Annotated Bibliography

GRAD 695-91- O-2021/Spring – Research Methodology & Writing

Suraj Pratap Samirlal Poddar

ID: 275644

**Internet of Things**

**Introduction**

IoT refers to Zillions of physical devices across the globe which are connected to Internet collecting and sharing data. Any device which can be connected to Internet and can be controlled for information, can be labelled as an IoT Device. It can be any smart Device ranging from a light bulb at your home which can be controlled/operated from your smart phone to Smart cities to a Driverless car/truck, pretty much everything that can add intelligence and provide a valuable information

**Jen Clark, “What is the Internet of Things (IOT)?” IBM, at** [**https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/**](https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/) **(November 17, 2016)**

The author of the article explains what is IoT and how does it works? The author describes IoT as a massive/large Network of connected objects and user, any device which can collect data and apply analytics to provide with a valuable information tailored as per their specific needs useful to help us think smarter

The Author also provides a basic example of how IoT can be useful in a car manufacturing business, by deploying sensors to align sales or to identify the components which sells fast or to determine where the customers line up the longest for most popular item can be achieved easily via an IoT device which can help the business owners to make smart decisions down the road when determining what items/components to stock up on by relying on real time information

IoT Platforms can be put to play to detect problems, determine patterns, provide suggestions/recommendations by analyzing the collected data

**Kumar, S., Tiwari, P. & Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: a review. *J Big Data* 6, 111 (2019).** [**https://doi**](https://doi)**.org/10.1186/s40537-019-0268-2**

The following paper published in 09 Dec 2019 states how Internet of Things has taken an revolutionary approach which has changed the normal way of living to a advanced life Style. IoT devices are being used in building smart houses, smart cities, smart transportation, industries almost everywhere where technology is available. This paper provides an overview from both social as well as technological standpoint

The paper describes & discusses various challenges and issues which needs to be addressed to achieve/unveil the most or to operate in full force with IoT. These can be related to architecture, application or even to expose the existing literature and their respective contribution to various aspects of IoT

The article helps us understand when and where IoT is applicable in the real world in this technological enhancement

**Daniel Burrus, “The Internet of Things is Far Bigger than Anyone Realizes” WIRED at** [**https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/**](https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/)

The article talks about the “buzz surrounding IoT”, as per the author IoT is increasingly found around machine-machine comms which is built on the Cloud and has networks to hoard data through sensors, most of the devices operating as IoT are mobile, easy to use and provides instantaneous connection which is going to make our lives easier from traditional way of living to adopting smart way of living

However, people still don’t realize how big of a deal this is, lot of them they focus on machine-machine comms i.e, devices talking to alike devices, however a machine is a tool or an instrument that is supposed to physically do something. Then author says when he cites making the machine smarter, he is alluding to the fact that it’s not strictly machine-machine but he is referring to sensors.

Sensors are not machines on the other hand, the concept of IoT can only be pulled together with a combination of sensors and machines, the whole point is not only to gather data but also to leverage it. The data gathered by the sensors are of no use if you do not have the underlying infrastructure or a workspace to analyze

IoT does not function without the cloud-based model, the cloud is what activates the application to work from anywhere /anytime

**Darren Anstee, “The Rise of the Internet of Things” by Security at** [**https://www.securitymagazine.com/articles/91570-the-rise-of-the-internet-of-things**](https://www.securitymagazine.com/articles/91570-the-rise-of-the-internet-of-things) **(January 20,2020)**

The article talks about the exponential increase of IoT devices and what does this means from a Security Standpoint. With IoT advancing at a faster pace, people have expressed concerns on how this could be an issue with security. The author describes how a new gen malware can now target and exploit Gadgets quicker and faster than before and the average time recorded to hack/compromise a vulnerable IoT device is less than 5 min

The article also describes about 5G I,e how a mm wave technology can be useful for IoT devices helping them transfer wide range of application and to make the matter worse making the devices obsolete. Even with different providers making software updates and releasing them in the form of patches are not subject to real time. They don’t consider whether a person is technologically aware to perform update nor they take the device location into consideration

IoT is driving a reforming technological and a lifestyle change revolutionizing our current IT perspective. They are to bring innovation in public, transport and health utilities. Users are eagerly waiting to leverage the features of high-speed transfer rate with advanced user experience. That being said both Business and consumers are only going to be safe with a strong security by ensuring privacy, reliability and availability

**Best,Jo, “Who Really Owns your Internet of Things Data?” ZDNet (January 11, 2016) at** [**https://www.zdnet.com/article/who-really-owns-your-internet-of-things-data/**](https://www.zdnet.com/article/who-really-owns-your-internet-of-things-data/)

The article brings some light to user data, there is no actual/exact way to measure data when referring to IoT devices. User data surrounding Twitter, Facebook, Google are slowly fading out and becoming irrelevant when compared with smart devices i.e, IoT devices. In Majority of the cases no one knows who the gatekeeper of data is or who is the owner of the data, the ownership has always been debated and is not something which consumers will like

