Keeping the world of Internet of Things Secured and Safe

Kyle A. Higginbotham

Abstract-

The world of IOT is a very progressing subject. It is becoming integrated in everyday life whether you like it or not. Cars, cell phones, computers, Alexa, google homes, even refrigerators are now starting to get integrated into the network. These can be seen as good or bad. It is a big leap forward but with that leap comes concerns. These include vulnerabilities and even the recording of information of data. These are a few of the concerns we will go over for you to judge if IOT devices are worth the problems that could arise.

Index Terms-

IOT- Internet of Things,
HUD- Head-up Display,
PC- Personal Computer,

I. INTRODUCTION

Most people understand the definition of the Internet of Things as a system of devices that are interconnected together and through networking such as the Internet. The internet of things was originally proposed from a concept introduced by Kevin Ashton.[6] Even now there is no clear definition of what the Internet of things stands for. It is such a broad term that so many devices, such as, sensors, machines, and autonomous objects are used within this term. The topic that all of those devices have in common is one thing, and that is that all of the physical items are connected to the virtual world in some way.[6]

The Internet of Things has broadened its outreach to devices in our everyday life. The devices are so widely used they have been separated into different categories. We have consumer applications, commercial applications, industrial applications, and infrastructure applications. These categories can break down even further.[7]

1) Consumer

Consumer applications can break down into smart home and elder care. Smart home devices consist of google homes, alexas, smart locks, nest thermostats, smart doorbells, security cameras, HUD lights, chromecast, and much more. The elder care devices are items such as devices like life alert or other devices that notify if something has happened.[8]

2) Commercial

The commercial applications side of the internet of things can be broken down into medical and healthcare, transportation, and building and home automation. The health care side consists of devices that usually help monitor patients in one form or another. The monitoring devices would measure vitals like blood pressure and heart rates and could send out an emergency notification if they dropped below a certain threshold.[9] There are medical beds also being implemented that would automatically adjust for a patient that is in an uncomfortable position without the manual need for a nurse. These beds would also monitor if it was occupied or if the occupant was trying to get up or escape the bed. Internet of Things devices are even going so far and advanced as becoming apart of pacemakers and helping out with prosthetics for amputees.[10]

The internet of things devices that work alongside transportation are items like street signs, cars, traffic control, mapping, smart parking, toll roads, and much more. These devices have gotten so complex and it has made driving require few less stops. The crowd sourcing aspect of map applications give you a more accurate arrival time compared to looking at a map and trying to judge a distance. Alongside with the light up boards on the road that will tell you of any traffic or accidents that may have happened along an interstate or freeway.

The building and home automation mainly consists of consumer devices but on a larger scale. This category mainly helps make buildings more energy efficient by monitoring the behavior of guests.[11]

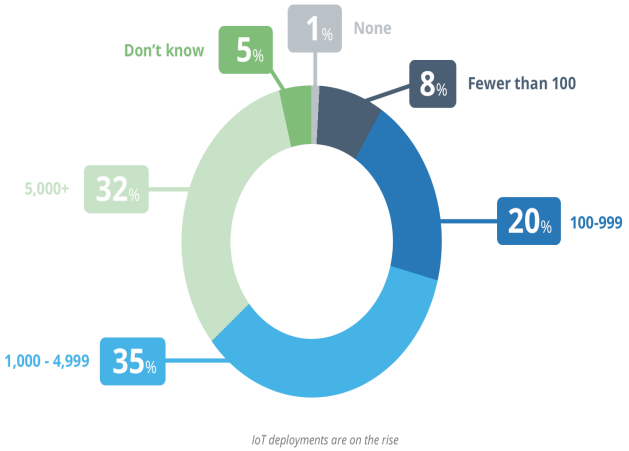

Fig. 1. Figure 1 shows the surveyed percentage of business' that have some type of IOT device implemented in their company[1]

3) Industrial

The industrial category is mainly made of manufacturing and agriculture. Internet of things helps develop rapid manufacturing of new products, a more dynamic response to the demand of products, real time optimization based on how machines are running at the time of production, and sensors to keep track of items that are produced.[9]

Most people would wonder how there is a use of internet devices in farming, but there are actually many uses for these devices. Some of those uses include, the collection of important data, how much fertilizer to add to the soil that will change based on the field[12], and even a new technique that was recently introduced to help with fish farming.[13] The IOT device monitors the water pump and counts how many fish are on the conveyor belt. The device then reduces or increases the effectiveness of the trap based on the amount of fish. [13]

4) Infrastructure

The last category of internet of things is infrastructure applications. IOT in infrastructure is mainly used for monitoring repairs or data.[14] IOT monitors data that has to do with real time. The internet of things devices can even help control infrastructures like bridges that would provide access for ships getting into harbers. One of the bigger internet of things deployment that has happened in the United States has to deal with New York City. In New York City, devices are connected to all of the vessels that travel on the waterways.[15] These devices monitor the vessels live and see things like energy, and even offer customers a paperless ticketing service.[15]

II. SECURITY AND ENCRYPTION

Internet of Things devices have been a major selling point and have started to sprout up all over the U.S. in the past few years. With new devices comes new challenges. One of the many challenges have to do with the transmission of data and how secure it is. Alongside many of the devices I mentioned, these devices all need to be protected somehow or they will become a vulnerability. It goes alongside the saying, "A chain is only as strong as its weakest link." If the Internet of Things device is the least secure then that leaves your network open to anyone knowing how to penetrate the device.

