JCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.6, Special Issue.11, Dec 2018 E-ISSN: 2347-2693

IoT- New Perspectives and its Security

P. Herbert Raj[1*], P. Joseph Charles [2], M. Merla Agnes Mary[3]

[1]ICT Department, SVSB, 16-J17, Lorong Lima, Seria, Brunei
[2,3]Department of Information Technology, St. Joseph's College, Trichy, India

Available online at: www.ijcseonline.org

***Abstract*:** After Cloud Computing a new development of technology is Internet of Things (IOT). The term IOT was coined by Kevin Ashton of Procter & Gamble in 1999.At that point, he viewed Radio-frequency identification (RFID) as essential to the Internet of things at that point which would allow computers to manage all individual things. IOT is a sort of "universal global neural network" in the cloud which connects various things. Other than the communication devices all the physical devices are all going to be connected to the Internet, and should be controlled by the wireless networks. Smart Things is another example in IT world. The Iot concept can be associated with Body Area Networks(BAN), Unmanned Aerial Vehicle networks and Satellite networks. The IoT creates and intellectual invisible network that can be controlled and detected. Future of Internet of Thingswill betransforming the real world objects into intelligent practical objects.

KeyWords: *Internet of things – challenges of IoT – Trends of IoT – Applications.*

I. INTRODUCTION

Internet of Things is an ecosystem of connected physical objects that are accessible through the Internet. In particular, 'things" might communicate autonomously with other things and other devices, such as sensors in manufacturing environments or an activity tracker with a smartphone. It is a giant network of connected things and people all of which collect and share data about. IOT is also a system of interrelated computing devices, mechanical and digital machines that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction[2].When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it swiftly.Internet of Things (IOT) term represents a general concept for the ability of network devices to sense and collect data from around the world, and then share that data across the Internet where it can be processed and utilized for various interesting purposes. In recent years, the concept of the Internet of Things is gaining momentum due to the development of the wireless networking technologies, such as Long Term Evolution Advanced (LTE-A), Wireless Fidelity (WiFi), Bluetooth, Zig Bee, and so forth[1].

Internet is a global system of interconnected computer networks that use the standard Internet Protocol suite (TCP/IP: IPv4/Ipv6) to serve billions of users worldwide. The "Internet of Things" refers to the codingand networking of everyday objects and things to render them individually machine-readable and traceable on the Internet.

II. INTERNET OF THINGS

The internet of things is the name given to the computerization of everything in our lives. Already you can buy internet-enabled thermostats, light bulbs, refrigerators, and cars[3]. Everything will be on the Internet: the things we own, the things we interact with in public, separate things that interact with each other. These things will have two separate parts.

One part will be sensors that collect data about us and our environment. Already our smartphones know our location and, with their onboard accelerometers, track our movements. Things like our thermostats and light bulbs will know who is in the room. Internet-enabled street and highway sensors will know how many people are out and about/and eventually who they are. Sensors will collect environmental data from all over the world[4].

The other part will be actuators. Our smart thermostats aren't collecting information about ambient temperature and who's in the room for nothing; they set the temperature accordingly. The system's smarts will interpret the data and figure out what to do. And the actuators will do things in our world. Just think the sensors as the eyes and ears of the Internet, the actuators as the hands and feet of the Internet, and the stuff in the middle as the brain. This makes the future clearer. The Internet now senses, thinks, and acts.

2.1 Definition

The term Internet of Things represents a vision in which the virtual world of the Internet is extended into the physical world of everyday objects. Internet of Things can be defined as a network that can achieve interconnection of all the things anytime and anywhere with accurate control, reliable transmission, complete awareness and intelligent processing using supporting technologies, such as wireless sensor network technology, micro-sensors, intelligent embedded technologies, RFID, integrated intelligent processing technology, Internet technologies and nanotechnology[5].

2.2 Working principles of IOT

An IOT ecosystem consists of web/enables smart devices that use embedded processors, sensors and communication hardware to collect, send and act on data they obtain from their environments. IOT devices share the sensor data they collect by connecting to an IOT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. These devices, often called ”connected” or “smart” devices, can sometimes talk to other related devices, a process called machine-to-machine communication, and act on the information they get from one another. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices-for instance, to set them up, give them instructions or access the data.

The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IOT applications deployed. Connected devices also generate massive amounts of Internet traffic, including loads of data that can be used to make the devices useful, but can also be mined for other purposes. IOT generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate exchange and consume data with minimal human intervention. These devices are popping up everywhere, and these abilities can used to enhance nearly any physical object.

