Internet of Things in Business

A study on applications, regulations, and security

In partial fulfillment of the requirements for the

degree of Master of Science

Program of Study Committee: Dr. Anthony Townsend

Spring 2022

By: Abhas Bhatt

Table of Contents

1.0 Introduction

Internet of Things is being used in all possible places as they provide promising opportunity to any user from a simple application to a network of complex operations. The advancement of technology is providing an imaginary space and a virtual playground for everyone to interact with each other. Machines are not exception to this, especially IoT devices. The low cost and easy compatibility of wireless technology and device sensors has made it extremely easy to use IoT devices in virtually any environment. Cloud technology is supporting the sustainability of these IoT devices through rapid and improved communication. The user of these devices most of the time do not have to worry about the implementation solution as various autonomous processes are built into these devices for collecting, processing, acting, and storing data. There are various applications of IoT devices in consumer and organizational spaces. In organizational space, medical and healthcare has a huge market for IoT devices. From remote monitoring to emergency notification system, IoT does it well. These are also very popular in clinical and health insurance settings. The accurate, real-time data with timestamps being generated by these devices has a potential to save huge expenditure in the health and insurance industry. Similarly for transportation sector, the sensors provide smart traffic control, smart parking, fleet management, digital toll collections, and as a whole safety to the consumers.

As the IoT hardware are being deployed, the software for those IoT devices is being created as well. And the variety of hardware and software vendors are not making it easy to centrally regulate the protocols and best practices when an IoT device is deployed in the network. As a result, there are various non-standard practices going on in the IoT world. In the IT Security industry today, one would even rename the term “Internet of Things” to “Internet of Trash”.

So, a business or an individual needs to be very careful in using such devices, especially when they interact with or connect to sensitive data, either of an individual or of customers.

Lately the IoT devices are also under scrutiny because their surface area for attacks is increasing because of wide usage. In the recent years more than half of the cyberattacks are being done to IoT devices. A successful compromise of an IoT device can be patient zero to move laterally in an organization network. And because of non-standard practices, launching attack vector from a compromised device becomes extremely easy to the attacker and extremely disastrous to a business. To mitigate the risk, there are various guidelines provided by federal and private agencies that a business can utilize to keep these devices safe and usable in a business environment.

Hence, this review overlooks the IoT device types, their application is various industries, the trends, and characteristics of IoT devices, how it interacts with the technology, the pitfall and security issues it brings to the workspace, examples of security issues in the past, real world analysis of an IoT device, and how we can mitigate and/or minimize those security issues to make them usable for organizational benefits.

2.0 IoT Technology

IoT relies on communication within local devices and outside network to perform programmed actions. There are many communication technologies that are being used based on the desired outcome. There are different variations of characters that the communication technology may have, like bandwidth, time latency, power consumption, cost, scalability, and range of communication. Depending on the application of use, different technologies have some advantageous characters over the others.

Here is a short list of IoT enabling technologies based on the range of communication (Wikipedia contributors, 2022b):

2.1 Short-range wireless: These include communication channels that are very close to each other ranging from about an inch to about a hundred feet. Few of the examples of short-range wireless are Bluetooth, Near-field communication (NFC), Radio-frequency identification (RFID), Wi-Fi, ZigBee, Z-Wave, Light-Fidelity, etc.

2.2 Medium-range wireless: These include high-speed communication channels, specifically for mobile networks. These generally have higher throughput and low latency. Examples include LTE networks, 5G mobile network, etc.

2.3 Long-range wireless: These are generally used where latency is compromised in place of power usage. Long range communication at a low data rate is usually adopted to reduce power and cost of transmission. Examples include Low-power wide-area network (LPWAN), Satellite communication (VSAT), etc.

2.4 Wired: These are used in places where absolute reliability is required during communication, without any possible interferences. The communication is using electrical or optical signal to carry power and data. Examples of wired communication include ethernet, power-line communication (PLC), fiber-optic, coaxial cable, etc.

The technology stack talks with the application via middleware. This is the software designed to be the intermediary between IoT devices and applications. While the IoT offers numerous exciting potentials and opportunities, it remains challenging to effectively manage things to achieve seamless integration of the physical world and the cyber one (Ngu et al., 2016). The middleware provides seamless integration of sensors in the application and sends the desired output to a network device either local or remote.

3.0 Application of Internet of Things

IoT devices are being used in almost all industry imaginable. The ease with which they integrate with current infrastructure and provide real-world, real-time data has been beneficial to any business they are being used in. Few of the industries that can be classified as a major user of IoT devices are as follows:

3.1 Medical applications

Internet of Things (IoT) refers to network-connected electronic objects that can collect and transfer data over a wireless, wired network. In modern world, data can be transferred without any human intervention to another internet-connected device and they can share data with each other(İleri et al., 2021). An example of IoT implementation in the medical field is elder care. The aging population is providing a huge challenge to care givers as the demand increases day by day. To offset some of the loads, a home can be equipped with assistive technologies, which an individual can use with as simple as speaking to it. Applications such as incorporating IoT and GPS Technologies together to design a mini tracking system for people with Alzheimer's disease. Wandering and getting lost are some of the signs of the disease, so the possibility of remote overseeing would help the caregivers and relatives of the patients (İleri et al., 2021).

With the diversification of terminals and development of internet technology, internet technology has come into the stage of Next Generation Network(NGN) technology (Wei Zhao et al., 2011). IoT devices uses these technologies to link various sensors together, primarily via wireless communication and provide intricate, diverse, and advanced services focusing on people, which have not been achieved (Wei Zhao et al., 2011). With the aging population we are seeing some diseases like hypertension, heart diseases, and other lifestyle diseases become common in the elderly group. Remote Monitoring and Management Platform of Healthcare information (RMMP-HI) can provide monitoring and management of these lifestyle diseases so as to reach the purpose of prevention and early detection (Wei Zhao et al., 2011). This system collects a variety of vital bodily data, analyze and process it and presents the potential outcome based on the data gathered by the IoT sensors. A byproduct of prevention or early detection of such diseases is the abundance of data. There are various standards that has been created to save a user's data from potential bad actors and the organization itself. To an organization providing such services, the potential business model through which they can generate revenue is by providing paid healthcare service that are needed based on IoT data and expert analysis, and the other potential business model can be providing the aggregated data to other healthcare organization to conduct research and move towards the betterment of healthcare as a whole.

