XIV International Conference on Recent Trends in Engineering, Science and Management
Osmania University Centre for International Program, Hyderabad (India) (ICRTESM-18)
29th July 2018 www.conferenceworld.in ISBN:978-93-87793-36-1

IoT For Healthy Eco System

Hiren Modha

[1]*Assistant Professor, E.C. Department S.V.I.T. VASAD, GTU (INDIA)*

ABSTRACT:

The Internet of Things (IoT) has the possible to propose dealing cost that goes ahead of operational cost savings. Providers in the IoT ecosystem have a principally unexplored chance to expand gripping IoT solutions that explore how the ability to accumulate and analyze different data, in real-time and across time, might transform the business. These developments will play out within and across enterprises, offering opportunities for sustained value creation and even disruption for those who can imagine possibilities beyond the incremental.

Keywords: IoT: Internet of Things

I. INTRODUCTION

By 2020, there will be more than 20 billion devices connected to the Internet of Things (IoT), according to Gartner that's roughly 2.5 devices for every single person on the planet. And that's just the beginning of what is swiftly becoming an explosion in connectivity, which could result in virtually every household item and all industrial electronic equipment being capable of exchanging data with other devices. We already rely on IoT on a daily basis, but this ecosystem will become even more indispensable in the future. Not only will it enhance quality of life for individuals allowing us to control our homes with just a swipe on our smart phones, for example it will allow companies to create new business models and to be more proactive in how they maintain their assets and equipment. And, in India, which suffers from congestion in many urban areas, IoT can act as a platform for smart cities by empowering local authorities to effectively manage traffic and to reduce noise and pollution [1]. According to Business Insider the IoT ecosystem is comprised on an entity (smart phone, tablet, etc) that functions as a remote to send a command or request for information over the network to an IoT device. The device w ll then perform the command or send information back over the network to be analyzed and displayed on the remote. This broad definition of the ecosystem can be applied to specific industries such as auto manufacturing companies that create smart cars equipped with sensors that send engine data back to the manufacture to improve on future models. With opportunities for leveraging the IoT ecosystem across an array of industries, every business from consumer facing devices to helping create smart cities [2].

II. IOT ECOSYSTEM OPPORTUNITIES

With over 24 billion devices expected to be installed by 2020 according to Business Insider, the IoT ecosystem will touch almost every industry, including transportation, insurance, utilities, telecom, healthcare, smart homes, oil and gas and more. The investment in these opportunities over the next five years are expected to result in $13 trillion return on investment (ROI) by 2025. The main barriers around the Internet of Things remains security, implementation and technological fragmentation. Horizontal management for IoT addresses several of these concerns. A standards-based, horizontal platform allows for greater access control to give control over Internet of Things devices and sensors. Organizations are able to manage data with end-to-end authentication and scale solutions across all vertices without having to be a solution for each application.[3]

III. SECURITY RISKS

Broadly speaking, IoT is great news for society as a whole, but, like all emerging technologies it fuels emerging risks. We need to understand these risks if we are to manage them and to help ensure that the technology is used as a means to achieve positive progress. Primarily, we have identified four main risks that require careful consideration and the implementation of strict cyber-security controls. The first, most obvious, threat is the risk of an IoT network being hacked, with potentially devastating results. Just think of the human and physical damage that a hacker could inflict by taking control of a self-driving car, for example. Security should be a fundamental pillar of any IoT network, and it should be in place from the outset. We must learn from the early days of the internet, when design, functionality and experience took precedence over security, for which the cost was deemed to undermine the business case. Similarly with IoT, taking short-cuts in security at the early stages will only lead to businesses having to make expensive reparations later, provided they manage to survive a breach and uphold their reputation. Secondly, testing IoT infrastructure presents a significant risk. The nature of the technology means that IoT is currently being implemented in a fairly agile way, with new devices and sensors being introduced on an ad-hoc basis and people experimenting as they go along. In the past, the rollout of new technology would only have been undertaken once thorough testing of an entire solution had been completed. With IoT, however, the infrastructure is not being tested at all rather; it is being honed and fine-tuned in a “live” setting. What’s more, no one is necessarily checking that the data sent by the sensors on different devices is actually accurate. Instead, people tend to assume that the sensors are properly calibrated and the information they provide is secure and correct.Having accurate data is critical in an environment in which machines are talking to other machines and making decisions without interacting with humans. Organisations should use tools like artificial intelligence (AI) and statistical analysis to identify those sensors that are producing accurate data, and those that are not. [4]

