The Cost of Connectivity

Saaduddin Ahmed

ITMS 578: Cyber Security Management

Introduction

What are IoT devices and why should we care for their security? Internet of Things (IoT) devices are a type of devices that connect wirelessly through your network to help transmit data. Though IoT covers a broader term of devices, such as radio-frequency identification, Near-field communication, or even smart devices, we can see several of these devices within businesses and our homes. Some examples of these devices are Alexa, Google Home, and Smart TVs. While these devices can be helpful such as letting you control your lights or fans with your voice, you also allow them complete access to your network. This can be a major concern in multiple ways, such as data and information collection. The application of data and information collection can be used to collect data on the population's height, weight, and other terms that might provide us any given insight. In terms of companies, users and IoT devices, data is collected as information about the person, what purchases they might make, and where they are most likely to be located. Ideally, the types of data collected on the users would be kept within the company and locally on your IoT devices, to be used with the utmost care. However, the real-world application of this is anything but that, as these factors are used to make a profile of you which are then sold to advertising companies, so they can better target you. User data is so valuable to companies, they are willing to offer their product to you for free in exchange for the data they can collect on you. We see this from major brands such as Google, Facebook, Twitter, and Instagram. The outreach from these companies does not only relay within their own websites either but extends towards other products you use as well. The login integration from Google, Facebook, Twitter, or Instagram might seem like an effortless way to create an account on a website, but that opens the gates to you allowing for the website to relay all that information to those companies as well. This type of data should be private, and kept only between you and the company, but that is

never the case. In times like these, the security of this data should be heavily guarded, but that all starts from the IoT devices manufactured and placed within your household.

Placing IoT devices within your home is like setting up multiple cameras and security measures around the perimeter of your house to protect yourself from any break ins or intruders, only to forget and leave the front door wide open, allowing anyone to go through your house as though it was a listing on Craigslist for free items. These IoT devices without any security measures are a target point for such breaches, as the data a person has on the internet is the embodiment of their digital life. Imagine if someone had a duplicate copy of you and could use that for any purpose they liked. Maybe they had robbed a bank, but the fingerprints left were yours and even the face looked exactly like you. How would you be able to prove your innocence when everything matches the description of you. This is how data is when attached to a user, as it can be used for nefarious purposes and the blame bestowed upon the user who had their information stolen. For companies this is also a major problem, as it not only shows that they are vulnerable and should not be trusted, but it also cuts straight into their revenue to profit off their users. The way I am viewing data and IoT Devices in this paper is from a security perspective rather than the means of what the company plans to do with the information. The argument could be made that companies should never collect data or only do so when it is crucial for an action, such as teaching the IoT device a user's action so it can be performed accurately and then deleted afterwards. While those ideologies could move forward, companies need to show investors a profit, and to do so they might take unethical means. This is not to say I agree with the ethics of what they do, rather I stand against them, but when it comes to security an entirely new book is opened in front of our eyes.

While data can hold tons of information, for example big retailers not only hold a person's address, identification, and number, they also hold links to the user's bank and credit card details, it is only gibberish numbers until it is put into information that can be accessed. This is where I believe the focus of information security should take place. Not only is information about the user important, but the information they hand over to the company should be kept in such a manner that even breaches do not result in the leaks of sensitive information such as banking details. Though safety measures have started to show face, there has been no regulation for IoT devices or companies dealing with such technology as there has been for food safety. Repeatedly we have heard of a website saving passwords or credit details in plain text, resulting in the entire database being poured out to the web all because there has been no regulation that they have been inclined to follow. Securing this type of information along with the IoT devices that allow the initial break in is crucial for cyber security, as allowing the opposition to get less information on us can control the risk points. It will give us the upper hand and would allow us to better build upon the resources we have.