3.2 Consumer applications

There are virtually unlimited types of IoT devices available to consumers needs with a variety of functions. From a very common function to a very niche function, one can find some type of IoT device developed in the relevant area. Experts predict that the Internet of Things will spread rapidly over the next few years and will offer a whole range of new services improving the life of the consumers as well as the productivity of companies ("Understanding the Internet of Things (IoT)," 2014). According to Bonnet, Buvat, & Subrahmanyam (2014), 96 % of questioned companies stated that they are going to adopt the IoT in some way within the next three years, and 68% stated that they are already investing in the IoT (Maier, 2016). The IT Services for IoT market will represent a 58 billion dollar opportunity in 2025, up at a 34% CAGR from 2020 (Gartner Research, 2021). The majority portion of IoT used by consumers is for home automation, making of a smart home. Almost all aspects of home are connected to a centralized network. Few of the common things include lights, home thermostat, HVAC system for heating and cooling, media server, security cameras, etc. And few of the obscure things that is starting to gain attention is toilet seats. These toilet seats are equipped with sensors to measure blood pressure, weight, pulse, oxygen levels, etc. Other than the immediate benefits like ease of use, remote access, and automation, the long-term benefits of using such IoT devices is energy savings and security (smart home having less home insurance cost compared to others (Sleight, 2021)).

3.3 Industrial applications

As vast as the industry is, we have a vast array of IoT devices integrated in the physical manufacturing, integrated with network, helping various industrial processes. The Industrial Internet of Things (IIoT) provides a bridge for communication between the entities and the information in intelligent manufacturing (Wan et al., 2018). It is industrial networks (e.g., wireless sensor networks) that can perceive physical resources in order to achieve reliable operation of the machine through real-time and effective monitoring in a smart factory.

Therefore, IIoT realizes the coordinated allocation of resources and dynamic scheduling, improves manufacturing efficiency, and reduces production costs and resource consumption (Wan et al., 2018). The resource allocation in any industry is a crucial part. Any wasted resource can be a source of revenue loss. Therefore, it is important to assure optimal resource allocation to meet any projected timelines. The primary objective on the IoT device here is to align processes and perform optimally with higher growth. For example: In the agriculture industry setting (and very likely other industries as well) the required information is scattered in various places which includes real time information such as market prices and current production level stats along with the available primary crop knowledge (Mohanraj et al., 2016). Monitoring modules in IoT devices can help manage the entire process of where the inventory and revenue are and where they will potentially go with a smart monitoring system.

Similarly in the maritime industry the deployment of IoT devices is making maritime users to have better experience. The expansion of communication networks toward the maritime IoT, emphasizes on the importance of using a secured and reliable communication system as these newly envisaged applications demand a reliable communication network with strong quality of service (QoS) (Rahimi et al., 2020).

To expand the horizon of Industrial IoT, they can now be integrated with technologies like blockchain. This helps in enabling the platform’s interoperability, portability, scalability, and security. The acquired data by the sensors can be locally processed and sent to blockchain platform which creates immutable digital ledger for industrial IoT applications (Mazzei et al., 2020).

3.4 Military applications

Use of IoT in Military application has become necessity of today's world as anti-military activities have increased and have become threat to Nations. Lives of soldiers are priceless, so it is important to protect their lives to the maximum we can. Remote movement tracking has become the necessity of Military forces over the course of time. These needs can be fulfilled by wireless communication techniques and IoT can give the solutions to these problems by the means of faster, better and safer way of transferring information with the help of powerful and reliable wireless communication (Gotarane & Raskar, 2019). Saving lives of soldiers is considered a high priority task in any battlefield and remote automation is the proposed solution to such task. There are organizations in the industry that specifically work on cutting edge military technology, its testing, and its deployment. Most of the times it only comes to public knowledge when the information is deemed non-classified and open to public. Logistics and resource management is how you win the battle in the field. IoT devices can automate and limit excessive resource utilization and automate the fulfilling of the resources that are getting low in inventory. An example of this is management of ammunition and other tactical gears. Ammunitions are excessively used in any military, be it a training ground or a battlefield. A smart system that tracks the ammunition usage, provides security while in storage, tracks transportation would be a crucial element in logistic support around ammunition. The IoT can be programmed to act upon a certain threshold of the inventory and process pre-defined actions based on the amount in the inventory. As every device or instrument on battlefield can communicate with each other, statistical analysis of this information can give probable upcoming problem and their solution as well to a soldier (Gotarane & Raskar, 2019).

Satellite based IoT integration is another interesting field which is primarily used by the military and/or the government. The main advantages of satellite based IoTs are elongated service availability, better reliability, larger coverage, connecting remote locations, remote control of resources and properties, fast operations in the remote places, lower costs, and easier integration (Routray et al., 2020). The usage of satellite based IoT not only helps with the active warfare, but with disaster management responses, border intrusion detection, deep space exploration, protection of airspace, etc. So, satellite-based applications of IoT helps with the defense, the offense, and humanitarian aid when needed. This application will remain as the primary source for the military for mission critical activities, intelligence gathering, and security monitoring.

3.5 Infrastructure applications

Monitoring and controlling operations of sustainable urban and rural infrastructures like bridges, railway tracks and on and offshore windfarms is a key application of the IoT. Driven by the recent adaptation of a variety of enabling device technologies such as RFID tags and readers, near field communication (NFC) devices and embedded sensor and actuator nodes, the IoT has stepped out of its infancy and is the next revolutionary technology in transforming the Internet into a fully integrated Future Internet (Gubbi et al., 2013). An IoT device can be used to monitor the urban and rural infrastructure for any events or changes in the load baring structure that can possibly compromise the structural integrity and increase risk.

