FUTURE AND CHALLENGES OF INTERNET OF THINGS

Falguni Jindal[1], Rishabh Jamar[2], Prathamesh Churi[3]

[1,2]Bachelors of Technology in Computer Engineering
SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering, Mumbai, India
[3]Assistant Professor (Computer Engineering)
SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering, Mumbai, India

ABSTRACT

The world is moving forward at a fast pace, and the credit goes to ever growing technology. One such concept is IOT (Internet of things) with which automation is no longer a virtual reality. IOT connects various non-living objects through the internet and enables them to share information with their community network to automate processes for humans and makes their lives easier. The paper presents the future challenges of IoT , such as the technical (connectivity , compatibility and longevity , standards , intelligent analysis and actions , security), business (investment , modest revenue model etc.), societal (changing demands , new devices, expense, customer confidence etc.) and legal challenges (laws, regulations, procedures, policies etc.). A section also discusses the various myths that might hamper the progress of IOT, security of data being the most critical factor of all. An optimistic approach to people in adopting the unfolding changes brought by IOT will also help in its growth.

KEYWORDS

IoT, Internet of Things, Security, Sensors

1. INTRODUCTION

The Internet of Things (IoT) is a synonym for the fully interconnected world [1]. It connects all the things with technology and makes a whole new separate world for them to interact with each other with the help of internet. IOT is not just a concept but can prove to be a revolution in advancing technology to change the lifestyles of humans altogether [2].

IOT is something that will not leave any physical or theoretical concept unaffected. As it demands communication between objects, everybody should be able to fetch any content from any device at any point of time from anyone located anywhere and who is a part of any business or service, through any path or network. Constructively, 'availability' is a critical factor that affects the performance of IOT [3].

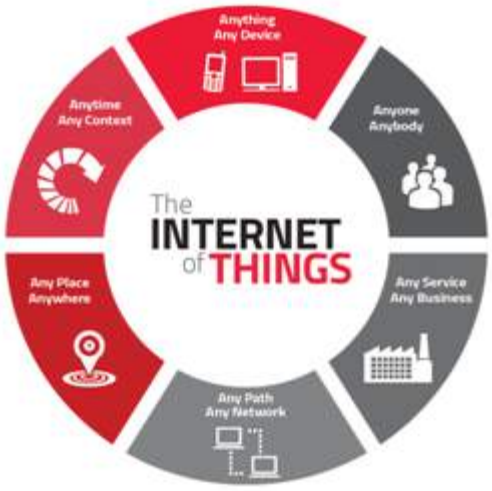

Fig. 1. Broad Definition of Internet of Things

To understand it better, let us consider this scenario of driving to a train. There is a network of the internet to which all the things like AC, alarm, cars, coffee maker, maps, calendar, fuel indicator etc. are connected. Now suppose your meeting got delayed and will start 45 minutes. Later in the morning than scheduled, the system will notify that you might want to sleep 45 minutes. Late because of the change. The system also indicates the change in train schedules and fuel levels. The traffic clogging indications by maps can help you avoid delays and change routes before engaging in accident scenes, to reach on time. While all this is happening, it is also communicated to things like the alarm which automatically snoozes for 5 minutes.., the car melts the ice that accumulated overnight, and the coffee maker is made ready to make coffee after 5 minutes [4].

Fig. 2. General Example of Internet of Things

According to a survey done in 2014 – 2015 [5], there was a grand movement in the understanding and prioritisation of IOT among people in just one year. When asked about their interest in IOT and their engagement with it, some awareness parameters seemed to have almost doubled their percentage values from the last year.