Outline

The paper will dive into the idea of Internet of Things (IoT) devices, explaining the application of such devices including what they are, how they function, and how the security of these devices can be breached. Moving on from that, the paper will dive into security of IoT devices, to better institute what breaches are performed and what types of data can be taken from them. From there it will move onto dealing with businesses and enterprises with IoT devices, to talk about what policies we can institute to help protect and mitigate against such risks. This will allow the paper to set an outline and explanation for the various cyber security frameworks, such as the National Institute of Standards and Technology (NIST) Cyber Security framework to

better understand what we can do to mitigate our risks. We never know whether the attacker will use social engineering or other tools to attack our data, so we should be covered for both while also figuring out how much risk it will cause to the business. Before closing the paper, I will also be talking about how we can continue to use the current IoT devices, but we should be more wary of the risks that come with it. Using all this information, the goal of the paper is to put forth why smart devices' security is necessary and how important it is to us all even if we do not currently make use of such devices in both our home and business settings.

Application of Internet of Things (IoT) Devices

Internet of Things (IoT) Devices covers an umbrella of various devices, such as radio-frequency identification (RFID), Near-field communication (NFC), and smart devices. The application of these devices varies between scenarios, but they all have their own flaws and benefits. The focus of this paper will be on smart devices and their application. Smart devices work by using a form of communication and gateway to allow for the use of data to be transported between the device and a wireless protocol such as a hub, Bluetooth, or wireless network. The user is then able to control these smart devices by using an interface or through a virtual assistant.

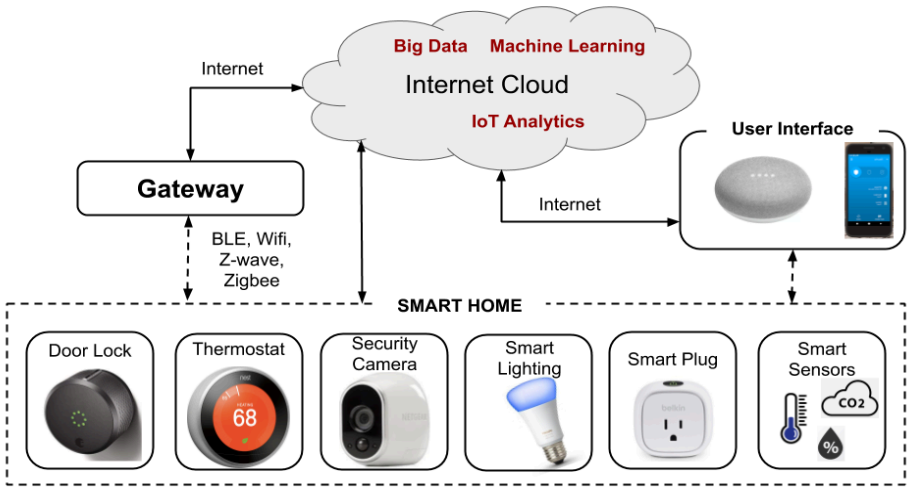

Figure: Smart Device Connectivity architecture

Source:

https://www.smlease.com/entries/automation/what-is-smart-home-technology-and-how-it-works/

These smart devices can better help with managing the lifestyle of a business. Small scenarios such as smart lighting can help manage the electricity waste you might have, only turning on the light when movement has been detected through a motion detector. Another practice is smart thermostats or security, which adjust how they work based on when people are present or not within a business. While these may seem small in comparison to businesses' need, these smart devices can also help in production, upkeep, and even prediction to inform the business when a certain machine is breaking down. Predictive analysis for businesses using smart devices can help cut down on downtimes and loss of productivity, which can help lower the $50 billion dollars being spent on repairs and maintenance that was reported by the Census Bureau and Bureau of Labor Statistics (Douglas S. Thomas, 2018).

The allowance of these smart devices to communicate with each other while also letting a human intervene when needed has helped boom the usage of these smart devices. Though the use of the smart devices varies on a case-by-case basis, it is estimated that by 2025 there will be about 75.44 billion connected smart devices in usage throughout the world according to Statistica (Tanweer Alam et al. 2018). While the production of these smart devices has been growing at a linear pace, the security behind them has yet to catch up, allowing for early adopters to have convenience but with the possibility of a backdoor to their network.

