Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 15 (2020) pp. 153-177
© MIR Labs, www.mirlabs.net/jias/index.html

Internet of Everything (IoE) and Internet of Things (IoTs): Threat Analyses, Possible Opportunities for Future

Amit Kumar Tyagi[1][0000-0003-2657-8700], **Meghna Manoj Nair**[2]

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

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

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 provide 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 provide 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, 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". The digital world interacts with the physical world using many sensors and actuators. 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."

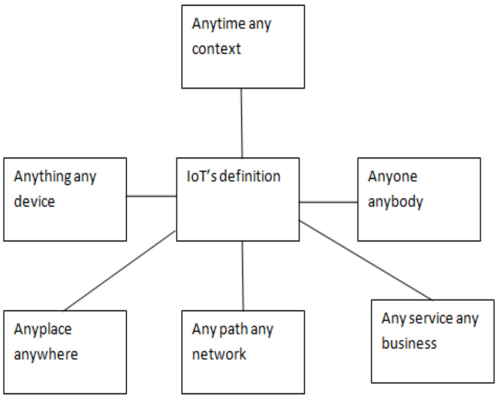

Figure 1: Definition of Internet of Things [5]

- 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”. Figure 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”. The underlying infrastructure of virtually represented “things” in an Internet-like structure includes components/ sensors for making communication using Internet and network developments [6, 7]. The upcoming services and implementations are classified to be highly autonomous in nature with respect to data capture, transfer of events, connection of networks and multi-disciplinary operations [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 be 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 storage purpose, integrates monitoring devices, storage devices, analytics tools, visualization platforms and client delivery. 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 recognition of the scenario of its’ users along with their appliances,

b) Software frameworks and persistent networks to analyze and portray the content to wherever it is relevant,

c) The analytics tools in the Internet of Things that aims for autonomous and smart 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.

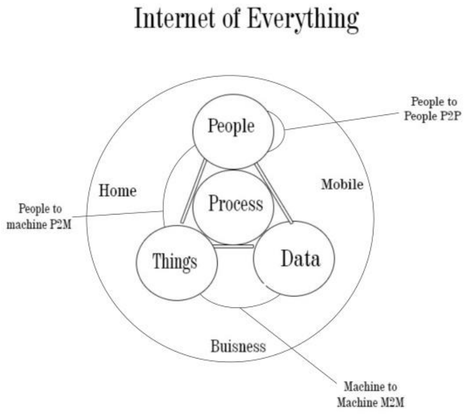

Figure 2: Components of Internet of Everything [8]

Figure 2 discusses several components of Internet of Everything. 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 discuss 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. This paper provides answer to following questions:

- In which manner will Machine Learning (ML) algorithms prove to be useful to the smart data in IoT?
- What's the nomenclature of ML algorithms which can be applied in the field of IoT?
- What are the possible features of IoT data in real life?
- How can we consider smart city to be a significant application of IoT?

Difference between Internet of Things (IoTs) and Other Networks

It is because of the above reasons that IoT stands out from other stereotypical IT frameworks and they're to be noted because they deeply affect the growth of safety and privacy solutions for IoT devices. The amount of resources available at the end devices forms the major distinguishing factor between common networks and IoT [21] and IoT is known for comprising of Devices similar to Radio-Frequency IDentification (RFID) and sensor nodes. The unique characteristics of any conventional IoT device is its' low memory, reduced processing power, and small battery life. On the contrary, the typical networks comprise of efficient computers, servers, and other gadgets which have sample resources and hence, we can prove that the sophisticated and inter-disciplinary safety rules and regulations can be secured. On the other hand, lightweight safety algorithms and codes which help in striking a balance between security and resource usage are a necessity for IoT devices. IoT gadgets are mainly used to interlink internet or other gateway devices via low bandwidth and low power consuming communication media like 802.15.4, 802.11a/b/g/n/p, LoRa, ZigBee, NB-IoT and SigFox. However, devices in the typical IT fields transfer data through highly secure and faster wired/wireless modes like fibre optics, DSL/ADSL, WiFi, 4G, LTE and so on. Another key distinguishing factor is that the typical network devices mostly have similar OS and data format, however, in IoT, due to the presence of functionality specification and absence of OS, there are a number of contents and formats. This intense diversity poses a hinderance for the development of a usual security protocol which fits all IoT gadgets and devices. Hence, a plethora of IoT adversities are still to be corrected which may tend to threaten the safety and privacy of the users.

On considering the design perspective of security design, it can be noted that the traditional and typical networks are tightly secured by a combination of constant network perimeter defence which is completely based on firewalls, IDS/IPS, as well as the end devices are procured by host-based approaches including anti-virus and software catch ups, whereas, IoT devices can not implement host-based security perspective [22]. Since IoT devices have a lot of vulnerabilities including those of absence of physical safety, host-based defence methods, regular software updates, etc. The standard defence algorithm does not have the capability to protect the IoT devices from any of the insider attacks and physical abuses carried out by unauthorised employees. IoT devices often expose themselves to harmful attackers because of their low bandwidth, low power consumption and less security protocols [23, 24, and 25], weak web application and programming interfaces [26, 27]. Furthermore, the absence of integrity and conceptualisation in IoT solutions leads to the existence of issues pertaining to interoperability, manageability, etc. all across the globe [28].

Internet of Things Environment

The possible vulnerabilities are likely to increase with a steep rise in the devices connected to IoT systems [68] in the upcoming years [32], thus leading to security and privacy issues in IoT systems and networks. However, the successfully accomplished attacks like Mirai, Ransomware, Shamoon-2 and DuQu on IoT and Industrial Control Systems (ICS) down the lane have proven the inefficiency of the current rules and norms thus, portraying the vulnerable nature of IoT devices to cyber-crimes and attacks, paving way for ransom payment, data theft and forgery, and other suspicious behaviours including botnet attacks. Moreover, IoT devices are quite exposed to physical compromise and can be easily exploited in an unprotected environment.

With the help hardware gadgets like UART devices, authors of [33] have negotiated on a smart controller of a house automation system, after which they were permitted to access the start-up sequence. On altering the boot parameters, they were able to acquire low-level access to the gadget and brute-forced the root password, launching network tiered attacks consisting of port scanning, network scrutiny, etc. However, in spite of authorising a centralised and controlled permittance to data, even the cloud supported IoT is likely to be attacked with respect to security and privacy [34]. It is approximated that almost one-fifth of the files being uploaded to file transfer services consist of sensitive data and 82% of the cloud service providers assure secure data transfer even though, only 10% of them encrypt data on being stored in the cloud [35]. Cloud is highly susceptible to single point of failure, data privacy fissures including unsanctioned data access and data analytics [34]. The exposure of private data pertaining to around 87 million by Facebook Inc. in April 2018 is a great example of possible cloud vulnerabilities [35]. So, we can prove that security and privacy flaws in IoT lead to attacks on device consistency, data integrity, privacy etc. [36]. The existing issues in IoT can be acclaimed to be caused by weak design of devices, lack of sufficient memory, and trust in cloud-based applications.

Organisation: The organization of this paper is follows as: section 2 discusses 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. Section 4 discusses scope and importance of IoT and IoE in 21st century. Further, section 5 discusses taxonomy and analysis of security protocols for Internet of Things and Internet of everything. Further, section 6 discusses about Blockchain Technology Integration with Internet of Everything (IoE) and Internet of Things (IoTs) in detail. Then section 7 discusses several Problems in Existing Internet of Things based Cloud Platforms. Open Issues and Challenges in Internet of Everything (IoE) and Internet of Things (IoTs) are discussed in section 8. Later, section 9 discusses future research issues and challenges (also discussing challenges in IoT - Blockchain and IoE - Blockchain Integration) with analysis of several/ different attacks, and also discusses a real world example (i.e., Smart Home Security) with explaining attacks and suggested solutions for protecting the same. Then, several future research directions in internet of things and internet of everything (with respect to Security, Privacy and Trust) with respect to security and privacy will be discussed in section 10. In last, section 11 concludes this work in brief.

Also note that 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. Also, the terms "Internet of Things" or "Internet of Objects" or "Smart devices" or "Smart things", or "Internet Connected Things will be used interchangeably throughout this work.

II. EVOLUTION OF THE 'INTERNET OF EVERYTHING' AND 'INTERNET OF THINGS'

It is indeed restricting to be talking about 'Internet of Things' without considering the inclusion of people and other dimensions, especially in this world which has evolved extensive techniques for the automation of a hefty number of 'things' which are for or by the people and the production and its' quality affect people in a variety of ways. In fact, we need to extend the idea of 'things', way beyond its' semantical form. One way in which this can be implemented is to expand the term 'Internet of Things' to 'Internet of People and Things', which provides a huge foundation for the process of communications and relations. For example, IoTs can prove to be helpful in the sector of applications like captivating user's source point or other variables/devices/vehicles at anytime from anywhere. Furthermore, information on people can be presided over that of social media which tops up the existing content. It can be noticed that the 'Internet of People and Things' can provide access and connectional relations with every other instance in a suitable context. Many of the other researchers have found 'Internet of Everything' to be a prime topic of discussion these days, which involves the virtual connection of all devices and their real-time connection with human beings. But, this work throws light mainly on 'Internet of Things', irrespective of terms like 'Smart Things' or 'Internet Connected Things'.
Efficient and transparent communication between two computers were made possible with the help of computer networks in the late 1960s along with the introduction of TCP/IP in the early 1980s, after which the commercial use of internet began in full swing. Social networking, blogs, etc. became the best source of creating and circulating content on Web and is hence called "Web of People (WOP)". With enhancements in technology and sciences, WoP underwent drastic transformations. The aim and target of transforming the web services to be innate, precise, aware and autonomous has resulted in the weakening of links existing between "people" from the loop, and acclamation of things into the networks [30, 37].

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" [37]. 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 traces 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 require 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. MOTIVATION

Now days IoT are being used in every sectors/applications to increase productivity and fulfill need of society. IoT is the infrastructure that allows all types of devices (also machines) to communicate with each other, for example, cyber infrastructure, medical cyber physical systems, etc. This (IoT) links physical systems around the world such as power meters, cars, containers, pipes, wind turbines, sales devices, personal accessories, etc. Today's IoT technologies are used in all fields (or industries) possible, as well as providing many possibilities for other sectors such as fleet management, energy management, connected vehicle, health monitoring, and cargo management. Internet of Everything is the enhance version of Internet of Things (or Internet connected things) which consist intelligence everywhere via using smart objects (in real world’s applications). For example, a daily life example has been discussed in [36] in detail. As another real world example, such devices are very much useful in decreasing total number of accidents over the road via continuous sensing nearby objects and responding to users (e.g., autonomous car). In near future, IoE will be everywhere and each object have intelligence and able to respond immediately with the help of IoTs. On another side, with (using) such devices we are facing many serious concerns like security of our personal information (or data), privacy of our identity (or location/ information), trust in devices (or smart things), and lack of standardization of tools, etc. Serious vulnerability is getting traced by these smart devices/ things, which is a serious issue (because via hacking or threats an attacker can try to steal user’s information and can use for its financial gain/purpose). Finally, we should not forget that in the future we will be able to use IoT and IoE tools for sustainable development and to take urgent action to combat climate change and its effects on nature.

