International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 12 (2020) pp. 113-124
© MIR Labs, www.mirlabs.net/ijcisim/index.html

Received: 13 Jan, 2020; Accepted: 20 May, 2020; Published: 28 May, 2020

Internet of Things: Future Challenging Issues and Possible Research Directions

Amit Kumar Tyagi[1] and Ajith Abraham[2]

[1]School of Computer Science and Engineering,
Vellore Institute of Technology, Chennai Campus,
Chennai, 600127, Tamilnadu, India.
amitkrtyagi025@gmail.com

[2] Machine Intelligence Research Labs (MIR Labs), Scientific Network for
Innovation and Research Excellence
Auburn, Washington 98071, USA
Email: ajith.abraham@ieee.org

***Abstract*: Internet of Things (IoTs) or Internet Connected Things are changing human's being life a lot (in terms of living or accessibility). IoTs is merging of several "things" for building an infrastructure (like cyber physical systems, smart ecosystems) with using internet (for making communication system) to establish a smart interaction among people, applications and surrounding objects/ devices (like Road Side Units, access points, street light, etc.). Together this, Cloud is recognised as a crucial component of IoTs, which is used to provides valuable applications/ specific services in several areas like defence, farming, Transportation, home automation, etc. Also, cloud is used to provide storage to these connected devices. Now days, several IoT cloud providers are emerging into the market to increase the need or fulfil need of users/ consumers (i.e., by IoT based services). In result, Internet of Things (IoTs) based cloud (or cloud based IoTs) are everywhere in our daily lives/ applications like homes, hospitals, streets, prevent fires, and many more beneficial applications. This scenario is known as Internet of Everything. But, using such devices/ technology or much involvement of these IoT based clouds create several issues and challenges which has been presented in this article as a literature (in detail). In summary, this work investigates several research issues for future researcher (which are need to be focused), it also provides a direction for future (i.e., with respect to device management, system management, heterogeneity management, data management, tools for analysis, deployment, monitoring, visualization, and research). In last, few challenges also have been discussed that the researchers should take focus on in near future (in the next decade). This article provides a road to future researchers to work in respective area or in Internet of Things (IoTs) based cloud (or cloud based IoTs).**

***Keywords*:** Internet of Things, Internet Connected Things, Intent of Everything, Future Research Directions, Cloud, Issues and Challenges.

I. Introduction

Internet of Things is "a world in which all electronic devices (smart devices) are networked and every object, whether it is physical or electronic, is electronically tagged with information pertinent to that object." Several technologies drive the IoT's vision. This is the age of all pervasive connectivity - the "Internet of Things" (abbreviated as IoT). In [1], authors define that "Internet of Things as simply an interaction between the physical and digital worlds". Using many sensors and actuators physical world is interacted with digital world. These sensors/ actuators are connected with people through Programmable Logic Circuits (PLC). Note that IoTs build an infrastructure using cyber and physical space (called cyber physical system). Another definition by [2] defines the Internet of˝ Things as "a paradigm in which computing and networking capabilities are embedded in any kind of conceivable object". Hence, some other definitions are IoTs are included as:

- Definition by [3]: "Things have identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environment, and user contexts."
- Definition by [4]: "The semantic origin of the expression is composed by two words and concepts: Internet and Thing, where Internet can be defined as the world-wide network of interconnected computer networks, based on a standard communication protocol, the Internet suite (TCP/IP), while Thing is an object not precisely identifiable. Therefore, semantically, the Internet of Things means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols."
- Definition by [5]: "The Internet of Things allows people and things to be connected Anytime, Anyplace, with anything and anyone, ideally using any path/network and any service". Fig 1 gives a pictorial representation of the same definition. In simple terms, the IoT is "a global network infrastructure, links uniquely identified physical and virtual objects, things and devices through the exploitation of data capture (sensing), communication and actuation capabilities". In an Internet-like system, the underlying architecture of digitally embodied "stuff" involves components / sensors for connectivity utilizing Internet and network developments [6, 7].

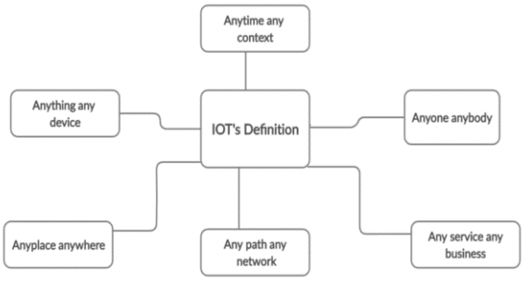

Figure 1: Definition of IoT **[**5]

A high degree of autonomous data collection, event transmission, network communication and interoperability would define digital technologies and applications [8]. In the development of IoT, it has become necessary for business organizations to integrate the product and devices with processes (for tracking products, etc.). The idea of applying any innovative technology arises several questions. There will always of requirement/ necessity of trade-offs. The organizations should always deliberate on the consequences and complex issues that follow the application of a new technology. IoT has developed leaps and bounds with the advent of technologies like LPWAN (Low-power wide-area network or low-power wide-area network or low-power network) and became ubiquitous. However, digitalization has its own virtues and vices. Digitalization can enhance a product's capabilities and strengthen the value chain by improving Customer Relationship Management (CRM). At the same time, digitalization can lead to catastrophic effects as one has witnessed in the downfall of newspaper and media giants. The IoT is a heterogeneous collection of connected devices and systems such a Wi-Fi enabled sensors, wearable smart gadgets, smart phones, etc. Hence, there is no single/ uniform IoT architecture/ definition is not sufficient to address various varieties of applications/ IoT having varied requirements.

Generally, in the Internet of Things (IoT), the objects connected using different types of networks like Radio Frequency Identification (RFID), sensor network technologies. The main application of RFID tag is port containers [9]. These networks (in integration) help in blending the information and communication systems seamlessly into surroundings of citizens (of a nation/ country). As discussed in [10], IoT devices (in connected/ integration) produce large amounts of data, which need to be stored, processed and presented in an efficient, accurate and easily interpretable form. On the other hand, cloud computing [11] provide virtual services to users/ firms/ organizations based on pay and use strategy. The virtual infrastructure which is built by IoTs devices and interlinked with cloud for computing purposes, tracking software, networking apps, measurement applications, reporting systems, and distribution of customers. Using such services (i.e., of cloud with IoTs or IoTs based Cloud), user can use cost based services or pay and use services when they want (i.e., end-to-end service for their purpose/ any business purpose) to access any applications (based on demand) from anywhere, anytime. Note that IoT based clouds (i.e., IoTs with cloud computing) requires:

a) a common awareness of the condition of its users and their computers,
b) technological systems and omnipresent contact networks for storing and sharing qualitative knowledge where appropriate,
c) computational capabilities on the Internet of Things aimed at autonomous and intelligent behavior.

