International Journal of Engineering & Technology, 7 (2.7) (2018) 610-613

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

IoET: From Paradox To Paradigm

Manas Kumar Yogi[1]*, Darapu Uma[2], K.Mahesh Kumar[3], P. Bhanu Prakash[4]

[1]Assistant Professor, Dept. of CSE
[2]Assistant Professor, Dept. of CSE
[3]B.Tech. II Year Student
[4]B.Tech. II Year Student
**Email: manas.yogi@gmail.com*

Abstract

The current importance and future promises of the Internet of Things(IoT), Internet of Everything(IoET) are diligently discussed in this paper. The analysis clearly distinguishes between IoT and IoET which are mostly considered to be the same by novices. Upon examining the current advancement in the fields of IoT, IoET, the paper presents scenarios or the possible future expansion of their applications also considering security aspects as same.

Keywords: *IoT; IoET; Security; M2M; T2T.*

1. Introduction

In the recent years IoT has gained a lot of popularity among the latest technologies IoT: The Internet of Things (IoT) is the digital world in which devices are connected over a network with sensors enabling them to communicate with each other and exchange data. All these devices perform tasks without the necessity of human interactions to perform the job. So there exist Machine to Machine interactions i.e., communications among machines (Things) for data transfer and sensor actuations.

Current Estimation of devices: There are more than 9 billion IoT devices worldwide and over the next ten years this range is expected to grow, with predictions ranging from 9 billion to 25 billion in 2025 from McKinsey estimates. By 2025, there will be a total of 25 billion IoT devices as said in a report by Cisco.

2. Limitations of IoT

Regarding the limitations of IoT, there are mainly six key areas to be worked upon.

2.1. Security

Security is a complicated issue to address in IoT.IoT applications collection make large amounts of data. Data processing is significant aspect of the entire IoT system. Also, a large percent of this data contains personal informationthusis essential to be secured through encryption of information. We can use SSL (Secure Socket Layer) protection to solve Page style the security issue of IoT. Vulnerable data such as location must be only provided to the concerned user and no other person should have access to it.

So we have to use a wireless protected connection with inbuilt encryption.

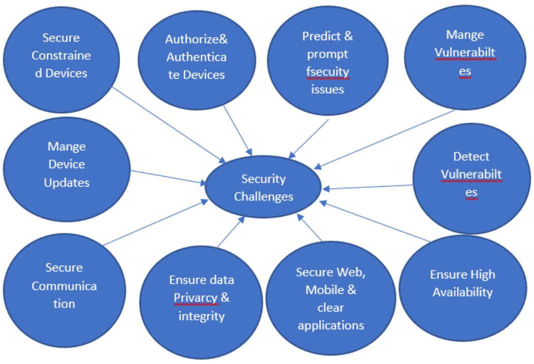
Secure Constraine d Devices
Authorize& Authentica te Devices
Predict & prompt fsecuity issues
Mange Vulnerabilt es
Mange Device Updates
Security Challenges
Detect Vulnerabilt es
Secure Communica tion
Ensure data Privarcy & integrity
Secure Web, Mobile & clear applications
Ensure High Availability

Fig.1 . Security Aspects of IoT

2.2. Privacy

Privacy is the biggest concern of all the time. Unencrypted data can become easily accessible to exploiters which can lead to destructive consequences if misused. Also some products may collect unnecessary user data which can be malicious. For example, a smart wearable (with a heart rate monitor) can also collect and send the user's heartrate data to the manufacturer which is not recommended. A poorly secure device can be highly dangerous even if it is perfect one for doing the task well.

2.3. Interoperability/Standards

Interoperability issues arise when there are different protocols of networks employed in the same system. These issues arise mainly when the devices can't connect to other devices, systems and exchange information as desired.

To overcome this interoperability issues, all the technologies used should be standardized. Even all the devices don't employ the same technology; they must be able to communicate with each other to perform the job.

2.4. Connectivity

In an IoT system, when millions of systems join together in a common network for a centralized operation the performance gets decreased. That is a bottleneck phenomenon occurs in the performance of the whole system.