Hence, this section discusses motivation behind writing articles regarding to this emerging area. In that, we found that IoE is need for next decade and will be implemented with every system/ devices (to make people life easier). Now next section will discuss importance of IoE over IoT in 21st century (in detail).

IV. IMPORTANCE OF INTERNET OF EVERYTHING (OVER INTERNET OF THINGS) IN 21ST CENTURY

In general, terms IoE and IoT are being used interchangeably in this work (also in general-use), but IoT is not a synonym for IoE, it is an essential component of IoE. For example, IoE includes people, artifacts, and system interactions in which IoT is one of the components. Internet Connected Things make environment for IoE and crate communications like (for) Machine to Machine (M2M) communication, Industrial Internet, industry 4.0, etc., for many industries [30]. These smart technologies are being used in several critical applications like healthcare, defence, or aerospace, manufacturing etc. Then, they have very essential role in making effective decision or predict accurate results (with respect to respective application), saving maximum human lives (around the world). Using IoE in different industry increase the productivity, reduce production cost and save time for completing any task. Hence, keeping importance of IoE in our mind, we are explaining several essential terms here, which are:

Machine to Machine (M2M) Communication Today and in Future: Machine-to-Machine (M2M) communication is made by integrating of many devices (called IoT or smart devices). There are a number of key components in an M2M system consisting of sensors which include, Radio Frequency Identification (RFID) tags, Wi-Fi or cellular connections, autonomous software used for communicating between devices and making apt decisions, i.e. interlinked through internet/other networks. Even today's M2M is an important aspect of warehouse management, remote control, automation, traffic control, logistics, supply chain management, fleet management and telemedicine). This method of communication and interconnection have large levels of position in a number of business models including security on video-based content, vehicular information services, healthcare solutions on mobiles, alternative energy solutions, building of smart cities, and so much more. A plethora of industries or organizations can collect revenue via using M2M technology, or via providing new opportunities to customer choice and service. For example, operational costs in manufacturing, automation and logistics are decreasing day by day, also M2M communication are increasing in various applications/ sectors like healthcare, automotive, and consumer electronics. The advancement in M2M development also permits businesses to pay more attention on solution alternatives that would solve issues globally. A plethora of transportation companies are able to save large amounts of fuel by drastically decreasing its’ consumption by making productive use of the data which is captured, transferred, and analyzed (in real-life).

Industrial Internet: Industrial Internet provides enhanced visibility and deeper insight into equipment and resource quality. Asset performance management helps in following records of all responses which have relevant equipment, unexpected failures, etc. Digital internet enhances the techniques through which communication occurs between people and machines with the implementation of data analysis, increased performances and total operational excellence. The digital internet provides valuable new insights through the integration of machines with powerful (best) analytics. Industrial Internet's popular feature is that it consists of / installs knowledge above the level of individual machines. Internet-connected smart devices (Internet of Things (IoTs)/ Internet Connected Things (ICT), Internet of Services and Cyber-Physical Systems) can automatically improve performance, security, reliability, and energy efficiency by collecting data/ information, interpreting data, and taking appropriate information action and transmitting it to the respective user. Industrial Internet solutions enable sustainable development through enhanced resource efficiency, resulting in savings in energy and water, increased performance, and higher output rates of industrial machines. Simply put, by internet convergence of smart devices, Machine to Machine (M2M) interaction maximizes the use of all industrial tools. Consider this case, street lightings which efficiently control traffic congestions, alternative energy usage in bigger cities through Wireless Control System (WCS) to ensure remote operation and analysis on lighting equipment via web-enabled centralized system control. This not only saves energy and money, but also enables controllers to switch off or dim streetlights when required, i.e. to provide unique versatility and utilization of resources. Remember that street light can also feel vibrations that can help identify structural integrity problems while placed on bridges. With similar examples, IoE can use useful a lot and provide different experience to users/ citizens.

Industry 4.0: Near future technology belongs to centralized structure with explaining or telling machines “what to do”. For example, we can connect embedded system production technologies to other business industries (for smart production processes) which create a new technological age, also change/ transform industry (also business models), etc., and work as smart factory. Automation (increased by interaction with M2M) would mean advanced robotics that will make automation more efficient and cheaper. Through such technologies as sensors and actuators, wireless networks, high-performance cloud computing and big data analytics, this interaction or automation phase is allowed. Virtual industrial transition is Industry 4.0 (emerged in 2011), which is the industry's new revolution. Industry 4.0 innovations has proven to be of great support and help to all farmers in emerging countries, helping them stay hand-in-hand with milk production and many other featured characteristics which seem to be improving the essence of life, stepping up the economic growth in under-privileged areas. Automation also calculates the percentage of milk, cream fat and non-fat solids, while queue management ensures prompt refilling of silos without delay to maintain continuity. Note that M2M communication/ automation ensures sustainable consumption and production patterns of an organization. The next phase of digitization of industry 4.0/ manufacturing sector include four trends:

- Voluminous amounts of bulk data, processing capabilities and linkages, especially in the low-power networks,
- The enhancement of skills in data analytics and management intelligence,
- Novel methods of communication between human beings and rapidly growing technologies, like touch interfaces and augmented reality sectors, and,
- New forms of communication between human and machine, such as touch interfaces and augmented reality systems, and,
- Growth in the field of transmitting data/digitalized algorithms physically, as in the case of 3-D printing and advanced robotics.

Note that here digitalization of the industry means is ability of real-time data (by machines) by efficient analytics tools. In the production environment, for example, cyber-physical systems (CPSs) include smart machines, storage systems, and production facilities that exchange information autonomously, trigger actions, and independently control each other. This improves the manufacturing, engineering, material use and supply chain and life cycle management processes involved in industrial processes. On the other hand, data generated from Global Positioning Systems (GPS) and agricultural sensors (and using big data analytics) will allow farmers to improve or increase their crop productivity through proper (field) water utilization. Farmers can also benefit from reliable guidance on the seeds to be planted, time to harvest, and estimated yield using data and analysis. Monitoring crops and weather patterns can be tracked in the near future to specific regions to issue early warnings of drought or protect crops from extreme natural disasters. Such attempts may be useful for government to take preventive measures in risk areas. Industries 4.0 therefore offers new tools for smarter energy consumption, greater storage of information in products and pallets (so-called smart lots), and optimization of real-time yields. Industrial Internet and Industry 4.0 can be used to improve health, resource efficiency and sustainable development in the near future.

IoE Today: Through describing the current and evolving elements of IoE: IoT, M2M, Industrial Web, Industry 4.0, and the environment they work in (i.e., cloud and Big Data Analytics), we discuss several benefits and risks caused by the respective application. Today internet has changed various application/ sectors in terms of efficiency. What's next, then? How is the Internet going to evolve and keep changing and improving the world? Such things are discussed here or things are in supporting the IoE today are discussed here as.

Transforming the World’s Largest Cities via providing Smart Solutions to Transportation Sector

On nearby smartphones, tablets and laptops along the highway/ road, smart screens can be accessed via Wi-Fi. The aim of smart Screens (in cities) are to:

- By connecting people immediately with information relevant to their immediate proximity, notify them.
- Secure by providing local police and fire departments with a citywide network of sensing, communications and response capable of directing required staff and assets precisely where and when necessary
- Revitalize by increasing levels of commerce, investment, and tourism

We need to create innovative solutions to the major environmental, social and health challenges facing cities, i.e., [39] skill. Smart traffic can also solve several critical problems like traffic management, etc. The implementations of IoT devices/IoE in portraying real time data to support and help the emerging drivers in the cities acquire parking easily and quickly is a concept well explained by M.Mazhar Rathore et.al [39]. Furthermore, logistics companies have the potential to receive traffic footprints of urban systems in order to imply cost and time efficient routes for vehicles engaged in delivery.

Resource Efficiency: The key area where IoT can bring significant benefits is energy management. The control of water is a good example. As per existing records and systems, large-scale water systems loose at least 20% of water due to the leakage factor before reaching its’ final destination. Such a system would bring a whole new level of efficiency to water consumption around the world. The major advantages of resource enhancement include increased optimization of capacity and demand, good control of network and leakage, reduced volume of water which are unbilled, etc. The new reality has many connected devices rapidly improving computing power and economies of scope and scale (also increasing the use of cloud computing and big data analytics). The technology transition provides multiple opportunities (which we have not seen before) for both the public and private sectors to develop new technologies, enhance productivity and efficiency, enhance real-time decision-making, solve issues relevant to critical society, and develop new and innovative user experiences. IoE covers a wide range of items, including M2M and the digital Internet. This section addresses the nature and significance of the IoE age and the near future for different applications. Now, the next segment will be addressing important and useful IoE interfaces/ connections in the near future with other smart devices /objects.

V. Taxonomy and Analysis of Security Protocols for Internet of Things

Various security issues, threats and attacks which are mitigated an included in this section. The IoT devices use the internet for transferring the data collected by sensors to server for data analysis, so all the network security requirements necessary to an IoT ecosystem also. Moreover, the IoT is an agglomeration of various heterogeneous sensor enabled devices across divergent networks and computing infrastructures. So, security protocols/ mechanisms that work in traditional computing architecture with domain specific applications are not robust enough to handle IoT architecture. Taxonomy of various security mechanisms like key management, user and device authentication, access control, privacy and identification management is discussed (see figure 3).

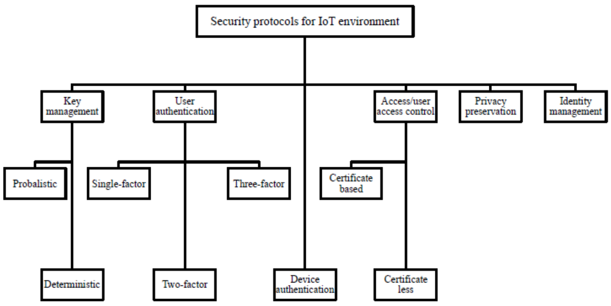

Figure 3: Taxonomy of Security Protocols in the IoT Environment

The best IoT framework should be “consensus-based dynamic policy formulation framework”, also require two essential features:

- Increasing the active involvement of humanised parameters in “dynamic policy formulation” and also in governance.
- Reduce the involvement of human parameters in the “policy adherence” to enhance the policy acquiescence (or make the machines “smart” enough to obey the policies and refuse any deviation from those).