Note that with these three requirements, smart connectivity using smart devices with cloud (for storage or any services in terms of infrastructure, platform, and software) can be completed/ achieved. Basically, these smart devices are embedded with some sensors to keep tracking or sensing activities (in its surrounding). These sensors are open wireless technology like Bluetooth, Radio Frequency IDentification (RFID), Wi-Fi, which are used everywhere/ in all applications (almost). For example, telephonic data services contain/embedded with sensor and actuator nodes, whereas, these sensors are connected with Programmable logic circuit with the physical world (physical space). Hence, IoT is building or providing services to cyber and physical space (both), for example, cyber physical system, a smart environment using smart (or IoTs) devices [22]. We can say that, "IoT has stepped out of its infancy and is on the **verge** of transforming the current static Internet into a fully integrated Future Internet" [9]. Now days, Internet is changing the world with interlinked with several devices (billions in numbers), and in upcoming future (or years), it will lead to the interconnection between people, objects (devices) at an unpredicted scale and growth. As IoT is going to be popular in coming years and this technology will stay for a long time, the authors wanted to develop a cloud centric vision with the worldwide implementation of IoT. An IoT contain certain components to visualize the smart architecture. There are three IoT components which enable seamless ubicomp:

- Hardware – It is composed of sensors, actuators and built-in contact hardware
- Middleware – It gives services based on demand storage and computing tools for data analytics
- Presentation – Using this, visualization of a smart environment and presentation of interpretation tools are easy to understand (which can be viewed freely on various networks and which can be tailored to specific applications) [12].

Some applications of IoT [7, 13] can be categorized into several types like Personal and Home (Home automation, health care, wearable software, etc.), Enterprise (Traffic management, environment monitoring, crowd monitoring, etc.), Utilities (Video based IoT [14] such as surveillance, water network monitoring, etc.), and Mobile (Mobile logistics, traffic control systems, etc.), etc. Hence, main IoTs applications are included as: smart energy, smart health, smart buildings, smart transport, smart living and smart city [7]. Khalil et al. [15] discussed the integration of Wireless Sensor Networks (WSNs) into IoT. Successful implementation of these IoT devices requires universal platforms, similar standards, and vertical application domains into a single, unified, horizontal domain, often referred to as "smart life". IoTs create automated control systems/ cyber physical system, when they integrated/ connected together on a large scale, like cybernetics, cyber space. Cybernetics is "the science of communications and automatic control systems in both machines and living things" [16]. Many crimes or attacks like physically (tempering of devices) and cyber are being traced now days. These crimes

influence our society or smart environment a lot, which we need to overcome and plan to identify/ detect such crimes (cyber-attack on open network) in IoT based applications with having proper organising, planning and execution methods/ rules. For example, Similar, attacker may attack on autonomous system/ vehicle to take control of such vehicles for its benefits. We can use blockchain in autonomous application to stored communicated information (data in motion) securely (in near future, as future work). Also, we need to protect such possible attacks on autonomous vehicles through efficient security mechanisms.
No author discussed about protecting IoT attacks against insider attacks or tempering attacks. Also, no one discusses about protection of information which is shared by smart devices (static/ dynamic). We need to provide such strong privacy preserving mechanism for leaking of privacy issues

Hence, the organization of this paper is follows as: section 2 discuses about evolution of Internet of Things in brief. Further, several problems existing in IoT based cloud or cloud based IoTs (with investigating some work for future) will be discussed in section 3. Later, section 4 discusses future research issues and challenges with analysis of several/different attacks. Then, several future research directions in internet of things with respect to security and privacy will be discussed in section 5. In last, section 6 concludes this work in brief. Also, in this work term 'IoTs based cloud' is being used with terms like Cloud based IoTs (or Cloud based Internet Connected Things), or IoT cloud or Cloud IoTs interchangeably.

II. Evolution of The 'Internet Of Things'

Possibly, thinking about a 'Internet of Objects' to the exclusion of humans (or certain dimensions) is overly restricting, particularly in a society where many 'things' are people's automations and 'things' are about or about people. However, individuals are influenced by 'events' and the nature of the knowledge they generate. As a consequence, getting a definition broader than just 'things' is necessary. One solution will be to expand the 'Internet of Things' to the 'Internet of People and Things' offering a wider base of interactions and contacts. Information dependent on the population may involve sensors that 'reflect' population. For instance, IoTs can provide services in applications like capturing user's location or other variables/ devices/ vehicles (anytime, form anywhere). Additionally, knowledge focused on individuals may involve social networking, including more background details. In a similar way, the 'Internet of People and Things' will include connectivity and communication to certain organizations. Many scholars also been dreaming of the "Internet of Everything," where practically all is linked to the Internet and is able to interact with everyone else. However, this work mainly focuses on using the term "Internet of Things" in this work, irrespective of using any other similar terms like 'smart things' or 'internet connected things'.

In the late 1960s, contact between two machines was made feasible via a simple computer network. The TCP / IP stack was implemented in the early 1980s. Then, Internet commercial usage started in the late 1980s. Services such as social networks, forums, and micro-blogs later become a significant web content development outlet. This version of the Web is called the People's Web (WoP).' The WoP went through further changes over the years. The goal of making Internet infrastructure more efficient, reliable, context-aware and automatic (less reliant on human mediation) has culminated in a weakened interaction (or even total exclusion) of "people" from the system and the incorporation of "information" into the networks [6]. IoT is a collection of both inanimate and animate things
. This form of Web is called the "Web of Things (WoT)" or the "Internet of Things (IoT)". The IoT attempts/ tries "for minimizing the human mediation in the sensing and feeding of information into the virtual world, and/or associated actions carried out in the physical world based on the information in the virtual world" [6]. In general, the internet system can be discussed with three layers: perceptual layer, network and transport layer, and application layer. Here, each term can be defined as:

- Application Layer: It represents the intelligence for processing the data for achieving desired functionality.
- Network and Transport Layer: It includes "infrastructure and technologies enabling wired/ wireless connections, unique addressing schemes, and reliable and secure transmission and storage of the collected data".
- Perceptual Layer: It includes "elements and technologies which help collect data from the real physical world and make it available to the virtual world".

For example, with integrating multiple sensors with moving objects/ devices, user can trace the movement of their objects or can control their objects/ devices from a remote location (using a chain of sensors, implemented/ fixed/ nearby). Using these sensors, users can know about current traffics status or running train status, or temperature of outside environments, etc. But, note that these sensors are proving accurate response only using internet or when are connected with the internet. Internet is mandatory things or connection to run these smart devices or run these sensors (at back end). Which is also a biggest disadvantage of these IoTs devices (apart from battery/ energy issue), and it require some efficient solutions (attention form research community) to run/ these devices without using internet. Here, data generated by user over the devices (or IoTs) called user generated content, whereas data generated by "devices" together called machine generated content. This data also requires biggest storage systems and unique standards to analyse.