2.5. Compatibility

Many new technologies are arising to compete with existing ones to become the standard for the future. This arises compatibility issues with newer hardware/software trying to cope with existing hardware/software and vice versa. Also, various manufacturers deploy various technologies in their products which lead to compatibility issues. For example, a product from a manufacturer A with some technology may not be compatible with another product from a manufacturer B with other technology.

2.6. Complexity

IoT systems are complex to understand and debug. They can be handled only by expert persons. General users find it complex to handle them in case of a bug or a failure. So, maintenance is an issue with IoT systems. Also the sensors are fragile so any mishandling of the system can break the system completely.

3. Scope of IoT to combine with another tech

The limitations of IoT can lead to malfunctioning or inefficiency of the system. To increase efficiency IoT should be combined with other technologies currently arising in the world. Some of those technologies are cloud computing, big data analytics, Artificial Intelligence, humans' interactions etc.

3.1. IoT with cloud (Cloud of things)

Cloud computing catalyses the efficiency and performance of IoT systems. They are reliable, scalable, economic and easy to maintain as compared to traditional systems. Also IoT cloud systems can be managed on the go almost anywhere on the planet.

3.2. IoT with big data

IoT devices produce great volumes of data. Big data analytics can make predict changes or produce results which help the IoT devices work faster and efficiently. The data can be used to make changes in the future devices, products for better productivity. This data and the devices go hand in hand in the very near future and data drives the IoT.

3.3. IoT with AI (Intelligence of Things)

Artificial Intelligence is the trending in technology in the world right now. The power of AI is unpredictable. AI can make wonders and change the entire world. When IoT combines with AI, everything in the world will be automated without any human intervention. People can get things done with minimal or almost no human effort. The scope of Intelligence of Things is immense and dimensionless. One such technology is IoE which is the combination of people, things, data and process.

3.4. IoET

IoET is the alliance of Machine interactions with human interactions along with combination of data to connect all the things. In a world of everything connected, every object will have sensors and connected to networks to detect and measure its state to make actions.Pillars of The Internet of Everything (IoE)

People: Through the internet people are connected to form the end-nodes of the system. They constitute a part of IoET, by interacting with the Things and generating data from devices interacting with them. Examples of such things are fitness bands, heart rate monitors and other sensors.

Things: Things are the devices which process the data and communicate with each other for decision making. These include the objects, that are connected to the internet, such as sensors, CPUs (Arduino, Raspberry Pie), actuatorsand other items.

Data: Data produced from IoT devices is in its original for which is raw. Taking actions by the system and making decisions are done by productive information which needs to be processed

The data generated from the sensors, IoT systems constitute a great part of IoET as it is driven by data.

Processes: The actions taken and done by the sensors, actuators and analysis of data to take decisions are the processes in IoET environment.. Examples of such processes are showing personalised advertisements related to our health data generated by our smart fitness bands and many more.

Diagram showing people, things, data and process in middle.

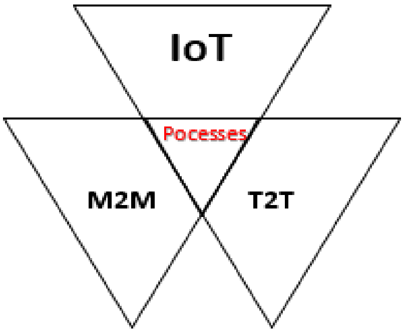

Fig.2. Specturm Of IOET Processes

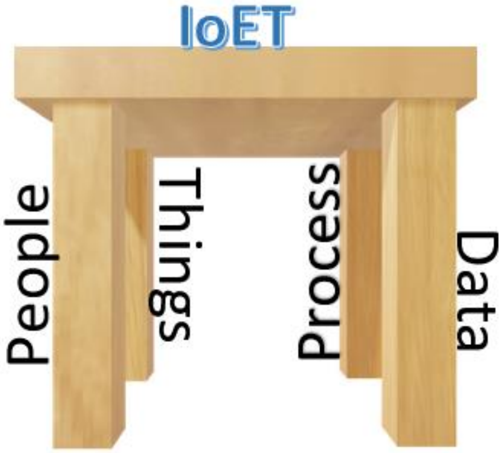

Fig.3. Four Pillars of IoET

4. Organization working towards IoET

Cisco: Cisco has big plans for IoET. It is developing various solutions with IoE in various fields such as education, defence, Navy, drones, oil and gas, banking and many more.