Security and privacy necessities are important in the IoT environment [34] just like in every other network:

- Authentication: Validation of all devices used for sensing applications, users and gateway nodes before permitting or granting access to a confidential-resources, or exposure of crucial details are all involved in authentication.
- Integrity: All entities under analysis must not be changes to assure consistency.
- Confidentiality: Discretion or privacy of the wireless method of transferring data through data channels helps in protecting crucial data content from its unwanted exposure.
- Availability: The required network services are to be made accessible to the legal users even if the system undergoes attacks similar to that of denial-of-services.
- Non-repudiation: It ensures that masked entities/ instances do not have their actions under cover as well.
- Authorization: It concludes that only the genuine IoT smart devices used for sensing can supply data to the network which can further avail the services.
- Freshness: It assures that all the data and content id quite fresh and the past messages cannot be redone by any of the opponents.

Forward and backward secrecy are the other two important security necessities that need to be abided by: i) Forward secrecy: If a node corresponding to IoT sensing leaves a network, all messages pertaining to that particular node must be prohibited in the future ii) Backward secrecy: If a novel node has been introduced in a particular network, it should not have the ability to read any of the messages which have already been transmitted. It is also important to keep in mind that the design of the security norms should be such that it prevents any attack on the environment. Here, few of the attacks can be listed as:

- Replay attack: This involves the intervention of an opponent, who indulges in the malpractice of deceiving the legal user by interrupting data and content during its transmission wherein, he/ she can keep a track of all the data being transmitted.
- Man-in-the-middle attack: This attack involves the modification/deletion/alteration of content stored in data which is to be received by the recipient.
- Many logged-in users with the same login-id attack: If a particular system contains the verifier table for verification of the login details of the user, it can be exposed to a number of currently signed-in users who are likely to possess the same login-id threat. In short, we can observe that even if an authorised user uses the same identity and password in such kind of a scheme which is also accessible by other sincere users, none of the users will be able to kick-start this attack.
- Stolen-verifier attack: This attack is likely to take place if there’s and existence of Gateway Node (GWN) presiding in the IoT network which stores the password details for user/device cross-checking. This variety of attacks involves stealing the user’s personal details and authorisations from the table. Thus, it is of prime concern that design of these safety norms must not contain any password table for authentication, as this would be the best way to form resilience and protection armour against this type of attack.
- Stolen/ lost smart card attack: If a person misplaces his/her smart card, they always have the opportunity to retrieve the data credentials into its memory with the help of techniques like power analysis attacks. With the extracted details, the person can extract all of the personal details and credentials. Hence, it is necessary for the designed security protocol to handle and tackle the issues of

the smart card being lost by ensuring that there’s no explicit way through which the personal credentials can be retrieved.

- Password guessing attack: In a scheme involving password. A person has high chances of guessing the password of an authorised user who may be in online or offline mode by utilising all the eavesdropped messages and the stowed details in the system/ mobile. Hence, these confidential credentials should not be stored in any such accessible devices which may form a loophole for the intruder to retrieve the details.
- Password change attack: In this type of an invasion, the intruder is likely to modify the password of a legally registered user. For example, if a smart card-based scheme of an authorised user is negotiated, the invader can always extract the stored information, replacing the original password with a forged one.
- Denial of Service attack: This attack hinders the full-fledged action/function of a system or network and is mainly caused by software bugs, system failures, surrounding limitations or over-consumption of available resources.
- Privileged-insider attack: This attack revolves around any loyal user within the organisation, who takes the role of an attacker. Any insider has direct access to the private details of a registered user during the implementation of authentication scheme, which are further ill used by them. This is the very reason why, the safety and security norms which are developed for an IoT environment must supress the rise of such issues and attacks.
- Impersonation attack: In this type of an attack, an attacker tries to forge fake messages to defraud entities and instances of other recipients in a network on behalf of the sending entity. Due to this, the receiver is forced to believe that the message has been outsourced by a legal entity.

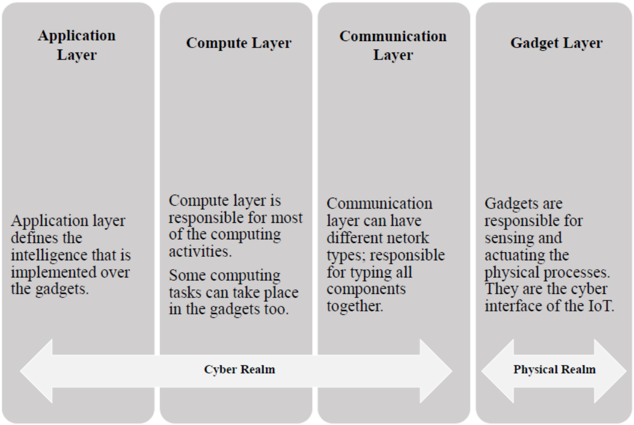
Application Layer
Compute Layer
Communication Layer
Gadget Layer
Application layer defines the intelligence that is implemented over the gadgets.
Compute layer is responsible for most of the computing activities.
Some computing tasks can take place in the gadgets too.
Communication layer can have different netork types; responsible for typing all components together.
Gadgets are responsible for sensing and actuating the physical processes. They are the cyber interface of the IoT.
Cyber Realm
Physical Realm

Figure 4 Security Problems of Internet of Things all layers are facing [34]

- Resilience against sensing device capture attack: Besides the GWN (Gateway Node), physical protection of a large number of IoT sensing devices are yet to be acquired, and this ensures that extraction of information from these devices causes a compromise on the transmittal and receival of the other devices. The adaptability of the sensing devices captivates attacks in the IoT environment by approximating the number of all safe and sound communications which are compromised by soulful duty of any sensing device. In other terms, for all the non-compromised sensing devices SDj, we calculate the chances of the attacker trying to leak the details from the existing communication happening between SDj and the corresponding user Ui. For example, in the case of controlling access, schemes for authentication of devices, and key management, the chances and rates at which the attacker is likely to extract the data from communications happening between non-compromised sensing gadgets creates an issue. It is necessary to acquire the probability of compromising secure transmission of data between genuine users and other illicit sensing devices in the IoT network. Consider Pe (nc) to be the probability and if it equates to 0, this arrangement will be recorded to be highly secure against sensing the presence of a typical capture attack.
  So, the protocols and norms should be such that that they are highly robust and resistant towards sensing the capture attack of the devices.
- Resilience against new sensing devices deployment attacks: All schemes which have been formulated for controlling the access verifications, like those of Sybil, sensing device duplication, etc. Wormhole attacks [34], in which an intruder tries to channelize the data amid to distantly situated places using in-band or out-of-band channel are quite common. These tunnels are developed easily by two nodes classified as attackers, leaving an impression that the two nodes, though are far apart, are close to each other. Thus, it can be easily seen that wormholes implement the tactic of deception are able to breach large volumes of data, allowing these devices to gain hands over managing the traffic. Sniffing, modifications and alterations, dropping, etc. are few of the possible attacks using the wormhole tunnel.
- Sybil attack: This type of attack is prone to take place when dangerous devices tent to presume a variety of identities which may/may not belong to the currently used sensing devices. These sensing devices often fall prey to attackers directly or physically. In attacks which involve the replication of devices, attackers create a large number of duplicates of a particular device which is to be kept in the network. This is helpful for the attacker as he can easily retrieve the details from a selected senor and install it into all of the other sensors leading to a malicious and extensive spread of unwanted sensing methods, destroying the rapport between the devices in the network.

Figure 4 portrays all plausible tiers of the surrounding environment of IoT which are likely to be destroyed by future attacks later. The next portion gives briefings on the interconnection of Blockchain and IoE and IoT.

VI. Blockchain Technology Integration with Internet of Everything (IoE) and Internet of Things (IoTs)

Internet of Things (IoTs) has been transmuting and augmenting all physical and manual methods to integrate them with the era of technology, gaining bulk amounts of data which provide knowledge to great extends. The knowledge obtained proves to highly effective as it tends to be the key to the lock of developments in the field of smart applications, efficient life sustainability, thus leading to a digitalized world and community. Earlier, cloud computation had proven to be an integral part of IoT as they performed the major function of comprehending and operating over data, processing them into actions and words of wisdom [30, 31]. This enormous increase in the field of IoT threw out a number of chances including methods and techniques to retrieve and pass on details and data. The open data archetype is the zenith of these types of initiatives. However, one of the major issues of this initiative is the reduced confidence. Frameworks with a central form of control have played a vital role in the creation of IoT, but when it comes to transparency of information, they are equivalent to those of black boxes and there's no possible way for the participants to realize the different ways through which they can use the information.

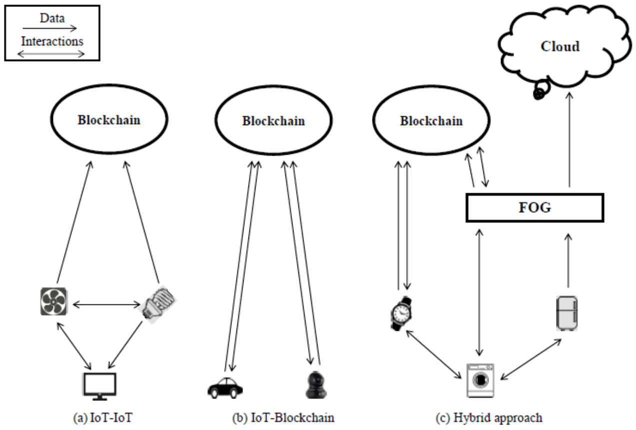

Figure 5: Blockchain – Internet of Things (IoTs) Integration

The rare and unique combination of IoT and cloud computation along with the revolutionizing involvement of Blockchain has proven to be of great success by ensuring a safe method of sharing services in a reliable and retraceable manner. The data source can be acknowledged easily and are not subject to changes or other unwanted modifications. For example, the ability to track the process and procedural paradigms of various food products is the best way to assure safety of food and requires the inclusion of a number of parameters like manufacturing, feeding, treatment, distribution, etc. The probability of data leakage in any one part of this crucial procedure can result in multiple fraudulent adaptations which poses dangerous threats to the lives of the citizens along with the deployment and economic crises of huge establishments and companies [34, 36]. Empowering the rhetorical and controlling skills in this area would enhance the food safety conditions, increasing the possibilities of sharing data and decreasing the time spent in foodborne epidemics. After all, in assurance of reliable data sharing techniques would further encourage the real-life applications of smart cities, smart services and smart cars. Hence, we can conclude that Blockchain proves to be one of the best parameters to complement IoT by supplying consistent and steadfast details and data. This has been gravely addressed in [40], wherein Blockchain technology is one of the most implementable solutions to scalability, privacy, etc., with respect to IoTs (or wireless devices or wireless sensing devices) in many sectors like e-healthcare [66, 67], agriculture, transportation, manufacturing, etc.