Hence, this section discusses about evolution of Internet of Things and how this technology become popular. Now next section will discuss about several problems raised in IoT based cloud platforms (with future works and some respective solutions).

III. Problems in Existing Internet of Things Based Cloud Platforms

Today's existing cloud solutions contain/ incorporate Internet of Things or Internet Connected Things based smarter applications (like smart homes, smart meters, smart automation systems, etc.) for solving a number of problems/ challenges of various areas. Some problems in Internet of

Things based Cloud Systems (or Cloud based Internet Connected Things) are listed as:

i. Heterogeneity: IoT is a combination of various heterogonous devices, communication protocols, networks, etc. Any clouds cannot communicate with heterogeneous (different) modules or communication technologies in that way. It increases confusion between different types of devices (via different communication technologies). It results in network rude actions to be dishonest and end-to-end resources slow. In [17], authors addressed the management of linked artifacts by promoting via collaborative effort among different things (hardware components/ software services) and handling them (after providing respective/ correct addressing process, detection, and optimization at the architecture and design and protocol levels), but doing these things in Cloud based IoTs is a critical research problem. Hence, IoTs inconsistencies lead to security threats such as confidentiality, authentication, delays, etc.

ii. Context awareness: When trillions of sensor-enabled items (or sensors are installed in devices) are linked to the Internet (to allow communication), the consumer community will not be able to manage all the sensor-collected data. Context-conscious computation methods must be used to process the data and strip out redundant details. This data may create several problems like data acquisition, data retrieval, data management and data storage. Context-awareness computation methods need to be properly utilized to help decide which data to interpret or evaluate. Existing clouds today have little potential in terms of background awareness, is a big concern. As a consequence, the negation of the validity of knowledge is ascertained in the form of a continuous interrupted operation.

iii. Middleware: Today’s middleware available in IoTs is critical to design to handle domain specific needs. It can process horizontal flow of data among the devices across different (multi) platforms need to be developed. But, a middleware can provide a unique platform to run or execute all pre-processing work/ achieve specific goals, i.e., like multi-localized (geographically) modules. From [1, 7, and 10], we may claim that Middleware (in IoT's architecture) protects the horizontal data/ information flow between computers, protocols, and apps. All applications can be used over the data sets, and queries can be solved (centralized) on internet-connected devices.

iv. IoT node Identity: IoTs network typically comprises an extremely high number of nodes. Both equipment and data connected to them shall be recoverable. The shared identification in these situations is a must for successful point-to-point network configuration (i.e., using IPv4 address mechanism, 4-byte address to each node). But now days, the availability of IPv4 address are not enough to give address to each and every connected device (due to having a large number of internet connected devices) via internet/ IoTs devices. So, we require a new addressing mechanism/ policy to solve this problem, for that IPv6 is a strong mechanism. Note that existing systems mostly use IPv4 addressing scheme (for making a communication with other intent connect devices), but this structure (of using IPv4adressing) will be changed soon.

v. Energy management: This is an essential issue in internet connected things or in IoT based cloud systems, i.e., in IoT devices, Network Antennas. Hence, in IoTs devices, dependent passive modules along with the core algorithms should properly be maintained/ installed/ used while consuming a lot of energy. Otherwise, we need to use/ consider other non-conventional source of energy as perfect solutions (to provide energy to IoTs devices or testing a cloud while developing cloud systems based on IoT) such as solar power, wind, biomass, and vibration, etc. In near future, researchers need to get involved in this area/ to work on the other energy sources. In summary, energy is a critical issue in (for) IoTs devices (like smart phone, RFID/ embedded chips, battery). For such devices, future solutions should think of utilizing solar power, wind, etc., solutions to overcome from this issue.

vi. Fault tolerance: Fault tolerance is another important design issue which directly affects quality. To make a system perfect (with high accuracy, efficiently), the machine's fault tolerance level will be held very high, so that the device continues to operate through technical errors. Even in case of any technical error, IoT based clouds should consist fast recovery. Hardware component in IoT devices may fail due to less battery or any other malfunctions (external) reason [9, 24]. Also determining inaccurate value by embedded sensors (in a device), faulty calibration, and link or route failure (in making a communication) may lead to failed/ fault situation. As perfect solution of battery (energy) problem (or to battery enabled devices), solar or wind energy can work as a better alternative. Note that having communication with devices for a long time increases the requirement of power consumption. But, giving more energy to some devices and less energy to some devices can raise an issue of “distributions of energy” among IoT devices. But, we can provide equal energy to all devices, because sometime only some devices are performing any actions and some devices are in neutral mode (i.e., not working anything). Such cases need to identified (as much as earlier of data analytics), but identified such devices is really a critical task. And proper care (identification of any failure) needs to be rectified prior to final installation. Hence, IoT based clouds need to be implemented with efficient energy aware algorithms to lower down the power consumption in near future.

vii. Standardization: The available IoT based cloud platforms do not have any uniform data and process formats or any standard about generated data, which leads to interoperability issue. Here, standards mean security, communication and identification. If a standard for such devices, various things will improve the end-products or services (or will solve several real world problems). Today’s current clouds/ IoTs based Cloud do not have any standardized format for representation a data/process. Standardization in IoT based cloud shows to lower down the initial barriers for the service providers and active users [17], and improving the interoperability issues between different applications/systems. Also it received competition among the developed products/services (presented at application level). Hence, Security standards, communication standards and identification standards need to be improved with IoT based cloud technologies/other emerging technologies (working after connecting with internet). So, researchers from several communities need some specific guidelines and standards for efficient implementation of IoT in near future.

Hence, as discussed above data is not scalable (generated by IoTs devices), in standard, and it (data) is present in heterogeneous form. For that, we provide some future works which are need to be focused by future researchers. For example, in future, IoT based Cloud/ Devices with Internet will make a huge network, i.e., that may be densely crowded, rendering it impossible to place a single identification on the nodes/ devices. Existing IoT based clouds are working with IPv6 addressing mechanism, which should be increased in near future/ years. In future, networks connected device will require IP6 addressing schemes as mandatory (due to not having sufficient addressing numbers in IPv4). Further, we need unique/ some specific guidelines and standards for efficient implementation of IoTs in near future.

Hence, this section has discussed several problems with respect to IoT based clouds based on their heterogeneity, structure, applicability and usability. So, these above discussed issues can be used as a guide to do research in near future. Now, next section will discuss several research issues including challenges with analyzing several attacks in detail.