Cisco also partnered with AT&T to develop IoE solutions for health care using cellular-connected products. To develop IoETproducts It has partnered with Qualcomm and solutions.

General Electric:General Electric is an American company which is also interested in IoE.It also starting working in railway sector for providing the improved solutions for railway network.There are even more organisations moving towards IoET and revamping their whole infrastructure to suit the needs of the industry

All title and author details must be in single-column format and must be centred.

4.1. Applications

Health Care:
Screen Patients at Home
Envision organize empowered checking gadgets transmitting data through the cloud to trade data with the human services supplier's data frameworks.

Interface Patients with Parents :
Envision ongoing video and propelled observing enabling guardians and guardians to keep a nearby watch on their new-born children amid extremely basic circumstances.

Advanced Care and Improved Efficiency :
Envision arranged associations that transmit noteworthy data which may be utilized to stop sickness, expel squandered endeavours and time, maintain a strategic distance from intense medical problems, and furthermore may spare lives.

Enhanced Caregiver Efficiency at the Hospital :
Envision utilizing a mix of Local zone system and GPS-based area administrations to track persistently of wherever parental figures, restorative gadgets, and instrumentality is inside the office control.
Offer Data with Emergency Personnel
Envision interfacing specialists on call with understanding information at the purpose of care.

4.2. Tourism

The Smart tourism plan : Smart tourism can result as associate degree merger of the present on-line business model with the trendy data and Communication Technology (ICT). it's associate degree extension of the already existing on-line business model that functions through the websites and on-line bookings. it'll offer services to its users in conjunction with up-to-date data throughout and before their tour.
The various technologies that interaction to produce sensible tourism services are going to be the net, mobile, cloud computing, net of Things (IoT) and large knowledge analysis. easy devices like our mobile phones square measure equipped with camera, microphone, sensors to discover movements etc. the data collected by such sensible phones will be processed on servers and thence used for sensible living. sensible living needs sensible homes and sensible work conditions. which means all the services used for living like attention, education, tourism etc ought to flip sensible still, summarizes the ideas of sensible tourism

4.3. Smart tourism Ecosystem

The traveller customers (TC) work closely with the Residential customers (RC) so as to act as a neighbourhood of the local economy. tourism Suppliers (TC) supply services to the tourists through technology and network. alternative services (OC) like medium operators; banks etc. conjointly play a task within the system. They collaborate with one another and also the TCs to produce best services to the tourists. Destination selling Organizations (DMO) performs selling and data sharing through net and sensible devices. The whole interaction happens with the assistance of sensible technology and devices. this can be the explanation behind the smartness being introduced into the tourism sector that is preponderantly supported on-line websites-based business model. sensible tourism would force the utilization of net in an exceedingly completely different method. The initial bookings is also done through websites however the particular expertise of itinerant an area can all be managed by the sensible coordination of the objects at that place which can enhance the expertise of the traveller. as an example, once the traveller arrives in an exceedingly town and needs to go to some widespread website, the data relating to the location just like the shortest route to achieve there, traffic jam in this route, alternate ways in which to achieve the location etc. will be provided to the traveller within the sleeping room itself. Mobile tours will be provided to the travellers giving details of all tourist attractions, native restaurants etc. and aiding them throughout their trip.

5. Implications Of Sensible Tourism

There square measure bound implications which require to be self-addressed in sensible tourism. The foremost matter is that the privacy and security of customer’s knowledge. Further, as vast amounts of knowledge is made throughout the keep of the traveller, the digital traces left behind shall not be used for functions apart from providing higher tourism expertise. the largest concern is but, the deep dependence of the system on technology and network services. it's not possible to implement such a system while not the utilization of sensible phones and high-end infrastructure. For a business to adopt this concept, the full business model has to be revolutionized. Trained and knowledgeable workers is needed to figure within the new model. the full plan is to collaborate with alternative businesses like medium etc. and are available up with a united image of services

6. Security Considerations

Security issues can be classified into 2 categories based on their physical nature

6.1. Hardware

This relates to the physical sensors, things, machines which can be seen with our eye which are connected over a network and can communicate with each other. To prevent system or sensor hacks, the following measures can be taken.

a. Locking at sensor level: The IoET hardware designer provisiona a locking facility by entering 4-digit 16 code.

b. Locking at chip level: the hand of manufacturer, so This provision is purely in this lock is controlled from manufacturer side.