2.3 Enabling Technologies

The concept of combining computers, sensors, and networks to monitor and control devices has existed for decades. The recent confluence of several technology market trends, however, is bringing the Internet of Things closer to widespread reality. These include Ubiquitous Connectivity, Widespread Adoption of IP-based Networking, Computing Economics, Miniaturization, Advances in Data Analytics, and the Rise of Cloud Computing[6].

2.4 Connectivity Models

IOT implementations use different technical communications models, each with its own characteristics. Four common communications models described by the Internet Architecture Board include: Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data Sharing. These models highlight the flexibility in the ways that IOT devices can connect and provide value to the user[7].

2.5 Transformational Potential

The potential realization of this outcome- a “hyper connected world” is testament to the general-purpose nature of the Internet architecture itself, which does not place inherent limitation on the applications or services that can make use of the technology.

III. SECURITY CHALLENGES IN IOT

3.1 Security

Security is an essential pillar of the internet and one that ISOC perceives to be equally essential and the most significant challenge for the IOT[8]. Increasing the number of connected devices increases the opportunity to exploit security vulnerabilities, as do poorly designed devices, which can expose user data to theft by leaving data streams inadequately protected and in some cases people health and safety can be put at risk.

Security attacks are problematic for the IoT because of the minimal capacity “things” being used, the physical accessibility to sensors, actuators and objects, and the openness of the systems, including the fact that most devices will communicate wirelessly. The system must also be able to adapt to new attacks unanticipated when the system was first deployed. In the system operates with a base level of support including strong attack detection capabilities. To heal from security attacks, a system needs to detect the attack, diagnose the attack, and deploy countermeasures and repairs, but perform all of this in a lightweight manner due to the types of low capacity devices involved. It is likely that significant hardware support will be necessary for providing encryption, authentication, attestation, and tamper proof keys.

To deal with all these unique challenges, there is a need for collaborative approach to security. A lot of users are ultimately going to have to compare the cost against the security, which is related to the mass scale deployment of the Internet of Things devices.

3.2 Privacy

The IoT creates unique challenges to privacy, many that currently exist. Much of this stems from integrating devices into our environments without us consciously using them. The ubiquity and interactions involved in IoT will provide many conveniences and useful services for individuals, but also create many opportunities to violate privacy.

This is becoming more prevalent in consumer devices, such as tracking devices for phones and cars as well as smart televisions. In terms of the latter, voice recognition or vision features are being integrated that can continuously listen to conversations or watch for activity and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. Apart from this, there are a number of IoT scenarios that involve the data collection and the deployment of devices with a global or multinational scope that crosses cultural and social boundaries.

In Internet of Things, strategies are going to have to be developed that respect the individual privacy choices while fostering innovation for new services and technologies. Consequently, the IoT paradigm must be able to express users' requests for data access and the policies such that the requests can be evaluated against the policies in order to decide if they should be granted or denied.

3.3 Standards

A lack of documented or standard best practices has had a much larger impact on Internet of Things devices that goes well beyond simply limiting their development and potential. An absence of standards ma well enables inappropriate behavior by IoTdevices[9]. Without the right standards to guide and regulate manufactures, developers may design products that operate in any number of disruptive ways online without regard for their impact.

A lot of this is caused by cost constrains as well as the need to develop products and get them to market before their competitors.

3.4 Regulation

Just like privacy, there are a number of legal and regulatory questions that surround the Internet of Things Legal issues concerning Internet of Things devices aren't limited to potential violations of civil rights because of law-enforcement surveillance. Other issues that must be considered are cross-border data flow, legal liability when it comes to unintended use, privacy lapses and security breaches. Also, technology is advancing at a much faster pace than regulatory policies, and the agencies charged with setting and supervising IoT guidelines cannot keep up.

3.5 Development

The broad scope of the IoT challenges is not going to be confines to industrialized countries. In fact, the IoT has a lot of promise when it comes to delivering economic and social benefits for developing and emerging economies. Like the rest of the world, the less developed regions are going to have to address the policy requirements, technical skill requirements, technical skill requirements, and market readiness to take advantage of the potential of IoT[10]. This a huge server farms to handle all the data. You will need to have a lightweight network that can seamlessly transfer data between servers and devices.

IV. TRENDS OF IOT

IoT technology continues to evolve at an incredibly rapid pace. Consumers and businesses alike are anticipating the next big innovation. They are all set to embrace the ground-breaking impact of the Internet of Things on our lives like ATMs that report crimes around them, forks that tell you if you are eating fast, or IP address for each organ of your body for doctors to connect and check.