IV. Future Research Issues and Challenges

As discussed above, a lot of data is being generated everyday by Internet of Things (IoTs) devices. We require to make some decision from this generated data, which may helpful for human –being for identifying some solutions of real-world problems like about a disease, raining at unexpected day, a natural hazard suddenly, etc. The data processing (using correct tools) adds greatly to IoTs. IoT will resolve several big obstacles in order to harness the maximum capacity of data processing to derive new ideas / decisions from results. This can be divided into different categories:

- IoT Data Characteristics: Data is the foundation of knowledge extraction; high-quality information is essential. It will directly influence the quality of information extraction as IoT provides a large number, fast velocity and different data varieties. So, maintaining the consistency of the data (all the time) is a problem here. While many approaches have been developed to address this data quality issue, no one can handle all facets of data characteristics in a specific way (due to the centralized complexity of big data management systems and frameworks for real time processing). The abstraction of IoT data is low, i.e., data which collects from different resources in IoT, presents in raw form or called raw data, which is not sufficient for analysis. Hence, some solutions need to be done in existing work for further improvement, like semantic technologies aim to increase the complexity of IoT data by means of annotation algorithms, although more efforts are needed to resolve its velocity and quantity.
- IoT Applications: In IoT applications, several issues have been raised which can be discussed in different categories (based on their unique attributions and features). Privacy need to be provided to user’s personal data/ information or organisational data (which is collected and stored by IoTs devices). Then security of IoTs devices is also need to be protected in terms of physical security. IoTs devices are creating an environment with cyber and physical space, so both spaces need to be protected equally. Data access by malicious users leaves a system un-trusted, i.e., it is a tremendous, and potentially costly, risk for user/firms (for any business). Ignoring protection in architecture and execution, even even physically, a compromised IoT computer network may result in a failure.
- IoT Data Analytic Algorithms: As discussed in above discussion, IoTs are generating a lot of data which is called as ‘Big Data’. This smart data requires efficient analytic algorithms to make meaningful decisions from itself. This data consists several V’s and growing day by day (by billions of devices), which is also a big reason to handle this large data. These devices (Internet of Things/ Internet Connected Things) require efficient mechanisms/ algorithms to analyse this data (in which 80% data is unstructured) which is collected from a variety of applications (like e-healthcare, defence, etc.), i.e., by real-world applications/ in real-time. In the past decade, several researchers have proposed many tools for analytics. For example, Data mining, Machine learning, and Deep learning techniques. Deep learning algorithms solve problems with using neural networks. This technique is highly used in several real world applications to analysis large amount of data (including unstructured data). This technique provides high accuracy if they have enough data and time. Note that such algorithms (Deep learning) can easily modified by noisy or outlier data. Also, with this solutions (i.e., using neural network-based algorithms) lack interpretation, i.e., they cannot say “How result was given”, or “reasons about a model result”. Like this learning technique, semi-supervised technique (a technique of machine learning technique) analyses a small amount of labelled data with a large amount of unlabeled data (with the concept of reward based learning) to assist IoT’s data analysis.

Some other certain issues also addressed in IoT applications like security of running (and stored) data, analysis of data properly with appropriate/ efficient tools in IoT applications (for high accuracy). In big data analysis, machine learning is a major tool for IoTs/ IoTs based cloud [18]. Note that to gain more knowledge from existing/ collected/ to make further opportunities from this big data, we need to look at/ overcome these challenges:

a) To harness the big data characteristics like velocity, variety, volume, many solutions have been proposed but all these solutions require further improvement in terms of data accuracy.
b) Preserving Privacy and security of data are of utmost importance to any real time IoT application. Any over ambitious attempt in designing and implementing a new technology without considering this issue leads to catastrophic situations.
c) All neural network based algorithms require high volumes of data and time to reach accurate interpretations.

Hence, IoT is a global network system, linking individually defined physical and virtual artifacts, artifacts and computers through leveraging resources for data collection, connectivity and modulation. To extract information from the data collected a variety of machine learning algorithms can be applied [18]. But choosing the appropriate algorithm requires the understanding of three major important aspects, i.e., IoT application, underlying communication protocols and computing architecture and the attributes including significant features of data collected from the IoT devices. Further, we require to put some efforts on this analyzed data. It should be used with real-world problems, for improving the existing solutions for near future (to enhance the accuracy and security of the information extracted from the data). Hence, further following issues also need to be addressed in IoTs devices:

a) The issue of scalability: It is highly essential issue which is needed to overcome in IoT things/ require attention from research community. A single device can produce huge data, so organization/ its infrastructure need to handle this data efficiently. Scalability leads to the idea of augmenting IoT with cloud computing technologies.
b) The issue of sufficient or incorrect data/ accurate data: Accurate data can be regarding to location, nature of problems, etc., which may affect the efficiency of a system/algorithm/process. So, we require as much accurate data to get efficient results from our effective service process models, to solve real-world problems.
c) The issue of selling data/ losing of trust: The collected/ generated data from a connect product (by IoT devices) can be shared or sold by an organization to another organization or can be used their financial use. This data is being used one shared with other users/ organizations without user’s permission/ concerns, which is an issue of losing trust, which require to be built at much as strong. A use has ownership for his/ her data, it should not be shared with any unknown user or any third party without user’s permission.
d) The issues of safety and security of data: Last but not least is the task of mitigating safety and security related issues that are inherent in any connected product.
e) The issue of collecting data automatically: The automatic collection of data leads to informating. The data collected can be analyzed to make better business policies/ improve business. However, handling continuous streams of data requires efficient and modern technologies (with skilled people).
f) The issue of Horizontal or Vertical diffusion: A connected cloud based IoTs/ product requires refined skill set, i.e., it consists opportunities in the similar field or proliferate to related areas. Thus, it is again the discretion of the industry’s management to choose either of them or both.
g) Application of Big data analytics to IoT: Generated data by connected IoT devices (together) called Big data. Appropriate tool or analytics tools are not available to refine this large data.

We can conclude that IoT is a collaborative effort of communication, coordination and mutual agreement between trusted parties. Hence it requires a premeditated deliberation for any firm to jump start an IoT project.