Another example of a large deployment is the one completed by New York Waterways in New York City to connect all the city's vessels and be able to monitor them live 24/7 (*STE Security Innovation Awards Honorable Mention: The End of the Disconnect*, 2012).

Energy management is another big area that IoT automations can help. Consumers are highly motivated to autonomize their smart homes to be as efficient as possible. On a larger scale they help organizations to implement a smart grid and act on the distribution side of energy and power related information to improve the efficiency of the production and distribution of electricity.

The IoT devices can also help monitor environmental variables such as air quality, water quality, atmospheric or soil conditions, etc. They also help monitor the movement of wildlife in their habitat. Monitoring environmental activity also helps in getting early alerts of possible natural disasters and the same system can be used by emergency services to provide aid to the affected area.

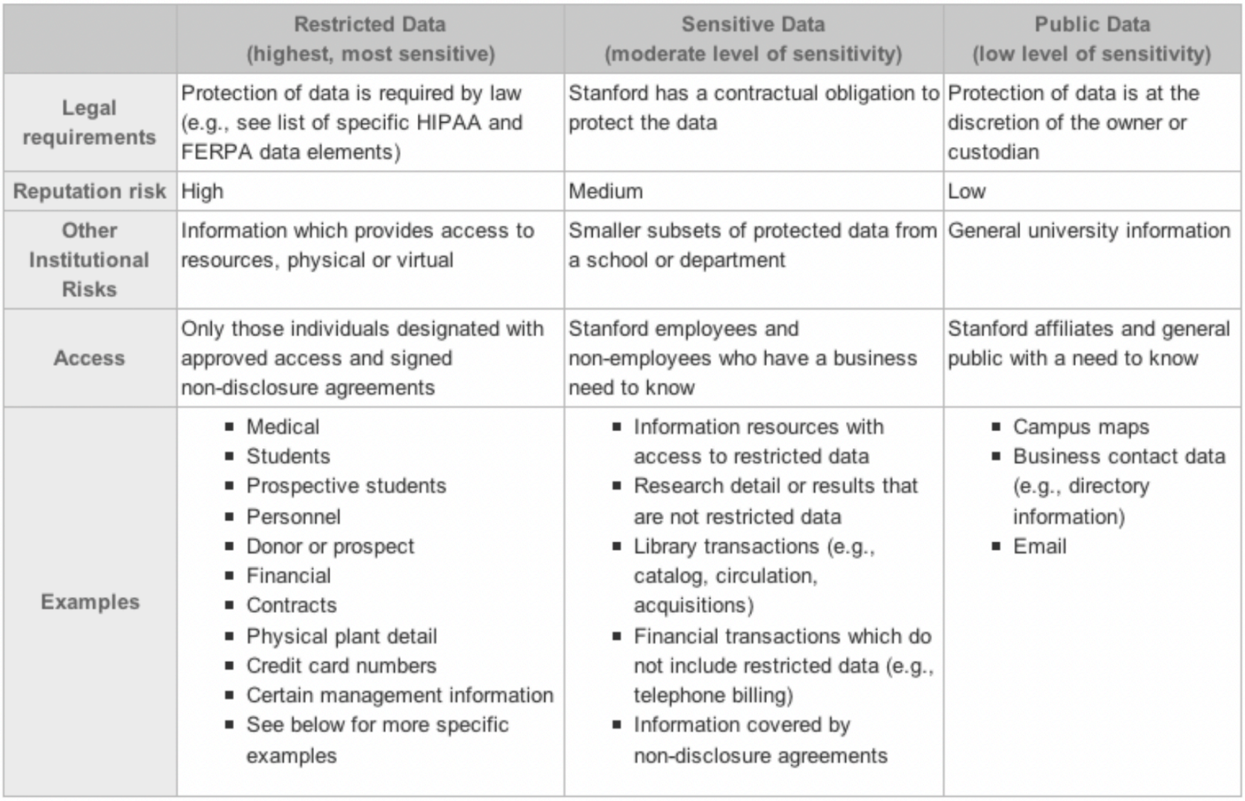
3.6 Digitalization and everyday usage

IoT is now being used so ubiquitously that one doesn't even think of it using as an IoT devices. An example of this is the widespread use of QR and other barcodes. These are used to relay information that otherwise would be through a physical medium. A QR code is a passive data, which a consumer interacts with and uses the information gained to a service or a process via internet. This has especially come in handy recently because of COVID-19. Restaurants are starting to use QR codes to point the consumer to their menu, instead of handing out a physical menu. This helps alleviate the spread of virus/bacteria to some level. In the supply chain industry the integration of IoT and blockchains make supply chain resilient, truly distributed peer-to-peer systems and provide the ability to interact with peers in a trusted, auditable manner (Pundir et al., 2019).

4.0 Regulations and compliance

In the past few years, Internet of Things (IoT) devices have emerged and spread everywhere. Many researchers have been motivated to study the security issues of IoT devices due to the sensitive information they carry about their owners. Privacy is not simply about encryption and access authorization, but also about what kind of information is transmitted, how it used and to whom it will be shared with. Thus, IoT manufacturers should be compelled to issue Privacy Policy Agreements for their respective devices as well as ensure that the actual behavior of the IoT device complies with the issued privacy policy (Subahi & Theodorakopoulos, 2018). Unfortunately, this is not the case as Subahi & Theodorakopoulos discovered in their research. And some IoT devices infact go against their privacy policy agreement and does not comply at all.

The National Institute of Standards and Technology (NIST) provides framework to foster cybersecurity for devices and data in the IoT ecosystem. NIST's Cybersecurity for the Internet of Things (IoT) program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices, products and the environments in which they are deployed (Joint Task Force Interagency Working Group, 2020). IoT generates huge data on day to day operations. It is either processed locally, remotely, and/or stored for future uses. These data can be classified in three categories based on their sevirity and possible adverse effects. These classification dictate the level of interanal controls to protect that data against theft, compromise, and inappropriate use (Markham, n.d.). Figure 4.1 below shows the top-level overview of data classification, legal requirements, institutional risk, and examples of data.



