Abstract

It is evident through global market trends that people of the world are directing their lives to be more and more smarter. That is where smart devices come in to play. Smart devices industry has the needed potential to gain speed in innovation. However, first, this industry of manufacturing smart devices needs to be reformed in terms of security measures taken within the devices and Artificial Intelligence to be embedded. The research for this essay was done by viewing informative videos on Youtube and reading various news articles.

Introduction

Do individuals of the world perceive that a fully modern and automated home with latest IoT (Internet of Things) devices will give them a medal of satisfaction and modernization for achieving to fully automate their home or bringing out new devices? Mainly, is it merely possible to do so? Well, if we put it in to more context, it solemnly depends on the various implementations, that exact individual desires to impose on a target house which they seek to modernize. Smart homes that are well implemented with ideas of full home automation are undoubtedly becoming the norm, as the whole world is upgrading all of their current systems, and latest upcoming devices being rolled out to the world market in the near future to definitely be 5G compatible. We often see major telecommunications companies, that dominate the world stage like Apple, Huawei and Samsung are seen always at the first to bring out new world changing IoT devices. An extremely good example of a country that has a good implementation of IoT services and is a hub of the newest 5G devices implemented is South Korea. The country not only has a good telecommunications infrastructure, when it was already using 4G technology, but also it is the only country in the world at the moment where everything and anything can be done by using IoT devices and the power of the internet. China comes a close second. It somehow always starts with the most simplest things, that we as individuals use on a day to day basis. The devices ranges from refrigerators, toasters, televisions, game consoles and the list goes on and on to expand our imagination of what we could use for IoT. It is clearly evident that even independent IoT devices could use help from a server and well implemented Artificial Intelligence system only catered for a universal or set of IoT devices by a desired company. Even if we were to develop a brand new Artificial Intelligence ecosystem or use an already available ecosystem for example probably by Samsung or Apple, devices that these companies manufacture can function seamlessly inside of our smart home fully equipped with the latest and greatest industry leading smart technologies with Artificial Intelligence built inside.

Body

The main question being, what actually is a smart home? A Smart Home can be defined as a home that implements smart devices connected to the Internet that has the potential to remotely monitor and manage various other systems and appliances that exist inside a home or a building. A number of prerequisites are needed to be fulfilled before we can declare any home or a target project we have in mind to be built as a "Modern Smart Home". The general prerequisites needed to be fulfilled before we can declare a home to be smart, ranges from type of device, firmware, security aspects and hardware. As a first thing clearly to mention, for anyone who is set out to build a smart home, that individual obviously needs smart IoT devices, embedded with the latest industry leading hardware and firmware for end users to implement well inside the systems of a target project or home. According to the informative article published on (PCMAG, 2020), devices ranging from the new Amazon Echo Family, to the Google's Nest Family, are two of the many essential IoT smart devices needed to be implemented by any individual seeking to build a new smart home in this day and age. Whilst giving a tour (Hey Ashley Renne, 2019) around of her smart home, went on to gave really good 21 ideas of what a mere perfect smart home implemented with tons of smart IoT devices, will look and feel like, both instances of devices being used inside and outside of her home. Outdoor devices such as solar panels, lawn mower's and water sprinklers for the outdoor porch can be connected and controlled through our personal devices with an application via an internet connection. Her smart home tour shown in the video is one of the many projects where IoT and smart devices have been implemented and has thrived in their use.

As mentioned heavily before above, modern smart devices play a key role to making a smart home, and not only smart devices are needed to fulfill the task of building a smarter home. One of the main key features, of a good smart device is the smart device having a good built-in firmware needed for these smart devices that we want to use in our smart homes and elsewhere. Firmware of a smart device play's a pivotal role, on how the smart devices are used by the end user, and how successful it becomes in the World market. Any company can come up with the latest device, but if the firmware of that device is not up to par, then it will not be accepted by consumers and the smart device will lose their credibility in the consumer market. One of the main reasons being, smart devices with poor firmware has the potential to receive low reviews by end users for poor user friendliness.

Ken Muro a Security Researcher and an ethical hacker (TEDx Talks, 2018), gave an insightful talk about Internet of Things and various security aspects and vulnerabilities associated to it. In his talk he stated that manufacturers of various IoT devices that ship out new devices to the World market rarely or never focus on the security of IoT smart devices they manufacture. He further went on to

explain, that how easy it is to unlock various devices by ethical hackers such as him, and that simple household used smart appliances, such as smart electric kettles using customary apps, Bluetooth and WiFi could easily be exploited. Yes, the IoT smart devices can be easily hacked by hackers, and most of the times hackers will often do so without being near to any of these devices. They will seek various vulnerabilities and implications in your IoT smart devices from afar to later gain access to your personal internet connection to further exploit your system. Other smart devices that happen to be connected to the target internet connection will be manipulated by the hackers. Ken further went on to mention on how easy again it is, for ethical hackers to steal your personal home's WiFi username password just from exploiting a simple IoT smart device such as smart thermostat connected to the internet to compromise again, all of the other existing devices that are used inside that target internet connection. Then he brought out a IoT child's toy as an example that could be hacked so that it can be used to listen, talk and spy on people who use it and others who are close to toy's owner as well as, how IoT smart devices we use on a day to day basis can be weaponized by hackers to hold our devices on ransom.