A. Future Challenges in Internet of Things

The cloud-centric dream is to provide Plug n' Play smart objects that can be installed with an interoperable backend in any area, enabling them to integrate with other smart objects around them. Several challenges have been investigated in IoTs based cloud/ internet connected things. So, these challenges can be broadly classified into (for future researchers):

a) Architecture: Internet of Things-Architecture (IoT-A) [19] have been addressing the challenges particularly from WSN perspective and have been very successful for defining the architecture for different applications. The existed Cloud Centric Architecture (CCA) [20] (for providing IoTs based services to end users/ devices) is not sufficient to handle domain specific applications. So, there is a need for user centric architecture, where a user will be at the center and uses the data and the cloud infrastructure to develop more sophisticated application.
b) Energy efficient Sensing: The IoT environment is made up of devices that are connected to various heterogeneous (different) networks sensing continuous and random samplings. Hence, an effective energy sensing framework is essential to handle both spatial and temporal data, i.e., for saving energy during sensing.
c) Secure Re-Programmable Network and Privacy: Any IoT device is made up of 3 basic components, i.e., RFID, WSN and Cloud. Out of these listed (notified) devices, RFID carries most sensitive information. So, the issue of protecting privacy is a major research area and a challenging task for every device. Wherever devices are in billions, so protecting this much large information itself a big task. Also, there is a need for secure reprogrammable network as the smart devices enter and leave the network. Also, the security and authentication are major issues in a hybrid cloud. Note that cloud types are public, private and hybrid.
d) Quality of Service: Different networks have different bandwidth, which leads to delays. Throughput and latency are very important factors

that influence the Quality of Service (QoS). As heterogeneous networks work together to provide a service, QoS is at compromise/ danger. Thus, QoS in cloud computing is a major research area.

e) New Protocols: The traditional Time Division Multiple Access (TDMA), Carrier Sense Multiple Access (CSMA) protocols are not efficient to handle IoT based cloud network. There is a need for highly intelligent self-adaptive protocols to handle sensors in an IoT based cloud environment.

f) Participatory Sensing: People centric sensing is applicable only to resolve data ownership and privacy issues. People centric sensing cannot use for data collection as there will be inconsistencies and delays in sample gathering.

g) Data Mining: Deep learning is an evolving field of analytical (future decision-making) machine learning technology that aims at understanding several levels of abstraction that can be used to analyze results.

h) GIS based visualization: New visualization schemes for heterogeneous sensors (in 3D landscape) embedded in IoT devices are necessary [21]. Note that here collected data need to be visualized (within IoT) with respect to geo-related and sparsely distributed. A framework based on Internet Geographic Information System (GIS) is required to solve such challenges.

i) Cloud Computing: There is a need to support programming tools of particular domains and nonstop execution of applications across various networking platforms without comprising quality of service.

j) International activities: Several countries (jointly) are trying to implement these (IoTs) together to provide good and better life to their citizens. For example, Significant attempts are under way in Europe to integrate the cross-domain operations of study groups and organizations covering Machine to Machine (M2 M), WSN and RFID into a common IoT system. Countries such as Japan, China, the US, and Australia are all growing the usage of IoT systems in manufacturing, their related organizations, and policy agencies (with different programs). This involve smart community projects, smart grid systems that integrate electronic metering technology, and high-speed internet network roll-outs. Similarly, in China also IoT based development activity is also in under construction, they are focusing on such fields like (in IoT development): Smart grid; smart transport; smart warehousing; smart home; environmental and safety testing; factory management and automation; health care; good agriculture; finance and service; and military defense.

k) Security Concern: The security issue is a biggest challenge in IoT or IoT based cloud [7, 13]. IoT application data may be commercial, business, customer or personal. These application data must be protected and held private against theft / tampering of some type. For example, the IoT apps that store the results of a patient's health or shopping store. Furthermore, the IoT facilitates connectivity between devices, but there are issues such as scalability, usability and response time. When the details was shipped through foreign boundaries, the protection intervention act can be enforced through government legislation such as the Health Care Portability and Transparency Act (HIPA). Some of the general security challenges of IoT system are represented in figure 2. Among several security challenges, some other important challenges in IoT based cloud also required attention from future researchers (in near future), which are included as:

   i. Data Privacy: Some smart TV manufacturers collect data about their customers to determine their viewing habits such that during transmission the data collected by the smart TVs which present a data privacy challenge.

   ii. Data Security: Data security is a huge challenge, too. It is necessary to hide from observing devices on the internet while transferring data effortlessly.

   iii. Insurance Concerns: Insurance companies who install IoT devices on vehicles collect health and driving status data to make insurance decisions.

   iv. Lack of Common Standard: As there are several requirements for the production of IoT products and IoT sectors. Hence, discriminating between permitted and prohibited internet-connected devices is a major challenge.

   v. Technical Concerns: The traffic produced by such devices is also growing, leading to the expanded usage of IoT technology. Therefore, there is a need to expand network bandwidth, because processing the large volume of data for review and more final storage is indeed a problem.

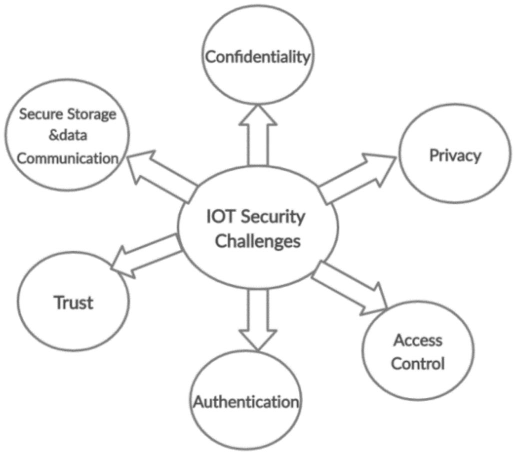

Figure 2: Intent of Things security challenges [22]

l) Intent of Things middleware: The challenges, which are addressed by any IoT middleware, are as follows:

   i. Interoperability and programming abstractions: There are three forms of interoperability: network, semántic, and syntactic. Interoperability of the network deals with heterogeneous interface protocols for interdevice connectivity. This prevents specific systems from the nuances of the numerous protocols. Semantic interoperability is about abstracting the interpretation of the data within a defined context. And Syntactic interoperability means programs are ignorant of different data types, implementations, and encoding.

ii. Device discovery and management: The middleware provides Application Programming Interfaces (APIs), which are used to list the IoT devices, their services, and capabilities. Lastly, every IoT middleware needs to do load balancing, control devices depending on their battery power rates and report system issues to users.

iii. Scalability: The approach must be scalable, because the devices in an IoT network will expand. Middleware needs to scale up as the IoT infrastructure evolves over a period of time.

iv. Big data and analytics: It need to process huge data generated by IoT sensors.

v. Security and Privacy: Any IoT applications using Radio-Frequency IDentification (RFID) technology is able to track personal information. So, Security and privacy issues are the critical. The middleware should be equipped with require cryptographic algorithms to protect the data from malicious users.

vi. Cloud services: Cloud computing infrastructure helps in handling the enormity of IoT data. The middleware should be adaptable to different types of cloud environments.

vii. Context detection: Context detection algorithms help in gaining insights into collected data. Understanding the context helps in providing more enhanced services.

m) Other challenges: Notice that an interconnection between extremely heterogeneous networked entities (IoT devices), meets a variety between connectivity patterns: Human-To-Human (H2H), Human-To-Thing (H2T), Thing-To-Thing (T2T), or Thing-To-Things (T2Ts) [23]. Providing efficient services among such integration (of devices and human-being) is a challenging task.