From our viewpoint, IoT has the audacity to benefit greatly from Blockchain and also support many other mechanisms and paradigms for their further development. This is a field/topic which excites a number of researchers and is still in its' primary stage. Further improvisations [31] which can be brought about include:

a) *Decentralization and scalability*: moving to a P2P (peer to peer) distributed framework from a centralized one which will indeed remove all possible nodes of failures and bottlenecks. This helps prevent situations where the power to access and handle the data of a large number of people are vested in the hands of a few companies alone. It also ensures that there's perfection in the system of fault tolerance and scalability which gravely reduces IoT silos.

b) *Identity*: Blockchain systems help the users to identify the devices with ease. To top it up, the data is undisputable and helps in the primary identification of the corresponding device. Blockchain can also provide a reliable source of verification and approval of devices for IoT managements.

c) *Autonomy*: Blockchain technique also promotes new-gen application allowing the advancement of automated credits and hardware as services. Blockchain allows the communication of devices with each other without the help of servers and IoT implementations can profit from this to portray device-agnostic and decoupled-applications.

d) *Reliability*: The information pertaining to an IoT device remains unchangeable with time in Blockchain and the users have all the authority to ensure the originality of the data. Moreover, developments have assured the enabling of data traceability and liability.

e) *Security*: The secured procurement of data and communications can be attained through Blockchain allowing it to treat the messages as transactions and Blockchain plays a key role in optimizing the present protocols used in IoT.

f) *Market of services*: All systems which involve the carrying out of processes without authorities can be easily extremified by using a combination of Blockchain and IoT. The deployment of micro-services would've been an easy task to accomplish with payments being done in a safer environment, increasing the access to data from IoT.

g) *Secure code deployment*: With more attention and care, codes can be easily inserted into devices in a safe and secure manner.

Another key aspect which needs to be looked into is the part of communication which forms the foundation for IoT devices. This interaction can take place either through IoT, or a combined design of IoT and Blockchain [31, 40] or through Blockchain alone. Fog Computational process has provided novel perspectives to IoT combined with Blockchain and given below are few of the advantages and disadvantages of the provided substitutes (in the figure).

- IoT–IoT: this appears to be the quickest approach with respect to latency and security as it is capable of functioning offline as well. The discovery and routing mechanisms enable interaction between the IoT devices and only a small portion of the data is stored in the Blockchain while majority of the others do not require the presence of Blockchain for this purpose (see figure 5a). This is extremely helpful in cases with highly confidential IoT data where communication happens with low latency.
- IoT–Blockchain: in this method, it is a manifestation that all communicative interactions take place through the Blockchain, permitting an undisputed array of interactive sessions. This assures cent percent traceability of any communication process as their information can be interrogated in the Blockchain which enhances the sovereignty of the IoT devices. We can observe a significant enhancement in the bandwidth and data in Blockchain which proves to be one of its' major challenges (see figure 5b). On the contrary, IoT data complementing the transactions need to be stored in Blockchain as well.
- Hybrid approach: Last but not the least, this is a fusion of designs wherein, only some of the interactions occur in block chain while the others are distributed between the IoT devices. However, the herculean task is to channelize which interaction must occur through blockchain and which one must not. The apt composition would be to combine both the techniques as it forces the advantages of Blockchain and profits the real-time IoT communication processes. This opens way for fog computation along with cloud computing as well, because it uplifts the disadvantages of Blockchain and IoT. For example, fog computation includes lesser number of devices such as gateways and is a potential target for mining of processes that use other IoT devices [41, 42] (see figure 5c). In a typical IoT arrangement, limited devices are used for nodes which are used for communication with gateways that are soul reason for passing sensor data to the superior tiers. During the integration of Blockchain, cryptographic functionality is applied in IoT devices for the interaction between end nodes and Blockchain. This forms the foundation for automating IoT, which requires complicated hardware and more expenses (in [40] an evaluation of the cost of using Blockchain in IoT devices is discussed). Integration of gateways is a suitable solution though the profits of using Blockchain in this method are limited.

It would be a drastic waste to employ Blockchain in a number of applications where databases provide sufficient operations. The necessities of the Blockchain is what decides the extend of need for Blockchain. For example, in scenarios where premium performance is required, Blockchain along with a few other approaches prove to be the optimized solution. In [40], author has suggested many methods and techniques to spot the requirement of Blockchain based on the problem. We now move on to how such technical achievements can be made for IoT devices.

Alliances amid popular companies are quite common these days, just like the trusted IoT Alliance [43], to fix the gap between IoT and Blockchain. Further, with increasing number of sensors being linked with Blockchain, they are sold in the markets these days like [41, 42, and 44]. EthEmbedded [41] ensures the configuration of Ethereum full nodes on Raspberry Pi [44], Beaglebone Black and Odroid. Raspnode [42] and Ethraspbian [45] complement the configuration of Bitcoin, Ehtereum and Litecoin. And hence, this form of router can be easily implemented in smart homes along with fog computational environments and Bitcoin and Litecoin support Raspnode for e-wallet situations. Though mining can be done on IoT devices, it proves to be highly inefficient and hence, become a crucial challenge for AASIC chips and other hardware systems, the key reason for which IoT devices involve very little mining processes. Full nodes must have the efficiency to store all portions of the Blockchain for complete endorsement of transactions and other methods. However, the consensus protocol can be easily laid back to accommodate IoT devices, though it may have to compensate with the security of the implementation strategy. Consortium Blockchains tend to implement this technique and in the application of light weighted nodes, the originality of processes is legalized without the need to download Blockchain as a whole, and can thus, contribute to it, facilitating easier methods to continue and control the IoT devices. These nodes, can easily bridge the gap between two technological developments and needs to be complemented by full nodes for validation. However, majority of the Blockchains do not uplift light weighted nodes just like in the case of Ethereum, leading to under development. Even then, Blockchains can be used for services for external purposes and trustworthy storage techniques. The combination of IoT and cloud computation is one of the best integrations of Blockchain [31]. This technique has been used during the past few years to tackle the drawbacks of IoT in operations and functionalities, storage, and access. It is to be noticed that cloud computing indeed portrays a centralized form of system architecture, complicating loyal distribution with a plethora of users. The soulful combination between Blockchain and IoT aims towards handling and dealing with the past limitations along with the task of managing data in a reliable platform. Fog computation aspires to share and bring together end devices which follow a similar routine as that of Blockchain uniting a greater number of powerful gadgets than the sensors like gateways, edge nodes, etc. which may be useful for Blockchain instrumentation. Hence, we can prove that fog computation eases out the process of uniting IoT with Blockchain.

VII. Problem 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:

A. Heterogeneity

Internet of Things is a combination of various heterogonous devices, communication protocols, networks, etc. In that, some clouds are unable to interact with heterogeneous (different) modules or communication technologies. It enhances the complexity among various types of devices (via various communication technologies). It results in rude behaviour of network to be fraudulent, and delayed of end to end services. In [17], authors discussed the management of connected objects by facilitating through collaborative work among different things (hardware components/ software services) and managing them (after providing respective/ appropriate addressing mechanism, identification, and optimization at the architectural and protocol levels), but doing such things in Cloud based IoTs is a critical research issue. Hence, IoTs inconsistencies lead to security threats such as confidentiality, authentication, delays, etc.

B. Context awareness

When billions of sensor enabled things (or sensor are embedded in devices) are connected to the Internet (to make communication), it may not be feasible for the user group to handle all the data collected by the sensors. Context aware computing techniques need to be used to process the necessary data and filter out unnecessary data. This data may create several problems like data acquisition, data retrieval, data management and data storage. Context-awareness computing techniques need to be used in better way to help decide what data needs to be processed or analysed. Today's existing clouds have limited capability in terms of context awareness, is a main issue. In result, it results in ascertain the negation of information validation in form of continuous disrupted process.

C. 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 can say that Middleware (in IoTs architecture) covers the horizontal flow of data/ information among the devices, protocols, and applications. All applications can be used over the data-sets and queries can be solves on the internet connected devices (in a centralized manner).

D. IoT node Identity

Generally, IoTs network contain an incredibly high number of nodes. All the attached devices and data shall be retrievable. In such scenarios, the unique identity is a must for efficient 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 devices (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.

E. 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 designing IoT based cloud systems) 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.

F. Fault tolerance

Fault tolerance is another important design issue which directly affects quality. To make a system perfect (with high accuracy, efficiently), fault tolerance level of the system should be kept very high so that despite of technical error, the system keep working. 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.

G. 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., which may highly be populated, so that the unique identity would get difficult to be imposed upon 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.

VIII. Open Issues and Challenges in Internet of Everything (IoE) and Internet of Things (IoTs)

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. Data analysis (using appropriate tools) provides a significant contribution to IoTs. In order to exploit the full potential of data analysis for extracting new visions/ decisions from data, IoT must overcome some major challenges. These can be categorized into several types.

A. IoT Data Characteristics

Data is the basis of extracting knowledge, it is vital to have high quality information. It can affect the accuracy of knowledge extraction directly because IoT produces a high volume, fast velocity, and different varieties of data. So, preserving the data quality (all the time) is a challenging task here. Although several solutions have been proposed to solve this problem of data quality, but no one can handle all aspects of data characteristics in an accurate manner (due to distributed nature of big data management solutions and real-time processing platforms). 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 tend to enhance the abstraction of IoT data through annotation algorithms, while they require further effort to overcome its velocity and volume.

B. 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 security in the design and implementation or as physically, an infected network of IoT devices can lead to a failure.

C. Internet of Things (IoTs) Data Analytic Algorithms

As discussed in above discussion, IoTs are generating a lot of data which is called as 'Big Data'. This smart data require efficient analytic algorithms to make meaningful decisions from itself. This data consist 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 techniques 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 unlabelled data (with the concept of reward based learning) to assist IoTs 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, 46]. 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:

1) 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.
2) 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.
3) All neural network based algorithms require high volumes of data and time to reach accurate interpretations.

Hence, IoT is a global network infrastructure, links uniquely identified physical and virtual objects, things and devices through the exploitation of data capture, communication and actuation capabilities. To extract information from the data collected a variety of machine learning algorithms can be applied [18, 46]. 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 [34]:

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.

Hence, this section discusses several open issues and challenges related to IoE and IoT in detail. Now, next section will discuss challenges in integration of Blockchain and Internet of Things, and Blockchain and Internet of Everything.

IX. Challenges in Internet of Things - Blockchain and Internet of Everything - Blockchain Integration

Internet of Things, Internet of everything are accepted by many applications like healthcare, transportation, logistics, smart grid, automation, etc., to reduce complexity, i.e., complete complex task frequently (i.e., in minimum time). But, every technology comes with pros and cons. Similarly, these technologies also face several challenges (also these technologies are still in growing phase) in near future which are summarized in this work one by one, i.e., in sequence, in detail.