IV. PRIVACY ISSUES AND MACHINE DEPENDENCY

When fragmented data is collected and analysed from multiple end points, the possibility of it remaining anonymous is highly unlikely. What's more, it may yield sensitive information. When they sign up for services, customers should therefore be mindful of the data permissions they are granting and push vendors for transparency.Lack of awareness around privacy controls may expose customers' personal data so it can be used for unauthorised purposes. In addition, IoT devices generate a lot of unstructured data; any data analysis conducted on this raw data could generate an inaccurate representation of the individual and reflect incorrect behavioural patterns.

Finally, human behaviours and social engineering are major risk factors in an IoT environment. Take traffic lights, for example. We all know that red means stop, yellow means wait and green means go. What would happen if someone were to turn all the traffic lights in a smart city to green? Would people stop and think, or would they just keep driving? It is clear that, just as infrastructure needs to be protected from cyber threats, people need to be educated so they are able to challenge algorithms generated by machines that are responding to incorrect information. Ultimately, cyber-security controls can be perceived just as a means for resisting threats, or they can be viewed as a catalyst for transforming IoT into an ecosystem like that adopted by the airline industry. Safety, standards and regulation have all evolved since the industry first got off the ground in the 1920s, which may be why air travel is the safest way to travel today. If we implement IoT security with the same level of vigour that the airline industry applies to safety, the technology will engender trust and drive the creation of new businesses and industries. India is at a nascent stage when it comes to IoT, and adoption is slow compared with the rest of the globe. Many Indian organisations are still content with legacy IT over cloud infrastructure, making IoT a low priority in terms of changing business processes. Nevertheless, the government's 'Digital India' and 'Smart Cities' initiatives are accelerating India's journey towards adopting digitalisation. On this journey, it is imperative that adequate measures are taken to secure the IoT ecosystem, and to prepare organisations to unleash the full potential of IoT by mitigating the associated governance, privacy and security risks. The authors are EY Global Internet of Things Leader and Information Security Partner, EY India, respectively. The views do not necessarily reflect those of the global EY organisation or its member firms. The special issue invites original research in the field of IoT for eHealth, elderly and aging. Also high-quality surveys, tutorial and best practices showing the state-of-art and the latest trends are invited. Moreover, real case studies also constitute an interesting element of the special issue, to illustrate the applied aspects of IoT in healthcare, medical sciences, elderly care and aging, using real life scenarios.

Topics covered in the special issue include, but are not limited to IoT sensors for smart Health devices and Data Mining in Health.

V. AGRICULTURE FIELD

Demand for goods of agricultural enterprises is constantly growing to keep up with the world population growth. At the same time the development of the industry enterprises assumes not just horizontal scaling but also a way to increase efficiency. With the development of information technologies, emergence of new low-cost and reliable communication channels as well as electronics development undergoing a real revolution. In order to increase efficiency, the latest technologies are being introduced everywhere, and more and more processes are being automated. For vehicle like Tractor, tracking working hours of drivers and fuel consumption. Also for location finding use GPS. Proper storage and processing of agricultural products significantly reduces loss of raw materials or their depreciation. Automating such processes as cleaning, sorting, and processing can significantly increase the shelf life of crops as well as lower personnel costs. It is possible to perform remote monitoring and control of soil plants animals, irrigation system feeding and other process by multiple sensors using single network [3][4][5].

CONCLUSION

With use of Iot the operations of different process becomes flexible cost saving and it help issues related eco system. Also security and other factors can maintain. In next era of generation Iot is required for all purpose.

REFFERENCES:

[1] https://www.thehindubusinessline.com /opinion/time-to-secure-the-iot- ecosystem /article 23961720.ece

[2]https://internet-of-things innovation.com /iot-ecosystem/

[3] https://ieeexplore.ieee.org/document/ 8081906/

[4] https://**ieee**xplore.**ieee**.org/document /6755306/

[5] **ieee**xplore.**ieee**.org/document/795536