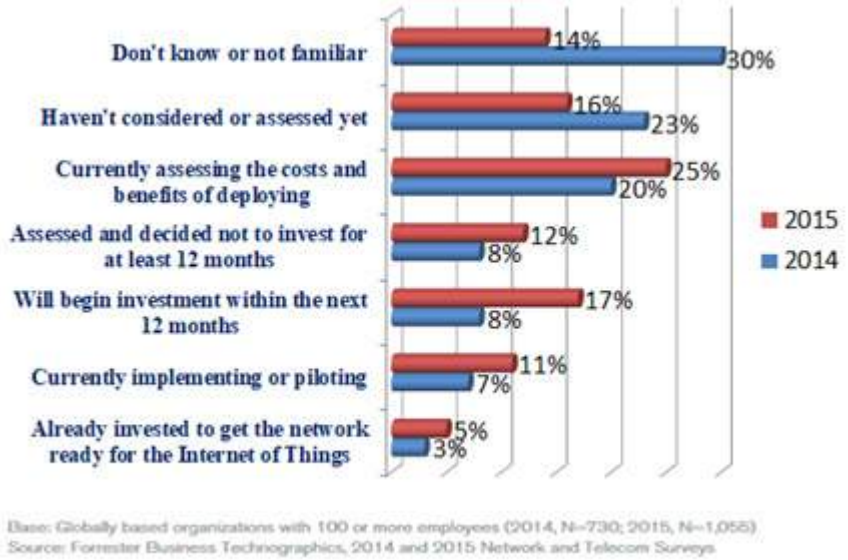

Fig. 3. Survey of understanding and prioritisation of IOT Technology

2. GROWTH OF INTERNET OF THINGS OVER PAST YEARS

The graph below depicts the growth of IoT over the years. In 1992, only 1,00,000 people were using IOT as a technology. Till 2003, the number grew to half a billion people. While 2009 marked the IOT inception, 2012 witnessed a sudden increase in the usage of IOT where the people using IOT reached 8.7 billion, and there was no looking back. The number of users has been growing exponentially over the years reaching 28.4 billion in 2017. It is expected that the number will broaden to 50.1 billion by 2020. [6]

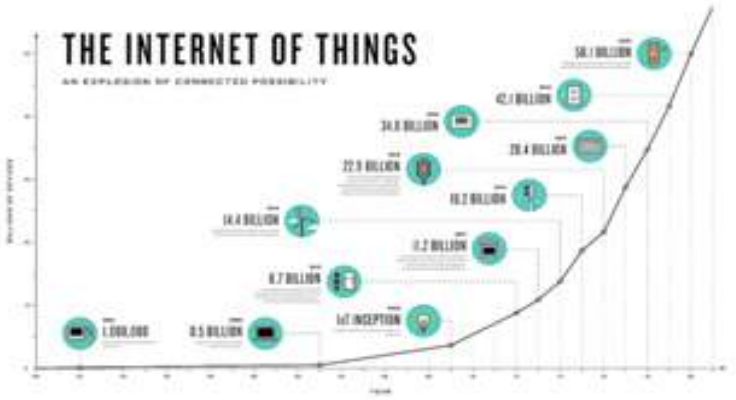

Fig. 4 Survey of Growth of Internet of Things over past years

3. IOT INFORMATION LIFECYCLE [7]

According to Red-hat Information Lifecycle cited in [21], Data that is generated and collected by sensors, actuators, human interfaces, control panels etc. are analyzed initially (field level) to produce information which can be used for further analysis and performing actions. This data is

further processed and examined to decide the desirable steps that need to be taken. The Information produced at this stage is used to trigger pre-defined business rules that correspond to it. The Intelligence of the system takes the normal actions required to respond to the environment. The information gained from this experience is then summarized and sent to the knowledge base where it is stored and used for deep learning and analysis to draw new conclusions. New rules created here are sent to the Intelligence module to add to its accuracy, and more optimized tactical tools generated in the knowledge base are forwarded to the Information module to add to its expertise in analysis of data. The knowledge base is controlled, modified and amplified by experts of the domain the system belongs to.

3.1. General View

IOT provides various kinds of services, works with some technologies and has a different meaning for different people. Sensing through accelerometer , pressure etc., embedding processing of devices (MCUs , MPUs, hybrid etc) and connectivity through Wi-Fi, cellular data, NFC, GPS etc. are used by software's to provide numerous services like Supply chain automation, auto safety , M2M, pedestrian navigation, remote appliance avoidance, air quality control and BLDG automation. These applications have given birth to smart health, tags, cars, lighting, grid, energy, parking and homes.

IOT has also resulted in various technology innovations including miniaturization, advancement in packaging process and flash.

3.2. IoT Technical Ecosystem

The IOT Ecosystem comprises of processors (Arm Cortex-M, Arc, and Quark etc.), operating systems (uCLinux, Embedded Linux, Android Auto, Ubuntu, TinyOS.) devices and aggregators (Access points, routers, ZETA platforms etc.), Infrastructures (Cisco lox (fog)) and platforms (BeagleBone, Rasberry PI, Arduino etc.)

It also consists of two essential members Interoperability and IOT Protocols. Interoperability term comprises of Open Interconnect Consortium whose mission is to develop technology standards and certification for devices involved in the IoT; APIs such as IOBridge, COSM etc.; Reference Implementations (Intuity) and Integration Frameworks which include Apple HOME KIT, Temboo, CROWNSet, WeMO and many more. Bluetooth, Cellular, DDS, DSRC, HTTP, Ethernet, Zwave, NFC, SATCOM etc. are some examples of IOT Protocols.