Internet of Things (IoTs) – Blockchain Integration

In order to identify some of the realistic issues pertaining to Blockchain adoption in IoT, we tried out an exemplary scenario of IoT-based chain supervision system. The user books a large amount of frozen food packets and also specifies a threshold temperature to be maintained for the food packet during its shipment process. Every time the specified temperature maintenance is deviated from, the customer is notified. This scenario is very well explained in the following figure 6.

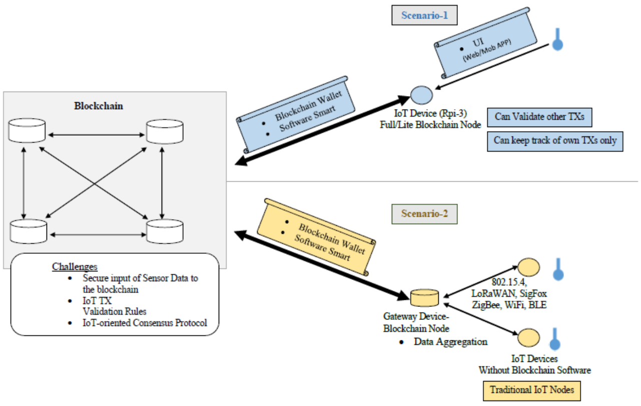

Figure 6: Challenges for a Blockchain-based Internet of Everything (IoE) System

a) Rpi-3 sensor node can be linked to the Blockchain directly, making it as a full node or a client as full nodes facilitate the validation of neighboring TXs, even though a lite client may keep an eye on its own TXs.
b) The temperature sensors help in sensing the surroundings and the values are extracted through a web User Interface or an application which are further linked to Blockchain nodes to force the sensor interpretations to the chain via smart services.

c) In the second scene, an Arduino device can also act as the IoT device which needs to detect and transmit the temperature readings to a gateway device nearby.
d) The sensor-node which is formulated from Arduino interacts with the gateway devices [47] using wireless means like 802.15.4, 802.11 (WLAN standards), LoRa, ZigBee, NB-IoT and SigFox. Moreover, this configuration further restricts the communication amid devices, as only the gateways devices have access to Blockchain or smart contracts.
e) Similar to the first scenario, gateways are also responsible for the connection of Geth node via web3 service provider and forces the details and collected information to the Blockchain system using a web or an application.
f) Nevertheless, there were a number of obstacles faced during this setup, the main one being – how to ensure a secure form of input of data collected from the sensors. Secondly, at present, none of the Blockchain platforms apply IoT-based TX authentication rules and related norms/ regulations. Finally, UI form the medium between the sensor node and the Blockchain, which is not capable of controlling cryptographic security, instead of which other web and security rules have to be implemented.

Moreover this, Few of the major challenges faced in IoT linked to Blockchain are discussed in [31, 40]. The major challenge observed in this field is that of availability of IoT focus protocols and regulations. TX/block authentication rules, consensus finalization, leverage too DoS attacks, etc. are some of the other inbuilt issues.

Internet of Everything – Blockchain Integration

This portion discusses about the major challenges which are to be addressed while applying Blockchain techniques in the field of IoT. However, the combination of IoT and Blockchain is not minor. A major portion of Blockchain transactions and processes are signed online, and hence, the devices functioning with currency have to be equipped with this paradigm. Note that IoE includes major challenges like IoT because IoE are combination of IoTs on a large scale/ for any application. A few of the challenges faced while incorporating IoE and Blockchain [31] are as follows:

1) *Storage Capacity and Scalability*

As mentioned, storage feasibility and scalability are still topics of discussion, but in the field of IoT, this limitation enhances the challenge. In this perspective, Blockchain appears to be completely unsuited for IoT application, though there are plenty of ways through which these issues can be eradicated. In IoT, this challenge poses a huge problem, as data is generated in large and bulk volumes. It is also found that a few of the existing Blockchain applications operate over a few processes per second alone, which can possibly be a potential bottleneck for the IoT. However, Blockchain was not designed to capacitate large data volumes formed in IoT and so; uniting all these techniques would definitely pose a long list of challenges. At present, though large amounts of data from IoT are stores, only some part of it is retrieved for the purpose of information and actions. A variety of techniques to screen, optimize and wrap up data from IoT have been put forward. IoT inclusive of embedded devices, interactions and services prove to be a support layer for multiple tiers. Data compression helps in easing out transmission of data, operation of tasks and storage of bulk amounts of data formed from IoT. Casual behaviors never necessitate extra details unlike ambiguous data. Finally, Blockchain along with its potential bottleneck, easily adapt to enhance the bandwidth and reduce the latency of the happening transaction, allowing better transformations to the field of IoT as put forth by Bitcoin-NG [48].

2) *Security*

Internets of Things (IoTs) applications are forced to handle security issues at various levels which are topped with sophistication because of reduced performance and high non-uniformity of gadgets used. Along with it, IoT also consists of a number of features which impact the security, like mobility wireless interactions or scale. An extensive comprehension of safety and security in IoT is way beyond the reach of this research, though you can refer [49, 50, 51, and 52] for more details. The growing attacks on IoT networks and frameworks followed by their drastic impacts, throws security issues under limelight. Many of the researchers today find Blockchain to resolve this issue in IoT. Though one of the challenges in the combination of IoT and Blockchain is the consistency of the stored data, Blockchain ensures that data is undisputable and can spot the transitions despite the corrupted nature of the arrived data. Corrupt IoT data arise from a number of situations, keeping aside those caused by the malicious issues. Wellbeing of IoT frameworks are impacted, apart from those caused by the harmful and the malicious ones. At times, the gadgets and the sensors themselves fail to function right from the start and this is not spotted unless and until the device has been screened. Apart from these, there are a number of threats which can adversely affect IoT like eavesdropping, DoS (Denial of Service) or management [50] due to which, IoT gadgets are required to be filtered thoroughly before their unification with Blockchain and are to be placed and concealed in the correct position to prevent physical junctures and for the detection of device failures. These devices can be hacked and cracked into easily as they restrict firmware updates which restrict them from actualizing over the plausible bugs or data breaches. Furthermore, updation of each individual device is a hectic task and hence, upgradation during run time and reapplication techniques is to be spaced in IoT to keep it running

Moreover this, GUITAR [53] and REMOWARE [54] permit architectures and updates during run time and processing are extremely important for assuring data consistency and integrity of IoT with Blockchain along with time, and they are prone to possess repercussions on IoT interaction. In the present-day scenario, CoAP and MQTT are security norms and regulations with implication to IoT for securing IoT interactions which are sophisticated and heavy along with the necessity of being centrally managed and controlled. In these networks, each device acquires its very own and unique GUID (Global Unique Identifier) and key pair which connect them to the network. This indeed helps simplifying the existing safety and security norms which has to transfer PKI (Public Key Infrastructure) certificates, allowing them to be made use of in devices with lower capabilities. Filament [55] is another highlighted project in aspects of Blockchain adoption. Filament, a hardware and software solution provides the availability of Bitcoin-based transactions and smart contracts in IoT. Filaments possess embedded crypto processors which complement 5 protocols: Blockname, Telehash and smart contracts to operate, and additionally Pennyback and Bittorrent protocols. Blockname, Telehash, etc. are used for identity management, assuring encrypted interactions, etc.

3) *Anonymity and Data Privacy*

Many IoT implementations handle highly confidential and top priority data just like when a person is connected to his/her device/personal digital assistant, it is of utmost necessity that privacy and security of data are taken care of. This is where Blockchain comes to the rescue, nevertheless just like in Bitcoin, there are quite a few implications which pursue anonymous identity gradation. The major issue in the parametric field with respect to IoT poses more of an issue as it involves data gathering and extends all the way to different application levels. Ensuring that the safely stored data is not easily retrieved by unwanted powers and users is another important challenge. Alternatives to all such issues must also consider the restrictions of sensors and the possible limitations in economic viability. Encryption is one of the major ways most of the techniques tackle their problem (IPsec, SSL/TLS, DTLS). Due to the limitations and hindrances they pose, the device makers are forced to use gateways and other light devices in order to instill the required security protocols and norms. Cryptographic hardware accentuates all types of cryptographic alternatives which may avoid the burdening of sophisticated and secure software norms. Another key feature in IoT combined with Blockchain is that of Trust and the authors of [56] have identified trust to be the epitome of success. Data consistency is another deciding alternative to ensure concurrent data access by keeping away over burdening of Blockchain with bulk volumes of data formed in IoT which may pave way for public systems which have the most efficient and constricted control powers. MuR-DPA [57] gives extensive data updates and the best authentication with the help of public auditing validation. The authors of [58] assure the data content via privacy preserving public auditing system. Refer [59] for in-depth details about the same. Finally, there are a few laws which are capable of regulating the privacy of data, like EU's data protection drives which are too looked into and altered to cover all new models as well. The merging of Blockchain into a legal platform must ensure privacy of data which follow the law.

4) *Smart Contracts (or Blockchain 2.0)*

They are the killer implementations of Blockchain technology in spite of the numerous challenges they pos. Practically, contracts as a collection of functions and details which are located in the particular Blockchain address and the publicly defined codes can be called by devices. To modify the mode of contract, the respective transactions are to be published in the network. These transactions are to be signed by the dispatchers if they are to be received by the network. IoT has the capability to detect and operate over the Internet in a large number of fields [31, 34 and 36]. Considering the example of tracing food, sensors are used for equipping food packages along with the additional task of measuring the surrounding conditions and to link to the Blockchain. A contract issues functions to commence the shipment, finish it and ensure the logging and the querying measurement process. If the measurements, cross a particular threshold, that event is likely to be fired. Management applications would be taking over these events while the shipping company, retailers, manufacturers and the customers would be informed. In the event of no such event appraisal, the Blockchain would guarantee the optimized shipment process of the food packages. Indeed, smart contracts provide trustworthy engine for IoT processing, recordings and managing the communications because of which actions tend to be the outcome of a synchronized processing technique. Hence, smart contracts replicate the conceptual scheme of IoT applications. Yet, the following obstacles and problems are to be faced in the process of integration. On one side, smart contract implies a pressing need of oracles for their efficient operations and authenticating these can be compensated for the stability of IoT. After all, trying to get hands on a number of data sources would over burden the contracts due to which they are shared and controlled in a decentralized manner though they're not capable enough to cater to a large number of computational processes. In fact, the perfect implementation of smart contracts requires just a single node while the execution is carried out by multiple nodes. This sharing of details has been done for the process of authentication alone. IoT has indeed leveraged the efficient capabilities of cloud computation and big data to enhance the power of computation. Since then, all methodologies lined to data mining have all information pertaining to IoT on the whole which mantled up a better insight of the IoT, i.e. the computational power enhanced by cloud processing. Big data has given access to bulk volumes of data concurrently, enabling the information to be retrieved from large datasheets, which used to be hard to accomplish initially. The combination of IoT and Blockchain along with that of smart contracts should boost up the shared nature in order to enable the computational powers put forth in other modules and are an essential part of IoT. Uniformity and restrictions which are a part of IoT are to be taken into consideration as well. Screening and indulging in group methods/principles are to be supported by smart contracts in order to allow applications and programs to address IoT based on the content and needs. Discovery mechanism would permit inclusion of many gadgets and devices, powering it up to the newer levels. Finally, actuation methodologies which are derived directly from smart contracts help in quicker responses with IoT.