Since majority of the IoT devices are built on smaller chips it becomes challenging to ask for Users permissions vs keying in accept or reject. In most of the scenarios IoT devices needs to be connected and configured by smart phone or an online service at least provides an opportunity to keep the users informed about their data processing terms and conditions

The article also talks about the differences in internal data vs external data and points out the external data should be used by consumers; they should have the full control to this data. Data ownership in IoT needs to be revisited and re assessed

**Nerming, Hajdarbegovic, “Are we creating an insecure Internet of Things (IoT) Security Challenges and Concerns” at** [**https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things**](https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things)

The editor has expressed concerns with the level of Security and respective challenges and its concerns on IoT devices. The first thing that comes to anybody’s mind when connecting to Internet is Security, that should be the foundation for IoT devices, however there is no harmony on how to build it and hence the IoT devices are susceptible to threats & malicious attacks. The Editor describes 3 key challenges for the upcoming future, Security Risk, Data collection and misuse of consumer data

It is known that the Hardware on IoT devices has always been a problem because of their tiny size, as the IoT market expands chipmakers will adopt to provide better security with every new generation as that can be a deciding factor for the users

Creating access control and binding them with authentication methods can be a plus, however creating security /controls on a cheaper hardware without compromising user experience and without adding additional resources looks to be little challenging. It becomes very important to understand the data risk associated with these devices and make sure to protect your data or keep as much private data as possible from IoT devices

**Paul, Stuttard, “The treacherous waters of IOT Security” at** [**https://www.itweb.co.za/content/o1Jr5qx9WjAvKdWL**](https://www.itweb.co.za/content/o1Jr5qx9WjAvKdWL) **(June 1st, 2020)**

The article provides insight to how Cyber-attacks can continue to linger on IoT platforms by providing a never before attack surface. We already know the use of IoT devices have been inflating 30% every year and more than 20Billion IoT devices was being estimated to be operational by the end of 2020 as per the research

Next Gen IoT devices which is well known for their data gathering, analyzing and tracking are widely becoming demanded by logistics, supply chain, finance, transport and many other industries who are trying to adopt this at a faster pace. In order to mitigate Risks, the organization has to undertake risk mitigation techniques to examine vulnerabilities in IoT devices. Fortunately, there have been new tools which are being released to identify the risk and report any anomalies if found

Unlike phones, IoT devices are manufactured by a wide variety of third-party vendors and therefore it becomes imperative to include critical information like the model, SN and manufacturer information with their respective location, OS and application running on the chip. On the other side the organization are confidently moving forward with toxic water of IoT security

**A. Yousefi and S. M. Jameii, "Improving the security of internet of things using encryption algorithms," 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, 2017, pp. 1-5, doi: 10.1109/ICIOTA.2017.8073627.**

The paper talks about a proposed hybrid encryption algorithm which has been tested to enhance encryption speeds by using less computational complexity at the same time by reducing safety risks. The entire purpose of an encryption algorithm is to design information confidentiality and integrity in exchange to IoT. As per the paper the algorithm has been simulated in Matlab to test the speed and safety in combination with conventional encryption

IoT in the paper describes about a wireless sensor in combination with radio frequency id to achieve reliable transfer and intelligent processing of information by protecting privacy and safety. The paper also describes about different network attacks which can be mitigated by properly placing them behind the Firewall and in the private network to protect from external world

The paper further describes about the encryption attacks and explains about the cipher and side channel information that gets generated from the encrypting devices. Providing security is challenging, however looking at the existing threats the level can be raised for the future upcoming IoT devices

**Jeff, Plitch, “IoT is more prevalent in Real Estate Than you may think” at** [**https://www.fool.com/millionacres/real-estate-investing/articles/iot-is-more-prevalent-in-real-estate-than-you-may-think/**](https://www.fool.com/millionacres/real-estate-investing/articles/iot-is-more-prevalent-in-real-estate-than-you-may-think/) **(Jan 31,2021)**

The article shows how IoT devices are being used in the current Real Estate business. It also stresses on how 5G can expand the overall bandwidth of the devices by allowing them to a greater adoption. In simple terms IoT is combining numerous interconnected devices and connecting them to the real world making this industry the perfect match for this technology

While dealing with Residential or commercial assets, cost savings from energy usage, elevators, pumps, fans, exhaust, water meter, HVAC, protecting or mitigating from potential leaks and many more which easily integrates with Vendor Management system or their respective energy management tools to deliver proactive measure from sensor data

**Shanika, Perera, “The Power of combining AI and Internet of Things” at** [**https://towardsdatascience.com/the-power-of-combining-ai-and-iot-4db98ac9f252**](https://towardsdatascience.com/the-power-of-combining-ai-and-iot-4db98ac9f252)

Artificial intelligence is a computational tool which can be a substitute for human intelligence, AI makes the machine learn from experience and tries to perform human like tasks. AI has replaced lot of human jobs already and will be continuing to do so as it becomes widespread. The combination of AI with IoT can bring some extraordinary performance

IoT devices are known to collect data which can then be integrated to AI. This can help identifying pattern and detect anomalies in the data it collects from various sensors. With AI powered IoT we can avoid unplanned downtime, enhance risk management, enable improved products and services and also increase operational efficiency with life changing performance