4. FUTURE OF IOT

The uncertainty and business risk is always present in any new technology. In case of IoT, it is observed that many of the dangers are physically not present somewhat they are distorted or misstated. While it will take time to develop the IoT vision fully, the building blocks to start the process are ready to be used.

The major requirements such as - hardware and software assets are either available in a less quantity or some of them are under development; it is also a fact that: the security and confidentiality concerns of IoT devices are not properly addressed over past decade. It is a whole and sole responsibility of stakeholders to collaborate and carry out the open standards to make

IoT reliable, secure and interoperable. Therefore, allowing secured services to be delivered seamlessly.

Over the next few years IoT is expected to make over $19 trillion [8]. However, the problem associated with this : these 'things' have myths surrounding them, some of which are impacting how organisations develop the apps to support them.

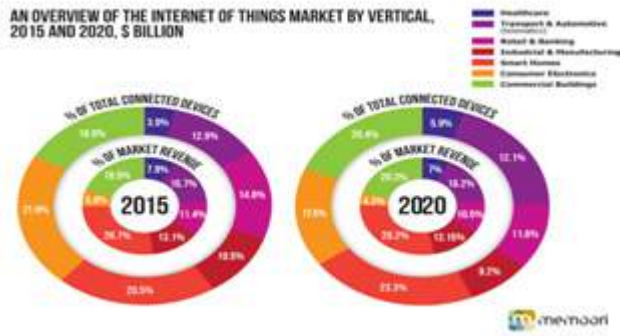

Fig. 5. Future of IoT in the year 2015 and 2020

In the above fig 5. An overview of the IoT Market in 2015 and 2020 is shown. The comparison of the percentage of total connected devices and the percent of market revenue of several verticals like Healthcare, Transport & Automotive, Retail & Banking, and Industrial & Manufacturing etc. in 2015 and 2020(expected) have been shown.

By observing the above figure, it can be expected that there might be an increase in percentage for some fields like Healthcare, Commercial Buildings, Smart Homes and Transport & Automotive while simultaneously a decrease might also be seen in Industrial & Manufacturing, Consumer Electronics and Retail & Banking over the years[9].

However, there are some myths [10] that hover around the certain future of IOT. Let us talk about each of them one by one.

4.1. IoT and Sensors

The data produced by most sensors are not used efficiently. To help the technology evolve, 62% surveyed manufacturers believe that its functionality can be improved by advancing analytics features. More training on analytics tool was also thought to be one way by 45% people. More mobility, computing power and capacity to store data were also some factors mentioned by the manufacturers.

4.2. IoT and Mobile Data

The effectiveness of the generation of data from IoT sensors is poor. The data is usually collected by smartphones which have an integral role in IoT. The user interface for IoT applications are provided by the smartphones. However, they are not a good option. The above fact is illustrated with the help of example below according to [11]:

Consider the example of home automation: in case of critical home-monitoring and security applications, is it worth to rely upon a smartphone. What will happen?

- When the person's smartphone goes into airplane mode during his travel?
- Does the electricity shut down or, his home security gets interrupted?
- What if the sensors stopped working abruptly?

Today, with no IoT administrations, most of the network traffic is through the access points of Wi-Fi. What happens when that information increments by "n" times? Likewise, mobile networks and communicating gadgets have extreme disadvantages in regions, for example, consumption of power, cost, reliability and availability.

So, will the smartphones and cellular communications will have a better place for running IoT Applications? The answer is absolute yes. But regarding performance, accessibility, cost, bandwidth, consumption of power and other key traits, the IoT will require altogether more varying and innovative variety of hardware and software solutions.

4.3. IoT and Volume of Data

The production of data of IoT applications is extensive. It is the fact that: The total amount of data being generated by IoT applications is not required to be stored on cloud as it consists of a lot of useless chatter generated by devices in which no change in state is observed [12]. The most significant challenge in this context is the selective storage of data on a cloud so that there will not be a storage issue in the future use of IoT devices. It also concludes that appropriate and correct data will be given to the user while rest (garbage) data produced by IoT devices will be deleted appropriately.