Security of Internet of Things (IoT) Devices

These advancements in technology and change in such usage have allowed us to view security from a distinct perspective. IoT devices are an example of such, as these smart devices that allow for the convenient control of your personal space with electronics have shown how various data breaches can take place from within them as well. An example of this took place in 2017, when a casino was hacked through a fish tank (Alex Schiffer, 2017). The hackers were able to jump through the fish tank's internet connectivity and move around in the network. Before cyber security experts were called in to monitor and allocate the problem, the hackers had used the fish tank to upload 10 gigabytes of data to servers in Finland, where the data exfiltration was stored for their personal gain.

Though the impact of the fish tank might seem bizarre and out of the ordinary, these types of hacks for data exfiltration are becoming more common as smart devices flood the market without any security guidance. Studies done in 2014 by Ponemon Institute have shown that the cost per incident of a data breach was around $5.9 million for organizations within the United States and resulted in $16 billion stolen from identity theft from individuals involved with the breach (Sen Ravi, Borle Sharad 2015). Higher levels of Information Security are critical in helping prevent and mitigate these types of breaches, as data is considered high priority within organizations. Financial institutions, insurance, retail, education, government, and even medical and health care are organizations that are critical targets for data, as they house personal information that can be used for identity theft. Annually, identity theft has resulted in around $50 billion stolen, with each victim's information being misused for around $4,800 (NCJRS, 2005).

Prior to our current time, information security was not heavily utilized in the real world. The usage of such security encryptions was saved for national security purposes, such as the foreign affairs, police, and embassy communication systems (Ruth M. Davis, 1978). Since then, the

dependence we have built upon technology has resulted in the daily consumption of various media forms. These forms allow for data to constantly be flowing onto the internet, from individuals using social media, companies uploading information, smart devices collecting information, and even from research articles being published. Additionally, data has also become a major factor in use cases, such as smart devices and machine learning. While it is convenient to use these new methods of communication, it is no stranger to breaches as well.

Many of these new smart devices have not undergone any type of security measures, leaving them wide open for many of the common attacks placed among them. Though covering every type of security attack for these IoT devices would be impossible, some of the more common ones we see are Man in the Middle, Cloning, Spoofing, Eavesdropping, Jamming, Lateral movement, and physical attacks (Denver Braganza and B. Tulasi 2017).

Man in the Middle Attacks

Man in the Middle (MITM) attacks occur when a perpetrator inserts themselves in a conversation that is occurring between two parties. In doing so the perpetrator uses the MITM attack to try and impersonate the second party, listen in, or alter the data being sent. Many of the smart devices deal with this problem, as MITM can occur when smart devices are trying to connect over Bluetooth instead of Wi-Fi. While sitting in the pairing phase, a MITM attacker sits in the middle of the connection listening in to impersonate the Smart device and function as though it is the client that was trying to connect. This can allow an MITM attacker to get access to the information secured behind them. Though as simple as it sounds MITM has two phases when it occurs. The first phase of MITM is copying the data down and getting a better understanding of the encryption that is tied to what is being attacked, while the second is decrypting and accessing

the resulting data as information. This makes it so that the attacker cannot connect to both devices simultaneously and must jump between both of them to perform the full attack.

Cloning Attacks

Cloning can be a major problem when it comes to Smart devices as cloning occurs when the IoT's data is duplicated. An example of this can be seen in the smart access cards, which is done through cloning a legitimate card, by reading the data on the legitimate card and downloading it to an external storage. This technique can be used for various purposes outside of IoT devices as well, such as gaining access to a facility to perform insider attacks or collecting sensitive data on a business.

Spoofing Attacks

Cloning alone cannot help achieve much besides the data, but Spoofing goes hand in hand with cloning, as the data that is cloned and downloaded can be spoofed onto a different IoT device and used as though it was the original. Spoofing can also be done on Smart devices through IP addresses and servers to disguise yourself as though you have clearance on information. The security risk is that it allows the Spoofer to grant you access to places, products, and other secured information and items.