	Restricted Data (highest, most sensitive)	Sensitive Data (moderate level of sensitivity)	Public Data (low level of sensitivity)
Legal requirements	Protection of data is required by law (e.g., see list of specific HIPAA and FERPA data elements)	Stanford has a contractual obligation to protect the data	Protection of data is at the discretion of the owner or custodian
Reputation risk	High	Medium	Low
Other Institutional Risks	Information which provides access to resources, physical or virtual	Smaller subsets of protected data from a school or department	General university information
Access	Only those individuals designated with approved access and signed non-disclosure agreements	Stanford employees and non-employees who have a business need to know	Stanford affiliates and general public with a need to know
Examples	▪ Medical ▪ Students ▪ Prospective students ▪ Personnel ▪ Donor or prospect ▪ Financial ▪ Contracts ▪ Physical plant detail ▪ Credit card numbers ▪ Certain management information ▪ See below for more specific examples	▪ Information resources with access to restricted data ▪ Research detail or results that are not restricted data ▪ Library transactions (e.g., catalog, circulation, acquisitions) ▪ Financial transactions which do not include restricted data (e.g., telephone billing) ▪ Information covered by non-disclosure agreements	▪ Campus maps ▪ Business contact data (e.g., directory information) ▪ Email

Figure 4.1

Source: http://www.stanford.edu/group/security/securecomputing/dataclass_chart.htm

NIST special publication 800-53 provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks (Joint Task Force Interagency Working Group, 2020). The primary objective of these controls are to manage risk across the entire organization. They are customizable to different needs of different organization. The consolidated control catalog also addresses security and privacy issue from functionality prespective and assurance prespective. This help illustrate the strength of function & processes and gives confidence in the security and privacy provided by the controls (Joint Task Force Interagency Working Group, 2020).

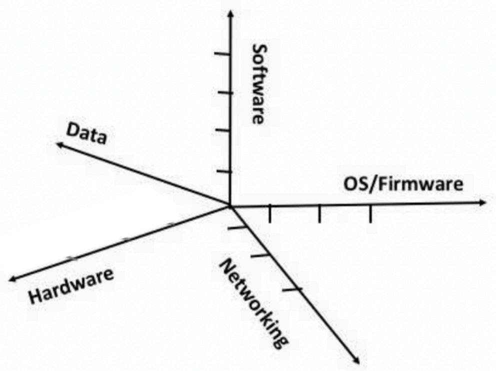
In parallel to the concept of data protection by design, the concept of data protection by default is also a legal obligation in the new regulation. Data protection by default entails that the protective measures of personal data should be the default option in any processing activity (Stuurman & Kamara, 2016).

5.0 Security issues and complications

Organizations should strive to understand challenges of integrating IoT device before it is acquired and integrated into a system. Due to several market and technological factors, IoT devices often lack cybersecurity functionality commonly present in conventional IT equipment (computers, laptops, etc.). Organizations need to define their key device cybersecurity requirements for an IoT system. Key device cybersecurity requirements are those the organization has determined the IoT device must possess and/or manufacturers and supporting entities must provide in order for the device to be integrated in the system. Because without the key factor the IoT device is not considered securable (Fagan et al., 2021).

At this point we have come across various instances where IoT devices are not properly administered and regulated, although the security issues with IoT infrastructures have been widely discussed and publicized. The threat can be categorized into two categories: threats against IoT and threats from IoT. Threats against IoT occur when a flaw in an IoT device or application, on the perception, network or cloud level is exploited by the hacker, and the device or application is compromised - i.e., a full or limited access to its functions and data is gained by an attacker. In case of threats from IoT, the compromised infrastructure is used to conduct various attacks against IoT or Internet-connected devices (Blinowski & Piotrowski, 2020).

To secure an IoT system, we must consider five dimensions: hardware, operating system/firmware, software, networking and data generated and maintained within the system, as shown in Figure 5.1.



Five Aspects of IoT Security and Privacy (Ling et al., 2018)

To summarize the above proposed dimensions, we can combine them into the following groups:

5.1 Hardware security:

This is the most essential aspect of security that one doesn't think of while implementing the system. The hardware backdoor can circumvent the checks that are built-in to detect any firmware compromises. The vulnerability list mechanisms include, but are not limited to debugging ports, multiple boot options, and unencrypted flash memory chips.

5.2 Operating system, firmware, and software security and privacy:

The issue with software is like any other computer system. There is a constant cycle where a bug is found and is patched. But unlike computer system, the firmware in IoT do not get regular updates causing the bug to be unpatched and vulnerable. A large-scale automated dynamic analysis using the Metasploit Framework of various firmware was conducted and a large number potential exploits were discovered (Chen et al., 2016). Metasploit is a opensource framework consisting of various tools developed for searching and executing exploits against a local or remote target machine (Wikipedia contributors, 2022a).

5.3 Network, data security and privacy:

The whole IoT system is interconnected with each other from end-to-end. While communicating encryption and authentication should be used consistently, but often is not. IoT rely on pairing and binding process to interact with other devices or network to function. In the pairing process the controller needs to connect to the IoT device in order to configure the "thing". Most Small Office Home Office (SOHO) IoT devices allow any controller in proximity to conduct pairing with no additional security measures (Blinowski & Piotrowski, 2020). This is problematic because anyone in proximity to the IoT device can usually connect to it and re-configure it to break into the system. Default settings/passwords are the primary attack vectors in most of these cases. Once the attacker is in the system, even the properly configured other network infrastructure is of no match. The attacker will be able to sniff even encrypted traffic, as the attacker has control over one of the devices that can decrypt the traffic. To summarize this most security problems emerging in today’s IoT systems results directly from buggy, incomplete or outdated software and hardware implementations. The number of IoT devices reported to be vulnerable is growing in the public domain.

6.0 Real world examples

At any time, there are thousands of IoT devices improperly configured exposed to the internet. These are devices ranging from smart home automation routers, internet cameras, bulbs, and other smart devices connected to the internet. The common practice in IoT devices is to enable non-used ports as well, because of negligence by the manufacturer. This causes non necessary ports open to the internet. If a user is not tech-savvy and doesn’t have a firewall at the network border, these ports are exposed to the internet. And a lot of times doing everything right is not enough to secure the IoT devices.