4.4. IoT and Datacenters

There is always constant argument that: Data in datacenters manages all the processes in IoT. It is a univocal fact that datacenter is entirely an essential factor for the IoT. We must also focus on the reliability of network which is used to run the IoT applications. High-speed Internet is equally important as its performance the functionalities like the reliable transmission of data, quick delivery of sensor data, fetching details from sensors to a cloud and vice versa [12].

4.5. IoT as a Future Technology

IoT is an evolution in the multidisciplinary world. Microcontrollers and Microprocessors, sensors and networking devices are some of the basic building blocks of the IoT and these are in widespread use today. They have turned out to be all the more effective today, even as they get littler and more affordable to create.

4.6. IoT and current interoperability standards

IoT in the long run included billions of interconnected devices over the internet. Looking at the boom of IoT, it will include numerous makers from around the globe producing numerous product categories [13].

The term interoperability states that: All these devices must communicate, trade information and perform closely synchronized manner. They should also show the task without compromising security standards and overall performance of IoT devices.

4.7. IoT and privacy and security

Security and privacy are the main concerns while designing and developing IoT devices —and addressing these concerns must be a high priority.
New technology often has scope for abuse, and it's smarter to solve the issue before it influences privacy and security, innovation or financial development. It is a responsibility of Manufacturers, standards organisations and policy-makers to address all the possible threats to the product.

As a part of network layer security, manufacturers must think about the implementation of new security protocols that will be important to guarantee end-to-end transmission of delicate data.

4.8. IoT and limited vendors

Open platforms have always been a proven way for developers and merchants to build innovative hardware with constrained spending plans and assets [14].

The behavior of IoT applications has heterogeneous nature. Hence it requires a wide variety of software and hardware. To manufactures all these IoT components, there must be a full number of vendors available in the market.

Fig. 6. IoT Security Threat Map

5. CHALLENGES OF INTERNET OF THINGS

Behind every success story is a hidden chain of problems. Same is the case of IOT. According to banafa A. et. al. It experiences three major challenges [15]:

- Technological challenges
- Business challenges
- Societal problems

5.1. Technology

IoT components are implemented using divergent protocols and technologies. As a result, these components have intricate configurations and poor design.

Technological challenges can be a reflection of five parameters [15].

- **Security:** IoT has happened to cause major security issues that have grabbed the attention of various public and private sector companies of the world. Adding such a massive number of new hubs to the systems and the web will provide attackers with a larger platform to invade the system, particularly as many experience the ill effects of security holes. Indications suggested that the malware captured infinite number of IoT gadgets that are being used in basic applications like smart-home devices and closed-circuit cameras and deployed them against their own servers. A further critical move in security will develop from the way IoT turns out to be involved in our lives

  Some study proves that cameras connected to the internet will contribute 30% to security concerns. Others are being 15% on house doors, 12% on cars, 10% on TVs, 6% due to iron, 6% on heating systems, 6% on smoke systems, 5% and 5% on an oven and lightening each.

Fig. 7 Concerns of IoT

There are six principles of IOT across the stack :

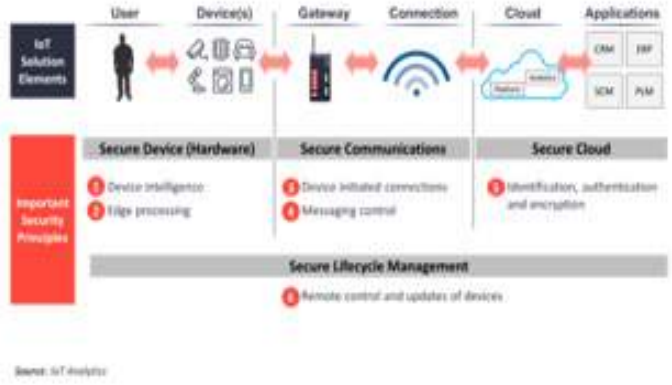

Fig. 8 Six principles of IoT security across the stack

- **Connectivity:** The most significant challenges of the future of IoT would be to connect several devices, this communication will end up resisting the currently existing structure and the technologies associated with it. Presently, a centralized, server/client architecture is being utilized to authenticate, authorize and connect several terminals in a network [16].

  This model is appropriate only for the current situation and is not scalable to cater future needs where billions of devices will be part of a single network. This scenario will transform the current centralized system into a bottleneck. Large amount of investments and expenditure in maintaining the cloud clusters of servers are required which can deal with humongous quantity of information exchange, as unavailability of servers can lead to a total system shutdown.

- **Compatibility and Longevity:** IoT is developing in a widespread manner. It is incorporating many technologies and will soon advance into a convention. This will pose serious challenges and will demand setting up of additional software and hardware in order to establish communication amongst the devices.