Eavesdropping Attacks

Another major vulnerability that opens itself up with Smart devices is Eavesdropping. When connected to a network that is not secure, Eavesdropping allows an attacker to listen in to the network and intercept the information being transmitted. Unlike other attacks such as MITM, Eavesdropping does not slow down or render any hindrance towards performance, so it is harder

to spot when it is occurring. An example of this was seen by the Common Vulnerabilities and Exposures (CVE), who discloses a public list of security vulnerabilities. The CVE list includes multiple security vulnerabilities about specific smart devices that can be exploited with Eavesdropping (CVE - CVE-2021-28372).

Jamming Attacks

Jamming attacks can take place on a variety of Smart devices and networks to interfere with communication by using radio interference or other methods to cause the communication between devices to become busy. Malicious attackers use this as a method for denial-of-service attacks, draining IoT devices' batteries, or not allowing them to connect to the network (M. Guizani et al., 2020). This can have security effects on both on-premises and online, as jamming can take down security measures such as wireless cameras, keypads, websites, and much more if not correctly secured and accounted for with backup measures.

Lateral Movement Attacks

One of the key issues from IoT devices we see are the Lateral movement attacks. While the attacks can only be performed after initial access has been gained, unsecured IoT devices such as smart bulbs, thermostats, or even coffee makers can grant an attacker that access. Following this the attacker can move throughout the network, looking for sensitive data that can be retrieved. Since the attacker is using lateral movement, the presence of the attacker is hard to detect and can be seen just as normal movement. This was the case in the Casino Fish Tank hack, before they had retrieved the information they were looking for and started uploading gigabytes of that data (Alex Schiffer, 2017).

Physical Attacks

While Later Movement attacks on IoT devices take place after initial access has been gained, physical attacks can also occur on IoT devices. Malicious attackers can gain access to the IoT devices being used in the business and manipulate it to their need, damaging or even stealing it (G. Wyss et al., 2007). This allows attackers to install or retrieve data from the IoT devices while also including their own malware onto it as well. In some cases, backdoor ports, such as USB analytical tools on the motherboard, are placed on IoT devices for technical support and data collection, but this can be abused by the malicious attacks to gain full control of the device. Defending against such attacks means properly checking whether the IoT devices can be taken apart and what security system they have put in place in case of such actions. Additionally, another step to secure the IoT devices in a business setting is to monitor the devices to watch out for tampering, so cases such as skimming attacks on credit cards and bank information could be avoided on our IoT devices.

Enterprise risk management

Smart device usage has not only gone up in homes, but also enterprises. As more devices are connected, attackers have more of a surface area to target. According to a report done by PricewaterhouseCoopers (PwC) in 2019, 93% of executives believe the benefits of IoT devices outweigh the risks and this has shown in projections done by various companies such as Cisco, who believe there will be five hundred billion IoT devices connected by 2030 (Ashley Watters, 2022). The projection Cisco has shown can further be illustrated by the numerous reports done on the current market share and size of such devices.