5) *Legal Issues*

The motto of unfettered Blockchain is a part of its essence and is also responsible for the emerging growth of Bitcoin. Blockchain, as seen from the viewpoint of virtual money, has a lot of controversial issues tagged along with it. The pressing need or chance to put forth control parameters over the network came out in the form of private and enabled consortium Blockchains. IoT is also gravely impacted by the rules and norms of a country including those of data protection drives. A majority of these laws are being superseded and need to be looked into or modified, especially because of the introduction of novel catastrophic technologies like that of Blockchain. The introduction of new norms and rules can simplify the validation of the security characteristics of the gadgets and it helps in building the safest and reliable IoT network. In this perspective, all laws which handle security of data and information still face many obstacles and issues and the reduced maintenance of these throw up a number of limitations. A few of the IoT applications virtue a globalist and unique Blockchain for gadgets and devices, though it is not sure if this form of interlink aims towards being managed by the producers or its users. Nevertheless, it will definitely need authorized rules and norms. These norms have impacts on the future developments of Blockchain and are likely to disturb the free form of Blockchain by putting forth a focused user like a country.

6) Consensus

With respect to IoT applications, the restricted usage of resources implemented by the devices makes them highly unadoptable to various consensus mechanisms and propagations, like PoW. As mentioned, there are a plethora of proposals for the protocols though they generally do not undergo rough and tough screening. Resource requirements completely lay foundation on one type of protocol in the Blockchain network and these alternatives try to embed these tasks into gateways or other unrestricted devices. At times, off-chain alternatives, which tend to push data out of the Blockchain to decrease the high latency, can provide the sufficient latency. In spite of the startups to embed Blockchain full nodes into those of IoT gadgets [41, 42], mining continues to remain a key challenge because of the limitations it possesses. IoT consists of devices which have restrictions on their resource usability, but in the global outlook, IoT has a potential for humungous computational power considering the massive number of devices. Researches should mainly emphasize on this topic and power up the distributed feature and worldwide opportunity of IoT to adopt the IoT consensus. Proof of Understanding (PoU) which is a new protocol introduced in Babelchain [60] targets to ensure complete adaptation of PoW for the IoT applications. With reduced energy usage, it suggests the method of interpreting proposals from a variety of protocols. In this manner, the hard work tends to focus more on reliable and productive computation while spontaneously overcoming major challenges in IoT interactions. Colleagues in the network tend to decide upon message definitions and Blockchain data gives learning sets.

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 Everything (IoE) and Internet of Things (IoTs)

The cloud centric vision is to have Plug n'Play smart objects that can be deployed in any environment with an interoperable backbone allowing them to blend 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):

1) Architecture

Internet of Things-Architecture (IoT-A) [16] 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) [11] (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.

2) 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.

3) 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.

4) 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.

5) 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.

6) Participatory Sensing

People centric sensing is applicable only to resolve data ownership and privacy issues. People centric sensing cannot used for data collection as there will be inconsistencies and delays in sample gathering.

7) Data Mining

Deep learning is an emerging area in machine learning research to do analysis (for making decision for future), which aims to learn multiple layers of abstraction that can be used to interpret given data.

8) GIS based visualization

There is requirement of new visualization schemes for embedded heterogeneous sensors (in 3D landscape) in IoTs devices [34]. 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.

9) Cloud Computing

There is a need to support domain specific programming tools and seamless execution of applications across various networking platforms without comprising quality of service.

10) International activities

Several countries (jointly) are trying to implement these (IoTs) together to provide good and better life to their citizens. For example, in Europe, substantial effort is underway to consolidate the cross-domain activities of research groups and organizations, spanning Machine to Machine (M2M), WSN and RFID into a unified IoT framework. Also, countries like Japan, Korea, the USA and Australia are also increasing usage of IoTs devices in industry, their associated organizations and government departments (with various programs). This includes smart city initiatives, smart grid programs incorporating smart metering technologies and roll-out of high-speed broadband infrastructure. 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; intelligent transportation; smart logistics; smart home; environment and safety testing; industrial control and automation; health care; fine agriculture; finance and service; military defense.

11) Security Concerns

Security and privacy is one of the key issues in IoT or IoT based cloud services [7, 13, 31 and 34]. The implementation of IoT branches across a number of fields like industrial, enterprise, consumer, personal, etc. This type of data calls for high security and confidentiality against modulation and theft. For example, IoT is likely to store the details of the health condition and situation of a patient. Furthermore, it improves the interaction process amid gadgets despite of which there are a number of issues like portability, time for response, and so on. It is to be noted that security is always an issue when considering the data to be transmitted over the World Wide Web (WWW), especially while transmitting it across international borders, safety measures tend to be taken care of by the government organizations like Health Insurance Portability and Accountability (HIPA) act. A few of the common security problems faced by IoT systems are elucidated in figure 7. Amidst all the challenges posed, a few major hindrances in IoT [34] also acquire prime attention from the novel researchers including:

a) Data Privacy

Some producers of novel smart TV's gather data and information pertaining to their users to comprehend their visual habits in order to ensure that the gathered data may possess challenges for privacy of data during transmittance.

b) Data Security

This is another major task. During the transmittance of data enormously, it is very essential to mask it from being observed by other devices on the internet.

c) Insurance Concerns

The insurance firms and companies who embed IoT devices on vehicular systems are able to collect and gather data about health and driving status to assure precise decisions about insurance.

d) Lack of Common Standard

Because of the presence of many standardised levels for IoT devices and IoT manufacturing industries, it is a huge challenge to differentiate between allowed and non-allowed gadgets which are linked to the internet.

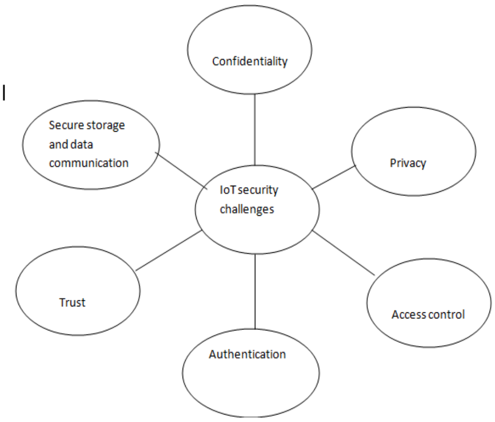

Figure 7: Internet of Things Security Challenges [22]

12) Technical Concerns

With increasing use of IoT gadgets, the created chaotic conditions are also rising. Hence, there's a pressing need to increase the capability and storage efficiency of the network.

a. IoT middleware: The challenges, which are addressed by any IoT middleware, are as follows:
   i. Interoperability and programming abstractions: Interoperability is of three types: network, semantic, and syntactic. Network interoperability deals with heterogeneous interface protocols for communication between devices. It protects various applications from complexities of different protocols. Semantic interoperability deals with abstracting the meaning of data within a particular domain. And Syntactic interoperability ensures that applications are oblivious of different formats, structures, and encoding of data.
   ii. Device discovery and management: The middleware provides Application Programming Interfaces (APIs), which are used to list the IoT devices, their services, and capabilities. Finally, any IoT middleware needs to perform load balancing, manage devices based on their levels of battery power, and report problems in devices to the users.
   iii. Scalability: The solution needs to be scalable because the devices in an IoT

network can increase. 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.

13) *Other challenges*

Note that an interconnection of highly heterogeneous networked entities (IoT devices), it follows a number of communication 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 appropriate interpretation and visualization of the large amounts of data, privacy to security, data retrieval to data management, etc. Further IoT based Cloud has challenges like privacy, participatory sensing, data analytics, Geographic Information System (GIS) based visualization, etc. Some other cloud computing challenges are: architecture, energy efficiency, security, protocols, and Quality of Service, Standardization of frequency bands and protocols. Hence, a systems need to overcome such challenges in near future. Further, strengthening or increasing of IoTs devices/ IoT's security is a major challenge. IoTs still an immature technology (not developed completely), a major issue affecting the acceptance and applicability of the Internet connected things is the lack of a mature and comprehensive security model and standards.

B. Analysis of Different Types of Attacks and Possible Solutions in Internet of Everything (IoE) and Internet of Things (IoTs)

Today's Internet connected things is facing various types of attacks like passive, and active attacks. In general, passive attack may easily disturb the functionality and abolish the benefits of its services. In this attack, a malicious user can sense the channel/ node and may steal the information, but note that it never attacks physically. 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 section discuss about different types of attack, nature/ behavior of attack and threat level of attacks. Different levels of attacks are categorized into four types (according to their behavior) and also propose several possible solutions to threats/ attacks in [24, 34], as Low-level attack (if an attacker tries to attack on a network and his attack is not successful), Medium-level attack (if an attacker/malicious user/ intruder is listening to the medium (as insider attack) but do not breach/ change the integrity of data), High-level attack (if an attack is done on a network and it alters the integrity/ modifies the data) and Extremely High-level attack (if an attacker attacks on a network by gaining unauthorized access (without owner's 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).

C. An Example: Smart Home Security Challenges in Future

Our investigation is presently looking into two advancements which are essential for a gateway-based Smart Home framework. The work is primarily in the elemental stage, so we put forward the issues and glitches as the stepping stone towards solving our problems:

1) *Auto-Configuration Support*

It is considered that with increasing smart home devices and gadgets, each of them is to be interlinked with each other. The absence of sufficient and required technical support and help is one of the greatest challenges in this field. House owners will be overloaded with herculean task and similar typed operations and functionalities for controlling these smart devices at home. Thus, for an effective application of Smart Homes, a safe and sound automated set up should be scrounged on to ease out the task and simultaneously augment the safety and security in this very process. Our approach calls for operations and procedural methodologies in cloud-based devices and services. On the introduction of a new device to an existing network, gateways make use of the ID unique to each device to query the web services and to attain more descriptive features of the device. This is a varied approach when compared to the usual autonomously configured perspectives with which, a tiny ID and web service data are sufficient for assuring the easy retrieval of data which remains updated regularly.