  Unavailability of standardized M2M protocols, Non-unified cloud services, and varieties in firmware and operating systems among IoT devices are some of the other compatibility issues. Devices working on these technologies will become purposeless in future as these technologies are going to become outdated very soon.

- **Standards:** Technology conventions incorporating network and communication protocols, and data-aggregation conventions, are the collection for activities that handle, process and store information obtained from several sensors. These enhance the data by increasing the scale, scope, and frequency of data available for analysis [16, 17].

- **Intelligent Analysis & Actions:** The final step in the implementation of IoT is the revelation about the data for analysis. The analysis procedure is based on cognitive technologies and models. There are certain parameters that cause intelligent actions to be incorporated in IOT, some of them being lesser device cost, enhanced device functionality, the machine "influencing" human actions through behavioral-science rationale, deep learning tools, machines' actions in unusual scenarios, information security and privacy and device interoperability [18].

5.2 Business

The main issue is a major inspiration for beginning, putting resources into, and managing any venture, without a full proof plan of action for IoT we will have another bubble, this model should fulfil every one of the prerequisites for all kinds of e-commerce; vertical markets, horizontal markets, and consumer markets. Be that as it may, this class is always a sufferer of administrative and lawful inspection. Usage of IoT technologies plays a significant role to create a source of additional income to reduce the burden on the existing communication infrastructure.

Fig. 9 Reasons Businessman are adapting IoT Solutions

5.3. Society

Understanding IoT from the clients and regulators point of view isn't a simple errand for the following reasons:

- Customer requests and requirements change regularly.
- New uses for devices—and also new devices—grow and develop dangerously fast.
- Inventing and reintegrating have features and capabilities that are costly and require significant investment and assets.
- The uses for an IoT technology are growing and changing—regularly in uncharted waters.
- Consumer Confidence: Each of these issues could put a dent in buyers' want to buy associated items, which would keep the IoT from satisfying its real potential [19].

IOT data is a very sensitive data which if leaked can give the control of the system in the attack's hands. Hence we have to have the strong and reliable technology to secure how IOT data is being used. Business policies and procedures pose some social challenges to IOT and government laws, and rules pose legal challenges to its use [20].

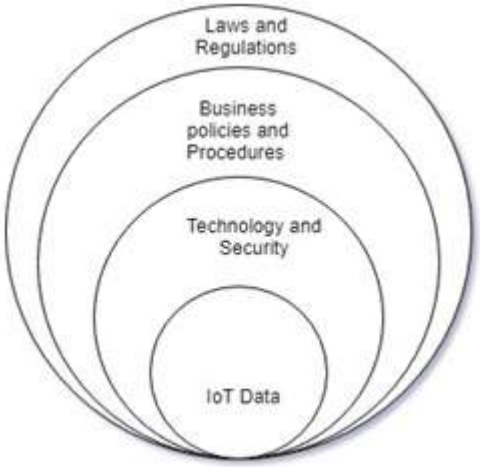

Fig. 10 Social Impact of IoT

6. CONCLUSION

The paper goes through the various aspects of what future of IOT looks like. Though chains of myths will always hold the future with uncertainty, the situation can be seen to become better shortly if we work on eliminating them. While using data collected from sensors wisely, dependency of IOT on mobile networks, significance of the data generated from different devices, importance of networks alongside datacentres, need of a secured service infrastructure with remote control options, evolution of interoperability standards, heterogeneity and openness are some of the issues that need to be addressed, security and privacy of data will play a major role in how the picture of IoT will look like in the coming decades. Parallel to it also comes the challenges faced by this technology that pose a threat to its success. Every aspect including technology, business, society and law resist the success rate of IOT. Acceptance of technology by people is also essential and should be taken into consideration during its development as people who are not fond of using gadgets, smart devices and do not feel comfortable dealing with technology will have a difficult time working with the complexity functionality IOT will engage them with. It's high time to deal with the factors that might significantly bring down the mighty future of IOT.

REFERENCES

[1] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

[2] Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.

[3] Guo, B., Zhang, D., Wang, Z., Yu, Z., & Zhou, X. (2013). Opportunistic IoT: Exploring the harmonious interaction between human and the internet of things. Journal of Network and Computer Applications, 36(6), 1531-1539.

[4] Banafa, A. (2014). IoT Standardization and Implementation Challenges. IEEE. org Newsletter.