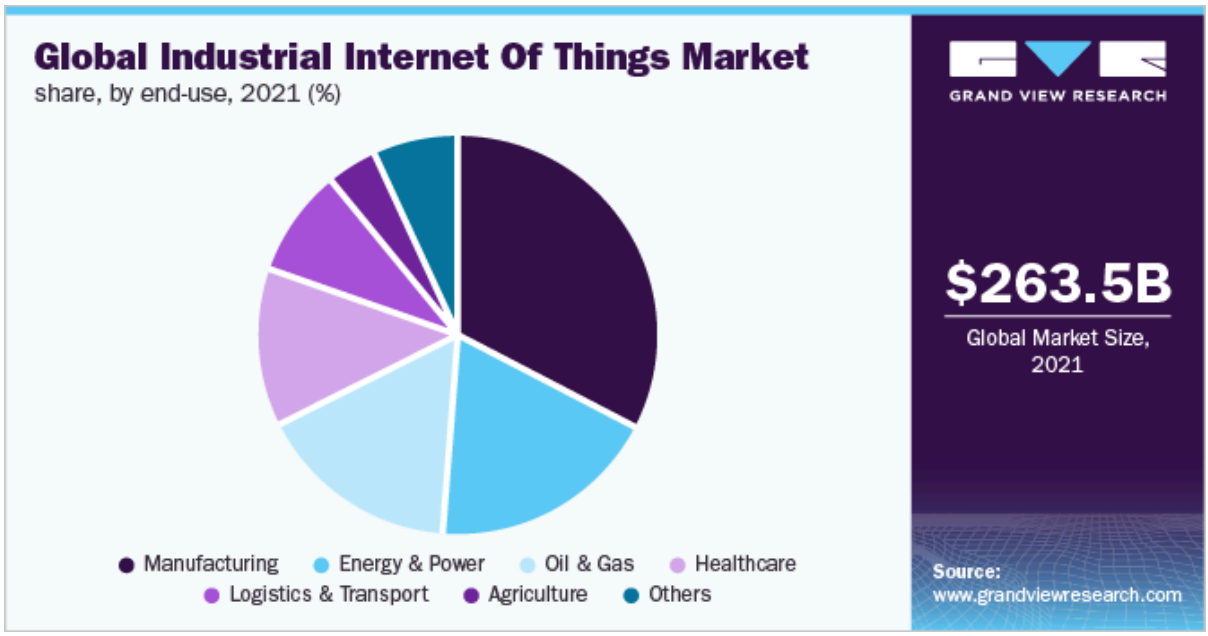

Figure: Pie Chart of IoT Market Share by 2021

Source: www.grandviewresearch.com/industry-analysis/industrial-internet-of-things-iiot-market

The projection of the market is estimated to grow at a compound annual growth rate of 23.1% from 2022 till 2030 which would result in the revenue of IoT devices reaching 1.69 trillion dollars (Grand View Research, 2021). Additionally, from a research report done by CompTia with 506 businesses based in the United States, 63% of them stated that they are incorporating IoT technologies within the business, but only 59% of businesses see cyber security for such devices as a priority, as they would rather focus on innovation (CompTia, 2019). To protect businesses from these attacks and help secure the data and IoT devices, various measures must be taken accompanied with encrypting the data, such as physical, personnel, network, and information security. A step in this direction is provided to us by the various security frameworks for both risk management and information security.

Like frameworks used in financial business, there are controls and guidelines used to help achieve better practice and accountability of any transactions being done. This same system can be taken for security frameworks as well and although it will not help us completely remove all risks regarding the security of our data, frameworks can help reduce the risk businesses and enterprises face. As different corporations have unique needs, there are many types of security frameworks used to accomplish that task. Frameworks such as the National Institute of Standards and Technology (NIST) Cyber Security help to better identify, protect, detect, respond, and recover against cyber security problems a business might face (CISA). NIST is by no means the only security framework, as others such as the Information Security Standard (ISO IEC 27K), Center for Internet Security (CIS), Health Insurance Portability and Accountability Act (HIPAA), along with many others coexist to help reduce the security risk by using their controls prescribed with others.

NIST

The procedure behind each of these frameworks vary as they put in controls to better incorporate cyber security within an organization. The NIST controls were originally made as part of an executive order by President Barack Obama, to better improve the critical infrastructure of Cyber Security (EXECUTIVE ORDER, 2013). The identify part of the NIST framework is in place to help better identify what type of security a business needs along with what assets can cause vulnerabilities. For businesses using IoT devices, a risk management strategy for securing them would need to be looked over. Following that the framework talks about protection to help better safeguard the business while ensuring the business can still operate. Teaching staff about cyber security and getting them through a training program is a part of the protection control of NIST. This can help safeguard against potential Data leaks and comply with the CIA triad of

Confidentiality, Integrity, and Availability. The next control in the framework is to Detect, which can help mitigate potential impacts of breaches by detecting anomalies and events that occur. Responding is the next step in the control and it helps ensure that actions are taken to contain the impact. Lastly, the framework teaches about Recovery plans, as it can help recover a business back to its normal operations after the impact. These controls help put the NIST framework together to better protect a business and be informed in case of any attacks or data leaks that may happen within an organization.