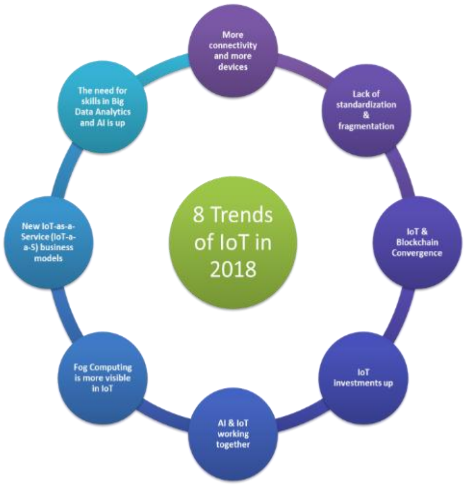
More connectivity and more devices
Lack of standardization & fragmentation
IoT & Blockchain Convergence
IoT Investments up
AI & IoT working together
Fog Computing is more visible in IoT
New IoT-as-a-Service (IoT-a-a-S) business models
The need for skills in Big Data Analytics and AI is up
8 Trends of IoT in 2018

Figure 1: Trends of IoT in 2018

4.1 Lack of Standardization

Digitally connected devices are fast becoming an essential part of our everyday lives. Although the adoption of IoT will be large, it will most likely be slow. The primary reason for this is lack of standardization.
The hurdles facing IoT standardization can be divided into three categories, namely:

platform: this part includes the form and design of the products (UI/UX), analytics tools used to deal with the massive data streaming from all products in a secure way, and scalability;

connectivity: this phase includes all parts of the consumer's day and night routine, from using wearables, smart cars, smart homes, and in the big scheme, smart cities.

applications: in this category, there are three functions needed to have killer applications: control "things", collect "data", and analyze "data". IoT needs killer applications to drive the business model using a unified platform.

4.2 More Connectivity and More Devices

The speedy proliferation of IoT in past 3 years has resulted in billions of interconnected devices. As the consumer continues to stay hooked to more gadgets. The number of connected devices grew exponentially every year. More IoT devices will enter the channels, more than ever before. A

clear indication of our direct dependency over the gadgets and that's how our future is shaped.
As IoT continues to expand we will certainly see an increase in devices connected to the network in different areas in business and consumer markets. Smart devices will become the de-facto for people to manage IoT devices.

4.3New Hope" for Security – IoT&Blockchain Convergence

As with most technology, security will be the major challenge that needs to be addressed. As the world becomes increasingly high-tech, devices are easily targeted by cyber-criminals. Security undoubtedly is a major concern, and vulnerabilities need to be addressed. Block chain is a "new hope" for IoT Security.

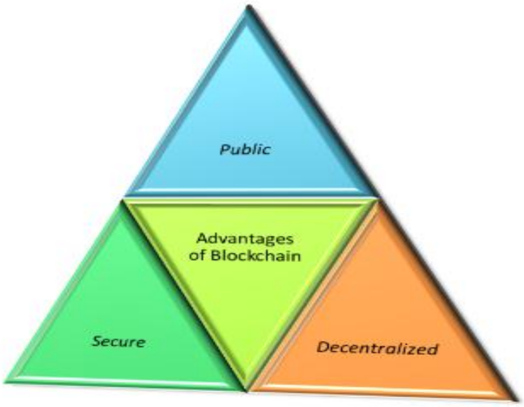

Figure 2: Advantages of Block Chain

The astounding conquest of Crypto currency, which is built on Block chain technology, has put the technology as the flag bearer of seamless transactions, thereby reducing costs and doing away with the need to trust a centered data source. Block chain works by enhancing trustful engagements in a secured, accelerated and transparent pattern of transactions.

4.4 IoT Investments Will Continue

IDC predict that spending on IoT will reach nearly $1.4 trillion in 2021. This coincides with companies continuing to invest in IoT hardware, software, services, and connectivity. Almost every industry will be affected by IoT, which means many companies will benefit from its rapid growth. The largest spending category until 2021 will be hardware especially modules and sensors, but is expected to be overtaken by the faster growing services category. Software spending will be similarly dominated by applications software including mobile apps.

4.6Fog Computing Will Be More Visible

Fog computing allows computing, decision-making and action-taking to happen via IoT devices and only pushes relevant data to the cloud, Cisco coined the term "Fog computing "and gave a brilliant definition for Fog Computing: "The fog extends the cloud to be closer to the things that produce and act on IoT data. These devices, called fog nodes, can be deployed anywhere with a network connection: on a factory floor, on top of a power pole, alongside a railway track, in a vehicle, or on an oil rig. Any device with computing, storage, and network connectivity can be a fog node.