Hence, a scalable cloud based IoT framework with enough flexibility to satisfy requirement of users/ overcoming such issues, is required in near future (in cloud based IoT integration devices). The framework allows networking, computation, storage and visualization themes (separately for individual domains in a shared environment). In proposing a new framework, several challenges need to be highlighted from adequate description and visualization of the large quantity of data, privacy to security, data retrieval to data management, etc. In addition, IoT centered cloud has problems such as anonymity, participatory sensing, data mining, simulation focused on the Geographic Information System (GIS), etc. Several other issues affecting cloud storage are: infrastructure, energy consumption, stability, protocols, and service quality, standardization of frequency bands and protocols. Hence, a systems need to overcome such challenges in near future. Further, strengthening or increasing of IoTs devices/ Security at IoT's is a big problem. IoTs are an emerging technology (not completely developed), and the absence of a mature and robust protection paradigm and guidelines is a big problem concerning the adoption and applicability of Internet connected items.

B. Analysis of Different Types of Attacks and Possible Solutions

Related items on the Internet today face increasing forms of attacks such as inactive, aggressive attacks. Passive assault will, in fact, effectively interrupt the efficiency and remove the advantages of its services. A malicious user may feel the channel / node in this attack, and can steal the content, but remember that it is never physically assaulting. On the other hand, the active attacks disturb the performance or a network/ information physically. Note that active attacks are classified into two types of attacks, i.e., internal attacks and external attacks. All these attacks need to be prevented/ identified from (in) a network, i.e., to communicate devices smartly. This segment addresses different forms of attack, nature / attack actions, and extent of attack hazard. Various rates of attacks are divided into four categories (depending on their behaviour) which often provide some potential responses to threats / attacks in[24], as a low-level assault (if an intruder tries to target a network which his operation is unsuccessful), Medium-level attack (when an attacker / malicious user / intruder listens to the channel (as an insider assault) but does not infringe / change data integrity), high-level assault (when an intrusion happens on a network and violates data integrity / violates data) and extreme high-level attack (when an attacker targets a network by obtaining unauthorized access (without owner knowledge) and perform some illegal operations, and making the network/ services unavailable, or sending messages in bulk, or may stop services through network). Hence, extremely high-level attacks have complete authority to do anything with network/ system once it occurred on a network/ systems. For providing efficient services, such kind of dangerous attack should not get occurred in a network.

Hence, existing network security technologies need to be protected IoT based cloud systems against such attacks/ threats. For that, we need to develop a reliable, effective and powerful security protection mechanism for IoT based cloud. Several authors in [7, 10, 13, and 17] have discussed several areas where a lot of research need to be/ should be carried out:

- Definition of Security and Privacy from the Social, Legal, and Culture Point of View,
- Trust and Reputation Management,
- End-to-End Encryption,
- Privacy of Communication and User Data,
- Security on Services and Applications.

Hence, this section discusses several future research issues and challenges in IoTs, including discussing several types of attacks and their possible solutions (in detail). Now next section will discuss few research directions in IoTs (i.e., with respect to security and privacy).

V. Future Research Directions In Internet of Thing's Security and Privacy

or future work, IoT can work/ function with many smart devices and form a large infrastructure. This infrastructure can be like smart city, which consist several smart things/ environments in it. Smart city consists smart home, smart grid, smart drainage systems, smart/ intelligent transportation systems, etc. Similarly, IoTs can be used in many areas like military, animal farming, aerospace (wireless), navigation (sending alert message), healthcare etc. Some of the IoT application and challenges are listed in table 1. In internet of military things, the sensor or computing devices attached to the soldier suit, helmet or other weapons are capable of retrieving biometric information of face, iris, fingerprint, heart rate etc. This generated information can be used to identify the physical and mental state of the soldier, to monitor the battlefield etc. In case of clinical care IoT play vital role in information management [25], remote real-time ECG monitoring etc. Together this, one more technology also in trend now days, i.e., Blockchain technology, which has distributed and decentralized nature. Its use was started with Bitcoin in 2008 by some anonymous users/ user [26]. Today's Blockchain Technology is used in many applications like autonomous applications, financial institutions to reduce fraud, smart grid, industrial control systems, etc. We need to elaborate each respective application and identified cybercrime on such applications. These cybercrimes are very critical and complex to mitigate (proactively, i.e., before occurring), also required attention from several research communities to recover. In table 1 different areas where Blockchain integrated with IoT, their issues and challenges are briefly described. Apart from all these Internet of Things creates unique and several security challenges for firms/ organizations. Now days, machines are becoming autonomous, they can integrate and work together (with other machines or devices) efficiently and make decisions for physical world or real world problems. But, building automated systems like cyber physical systems (a connection of devices: with cyber and physical space), created several issues and challenges for future researchers. This section discusses few future research directions with respect to IoT security and IoT privacy, which can be included as:

- Privacy security in IoT is fairly recent and wasn't much studied / presented in current literature. The implementation of lightweight and safe privacy-preserving techniques in resource-constrained IoT devices is therefore an important research activity in the future.
- In the immediate future, we need to plan and launch 'virtual IDM applications' into resource-constrained IoT computers. Managing Machine-To-Machine (M2 M) authorization frameworks among IoT / IoT-based cloud devices using the Idemix framework has therefore become another future mission.
- An Intrusion is an unwanted operation carried out within a network by an attacker (adversary). Depending on the capacities of the adversary, an intrusion may be passive (i.e., eavesdropping information during communication) or aggressive (i.e. deliberate invasion of packets and dropping of packets). An Intrusion Detection System (IDS) is viewed as a computer program (software) capable of detecting any unusual incident occurring in the network. If an adversary identifies a malicious IoT computer, we need to identify the device's identification rapidly so that no more harm will occur in the network. Yet we need to build lightweight IDS frameworks because of resource constraints of IoT devices for making the IoT environment secure.
- The Internet of Things will involve many integrated sensor systems, i.e. a Wireless Body Area Network (WBAN) which will offer various incentives for real-time tracking of the health condition of patients [27]. IoT should play a significant part in the provision of next-generation health treatment in the future [7, 27]. IoT links medical tracking systems to cloud services via smart phones / mobile devices, i.e. allowing real-time and non-invasive tracking of a patient's health status. Because patient information is private and confidential, the personal details that IoT devices gather (such as smart watches, caps, etc.) must not be revealed (passed) to any unauthorized recipient/ unknown user. Hence, we will also protect the health records of the patient by using modern lightweight and safe mobile authentication for Mobile-To-Device (D2D) communications.