For example, in January of 2021, a manufacturer of an IoT-enabled chastity belt was compromised in a ransomware incident. In October 2020, researchers at Pen Test Partners published details about a serious vulnerability that allowed a remote attacker to take control of any Qiui Cellmate device. They found that making a request to any API endpoint did not require authentication and that using a six-digit "friend code" would return "a huge amount of information about that user," such as location, phone number, plain text password (Ilascu, 2021). An increasing number of smart camera platforms are being targeted by thieves. At risk are privacy, security, and the risk of fraud, and criminal gangs are exploiting the spoils of data to their merciless benefits.

All the statistics below are collected from Shodan. Shodan is a search engine that lets users search for various types of devices connected to the internet. This is where most of the curious minded people come to gather intelligence on any service that is possibly open to the internet. They can be malicious users, black-hat or people purely focused on intelligence gathering.

Shodan, while potentially a dangerous tool, is also the absolute example of what can happen when devices with lax security enter our daily lives (Osborne, 2016).

In figure 6.1 we can see the top 10 ports that are open and exposed to the internet for USA. We can see some standard ports like 443, 80, and 8080, that is potentially being used for user interface to interact with users but opening port 22, 161 to the internet without any hardening measures is asking for trouble. One can probe the port until an exploit is found and when they get access, all the devices in your network have a chance to be compromised.

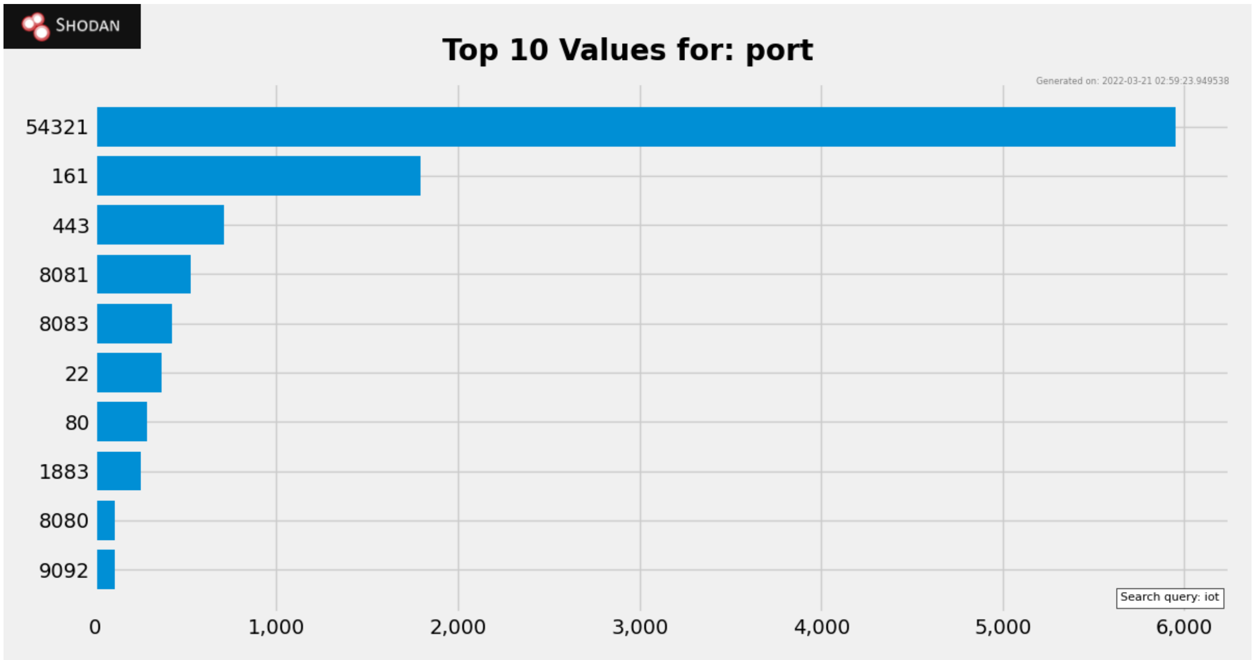


Figure 6.1

Figure 6.2 displays the type of IoT device running a specific service. The number one on the list is a Chinese company IoT devices running its own service. The second and the third are the common service that many IoT devices run, a light webserver and remote management for maintenance and configuration. When these are not properly configured, and left to have default settings, they provide an easy gateway to attackers to get a hold of a device in a user's network. This acts as patient zero in an attack-compromise case and the attacker can laterally move to other devices in the network.