The benefits of using Fog Computing are very attractive to IoT solution providers, some of these benefits: minimize latency, conserve network bandwidth and operate reliably with quick decisions. Collect and secure wide range of data, move data to the best place for processing with better analysis and insights of local data.

4.6 AI &IoT Will Work Closely

Amalgamation of IoT data analytics with AI for applications ranging from elevator maintenance to smart homes, will progress rapidly over the coming two years. Platform and service providers are increasingly delivering solutions with integrated analytics designed to feed data directly into AI algorithm. AI can help IoT Data Analysis in the following areas: data preparation, data discovery, visualization of streaming data, time series accuracy of data, predictive and advance analytics, and real-time geospatial and location (logistical data).

4.7 New IoT-as-a-Service (IoT-a-a-S) Business Models

Transformational business models will develop in many IoT verticals over 2018-2019, supported by Big Data and AI tools[11]. In these models, the value is in the convenience of the service for end customers (on-demand and not requiring heavy upfront expenditure), and the usage data that is collected, analyzed, and fed back into suppliers' businesses and processes.
IoT solutions can enable more of an ongoing, managed service relationship with both technology providers and end customers.

V. THE FUTURE

A number of crucial elements are very quickly creating a perfect soil for the IOT to thrive in. Smartphone dispersion is increasing in now a days and the cost of connecting of the internet has been decreased as broadband. More and more devices are being equipped with Wi-Fi capabilities. In the future everything has been connected to the wireless network.As the Internet of Things spreads, the effects for business model improvements are huge. Today's creativities will need to rethink their entire plan, as the Internet of Things opens a wide new array of active opportunities. With the growth of the internet usage IoT becomes trending in now-a-days. The data mining is also used to identify trends and behavior. Many IoT applications are developed by many industries fields like agriculture, healthcare and building management and so on. In 2020 the whole physical devices are connected together with IoT wireless connection and the world becomes as a connected one. Coming days the three parts of businesses are traveling the ways in which the IOT can improve their center processes and services.

REFERENCES

[1].https://www.schneier.com/essays/archives/2016/02/the_internet_of_thin_2.html

[2].http://ijesc.org/upload/8e9af2eca2e1119b895544fd60c3b857.Internet%20of%20Things-IOT%20Definition,%20Characteristics,%20Architecture,%20Enabling%20Technologies,%20Application%20&%20Future%20Challenges.pdf

[3].https://ieeexplore.ieee.org/document/7902207/

[4].https://www.sas.com/en_us/insights/big-data/internet-of-things.html

[5].https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[6].https://iot.ieee.org/newsletter/january-2018/eight-trends-of-the-internet-of-things-in-2018

[7]. L. Xu, L. Rongxing, L. Xiaohui, S. Xuemin, C. Jiming, and L. Xiaodong, "Smart community: an internet of things application," *IEEE Communications Magazine*, vol. 49, no. 11 pp. 68-75, Nov. 2011.

[8].https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/

[9]. https://www.semiwiki.com/forum/content/7291-8-trends-iot-2018-a.html

[10].http://ijsetr.org/wpcontent/uploads/2016/02/IJSETR-VOL-5-ISSUE-2-472-476.pdf

[11].https://pdfs.semanticscholar.org/2006/d0fca0546bdeb7c3f0527ffd299cff7c7ea7.pdf

[12].https://file.scirp.org/pdf/JCC_2015052516013923.pdf

Authors Profile

Dr. P. Herbert Raj has been working as an Associate Professor in Institute of Technical Education at Brunei. Previously, he worked as Assistant Professor in Department of Computer Science and Engineering at Alagappa University, Karaikudi, Tamil Nadu, India, from 2003 to 2007. He received his Ph.D. in Computer Science, Bharathidasan University, Tamil Nadu, India. His areas of research interests are *'Security issues and Load Balancing in Mobile Cloud Computing'* and have additional expertise in *'MPLS based Traffic Engineering'*. He has more than 10 years of research experience. He published more than 12 research articles in reputed international journals.

Dr. P. Joseph Charles has been working as an Assistant Professor in the Department of Information Technology at St.Joseph's College, Trichy. He received his Ph.D. from Bharathidasan University, Trichy His area of interest are Context Aware Mobile Web Services, Software Engineering and Operating Systems. He published more than 30 research articles in international and national reputed journals.

Ms. Merla Agnes Mary. M,is a Post Graduate student of Department of Information Technology, St.Joseph's College, Trichy. She is interested in IoT and its Security. She has published research articles in journal.