Sl .No	Applications	Advantages	Challenges
1	Health care	Smart hospitals, MHealth, Enhanced medical care, Reduce cost	Data management, data privacy and security
2	Smart cities	Smart homes, smart traffic monitoring, smart water/ other supply	Data volume, scalability, security, privacy, lack of standards
3	Defense sector	Logistics, healthcare and monitoring, training, energy management	Data security, cyber attacks
4	Telecommunication	Real-time data, cost effective, intelligent data model	Security, privacy, precision, compatibility, interoperability
5	Agriculture	Increase the revenue, live stock monitoring, high quality	Cost of implementation , lack of experts.
6	Supply chain	Real time inventory, efficient storage and distribution, better quality management	Identifying right device, power consumption ,data volume

Table 1: Different Internet of Things Applications and its Challenges

In recent years, already a lot of work, policies have been proposed/ implemented to secure critical IoT applications. Several attempts have been made to establish reliable contact networks consistent with the IP, which are useful for resource-constrained computers (using encryption techniques). In this, certain strategies need conservative, cohesive, enterprise-wide architecture and professional network engineers to develop and manage a cloud-based IoT infrastructure that is safe and stable. Hence, our work is not to provide “technical” security, also to provide “information security” and “Cyber Security” to IoT devices and its collected information. In last, we need system management like Smart Home security, i.e., how to properly install and maintain the security enabled by these powerful tools in IoTs. Note that IoT has been a long time coming, not a new technology, but still there is lot of enhancement need to be done in IoTs like using machine learning to analyze information to predict user’s movements or future moves. For example, suppose one person eating food at particular time daily, so an IoT device can easily remember this pattern and switch on and off lights or fan accordingly/ user’s patterns.

A. Privacy Goals

In above example, storing or learning patterns of user’s daily activities is ok, but it is critical when it is shared with unknown device/ users. It is a major and essential challenge (issue) to overcome. Privacy is a fundamental right, which needs to be protected. It can be protected with complete isolation from outside world/ Internet-world. A user starts to interact with other devices/ people; he/she starts sharing/ is willing to share information about itself with others. Hence, some privacy goals in IoT based Cloud are included as [5, 7, 10, and 13]:

- Privacy in devices: It relies on protection with regards to physical and commutation. In cases of computer misuse or failure, and resistance to side channel assaults, sensitive information may be leaked out of the system.
- Privacy during communication: It depends on system quality, and on the credibility and durability of the unit. To derogate the revealing of data privacy during conversation, IoT devices will interact only when appropriate.
- Privacy in storage: It is to preserve the privacy of data stored in devices, the following two issues should be considered: Potential volumes of data required to be stored in devices. Control must be expanded to ensure security to consumer data during end-of-service existence (deletion of the system data (Wipe) whether the computer is hacked, destroyed or not in use).
- Privacy in processing: It depends on credibility of the system and of contact. Data cannot be reported to third parties or held without the owner's information.
- Identity privacy: It is the identification of any computer that only the permitted person (human / system) can know.
- Location Privacy: It is the geographical location of the unit concerned should be discovered only by the designated person (human / computer) [28].

B. Internet of Things Limitations

Till now, overcoming/ improving IoT limitation is major issue in IoT devices. Battery life extension and Lightweight Computation are the major limitations of IoTs devices. Some limitation can be included as:

- Large-Scale Streaming Data: A huge number of data collection systems are spread and implemented for IoT applications, which constantly produce significant quantities/ lots of data [29]. Which results in an immense amount of continuous data.
- Heterogeneity: Various IoT data acquisition devices gather different information resulting in data heterogeneity. Heterogeneity in IoT device is a primarily concern.
- Time and space correlation: Sensor sensors are connected to a particular position in most IoT implementations and thus have a place and time stamp for each of the data objects.
- High noise data: Some data (in such devices) can be prone to errors and noise during processing and delivery due to tiny (small) bits of data in IoT applications.

Although having secret insight and insights from big data promises to increase the standard of our lives, it isn't a simple and transparent mission. New technology, algorithms and infrastructures are required for such a dynamic and demanding challenge that goes beyond the capability of the conventional inference and learning approaches [29]. Hence, this section discusses about privacy goals, few research directions in IoTs (i.e., with respect to security and privacy) and IoTs limitation in brief. Now next section will conclude this work in brief.

VI. Conclusion

Internet of Things is a very complicated heterogeneous network platform. It is connected and being used in several beneficial applications like smart home, smart metering, smart faming, smart transportation, etc. There are Billons and Billons of IoT enabled devices, which are being used today. In result, they are generating a large quantity of data which require storage to store it, tools to analyze it with efficiently or accuracy and addressing schemes to track every internet connected devices, etc. But, overcoming such issues has some limitations, i.e., either of Internet of Things or Internet connected devoices/ IoTs based cloud or on its own like battery life, heterogeneity of data, noise of data, etc. These IoTs based cloud produce continuous stream of data, in result a lot of issues and challenges in near future. Most popular is providing security and privacy to collected or generated data. These issues and possible challenges have been discussed in this article with sufficient information. Hence, we invite all future researchers/people from research community (from around the world, who are working in this respective area) to do their research in IoTs/ IoTs based cloud.

Author's Contributions

Amit Kumar Tyagi has analysed, and drafted this manuscript. Prof. Ajith Abraham has approved this manuscript.

Acknowledgements

This research is funded by the Anumit Academy's Research and Innovation Network (AARIN), India. The author would like to thank AARIN India, an education foundation body and a research network for supporting the project through its financial assistance.

Conflict of Interest

The author declares that they do not have any conflict of interest (in self-citation reference number 7, 13, 24, 27 and 29) with respect to this paper.

References

[1] O. Vermesan, P. Friess, P. Guillemin et al., Internet of things strategic research road map, in *Internet of Things: Global Technological and Societal Trends,* vol. 1, pp. 9–52, 2011.

[2] I. Peña-López, *ITU Internet Report 2005*: The Internet of Things, 2005.

[3] Networked Enterprise & RFID & Micro & Nano-systems, In: Proceedings of Co-operation with the Working Group RFID of the ETP EPOSS, *Internet of Things in 2020, Roadmap for the Future,* 2008.

[4] Mubashir Husain Rehmani, Al-Sakib Khan Pathan, Emerging Communication Technologies Based on Wireless Sensor Networks, *Book*, 2011.

[5] H. Sundmaeker, P. Guillemin, P. Friess, and S. WoelfÈ, Vision and challenges for realising the Internet of Things,' *European Commission Information Society and Media, Luxembourg, Tech. Rep.,* March 2010.

[6] Misra, Sridipta, Maheswaran, Muthucumaru, Hashmi, Salma, Security Challenges and Approaches in Internet of Things, *Springer Book*, 2017.