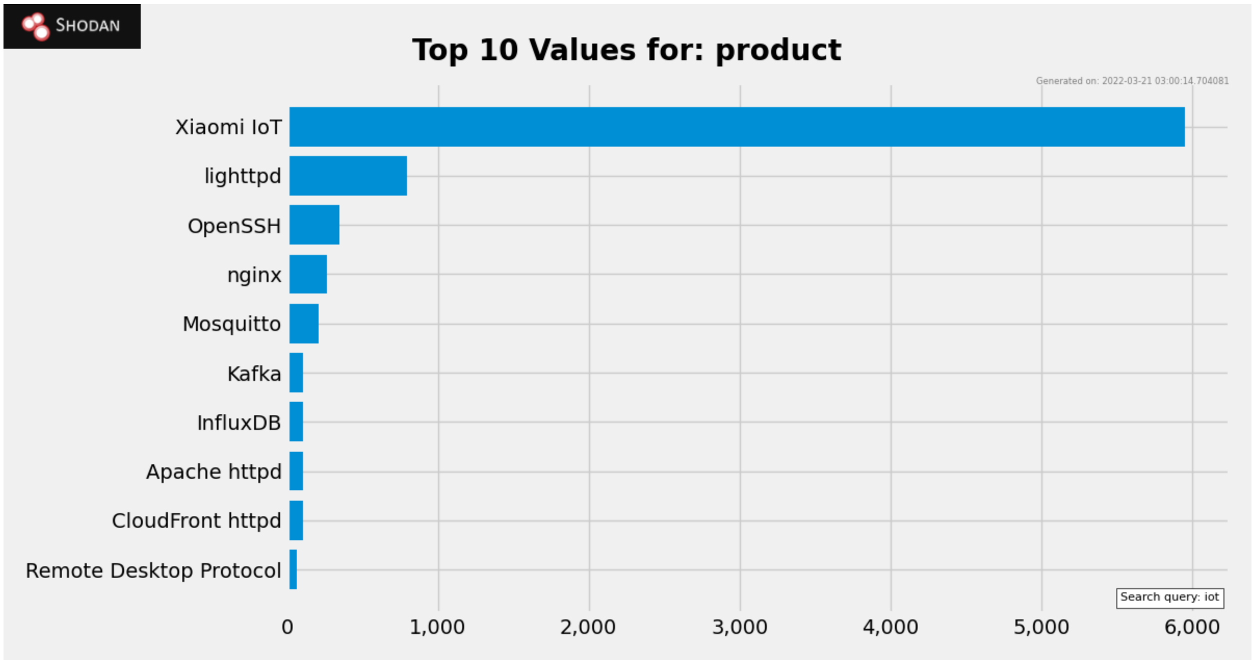


Figure 6.2

Figure 6.3 simply displays the total number of IoT devices exposed to the internet worldwide. From the chart we see that USA is on the 3rd to have exposed about 1200 devices with active exploit/access to the world for anyone to probe into.

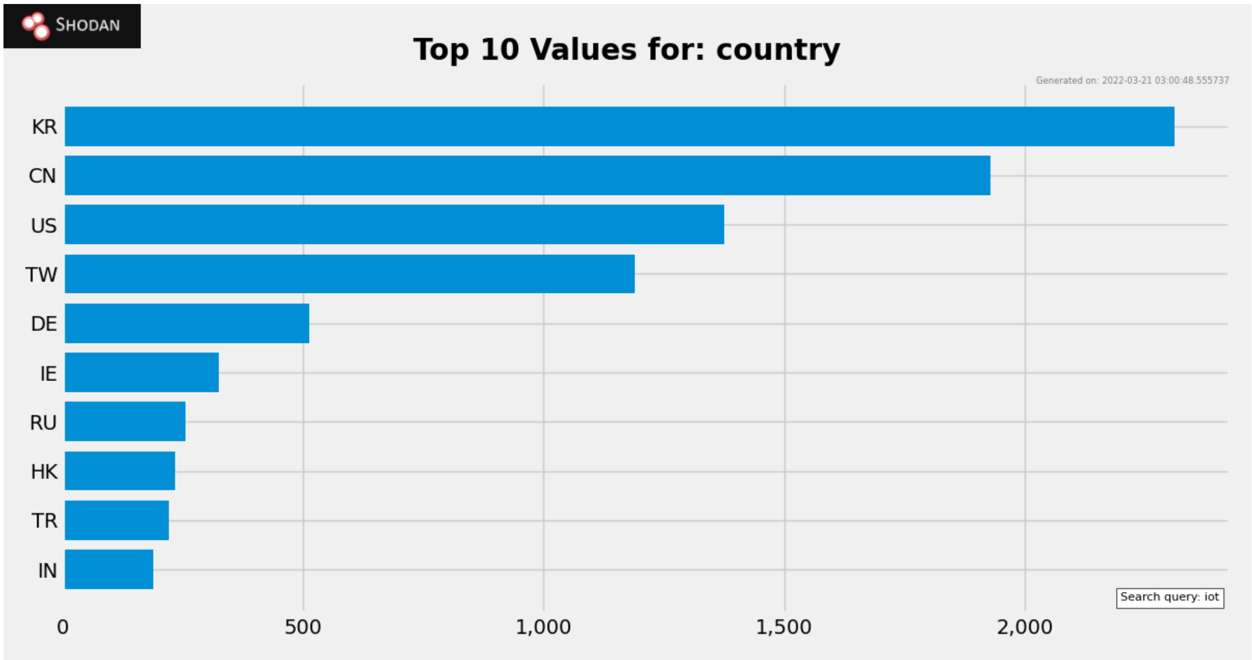
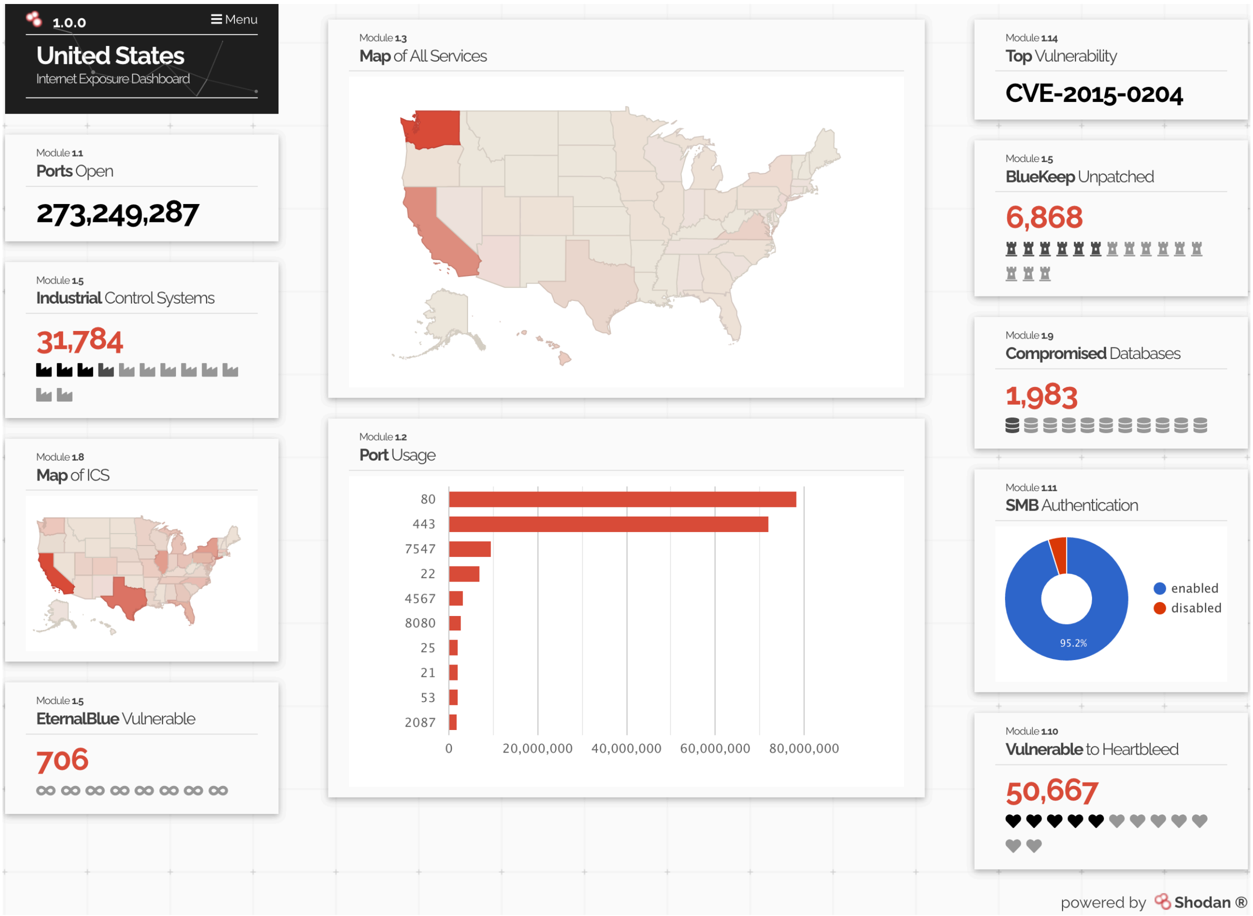