2) *Internet of Things (IoTs) Software and Firmware Updates*

Desktop operating systems are updated regularly and automatically as security vulnerabilities are identified and patched. Mobile devices such as smart phones also receive regular software updates, including mechanisms to verify the authenticity of the changes. Such systems are economically viable because the number of operating system variants and operating system manufacturers are small, and deployed devices are in the millions. No such regular update service is available for the hundreds of different IoT devices. An IoT device is a combination of hardware and software to perform specific, dedicated tasks. Firmware is a type of software that is programmed into the non-volatile memory of a smart device. It is an essential part of any IoT system since firmware is the program that directly interfaces with the hardware, controlling the system's operations and functions, from initializing the device, interfacing with users, processing of the requests and performing tasks. As a consequence, it is vital that smart device firmware is kept up-to-date to resolve security vulnerabilities, improve functionality, add new features and fix other bugs. Unlike the enterprise-scale environment which has its own dedicated IT department or technical team to manage and deploy the software updates, the Smart Home environment usually lacks technical support. The IoT devices for Smart Homes should have mechanisms to implement safe and secure firmware updates automatically, with little or no user intervention. Such functionality can be managed by the home gateway (see figure 8).

To promise consistency and validity of the updations and to thwart any type of mutations to an exposed firmware through malware injection, digital signatures should be compulsorily applied for all updates. Before any type of update, each and every one of the updates are to be strictly verified and cross checked with its corresponding digital signs, such that the digitalized certificates have to be verified to ensure that they're generated by loyal third-party authorities. The techniques used for the installation of updates call for serious thoughts. If the process of update verification is compromised on, in future it would pose a threat as hackers can easily hinder the novel updates from being downloaded and may attack or tamper the firmware. Intruders can easily replicate old version of firmware with safety liabilities as the recent version, leading to the firmware directing back to faulted versions. Hence, the device manufacturer should encode and sign the updates digitally along with the assurance that the information is not leaked to cybercriminals. Because of reduced bandwidth and restricted resource nature of smart gadgets, delta updations gravely enhance and reduce the time for installation. This would greatly reduce the probability of crashes during updates, especially for devices functioning on battery charge during the upgradation of firmware.

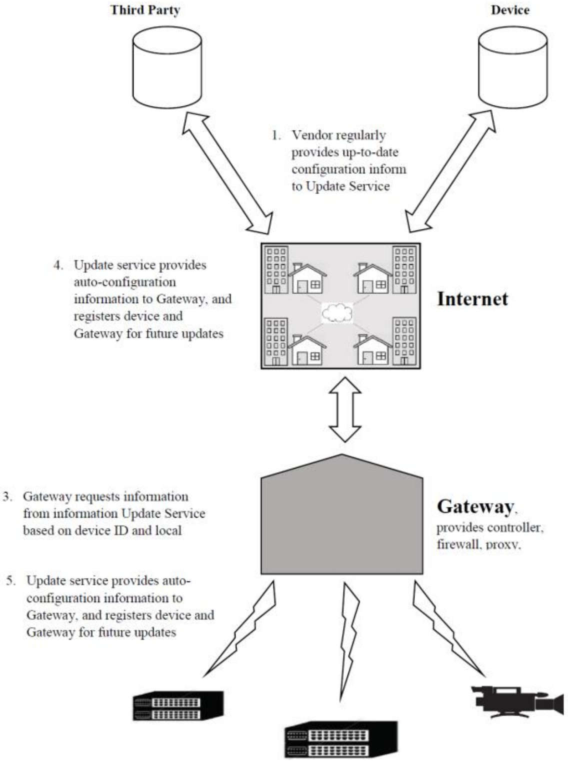
Third Party
Device
1. Vendor regularly provides up-to-date configuration inform to Update Service
4. Update service provides auto-configuration information to Gateway, and registers device and Gateway for future updates
Internet
3. Gateway requests information from information Update Service based on device ID and local
Gateway, provides controller, firewall, proxy,
5. Update service provides auto-configuration information to Gateway, and registers device and Gateway for future updates

Figure 8: Smart Manufacturing: Auto Configuration Architecture of Internet of Things Based Applications

Attacks: The different forms of harmful node attacks which pertain to IoT positioning can be summed up as:

- Conflicting behaviour attack: The loyal nodes transmit trustworthy details and information along with those of partially incorrect information.
- On-off attack: A single dangerous node is capable of transmission of flawed location related details and data at regular intervals.
- Sybil attack: It is a set of malevolent nodes which use more than two IP addresses so that they can resist and mask their original identity [61].
- Newcomer attack: A node which was earlier defined as malevolent can modify/alter its' IP address and re-enter the network architecture with a new face

Pre-Processing: Since smart devices are capable of gathering bulk and voluminous amounts of data, processing and storage which are highly efficient need to be used for comprehension and computation of the collected data. The most frequent resources used for processing and storage of resources are linked to that of Cloud because of the huge data handling, flexibility and scalability it offers (refer figure 9). But this is definitely not sufficient enough to fulfill the needs and requirements of a majority of the IoT implementations because of the below reasons:

- Mobility: A lot of smart devices are easily portable and mobile. The constantly varying locations make it a tedious task to interact with the cloud base due to the varying network at different spots and positions.
- Reliable and real time actuation: Interaction with the cloud base and receiving timely responses along with potentially sensitive applications, which require real time feed backs, are not fit for this model. Furthermore, there are chances of data losses due to wireless links, transforming data into its' unintegrated form.
- Scalability: Increasing devices imply growing cloud requests which further increases its' latency.
- Power constraints: Interchange of data makes use of huge amounts of power, especially when they're run on battery and hence, IoT devices cannot interact continuously all the time.

To tackle the issue of portability, researchers have put forward Mobile Cloud Computing (MCC) [62]. Yet, there are a number of issues clinging to it as well with respect to potential and power. A solution to all these issues can be formulated by considering some of the computational and storage resources rather than completely depending on every bit of processing on cloud and this concept is Fog Computation [63]. Fog, in simpler terms, also refers to cloud, but is more closely linked to the ground. Data and other information can be stored, computed, screened etc. before forwarding it to the cloud. Fog and cloud, together forms a unique combination which goes very well with each other because of its' complementary nature. Smart gateways can also be deployed for fog computation [31, 63]. A number of characteristics pertaining to fog computation have been illustrated by Rekha et al. in [63]. The functions of a smart gateway include gathering data from sensors, pre-computation, screening the data, storage and networking the respective services to the gadgets, interaction with the cloud, and so on. Some applications of fog computing are as follows [63]:

- Smart vehicular networks: Smart traffic lights are used in the form of smart gateways to spot the people and vehicular movement through sensors, measuring their speed and distance travelled, and also to infer the traffic status of a particular location and this proves to be an efficient method to warn the vehicles whizzing past by. These sensors also interact with the near by traffic signals for maintaining a regulated management of traffic. For example, if the sensors spot an ambulance nearing, they can easily swap their traffic lights to permit the swifter movement of the ambulance and will also circulate the information among other traffic lights.
- Smart grid: It helps in maintaining the balance of energy based on its usage and accessibility. This is carried out to ensure an autonomous process of switching to other energy sources which are conventional and reusable and this can be acquired with the help of smart meters or microgrids which are linked by gateways. The gateways are smart enough to comprehend and analyse the information and are capable of portraying energy requirements of the future, compute the availability and the cost of power, and supply them accordingly.

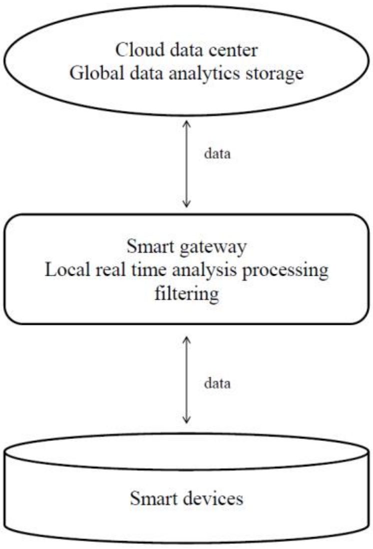
Cloud data center
Global data analytics storage
data
Smart gateway
Local real time analysis processing filtering
data
Smart devices

Figure 9: Smart Gateway for Pre-Processing

Note that IoT is an umbrella term that includes multiple different categories like Wireless sensor/actuator networks, Internet-connected wearables, Low power embedded systems, RFID enabled tracking, Use of mobile phones to interact with the real world (e.g. sensing), Devices that connect via Bluetooth-enabled mobile phones to the Internet, Smart homes, and Connected cars, etc.

X. Future Research Directions in Internet of Everything (IoE) and Internet of Things (IoTs) - Related to Security, Privacy and Trust

For 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 consist 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 (and healthcare) IoT play vital role in information management [25, 64], 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 [26, 40]. 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 community 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:

- The fortification of privacy in IoT is currently novel and has not been studied or portrayed in any of the present-day researches. Therefore, constructing light weighted and safe privacy-preserving methods and principles is an eye-opening topic for future researches.
- In the coming years, we would require “futuristic IDM systems” to be created and made use of in IoT gadgets and hence, M2M (machine to machine) validation processes amid these gadgets which use the Idemix system would turn out to be another upcoming project.
- Intrusions are similar to attacks or invalid tasks which are implemented by outsiders in a network. On the basis of the attackers’ efficiency, the attacks may be either passive (i.e., eavesdropping of information during communication) or active (i.e., malicious packet injection and packet dropping). An Intrusion Detection System (IDS) is a device which is capable of spotting any mishappening in the network. Once an IoT device has been spotted out to be malevolent, we need to spot and locate the identity of the corresponding gadget to prevent further destruction of the system. But due to the resource limited nature of the gadgets, the IDS created needs to be light weighted.
- IoT impacts a number of interlinked sensors, i.e., with a Wireless Body Area Network (WBAN) which can give different opportunities to manage and supervise the health conditions of a patient in real-time [27]. In the future, IoT is likely to play a considerable part in the new-generation healthcare delivery [7, 27]. IoT interlinks and brings together medical supervision gadgets integrated with cloud bases through mobiles and other electronic devices. Since the data pertaining to patients are private and need to handle with utmost care, the data collected should not be leaked to invalid users. So, we need to preserve the patients’ information by powering new light weighted and safe gadgets for Device-To-Device (D2D) communications.

In recent years, already a lot of work, policies have been proposed/ implemented to secure critical IoT applications. Several attempts have made to develop IP-compatible secure communications networks, which are useful for resource-constrained devices (using security techniques). In that, some techniques require careful, unified, system-wide design, and experienced network engineers to design and maintain a secure and privacy- preserved cloud based IoT system.