[5] Banafa, A. (2015). „What is next for IoT and IIoT". Enterprise Mobility Summit.

[6] Coetzee, L., & Eksteen, J. (2011, May). The Internet of Things-promise for the future? An introduction. In IST-Africa Conference Proceedings, 2011 (pp. 1-9). IEEE.

[7] Cai, H., Da Xu, L., Xu, B., Xie, C., Qin, S., & Jiang, L. (2014). IoT-based configurable information service platform for product lifecycle management. IEEE Transactions on Industrial Informatics, 10(2), 1558-1567.

[8] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In Frontiers of Information Technology (FIT), 2012 10th International Conference on (pp. 257-260). IEEE.

[9] Liu, Y., & Zhou, G. (2012, January). Key technologies and applications of internet of things. In Intelligent Computation Technology and Automation (ICICTA), 2012 Fifth International Conference on (pp. 197-200). IEEE.

[10] Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015, June). Security and privacy challenges in industrial internet of things. In Proceedings of the 52nd annual design automation conference (p. 54). ACM.

[11] Banafa, A. (2014). IoT and Blockchain Convergence: Benefits and Challenges. IEEE Internet of Things.

[12] Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). Big IoT data analytics: Architecture, opportunities, and open research challenges. IEEE Access, 5, 5247-5261.

[13] Desai, P., Sheth, A., & Anantharam, P. (2015, June). Semantic gateway as a service architecture for iot interoperability. In Mobile Services (MS), 2015 IEEE International Conference on(pp. 313-319). IEEE.

[14] Koivu, A., Koivunen, L., Hosseinzadeh, S., Laurén, S., Hyrynsalmi, S., Rauti, S., & Leppänen, V. (2016, December). Software Security Considerations for IoT. In Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on (pp. 392-397). IEEE.

[15] Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. Cluster of European Research Projects on the Internet of Things, European Commision, 3(3), 34-36.

[16] Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2011). Internet of things strategic research roadmap. Internet of Things-Global Technological and Societal Trends, 1(2011), 9-52.

[17] Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J., & Leung, K. (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. IEEE Wireless Communications, 20(6), 91-98.

[18] Theoleyre, F., & Pang, A. C. (Eds.). (2013). Internet of Things and M2M Communications. River Publishers.

[19] Coetzee, L., & Eksteen, J. (2011, May). The Internet of Things-promise for the future? An introduction. In IST-Africa Conference Proceedings, 2011 (pp. 1-9). IEEE.

[20] Ji, Z., & Anwen, Q. (2010, November). The application of internet of things (IOT) in emergency management system in China. In Technologies for Homeland Security (HST), 2010 IEEE International Conference on (pp. 139-142). IEEE.

[21] James Kirkland , "Internet of Things: insights from Red Hat" , Website: https://developers.redhat.com/blog/2015/03/31/internet-of-things-insights-from-red-hat/ , Accesed : 2nd February 2018

AUTHORS

Falguni Jindal is a final year student pursuing B.Tech in Computer Science from SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering (MPSTME), Mumbai, India. She is a passionate student and has a strong determination for gathering knowledge and learning new things every day. Falguni has published two research papers in the field of IOT and Web Security respectively. Currently, she is also working on a few other projects in other domains of Computer Science.

Rishabh Jamar is a final year student pursuing B.Tech in Computer Science from SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering (MPSTME), Mumbai, India. He is hard working, enthusiastic and his quest for more knowledge led him to gain interest in exploring new domains like Network Security, Artificial Intelligence, Data Analytics and Internet of Things. He has published four research papers in the same fields at national and International level. He has also done a major project on internet security and several other minor projects in different domains of Computer Science.

Prof. Prathamesh Churi is Assistant Professor in Computer Engineering Department of SVKM's NMIMS Mukesh Patel School of Technology Management and Engineering (MPSTME), Mumbai, India. He has Completed his Bachelor's degree in Engineering (Computer science) from University of Mumbai and completed his Master's Degree in Engineering (Information Technology) from University of Mumbai. He started his journey as a professor and has been working successfully in this field since past 3 years where outcome of learning is different for every day. He is having outstanding technical knowledge in the field of Network Security and Cryptography, Education Technology, Internet of Things. He has published many research papers in the same field at national and International level. He is a reviewer, TPC member, Session Chair, guest speaker of many IEEE/ Springer Conferences and Institutes at International Level. . He has bagged with many awards in the education field. His relaxation and change lies in pursuing his hobbies which mainly includes expressing views be it in public ¬writing columns or blogging.