[7] Tyagi, Amit Kumar and Sharma, Sonam and Anuradh, Nandula and Sreenath, N. and G, Rekha, How a User will Look the Connections of Internet of Things Devices?: A Smarter Look of Smarter Environment. *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)* 2019.

[8] M.Roberto,B.Abyi and R.Domennico et al, Towards a definition of the Internet of Things(IoT): *IEEE,* Issue 1, May 2015

[9] A. Juels, RFID security and privacy: A research survey, *IEEE J Sel Area Comm.* 24 (2006) 381–394.

[10] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, *Future Generation Computer Systems,* Volume 29, Issue 7, September 2013, Pages 1645-1660.

[11] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, *Future Gener Comp Sy*. 25 (2009) 599–616

[12] Kocovic, Petar, Behringer, Reinhold, Ramachandran, Muthu, Mihajlovic, Radomir, Emerging Trends and Applications of the Internet of Things, *IGI Global Book,* 2017.

[13] Tyagi, Amit Kumar and M, Shamila, Spy in the Crowd: How User's Privacy Is Getting Affected with the Integration of Internet of Thing's Devices (March 20, 2019). *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India,* February 26-28, 2019.

[14] I.F. Akyildiz, T. Melodia, K.R. Chowdhury, A survey on wireless multimedia sensor networks, *Comput Netw*. 51 (2007) 921–960

[15] N. Khalil, M.R. Abid, D. Benhaddou, M. Gerndt, Wireless sensors networks for Internet of Things, *in: IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP, Singapore*, pp. 1-6, 2014.

[16] Partha Pratim Ray, A survey of IoT cloud platforms, *Future Computing and Informatics Journal*, Volume 1, Issues 1–2, December 2016, Pages 35-46.

[17] Mohammad Saeid Mahdavinejad Mohammadreza Rezvan Mohammadamin Barekatain, Peyman Adibi, Payam Barnaghi, Amit P.Sheth, Machine learning for internet of things data analysis: a survey, *Digital Communications and Networks*, Volume 4, Issue 3, August 2018, Pages 161-175

[18] Shabir Ahmad, Lei Hang, and Do Hyeun Kim, Design and Implementation of Cloud-Centric Configuration Repository for DIY IoT Applications, *Sensors (Basel)*, 2018 Feb; 18(2): 474.

[19] European Lighthouse Integrated Project - 7th Framework, Internet of Things - Architecture. *http://www.iot-a.eu/* (2012).

[20] L. Ren, F. Tian, X. Zhang, L. Zhang, DaisyViz: A model-based user interface toolkit for interactive information visualization sytem, *Journal of Visual Languages & Computing* 21, pp. 209–229, 2010.

[21] S. Misra et al., Security Challenges and Approaches in Internet of Things, *Springer Briefs in Electrical and Computer Engineering*, 2017, DOI 10.1007/978-3-319-44230-3_2

[22] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, pp. 146–164. DOI:10.1016/j.comnet.2014.11.008

[23] Luis Filipe, Florentino Fdez-Riverola, Nuno Costa, António Pereira, Wireless Body Area Networks for Healthcare Applications: Protocol Stack Review, 2015, https://doi.org/10.1155/2015/213705

[24] Tyagi, Amit Kumar, Building a Smart and Sustainable Environment using Internet of Things (February 22, 2019). *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India*, February 26-28, 2019.

[25] Dongxin Lu, & Tao Liu. The application of IOT in medical system. 2011 *IEEE International Symposium on IT inMedicineandEducation.2011*. doi:10.1109/itime.2011.6130831

[26] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[27] Amit Kumar Tyagi, N. Sreenath, Future Challenging Issues in Location based Services, *International Journal of Computer Applications* (ISSN: 0975 –8887), Volume 114, No. 5, pp.51-56, March 2015. DOI: 10.5120/19978-1921

[28] Mehdi Mohammadi, Graduate Student Member, Ala Al-Fuqaha, Sameh Sorour, Deep Learning for IoT Big Data and Streaming, Analytics: A Survey, *IEEE Communications Surveys & Tutorials,* Vol. X, No. X, XXXXX 2018).

[29] Tyagi A.K., Rekha G., Sreenath N. (2020) Beyond the Hype: Internet of Things Concepts, Security and Privacy Concerns. In: Satapathy S., Raju K., Shyamala K., Krishna D., Favorskaya M. (eds) *Advances in Decision Sciences, Image Processing, Security and Computer Vision. ICETE 2019. Learning and Analytics in Intelligent Systems,* vol 3. Springer, Cham.

Author's Biographies

Amit Kumar Tyagi is Assistant Professor (Senior Grade), and Senior Researcher at Vellore Institute of Technology (VIT), Chennai Campus, India. His current research focuses on Machine Learning with Big data, Blockchain Technology, Data Science, Cyber Physical Systems, and Smart and Secure Computing, Privacy). He has contributed to several projects such as "AARIN" and "P3-Block" to address some of the open issues related to the privacy breaches in Vehicular Applications (like Parking) and Medical Cyber Physical Systems. He received his Ph.D. Degree from Pondicherry Central University, India. He is a member of the IEEE.

Dr. Abraham is the Director of Machine Intelligence Research Labs (MIR Labs), a Not-for-Profit Scientific Network for Innovation and Research Excellence connecting Industry and Academia. As an Investigator / Co-Investigator, he has won research grants worth over 100+ Million US$ from Australia, USA, EU, Italy, Czech Republic, France, Malaysia and China. Dr. Abraham works in a multi-disciplinary environment involving machine intelligence, cyber-physical systems, Internet of things, network security, sensor networks, Web intelligence, Web services, data mining and applied to various real world problems. In these areas he has authored / coauthored more than 1,300+ research publications out of which there are 100+ books covering various aspects of Computer Science. One of his books was translated to Japanese and few other articles were translated to Russian and Chinese. About 1000+ publications are indexed by Scopus and over 800 are indexed by Thomson ISI Web of Science. Dr. Abraham has more than 37,000+ academic citations (h-index of 90 as per google scholar). He has given more than 100 plenary lectures and conference tutorials (in 20+ countries). Since 2008, Dr. Abraham is the Chair of IEEE Systems Man and Cybernetics Society Technical Committee on Soft Computing (which has over 200+ members) and served as a Distinguished Lecturer of IEEE Computer Society representing Europe (2011-2013). Currently Dr. Abraham is the editor-in-chief of Engineering Applications of Artificial Intelligence (EAAI) and serves/served the editorial board of over 15 International Journals indexed by Thomson ISI. Dr. Abraham received Ph.D. degree in Computer Science from Monash University, Melbourne, Australia (2001) and a Master of Science Degree from Nanyang Technological University, Singapore (1998).