These devices are completely different compared to regular personal computers. The devices usually have a really basic software installed without all of the security measures that a PC with windows installed would have. Most of the Internet of Things devices also do not have the software that installs automatic updates which is a big security flaw if not taken care of.[5] If a security flaw is found on one of the devices and the device is kept in the system without being updated there will be a problem. Most IOT devices are only encrypted with password authentication and a few security protocols, unless the device is very sophisticated then it will not have a firewall. Most IOT devices that are found in the field have an average life cycle of around twenty years. This is around double if not triple the amount of time that an average PC is in the field.[5]

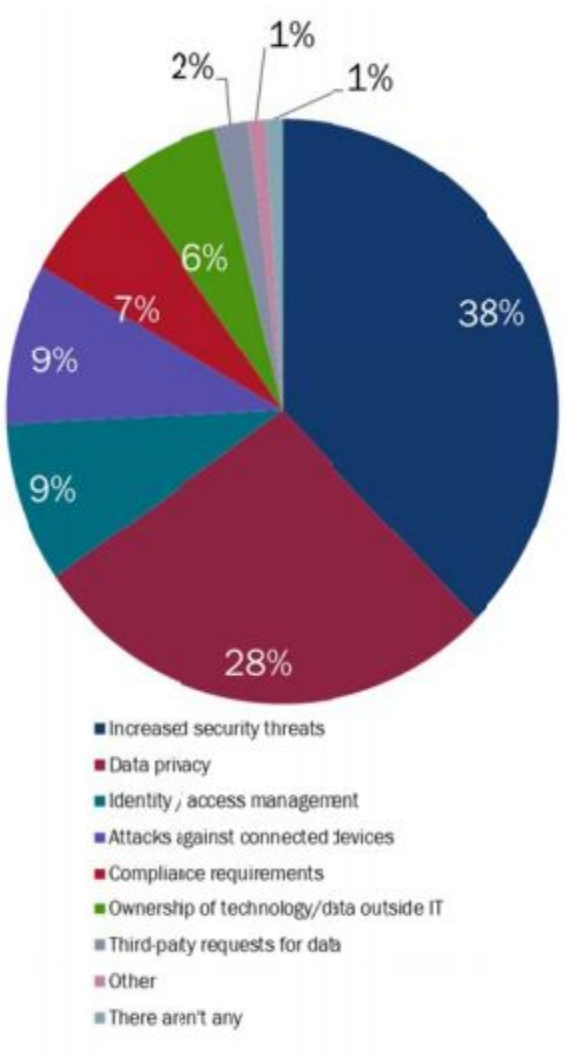

Fig. 2. Figure 2 shows what the consumers and enterprises think the major risk of implementing Internet of Things devices are.[2]

Hacking these devices can get in depth. Many organizations that are trying to infiltrate a device will use tactics like research, obtaining documents and developing plans about the device, and some groups will even purchase or obtain their own device they are trying to penetrate and try to reverse engineer the software that the device is encoded with.

There are multiple requirements that Internet of Things devices should check over to see if they are a security flaw. These include ensuring the firmware of the device has not been tampered with or altered, making sure the data is securely stored by the device, having a secure

communication between all other connections that attempt to interact with the device, and finally there must be a way to protect the device from cyber-attacks. The best way to manage all of these requirements is to check them off in the early stages of design and development of the IOT device.[5]

There is not a solution that is the best for every IOT device that is available. Security solutions that are implemented on the device pertain to what the device will be doing. The security of a manufacturing device like a satellite that is collecting data or a dam water manager that is controlling the flow of how much water is released will not be the same as the security implemented to secure a consumer device like a google home that is playing music or being asked questions. [5]