Every week or so we often see articles circulating on the mainstream news channels and on the Internet news websites about various security vulnerabilities and implications related to devices related to the Internet of Things. An informative video published by (The Hookup, 2019), in the video, the presenter discusses various vulnerabilities and the implications that follow relating to smart devices relating to Internet of Things. Later on he shed light upon few drastic steps people need to do to drastically decrease common seen vulnerabilities and increase the overall security of your personal home's internet connection and of your Internet of Thing's smart devices. An informative article (Krastev, V 2019) written in reference to the Anti-virus and security oriented company Avast, the article suggests that about 40% of smart homes that exist are extremely vulnerable to system exploitation by Grey and Black hat hackers. As well as, most of the most targeted devices by these hackers seem to be printers and internet routers.

With the implementation of Artificial Intelligence in various smart devices and making of smart homes with smart IoT devices will leap many walls of achievements that the IoT manufacture industry has been seeking to find for a long time. An article published on (Medium, 2019) describes in detail in that the coming future all homes that will exist globally and IoT devices will be equipped with the latest industry leading ideas of Artificial Intelligence. Already, in the world market, there are smart home devices such as Samsung's smart vacuum cleaners that has an inbuilt firmware that it helps to map out a path inside a given space for it to clean. Once the cleaning of the path shown is done, the smart vacuum cleaner goes back and attaches itself to the charging dock to be used for later. We already have the equipment and firmware needed to build an efficient IoT

smart device. All we need is a reliable major telecommunications company like Apple or Samsung, to develop a new series of smart devices with Artificial Intelligence, using ideas of Artificial Intelligence such as Machine Learning to further make the already smart device even smarter. Artificial Intelligence, once mixed with smart devices made available on the consumer market has the potential to become market changers. A simple device like a dishwasher, washing machine or a refrigerator could be fitted with Artificial Intelligence.

As well as, another step we could take is manufacturing of potential attachable devices. Which can be commonly found on devices like the Playstation 4/5 Video Game console's game controller's, Dji Pocket devices method of extra add on devices and many more could be a liable idea of implementation for existing and upcoming IoT smart devices. The second implementation just for the sake, that even when old technologies are left behind somehow that it should become relevant with refreshed technologies with Artificial Intelligence inbuilt in the devices that could have the needed potential to make the older smart devices with no current technologies renewable and even more long lasting when new technologies and various other smart devices roll out on the global marketplace. That will definitely make the older IoT smart devices laying around in various spaces in our home to be used again. The home still stays smart. So, that the smart device caters their services to the specific user rather than acting upon a series of commands engraved by the manufacturing company where the device was manufactured.

Conclusion

As we to a conclusion of this essay, it is good to state again for context's sake that various smart devices that come under Internet of Thing's, and various implementations of it when used with ideas of Artificial Intelligence as well as, simple home appliances embedded alongside the smart device's firmware which should also be well developed for each Internet of Thing's smart device is definitely the future for the world of Information Technology and Internet of Thing's. As well as, for a good Internet of Thing's smart device to be a reliable global market changer with credibility in firmware, hardware and security, the smart device definitely has to be innovative, as mentioned before, Artificial Intelligence to be embedded within it and the overall security of the device should always be up to par so that the user has a seamless use experience. As well as, the device has to be safe enough to use that it does not compromises other Internet of Thing's devices and the internet connection the smart device is connected to is not compromised at all leaving other devices available in that internet connection being exploited. Also that old devices to be used with new technologies.

References

Colon, A & Moscaritolo, A (2020) *The Best Smart Home Devices For 2020.* Available from: https://www.pcmag.com/news/the-best-smart-home-devices-for-2020 [Accessed 20 November 2020].

TEDx Talks (2018). Internet of Things Security | Ken Muro | TEDxDornbirn. *Youtube*[video]. 28 September. Available from: https://www.youtube.com/watch?v=pGtnC1jKpMg [Accessed 21 November 2020].

The Hookup (2019). IoT Security Vulnerabilities: Quick fixes and realistic discussion about smart home security. *Youtube*[video]. 13 March. Available from: https://www.youtube.com/watch?v=pGtnC1jKpMg [Accessed 21 November 2020].

Krastev, V (2019) *40% Of Smart Homes Currently Vulnerable To Hacking.* Available from: https://sensorstechforum.com/smart-homes-at-risk-to-hackers/ [Accessed 21 November 2020].

Joshi, R (2019) *IoT and Home Automation: What Does The Future Hold.* Available from: https://rasikaj39.medium.com/iot-and-home-automation-what-does-the-future-hold-d0a1e6145b9 [Accessed 21 November 2020].

Hey Ashley Renne (2019). ULTIMATE SMART HOME TECH TOUR: 21 Home Automation Ideas for 2020. *Youtube*[video]. 7 December. Available from: https://www.youtube.com/watch?v=9u9kqhHC6Ok [Accessed 20 November 2020].