NIST RMF

The NIST Risk Management Framework helps organizations approach cyber security from a risk-based method. Unlike the five functions of the NIST cyber security framework, the risk management approach includes steps to help prepare, categorize, select, implement, assess, authorize, and monitor your organization and their technology such as IoT and smart devices. The preparation control of the RMF is to help prepare your organization for security and privacy risks by assigning risk management roles, implementing the controls, and conducting an organization risk assessment. From there the organization should move onto categorizing, where the organization will determine the impact it would have when dealing with the loss of the CIA triad. The organization should move onto selecting the best controls that are tailored to their needs and risks from the SP 800-53 to better protect the organization. After selecting the controls, the organization should implement them while also documenting what these various controls are providing to the organization to help with assessing. This will help determine whether the controls implemented are working as intended or need to be modified to produce the results needed. While the organization can assess how the controls are being implemented a senior official is required to authorize the security and risk controls put in place to determine

whether they are acceptable. Lastly, these controls should be maintained and monitored by putting in security reports, analyzing the activities occurring, and dealing with risk management decisions.

ISO IEC 27K

Unlike the NIST framework, the ISO IEC 27K is a nongovernmental framework that outlines better practices to establish a standard internet security. The structure of the ISO IEC 27K consists of six major controls: context, leadership, planning, support, operations, evaluation, and improvement. Using the ISO framework, the context portion helps a business evaluate and clarify to better understand who could be the expected partiers that might try to attack them. It will also allow an infosec management system to develop to help manage the information security of a business. This leads into the leadership portion of the controls, where the business can establish an information security policy, assign information security roles, responsibilities, and authorities. Policies and administration such as this can assist with the vulnerabilities IoT devices have, such as locking down or not allowing unauthorized access to the network which can help mitigate against the risk the IoT devices have over your business. The planning control portion of the ISO framework helps a business assess what risks they have and how they plan on a security risk treatment process for them. From there the framework's control helps the business put together a plan for information security management with resources, awareness, communication, and its related needs such as organizational records. We move into the operations portion of the control, where the business will conduct information security risks assessments, create plans, and put controls in place. This will allow for the business to evaluate and monitor its information security while also helping set up an audit program. The last section

of the framework is to identify and improve problems by taking the correction action, while providing improvement to the information security management system as your business needs.

While there are many more information and risk security frameworks such as the CIS framework, which is more barebones and should be used in relation with the NIST framework and the HIPAA framework for protecting security on sensitive patient data, these frameworks all provide us with guidelines to help secure the business and provide a guideline for risk management. When dealing with IoT devices that have not been evaluated for their security, using these procedures and guidelines will help us better mitigate the risk and impact we would have and while giving the corporation a better understanding of what could go wrong if we used these smart devices without properly checking them. Not only does it help mitigate us from security breaches from IoT devices, but it also gives individuals the chance to learn about the risks smart devices, information, and data security has to help better protect themselves from it. After all, organizations are concerned about the major costs cyber security can bring when dealing with IoT devices and how much it can skyrocket if problems are found.

Conclusion

Smart devices provide us with a lot of convenience, but that comes with the hefty price of security. An organization can be devoured within minutes if the correct steps are not taken to protect themselves as funds, data, and information can be drained if attackers gain access. This ,however, does not mean we should stay away from IoT devices or that innovation should be halted; rather we should understand the risks that pertain to them and be cautious as we implement them within our organizations. An example of this is, having the convenience of one network can be useful and easy to implement, but it can be detrimental when an attacker lands

upon it and can gather information from every device connecting to it. For smart devices and other IoT devices, one of the steps we can take is to set up a separate network, to better mitigate the risks that come with them when they are un-secure or not set up properly, as lateral movement can be contained within it if a breach were to occur. This can also help the organization with its risk assessment to determine how protective various devices are and how much access to a network they should be allowed. Another step is to do a factory acceptance test on the IoT devices we use within the business to understand how secure they are and how much trust can be put within the devices and the company producing them. These are some steps we can take along with following the Security Frameworks to better secure ourselves from these security risks. As the research has shown, IoT devices are increasing at a high volume and organizations are starting to implement them even though they are aware of the risks. As they continue to grow it opens the doors for more attacks on both the organizations and the users, to avoid this we should take the appropriate steps to be aware of the consequences and what we can do to manage them and better secure ourselves and our organizations. The attackers will never back down from trying to pry any sensitive information, so why are we not trying to better our own security to protect against their advances.