Figure 6.3

The dashboard below (figure 6.4) displays the high-level live statistics on a country basis, this is for the USA. We can see that as of March 20, 2022, there are 706 EternalBlue vulnerable machines openly connected to the internet. What this means is any attacker finding the correct address to those machines can remotely login to the machine and extract all information from the machine. And much worse, the attacker can move laterally in the network to discover other non-exposed machines and exploit those as well.

As of today, the top vulnerability among the mis-configured IoT devices that are openly exposed to the internet is CVE-2015-0204. This is the vulnerability where an attacker can conduct a Man in the Middle (MitM) attack by intercepting a communication channel, downgrading the encryption being used to communicate, and facilitate brute-force decryption by offering a weak ephemeral RSA key. This enables the attacker to see all sensitive data being passed across the network.



1.0.0 ☰ Menu

United States
Internet Exposure Dashboard

Module 1.1
Ports Open
273,249,287

Module 1.5
Industrial Control Systems
31,784

Module 1.8
Map of ICS

Module 1.5
EternalBlue Vulnerable
706

Module 1.3
Map of All Services

Module 1.2
Port Usage

Module 1.14
Top Vulnerability
CVE-2015-0204

Module 1.5
BlueKeep Unpatched
6,868

Module 1.9
Compromised Databases
1,983

Module 1.11
SMB Authentication

Module 1.10
Vulnerable to Heartbleed
50,667

powered by Shodan ®

Figure 6.4

I am guilty of using IoT devices in my home as well. As a technical user, I was curious to see how the IP camera I am using holds up against other devices. While the camera I am using doesn't have any public exploits and I have configured it to avoid all the recommend mistakes, the camera still has open ports that is likely not needed for it to function. And because of manufacturers negligence or intention to keep those ports open for maintenance or to keep tab on customers, there is no good way to harden those open ports from the internet. Here is the short excerpt of the scan that I performed on the IoT device I am using:

```
80/tcp    open  http
554/tcp   open  rtsp    Lorex IP camera rtspd
1935/tcp  open  rtmp?
8086/tcp  open  d-s-n?
37777/tcp open  unknown
```

7.0 Conclusion

IoT devices and its applications already has tremendous influence in consumer and industrial settings. The advance machine to machine interaction aims to make tedious, mundane job easier. The global network infrastructure is already there to support such smart devices across the globe. This review barely scratches the scope of applications of IoT we will see in the future. It has already been implemented in almost all areas imaginable. The technology is still in its infancy and as the networking ability increase and artificial intelligence (AI) is incorporated in IoT devices, we will see and get more use out of these devices. We here talked mostly about technical (network and security) issues, but there are a variety of issues that needs further discussion and clarification. Issues such as ethics, responsibility, liability, insurance, governance, and accountability. The standards and regulations need to be carefully observed and adopted because of the data at stake. We also took a snapshot of the publicly exposed devices in the search engines geared towards white-hat and black-hat security researchers. At any point there are thousands of these devices on the internet, with default credentials and configurations, for anyone to access them over the internet. An example of an IoT device I am currently using to monitor external activity confirms this by showing the open services that are exposed to the internet. The attacks against Internet of Things (IoT) systems are emerging as IoT comprises millions of everyday items, the scope of these sorts of attacks is worrisome and even worse, the migration to internet-everything is unstoppable. We will be seeing security incidents for a long time, unless we adjust course quickly (Sayegh, 2021).

IoT's capability for business is endless. This includes leveraging capabilities such as automation, real-time data gathering and analysis, and take actions based on the analysis without causing harm or affecting other aspect of the business (Rayes & Salam, 2019). The concept of social network and interconvertibility is motivating consumers to adopt more IoT and as they are used more and more, different business models can be created around them for organizations to thrive and grow.

8.0 Reference

Blinowski, G., & Piotrowski, P. (2020). *CVE based classification of vulnerable IoT systems*.

Chen, D. D., Woo, M., Brumley, D., & Egele, M. (2016). Towards Automated Dynamic Analysis for Linux-based Embedded Firmware. *NDSS*, *1*, 1–1.

