networks allow people and device to interact and collaborate for information sharing over the internet, without any human intervention .however connecting device over the internet via IoT increase the chance of being prone to information leakage. As the Internet of things, the device becomes more popular, vulnerabilities countermeasure are not sufficient to protect the flaws under the IoT environment. These research paper focus on various IoT vulnerabilities panorama and provide further analysis to alleviate the risk associated with it, with a suitable mitigation plan

.

Introduction

The Internet of Things interconnects with various devices with help of IoT platform to send and receive the data, and these can empower the system to capture (Garg and Dave, 2019) store, analysis specific information about the surroundings without any human intervention which brings better productivity and cost-effectiveness for the organization hence IOT become the game-changer for an organization, which can act as middleware between the physical world and digital world. The IoT typically used Hardware-based sensors, which are used to collect information and send it cloud platform for Data processing, and based on information software provide analytical reports according to Organization requirement

IoT Architecture

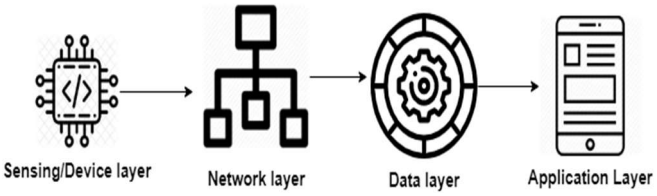

Fig-1 IOT Architecture

The IoT typically works on four-layer Architecture containing Sensing (Sridhar and Smys, 2017)Device layer, network layer, data layer and Application Layer [Cloud Environment] .the role of the sensor to collect the data from surrounding based on the specific function example temperature and light sensors and then the information delivered to the embedded device. afterwards, data can be sent to a cloud platform using a connectivity layer by using Wi-Fi Bluetooth or NFC technology, then a different type of the algorithm is being used based on the type of data collected to get meaningful information insights and patterns, and such type of information can be displayed on application layers

The IOT device communicate to Application using various Wireless technology such as WIFI, ZigBee, Bluetooth, RFID, which make it possible to communicate, monitor, analyse and execute the certain function using (Lounis and Zulkernine, 2020)single application The smart home, transport, health care, access and surveillance system heavily rely on the IoT platform

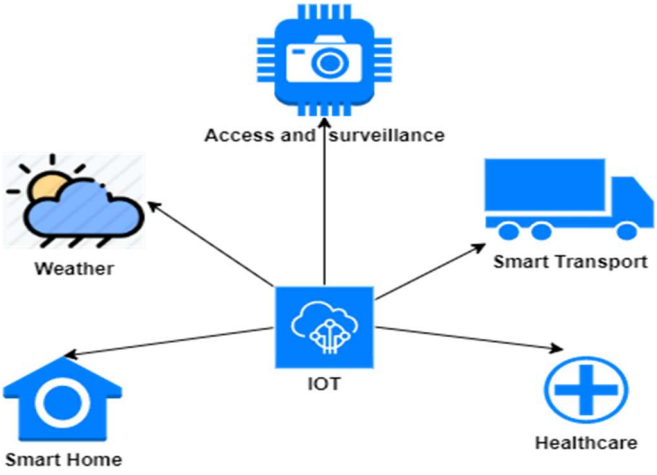

Fig-2 IoT Platform usage

The Rapid development for IoT(Gu et al., 2020) technology somehow may compromise the security and Privacy hence, nearly about 65000 devices are being infected by the attacker due to security Weakness In IOT platform and that create severe destruction and Outage under Mirai Attacks

#	Parameter	BLE	Z-Wave	ZigBee	Home Plug GP	Dash7
1.	Standardized by	IEEE 802.15.1	IEEE 802.15.4	IEEE 802.15.4	IEEE 1901-2010	ISO/IEC 18000-7
2.	Networks supported	WPAN	LR-PAN	LR-PAN	WPAN	WSAN
3.	Frequency	2.4 GHz ISM	915 MHz ISM(US), 868MHz (Europe) RFID	2.4GHz ISM frequency band	28 MHz	433 MHz, 68 MHz and 915 MHz unlicensed ISM band/SRD band
4.	Designed for	Low-powered devices with less data usage	Local area sensor data networks	To carry small amounts of data across medium distances	Smart Grid applications , home area network (HAN)	Open source RFID standard used for WSN
5.	Data rate	1 Mb/s	9.6/40 Kb/s	250 Kb/s	3.8 Mb/s	Up to 167 kb/s
6.	Throughput	270 kbps	40kbit/s	250 kbps	Exceeding 1mbps	200kbps
7.	Topology	Mesh and star	source-routed mesh	Mesh only	Ethernet in Bus topology	Node-to-node, star, tree