The main ways to secure your Internet of Things devices is through secure boot, secure code updates, data security, authentication, secure communication, protection against cyber attacks, intrusion detection and security monitoring, embedded security management, and device tampering detection. Secure boot is when you use cryptographically signed code to verify that the firmware has not been tampered with. Secure code updates is a method that whenever the system updates it uses signed code like in the secure boot to make sure the code is from the trusted site. Data security is just making sure that there is no unauthorized access to the data. Authentication is using strong passwords on a up to date authentication protocol. Secure communication is whenever data is sent it is using ssh or ssl or high bit encryption keys. Protection against cyber attacks requires an embedded firewall which means this security is really only used in super expensive devices. Security monitoring is letting the user know when passwords have been attempted but incorrect. Security management is where the security policies are updated to stop known threats. Finally, Device tampering detection is when there is a notification when a seal on the device has been broken. These are the protections that IOT devices use against the outside world to keep the network they are on safe. Using all of these methods do not make the devices full proof but it makes them a lot more secure.[5]

III. EXISTING TOPICS

The main protection that businesses and companies use to monitor the security and data of their Internet of Things devices are network log collectors. These log collectors could be pieces of software like Retrace or you can enable a type of logging on the system console based on what network device the company or business is using that is connected to the IOT devices.[3]

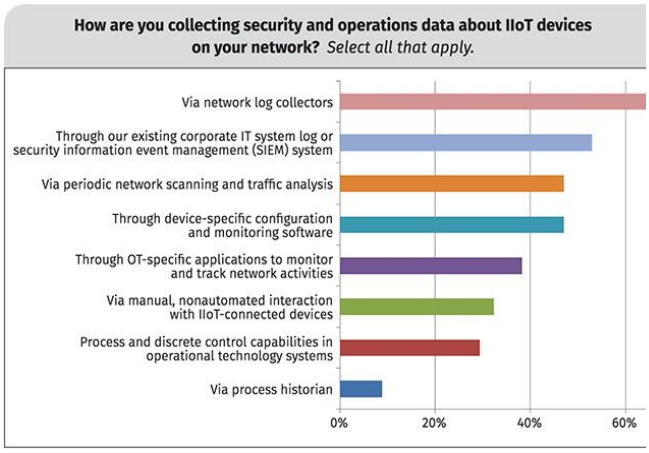

Fig. 3. Figure 3 is showing all of the ways that different types of businesses and companies are collecting and monitoring the data that is going through their Internet of Things devices.[3]

The reason that the network log collectors are the most frequent out of all the options is because most businesses have one running at all times to monitor where traffic is coming and going. The third highest collector is mainly talking about scanning and packet sniffing programs like wireshark or tcpdump. [3] These packet capture files aren't sorted automatically and a network analysis worker would need to sort/view the packets to make sure no data is getting leaked. These are done periodically since the network scanning happens over a period of time and there are multiple different packets and packet types coming through the network at one time that it would be too hard to monitor on a real time scan.

The most accurate type of monitoring for Internet of Things devices are OT-specific applications. Only thirty eight percent of companies and businesses use this type of monitoring for their devices. The OT-specific applications have diagnostic and prognostic data to show what an expected or normal output of data should look like. If the differences between the diagnostic data and the users data show problems like reduced output, reduction in quality, intermittent disruptions or other unusual behavior, then it could indicate a tampering of some sort (whether it's accidental or malicious), a configuration change, or even a threat that is already inside the system. The automated tools usually do not have the process oriented operation diagnostic like the applications do. [3]

IV. CHECKING FOR LEAKS

There is estimated that around two percent of all United States households own some type of voice-activated digital assistant. This is not including cell phones. These devices consist of google homes, alexas, apple tvs, smart thermostats, smart lights, and even smart refrigerators. That is estimated at around 2.8 million people. It is expected to

rise to 11.5 percent as of 2020. [4]

The way these Internet of Things devices work is based on a keyword or trigger. Once that trigger is pronounced or said it will start recording your phrase. The problem that arises there is that the microphones always have to be on to try and listen for that keyword or phrase. The information that needs to be known is what happens to the data that the device is monitoring to try and hear that keyword. Does it just disappear? Does it save it to the device? Or does it send it off to the manufacturer for them to use? Those are some of the questions that should be going through your mind when you are using a smart home device. [4]

In theory, you are trading convenience for privacy. Some people do not have anything to hide, so it would be fine with them, while others do not feel comfortable having a device that is listening to their every word. The problem with only recording key words is that some devices might think they hear a keyword. Whenever the apparent keyword is heard it starts recording. Even if you didn't say the exact keyword.

Some of these devices say they will capture certain keywords and phrases in their terms of service. They will use other key phrases like shopping stores or certain movies and websites to tailor ads to what you have been talking about. This is not all devices though. Some devices even have a mute button. This mute button is used so that the device will not listen for its keyword or phrase. The button is what could be used during sensitive conversations so that the device will not record even if it messes up and hears an apparent keyword. The real question is, does the mute button actually stop the device from listening? The only way that you can be 100% sure of a device not getting your data is by not having one or having it not connected to any power source at all.