6.2. Software

This relates to the programs that run the system and communicates with all the devices in the system and help in exchange of data over systems and machines. To prevent access to the software, it need to be protected with firewalls, authorized login and all other unnecessary ports need to be closed to prevent hackers accessing it.

a. Authentication: The software need to be protected with passwords, logins so that only persons with proper authentication can access it.
b. Authorization: A linguistics access authorization model composed of a proper cognitive content and access policy are appropriates for IoET surroundings. The cognitive content can accommodates ideas, properties (linking concepts), and instances of the ideas. Policy can contain the constraints that ar being developed exploitation the elements of the cognitive content. Access call are achieved through execution of policies. A policy execution surroundings device the authorization choices.
c. Use of biometrics: Biometrics have become most common but also highly secure things in the current world. Since no two persons can have the same biometrics (for example fingerprints), the chance of failure is very minimal. They can be used so that only right person accesses the system and they are highly secured.

Closing unused ports in the system: In the system, the devices access the system only through certain ports which are allocated to do the task. All the ports should be closed except the ports which are needed to communicate Otherwise, it can be easy for hackers to hack and crack the system

Apart from hardware and software, there is another most vital thing which is a great security concern is Data. Data plays a major role in the good and accurate functioning of the system. The data generated from the IoT devices is very huge. Since, the data is large and very confidential, it needs to be encrypted at the bit level (if possible) to prevent misuse of it.

From a human point of view, since IoET involves people in the system there is a scope of error, as human intervention causes error. Humans must involve in the system with unbiased nature to prevent any misuse or mishandling of the system

7. Research Challenges

The future of IoET is glorious and is going to change the world soon, but there is a catch there are a few challenges with it. These can cause various problems and can lead to destruction if not worked upon.

1. Improper/less security: As mentioned above, security remains the biggest problem encountered by the system. Security issues can be overcome by applying some of the techniques mentioned above. Also since technology evolves continuously, newer challenges arise in security which need to be worked upon, else the newer tech cannot become a standard.
2. Weak design principles: Design of the hardware need to be changed. Some sensors are very fragile and break very easily. This leads to economical loss.
3. Way of deployment of IoET: We can prefer either the semantic model for automated deployment of IoET services across platforms or we can choose QoS aware deployment of IoET applications through fog. Researchers are currently working on hybrid models to achieve optimal return on investments for enterprises.

Apart from the above mentioned challenges, the challenges for IoT also apply for IoE at one or the other point. But these are the main issues which are required for proper functioning of the system.

8. Conclusion

Our paper serves as a readymade guide for researchers working in the area of IoT, IoET. We put our attempt to present the particular aspects of IoET so as to pave towards future challenges in that area. We have observed that challenges in this regard are many and scalable design principles are need of hour to meet the challenges in IoET. We end our paper with a positive note that multiple top software organizations have already began research practices in this direction.

References

[1] https://www.annese.com/blog/bid/372957/5-Ways-the-Internet-of-Everything-IoE-will-Reimagine-Healthcare

[2] https://www.postscapes.com/companies

[3] http://blog.iiconsortium.org/2015/07/the-7-principles-of-the-internet-of-things-iot.html

[4] http://www.theguardian.com/advertising/digital-media-trends2014-trends

[5] http://www.gartner.com/newsroom/id/2637615

[6] Blaze, M., Kannan, S., Lee I., Sokolsky, O., Smith, J. M., Keromytis, A.D., & Lee, W. (2009). Dynamic Trust Management. IEEE Computer, Vol 42, No 2, pp. 44-52, 2009.

[7] Bennett, J. and S. Lanning (2007). The Netflix prize. In Proceedings of KDD Cup and Workshop. 5.Beynon-Davies, P., 2013. Business Information Systems. 2nd edition ed. s.l.:Palgrave Macmillan.

[8] https://www.bbvaopenmind.com/en/3-major-challenges-facing-iot/