Fig-8 Data Link Layer

Risk assessment of the Selected Vulnerability

Common Vulnerability exists in Various Layer

The different IoT layer has its specific technology that can bring the specific weakness that can be exploited b(Dorsemaine et al., 2016)y an attacker .the security issue are categorised according to IoT layer

Sensor Layer Risk

1. **Physical attack:** The attacker physically attacks the IoT components
2. **DDoS attack:** the attacker overwhelmed the current system function by sending a fake request
3. **Routing attacks:** in these methods, an intermediate malicious node might modify the routing path in data collection and forwarding state

Transport Layer

1 **MITM Attack:** The attacker act as an intermediary in between object and infrastructure and can be able to listen(Dorsemaine et al., 2016) the communication between object and infrastructure which might reveal the critical information

Application Layer

1. **SQL injection:** The SQL query can be utilized by the attacker to extract the username and password details from the SQL database
2. **Cross-site scripting:** the user deliberately redirects to the alternate website by the hacker using a malicious script

Use of IoT for Smart Home

In the Modern world, several smart appliances such as video camera,(Arzt et al., 2014) washing machine light bulb,voice-assistant devices are controlled with the Help of IoT Platform, and these conveniences bring more acceptance in terms of IoT deployment, as a consumer, they might be un-aware about that their privacy is being exposed over the internet by using such type device. hence its responsibilities of manufacturers to provide a better security mechanism to strength overall device function

Specific Vulnerability with IoT baby Monitor

The baby monitor is a video camera, which will provide convenience to the parents to monitor their baby activity from (Stanislav, Beardsley and September, 2015b)the internet .these device made from general IoT components such as firmware, chipset and software .hence it becomes ideal devices for the security exploration

Impact of Vulnerability

The home user, who are using the internet in the Presence of Baby monitor connected with the same network may have the risk that their private information, verbal communication, video camera footage can be hacked by the attacker

Fig-9 Vulnerabilities Identify in several Baby Monitor (Stanislav, Beardsley and September, 2015b)

CVE-2015-2886	Remote	R7-2015-11.1	Predictable Information Leak	iBaby M6
CVE-2015-2887	Local Net, Device	R7-2015-11.2	Backdoor Credentials	iBaby M3S
CVE-2015-2882	Local Net, Device	R7-2015-12.1	Backdoor Credentials	Philips In.Sight B120/37
CVE-2015-2883	Remote	R7-2015-12.2	Reflective, Stored XSS	Philips In.Sight B120/37
CVE-2015-2884	Remote	R7-2015-12.3	Direct Browsing	Philips In.Sight B120/37
CVE-2015-2888	Remote	R7-2015-13.1	Authentication Bypass	Summer Baby Zoom Wifi Monitor & Internet Viewing System
CVE-2015-2889	Remote	R7-2015-13.2	Privilege Escalation	Summer Baby Zoom Wifi Monitor & Internet Viewing System
CVE-2015-2885	Local Net, Device	R7-2015-14	Backdoor Credentials	Lens Peek-a-View
CVE-2015-2881	Local Net	R7-2015-15	Backdoor Credentials	Gynoii
CVE-2015-2880	Device	R7-2015-16	Backdoor Credentials	TRENDnet WiFi Baby Cam TV-IP743SIC

Vulnerability R7-2015-11.1:Predictable public information leak (CVE-2015-2886) in ibaby M6

The ibabycloud.com has a weakness by which any authenticated user to the ibabycloud.com service can view camera details for any other user, including video recording details, due to a direct object reference vulnerability.