These would change by devices. Some devices would be more trustful than others. You might be able to determine that the google home mute button does not transfer any data, but then learn that an Amazon Alexa does. This would require extensive testing with false keywords and monitoring data traffic that is sent across the network back to the servers of the device that you are monitoring.

The best way to go about knowing how safe a smart home device is, is by making it open source. This would give users of all types ways to look at the device and seeing what data is actually being transmitted. You would be able to see of any trigger words that, even if you didn't say "Hey Google" (or what other device you were using), would cause data to be sent data back to a server. The flip side to making it open source is that it shows even people with malicious intent the source code. If a big enough bug is found by someone who is doing the research for malicious intent it could cause catastrophic damage. This relates back to the number of households with some form of IOT device. The research opportunities are there, but there could also be consequences.

V. CONCLUDING REMARKS

All in all, Internet of Things devices provide many uses in society. They will never leave certain types of production and manufacturing, but you as a user can decide whether or not you want to purchase them to keep in your home. You need to decide if the security risk of certain devices is worth the convenience they bring. Smart homes are starting to get bigger and bigger. They will soon be implemented in most homes because of how common they are becoming. With the advancement of technology comes the advancement of security. Internet of Things devices will slowly start to get better, more efficient, cheaper security as time goes on. In turn, this will make the devices more reliable and safer to use than what we have now. Internet of Things are now a product of the present, not the future. You just need to decide if they are worth using in your own home.

VI. REFERENCES

[1]"Internet of Things," GreyWizard. [Online]. Available: https://greywizard.com/industries/iot. [Accessed: 06-Dec-2019].

[2]"Findings From ISACA's 2013 IT Risk/Reward Barometer," Risks and Rewards of the Internet of Things , 12-Nov-2013. [Online]. Available: http://www.isaca.org/SiteCollectionDocuments/Forms/AllItems.aspx?RootFolder=http://www.isaca.org/SiteCollectionDocuments/2013-Risk-Reward-Survey&FolderCTID=0x01200040E51F667638E34786B1DD06694147DE. [Accessed: 05-Dec-2019].

[3]B. Filkins, "The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns," SANS Institute InfoSec Reading Room, pp. 2–23, Jul. 2018.

[4]"You Said What? The Threat of 'Always-Listening' Digital Assistants," RedFiveSecurity, Mar-2017. [Online]. Available: https://www.red5security.com/white-papers/march_2017_you_said_what_the_threat_of_always_listening_digital_assistants.pdf. [Accessed: 06-Dec-2019].

[5]A. Grau, "What is Really Needed to Secure the Internet of Things?," Internet of Secure Things, 2014. [Online]. Available: https://www.automation.com/pdf_articles/Internet_of_Secure_Things.pdf. [Accessed: 06-Dec-2019].

[6]S. Haller, "The Things in the Internet of Things," The Things in the Internet of Things, pp. 26–30, Nov. 2010.

[7]J. Greenough, "The corporate 'Internet of Things' will encompass more devices than the smartphone and tablet markets combined," Business Insider, 25-Feb-2015. [Online]. Available: https://www.businessinsider.com/the-enterprise-internet-of-things-market-2014-12. [Accessed: 06-Dec-2019].

[8]M. Mulvenna, A. Hutton, V. Coates, S. Martin, S. Todd, R. Bond, and A. Moorhead, "Views of Caregivers on the Ethics of Assistive Technology Used for Home Surveillance of People Living with Dementia," Neuroethics, vol. 10, no. 2, pp. 255–266, 2017.

[9]D. Romascanu, J. Schoenwaelder, and A. Sehgal, "Management of Networks with Constrained Devices: Use Cases," Internet Engineering Task Force (IETF), 2015.

[10]C. A. D. Costa, C. F. Pasluosta, B. Eskofier, D. B. D. Silva, and R. D. R. Righi, "Internet of Health Things: Toward intelligent vital signs monitoring in hospital wards," Artificial Intelligence in Medicine, vol. 89, pp. 61–69, Jul. 2018.

[11]J. Haase, M. Alahmad, H. Nishi, J. Ploennigs, and K. F. Tsang, “The IOT mediated built environment: A brief survey,” 2016 IEEE 14th International Conference on Industrial Informatics (INDIN), 2016.
[12]Q. Zhang, Precision agriculture technology for crop farming. Boca Raton: CRC Press Taylor & Francis Group, 2016.
[13]K. Quach, “Google goes bilingual, Facebook fleshes out translation and TensorFlow is dope,” • The Register, 01-Sep-2018. [Online]. Available: https://www.theregister.co.uk/2018/09/01/ai_roundup_310818/. [Accessed: 06-Dec-2019].
[14]J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
[15]“STE Security Innovation Awards Honorable Mention: The End of the Disconnect,” www.SecurityInfoWatch.com, 10-Dec-2012. [Online]. Available: 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. [Accessed: 06-Dec-2019].