Fagan, M., Marron, J., Brady, K., Cuthill, B., Megas, K., & Herold, R. (2021). *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements* (NIST SP 800-213; p. NIST SP 800-213). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-213

Gartner Research, G. (2021). Forecast: IT Services for IoT, Worldwide, 2019-2025. *Gartner*. https://www.gartner.com/en/documents/4004741

Gotarane, V., & Raskar, S. (2019). IoT Practices in Military Applications. *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 891–894. https://doi.org/10.1109/ICOEI.2019.8862559

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Ilascu, I. (2021, January 9). *Hacker used ransomware to lock victims in their IoT chastity belt*. https://www.bleepingcomputer.com/news/security/hacker-used-ransomware-to-lock-victims-in-their-iot-chastity-belt/

İleri, K., Duru, A., & Karaş, İ. R. (2021). DEVELOPMENT OF IOT ENABLED GLOBAL TRACKING SYSTEM AND MOBILE APPLICATION FOR PEOPLE WITH ALZHEIMER’S DISEASE. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information*

Sciences, *XLVI-4/W5-2021*, 287–290. https://doi.org/10.5194/isprs-archives-XLVI-4-W5-2021-287-2021

Joint Task Force Interagency Working Group. (2020). *Security and Privacy Controls for Information Systems and Organizations* (Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Ling, Z., Liu, K., Xu, Y., Gao, C., Jin, Y., Zou, C., Fu, X., & Zhao, W. (2018). *IoT Security: An End-to-End View and Case Study*. https://doi.org/10.48550/ARXIV.1805.05853

Maier, M. V. (2016). *The Internet of Things (IoT): What is the potential of Internet of Things applications for consumer marketing?* (public). http://essay.utwente.nl/70001/

Markham, B. (n.d.). *Data Classification and Privacy: A foundation for compliance*. https://www.usmd.edu/usm/adminfinance/itcc/day/dpfound.pdf

Mazzei, D., Baldi, G., Fantoni, G., Montelisciani, G., Pitasi, A., Ricci, L., & Rizzello, L. (2020). A Blockchain Tokenizer for Industrial IOT trustless applications. *Future Generation Computer Systems*, *105*, 432–445. https://doi.org/10.1016/j.future.2019.12.020

Mohanraj, I., Ashokumar, K., & Naren, J. (2016). Field Monitoring and Automation Using IOT in Agriculture Domain. *Procedia Computer Science*, *93*, 931–939. https://doi.org/10.1016/j.procs.2016.07.275

Ngu, A. H. H., Gutierrez, M., Metsis, V., Nepal, S., & Sheng, M. Z. (2016). IoT Middleware: A Survey on Issues and Enabling technologies. *IEEE Internet of Things Journal*, 1–1. https://doi.org/10.1109/JIOT.2016.2615180

Osborne, C. (2016, January 26). Shodan: The IoT search engine for watching sleeping kids and bedroom antics. *ZDNET*. https://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/

Pundir, A. K., Jagannath, J. D., Chakraborty, M., & Ganpathy, L. (2019). Technology Integration for Improved Performance: A Case Study in Digitization of Supply Chain with Integration of Internet of Things and Blockchain Technology. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 0170–0176. https://doi.org/10.1109/CCWC.2019.8666484

Rahimi, P., Khan, N. D., Chrysostomou, C., Vassiliou, V., & Nazir, B. (2020). A Secure Communication for Maritime IoT Applications Using Blockchain Technology. *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 244–251. https://doi.org/10.1109/DCOSS49796.2020.00047

Rayes, A., & Salam, S. (2019). Internet of Things (IoT) Overview. In A. Rayes & S. Salam, *Internet of Things From Hype to Reality* (pp. 1–35). Springer International Publishing. https://doi.org/10.1007/978-3-319-99516-8_1

Routray, S. K., Javali, A., Sahoo, A., Sharmila, K. P., & Anand, S. (2020). Military Applications of Satellite Based IoT. *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 122–127. https://doi.org/10.1109/ICSSIT48917.2020.9214284

Sayegh, E. (2021, July 22). *Peloton Breach Reveals A Coming IoT Data Winter*. https://www.forbes.com/sites/emilsayegh/2021/07/22/peloton-breach-reveals-a-coming-iot-data-winter/?sh=361c88af3c08

Sleight, M. (2021, June 4). Smart home insurance discounts. *BR Tech Services*. https://www.bankrate.com/insurance/homeowners-insurance/smart-home-discounts/

STE Security Innovation Awards Honorable Mention: The End of the Disconnect. (2012, December 10). https://www.securityinfowatch.com/video-surveillance/video-transmission-equipment/article/10840006/innovative-wireless-network-connects-new-york-waterways-ferries-for-safety-security-roi-and-more

Stuurman, K., & Kamara, I. (2016). IoT Standardization—The Approach in the Field of Data Protection as a Model for Ensuring Compliance of IoT Applications? *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 336–341. https://doi.org/10.1109/W-FiCloud.2016.74

Subahi, A., & Theodorakopoulos, G. (2018). Ensuring Compliance of IoT Devices with Their Privacy Policy Agreement. *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, 100–107. https://doi.org/10.1109/FiCloud.2018.00022

Understanding the Internet of Things (IoT). (2014, July). *GSM Association*. https://www.gsma.com/iot/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf

Wan, J., Chen, B., Imran, M., Tao, F., Li, D., Liu, C., & Ahmad, S. (2018). Toward Dynamic Resources Management for IoT-Based Manufacturing. *IEEE Communications Magazine*, *56*(2), 52–59. https://doi.org/10.1109/MCOM.2018.1700629

Wei Zhao, Chaowei Wang, & Nakahira, Y. (2011). Medical application on Internet of Things. *IET International Conference on Communication Technology and Application (ICCTA 2011)*, 660–665. https://doi.org/10.1049/cp.2011.0751

Wikipedia contributors. (2022a). *Metasploit Project—Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Metasploit_Project&oldid=1078112797

Wikipedia contributors. (2022b). *Internet of Things*. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/wiki/Internet_of_things