Table 1: Different Internet of Things (IoTs) Applications and its Challenges

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, livestock 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

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. Security Goals

With building trust, and preserving privacy (in this smart era) of citizen/ people, we need to design a lightweight cryptographic framework for IoT (with considering critical constraints of hardware resources). It is can be achieved by proposing cryptographic primitives that need to be revisited and designed considering the constraints of IoT devices. We need to provide following security measures in IoT, i.e., Secure Routing and Forwarding in IoT, Robustness and Resilience Management, Denial of Service and Insider Attack Detection in IoT, etc.

B. 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 mainly depends on the physical and commutation privacy and security. Sensitive and intricate data and details have chances of being leaked in the case of device robbery and restriction to adjacent channel attacks.
- Privacy during communication: This completely depends on the accessibility of a gadget, along with device consistency and loyalty. IoT gadgets must interact only when required, in order to derogate the exposure of data during interactions.
- Privacy in storage: It is to preserve the safety and privacy of information kept in gadgets, and the following things are to be considered: Plausible volume of details and regulations must be relaxed to deliver the shield of client data after end-of-device life.
- Privacy in processing: It completely depends on the gadget and interaction consistency. Data has to be exposed or preserved from other third parties without the acquaintance of the data owner.
- Identity privacy: It is the uniqueness of any particular device which needs to be recovered by authorised instances alone.
- Location Privacy: It involves the geographical location of the respective devices which can be foreseen by authorised instances [28].

Today's Internet of Thing has become an integral part in various applications like remote patient monitoring, energy consumption control, traffic control, and smart parking system. In above discussed applications, we need to protect personal information of users/ patients, i.e., their movement, habits, and interactions with other people. In summary, we need to provide such goal in near future (in every framework): Avoiding Profiling and Tracking, Mitigating Localization and Tracking, and Securing Data Transmission.

C. Trust Goals

Trust plays an important role in various fields/ applications/ businesses, and so does it in this perspective as well. Sufficient and highly operative intellectual property safety and execution are necessary parts to policy architectures which continue to enhance the innovation and mind sets of IoE and this accompanies trust and its characteristics to a great extent [65]. When considering the role of IoE along with that of Digital Ecosystems program, it mainly aims towards supporting and uplifting all stakeholders to monetize the creative services online which are to be delivered all through a system of participants by integrating and managing these systems. This indeed creates trust among the partners as well as in the whole surrounding.

D. Limitations: Internet of Everything and Internet of Things

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 other limitations can be included here as:

- Large-Scale Streaming Data: A large number of data capturing devices are distributed and deployed for IoT applications, and generate large amount/ a lot of data continuously [29]. This leads to a huge volume 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: In most of IoT applications sensor devices are attached to a specific location, and thus have a location and time-stamp for each of the data items.
- High noise data: Due to tiny (small) pieces of data in IoT applications, much data (of these devices) may be subject to errors and noise during acquisition and transmission.

Although obtaining hidden knowledge and information out of big data is promising to enhance the quality of our lives, it is not an easy and straightforward task. For such a complex and challenging task that goes beyond the capabilities of the traditional inference and learning approaches, new technologies, algorithms, and infrastructures are needed [29, 34]. 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.

XI. 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.

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 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. Pe ña-L ópez, 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, 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 (March 11, 2019). Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE) 2019.

[8] R.Minerva, A.Biru, D.Rotondi'Towards a definition of the Internet of things,' IEEE, Issue 1, 13th 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, Pages 1645-1660, September 2013.

[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, 2009.

[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. 51 921–960 (2007).

[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, Pages 35-46, December 2016.

[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), 18(2): 474, Feb2018.

[19] European Lighthouse Integrated Project - 7th Framework, Internet of Things - Architecture. (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, 209–229, (2010).

[21] S. Misra et al., Security Challenges and Approaches in Internet of Things, Springer Briefs in Electrical and Computer Engineering, 2017

[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, 146–164.

[23] Luis Filipe, Florentino Fdez-Riverola, Nuno Costa, Ant ónio Pereira, Wireless Body Area Networks for Healthcare Applications: Protocol Stack Review, 2015.

[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.

[26] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System (2008).

[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.

[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, 2019.

[30] Sravanthi Reddy, Kavita Agarwal and Amit Kumar Tyagi, "Beyond Things: A Systematic Study of Internet of Everything", Internet of Things, 16-18, in Proceeding of Springer/ 8th World Congress on Information and Communication Technologies, GIET University, Odisha, India, December 2019 .

[31] Reyna, Ana & Mart ń, Cristian & Chen, Jaime & Soler, Enrique & D áz, Manuel. On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems (2018).

[32] Amit Kumar Tyagi, "Cyber Physical Systems: Analysis, Challenges and Possible Solutions", IJICIC, 2020 (in press).

[33] Bui, K. N., Jung, J. J., & Camacho, D. (2018). Consensual Negotiation-Based Decision Making for Connected Appliances in Smart Home Management Systems. Sensors (Basel, Switzerland), 18(7), 2206.

[34] Tyagi, Amit & Rekha, Gillala & Sreenath, N.. Beyond the Hype: Internet of Things Concepts, Security and Privacy Concerns (2020).

[35] https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

[36] 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.

[37] TanweerAlam, "A Reliable Communication Framework and Its Use in Internet of Things (IoT)", IJSRCSEIT, 2018.

[38] https://cdn.iccwbo.org/content/uploads/sites/3/2016/10/ICC-Policy-Primer-on-the-Internet-of-Everything.pdf

[39] M.Mazhar Rathore, Awais Ahamed et.al "Urban planning and building smart cities based on the Internet of Things using Big Data analytics", Elsevier, 2016.

[40] Amit Kumar Tyagi, "Decentralized Everything: A Practical Use of Blockchain Technology in Future Applications", Journal of Information Assurance and Security (JIAS), Vol X, 2020.

[41] Ethembedded, 2017.

[42] Raspnode, 2017.

[43] Trusted IoT Alliance, 2017.

[44] Ant Router R1-LTC The WiFi router that mines Litecoin, 2017. Available online: https://shop.bitmain.com/antrouter_r1_ltc_wireless_router_and_asic_litecoin_miner.htm.

[45] Ethraspbian, 2017

[46] Tyagi, Amit Kumar and G, Rekha, Machine Learning with Big Data (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.

[47] Finnegan, Joseph & Brown, Stephen. A Comparative Survey of LPWA Networking (2018).

[48] I. Eyal, A.E. Gencer, E.G. Sirer, R. Van Renesse, Bitcoin-NG: a scalable blockchain protocol, in: 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, pp. 45–59, 2016 .

[49] R. Roman, J. Lopez, M. Mambo, Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges, Future Gener. Comput. Syst. 78 680–698, (2018).

[50] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) 2266 – 2279(2013).

[51] J. Lopez, R. Rios, F. Bao, G. Wang, Evolving privacy: from sensors to the internet of things, Future Gener. Comput. Syst. 75 (2017) 46–57.

[52] M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future to internet of things security: a position paper, Digital Commun. Netw. (2017).

[53] P. Ruckebusch, E. De Poorter, C. Fortuna, I. Moerman, Gitar: generic extension for internet-of-things architectures enabling dynamic updates of network and application modules, Ad Hoc Networks 36 127–151(2016).

[54] A. Taherkordi, F. Loiret, R. Rouvoy, F. Eliassen, Optimizing sensor network reprogramming via in situ reconfigurable components, ACM Transactions on Sensor Networks (TOSN) 9 (2) (2013) .

[55] Filament, 2017.

[56] C. Fernandez-Gago, F. Moyano, J. Lopez, Modelling trust dynamics in the internet of things, Inform. Sci. 396 72–82 (2017).

[57] C. Liu, R. Ranjan, C. Yang, X. Zhang, L. Wang, J. Chen, Mur-dpa: top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud, IEEE Trans. Comput. 64 (9) 2609–2622 (2015).

[58] C. Wang, Q. Wang, K. Ren, W. Lou, Privacy-preserving public auditing for data storage security in cloud computing, in: INFOCOM, 2010 Proceedings IEEE, San Diego, California, USA, IEEE, pp. 1–9, 2010.

[59] C. Liu, C. Yang, X. Zhang, J. Chen, External integrity verification for outsourced big data in cloud and IoT: a big picture, Future Gener. Comput. Syst. 49, 58–67 (2015).

[60] Bitcoin Fog, 2016. Available online: http://www.the-blockchain.com/2016/05/01/babelchain-machine-communication-proof-understanding-new-paper/.(Accessed 1 February 2018).

[61] Tyagi, Amit & Sreenath, N. Preserving Location Privacy in Location Based Services against Sybil Attacks. International Journal of Security and Its Applications. 9. 175-196(2015).

[62] Shanklin, Mitchell , ‘ Mobile Cloud Computing’ , 2011.

[63] Rekha, Gillala & Tyagi, Amit & Anuradha, Nandula. Integration of Fog Computing and Internet of Things: An Useful Overview. 10.1007/978-3-030-29407-6_8, (2020)..

[64] M. Shamila, K. Vinuthna and T. Amit Kumar. “A Review on Several Critical Issues and Challenges in IoT based e-Healthcare System. International Conference on Intelligent Computing and Control Systems [ICICCS 2019], IEEE, 2019.

[65] Dave Evans, "The Internet of Everything: How More Relevant and Valuable Connections Will Change the World," Cisco Internet Business Solutions Group (TBSG), Cisco Systems, Inc., San Jose, CA, USA, White Paper 2012.

[66] Bruno Tavares, Filipe Figueiredo Correia, and Andre Restivo, A survey on Blockchain technologies and research, Journal of Information Assurance and Security, (JIAS), ISSN 1554-1010 Volume 14 pp. 118-128(2019).

[67] Jo˜ao Pedro Dias, Angelo Martins, and Hugo Sereno Ferreira,A Blockchain-based Approach for Access Control in eHealth Scenarios, Journal of Information Assurance and Security (JIAS). ISSN 1554-1010 Volume 13 pp. 125-136 (2018).

[68] T.Kavitha and D.Sridharan, Security Vulnerabilities in wireless sensor networks : A survey, Journal of Information Assurance and Security (JIAS), Vol.5 2010.

Author’s Biographies

First Author: 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.

Second Author: Meghna Manoj Nair is a student currently pursuing B.Tech course in Computer Science and Engineering at VIT Chennai. Venturing into completely different aspects in the field of Computer Science and following a plethora of other incorporations with respect to Artificial Intelligence, Machine Learning, Blockchain, Robotics, etc. which glamorizes and enhances the existing developments is one of the things She is passionate about. She has also had golden opportunities to share her bit of work to some of the trending research topics which include Cyber Physical Systems, Blockchain, Deep Learning etc. under the guidance of Dr. Amit Kumar Tyagi.