References:

Print Sources:

Alam, Tanweer. (2018). A Reliable Communication Framework and Its Use in Internet of Things (IoT). 3.

Braganza D, Tulasi B. RFID Security Issues in IoT: A Comparative Study. Orient.J. Comp. Sci. and Technol;10(1) http://dx.doi.org/10.13005/ojcst/10.01.17

Computer Security Division, I. T. L. (n.d.). About the RMF - NIST risk management framework: CSRC. CSRC. Retrieved from https://csrc.nist.gov/projects/risk-management/about-rmf

CVE-2021-28372. CVE. (n.d.). Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28372

Cybersecurity framework. CISA. (n.d.). Retrieved from https://www.cisa.gov/uscert/resources/cybersecurity-framework

Financial Crime and Identity Theft. Financial crime and identity theft. (2005). Retrieved from https://www.ncjrs.gov/ovc_archives/ncvrw/2005/pg5i.html

Industrial internet of things market size report, 2022-2030. Industrial Internet of Things Market Size Report, 2022-2030. (n.d.). Retrieved from https://www.grandviewresearch.com/industry-analysis/industrial-internet-of-things-iiot-market

M. Guizani, A. Gouissem, K. Abualsaud, E. Yaacoub and T. Khattab, "Combating Jamming Attacks in Multi-channel IoT Networks Using Game Theory," *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, 2020, pp. 469-474, doi: 10.1109/ICICT50521.2020.00081.

Outline of ISO IEC 27001 2013 information security standard. (n.d.). Retrieved from https://www.praxiom.com/iso-27001-outline.htm

P Thanapal et al 2017 IOP Conf. Ser.: Mater. Sci. Eng. 263 042049

R. Davis, "The data encryption standard in perspective," in *IEEE Communications Society Magazine*, vol. 16, no. 6, pp. 5-9, November 1978, doi: 10.1109/MCOM.1978.1089771.

Sen, & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, *32*(2), 314–341. https://doi.org/10.1080/07421222.2015.1063315

The five functions. NIST. (2021, May 12). Retrieved from https://www.nist.gov/cyberframework/online-learning/five-functions

Thomas, D. (2018), The Costs and Benefits of Advanced Maintenance in Manufacturing, Advanced Manufacturing Series (NIST AMS), National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/NIST.AMS.100-18

Wen, Li, X., Zanotti, T., Puglisi, F. M., Shi, Y., Saiz, F., Antidormi, A., Roche, S., Zheng, W., Liang, X., Hu, J., Duhm, S., Roldan, J. B., Wu, T., Chen, V., Pop, E., Garrido, B.,

Zhu, K., Hui, F., & Lanza, M. (2021). Advanced Data Encryption using 2D Materials. *Advanced Materials (Weinheim)*, *33*(27), 2100185–n/a. https://doi.org/10.1002/adma.202100185

Wyss, Gregory Dane, Sholander, Peter E., Darby, John L., and Phelan, James M. Identifying and Defeating Blended Cyber-Physical Security Threats.. United States: N. p., 2007. Web.

Online Sources:

2019 internet of things industry trends analysis: Internet of things: Comptia. Default. (n.d.). Retrieved from https://connect.comptia.org/content/research/2019-trends-in-internet-of-things

Admin. (2021, December 7). What is Smart Home Technology and how does smart home works? SMLease Design. Retrieved from https://www.smlease.com/entries/automation/what-is-smart-home-technology-and-how-it-works/

Mandiant. (n.d.). Vulnerability-disclosures/feye-2021-0020.MD at master · Mandiant/vulnerability-disclosures. GitHub. Retrieved from https://github.com/mandiant/Vulnerability-Disclosures/blob/master/FEYE-2021-0020/FEYE-2021-0020.md

Schiffer, A. (2021, December 5). How a fish tank helped hack a casino. The Washington Post. Retrieved from

https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

Watters, A. (2022, February 10). 30 internet of things stats & facts for 2022. Default. Retrieved from https://connect.comptia.org/blog/internet-of-things-stats-facts