Certain Investigation on the Challenges and Prospects of Internet of Things (IoT)

Vignesh V, Arokia Mary Celsia J, Indumathy N and Harida A
1,2,3,4Department of CSE
1,2,3,4KPR Institute of Engineering and Technology
vignesh.v@kpriet.ac.in

Abstract - IoT means Internet of Things. The Internet of Things is more than a catchphrase; IoT means a classification that is impact how humans interact with equipment, and how human beings deport yourself. The meaning of IoT means linking systems and devices that, until now, haven't been connected. In general, IoT is also referred as digital intelligence or dumb things. Let us consider an example, an owner of a house lock or unlock their door from a phone through a smart home security system using IoT, and they can adjust their home temperature or operate a security camera to see who is knocking at their door. Based on IoT, business applications were developed. Smart cars are based on the concepts of IoT, traffic has been controlled and adjust and also it is informed to humans regarding the fastest and shortest route. Rapid changes in the interaction between human and the machine.

1. Introduction

“The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.” Information can be transmitted and received when something is connected to the internet. User has the ability to send and receive the information in a smart manner [1]. IoT is a simple mode of connectivity which means connecting all the places and things in the real world connecting them through internet [2].

Smartphones is an example to listen any song in the world, due to unavailability of song available in the regular phone. Data is stored somewhere in the world, so the user can transit any sorts of data to and from the devices. There is no need of super storage or super computer because data can be access anywhere in the world by means of IoT [3]. In the Internet of Things are connected based on the following three categories,

1. Information about the things is shared between sender.
2. Information related on things are received between receiver.
3. Both category of operations performed on things.

The above said three categories has more benefits that compound on each other [4]. IoT applications will bring more value into one’s lives. Internet of Things takes more importance than wireless networks, superior sensors and revolutionary computing capabilities, in sharing of data its networks never arrive pre-assembled, they only grow over time [5]. The Internet of Things (IoT) has hardware and software to the internet to create a smarter and new world. It has been growing at a significant way in the world and also, it offers a multitude of opportunities for government and business. The flow of paper is conferred in Section 2 gains about IoT applications, and its challenges and the work related to it is binded together. Finally, the paper about the completion of work is elaborated in section 3.

2. Research Issues, Challenges and Applications of Internet of Things

To stunned the difficulties and contests in recognizing IoT applications many researchers and early buds have come up with an auspicious solution. The prospective of the application of IoT is to establish the success of bids and their functionality there must be proper feasibility into different domains [6]. It is used to sort out the challenges and implications of the research, IoT technology is adopted to meet it out. In this section, for the future use of IoT, the key challenges and its highlight is briefly explained. One of the fundamental underlining technologies for IoT is considered Wireless Sensors Networks (WSN).

Network Challenges

Diversity and scalability: In IoT under the same umbrella, the infrastructures and surplus devices are combined together. The architecture, protocol stack, and format of data is operated by each and every system by means of an object. The interoperability challenges in integration are very much complex for large-scale IoT ecosystems. These challenges support dynamic interconnectivity and found decentralized in nature, the communications needed to be adaptive between these heterogeneous devices. The internet is connected by trillions of objects.

Distributed Naming Service (DINAS) is a proficient service discovery protocol for WSN [7]. It is classified into three categories: i) Fabricating Bloom filters ii) Naming of Network address and advertisement queries iii) Storing of cache information. It performs the solutions are centralized. Data is secure in IoT network by means of Secure DNS Name Auto-configuration (SDNSNA). Domain names are automatically assigned for IPv6 and converting the IoT system into a DNS system. Authentication process supported the solution of security functionality [8]. The
smart IoT gateway is incorporated and operated under inter-portability and the heterogeneous objects are interconnected between [9] them. Ethernet, Bluetooth, Zigbee, Wi-Fi communication technologies enables data connectivity in IoT. Flexible type of protocol is used to receive data from different objects in a uniform manner. IoT devices uses insubstantial and finest protocol which equipped with limited resources to deliver the information and also supports and analysing the storage of local data.

Requirement of Energy Efficiency

Energy is consumed by powerful batteries in IoT devices in IoT paradigm. Self-sustainable wireless communication will soon be enabled with the help of IoT technology. Energy properties from various sources is very difficult and hard to understand the system. It gives high impact and hard to understand the energy harvesting adaptive algorithms. Energy resources such as Wind-solar, thermal energy, kinetic energy, hydroelectric harvesting is some of the very important resources to consumed energy in the system.

A centralized traffic-aware scheduling algorithm (TASA) has been introduced recently [10] to set up the Time Synchronized Channel Hopping (TSCH) is based on the traffic load and network topological structure is devised with the help of IoT. Low-power, and Lossy networks (LLN). Self-Organizing and Adaptive Dynamic Clustering (SOADC) is a solution [11] related to load of traffic available in the channel hopping traffic aware scheduling algorithm. It is used to maintain mobile data collectors-relay networks. Based on Service Zones (SZs), it divides the network into sub-groups. A greedy cluster formation algorithm was introduced [12]. It will create clusters and calculates the diameters of clusters in the network. The life time of network is enhanced by reducing the number of cluster diameters and delay of the network and also multihop is deployed through multiple sinks. High energy efficiency is achieved by means of Low power CoAP [13] in the network subsystem. By managing of power of the network removes the complexity for the application layer in the computer network. A cross-layer protocol is used to consumed the energy and increase in value of throughput and high QoS for Mobile WSN (MWSN). Two major concepts were incorporated in the IoT system 1) Broadcast packets were minimized to nearby nodes 2) Transmission power of the network is controlled and also depends on the closer distance between mobile nodes with all other nodes. In overall the system reduces time delay and packet delay and increase in packet delivery ratio [14].

Security Challenges

Safekeeping and concealment play a major role in IoT networks. It is very important to ensure privacy protection and security in various activities [15]. All devices which build through IOT contain sensors to transfer data. These are actuators that physically control the device. IoT uses IoT OS-firmware, IoT applications and WiFi communication, which enables the data to be sent and received via the internet router to the internet. The above components can be easily attacked by the hackers. Hackers can easily choose the above components to introduce malware and to compromise the system [16]. The steps and procedures to prevent the above attacks are 1. Scan and take over 2. Distributed DOS (Denial of Service) 3. Spam Attacks 4. Injection Attacks 5. Message interception using spyware and so on.

The vulnerabilities in the IOT application are recognised and reduced is ensured in the network. The IoT system is working properly is well monitored constantly. The methods used for prevention and monitoring is: 1. IoT application device updates are well managed and installed 2. Communication in secure way 3. Monitor and detect 4. Authentication and authorization 5. Data integrity and so on.

To conclude, these security challenges must be managed, monitored and avoided.

Fault Tolerance

Fault tolerance is the major problem area of Wireless Sensor network and Internet of Things. These technologies involve multiple heterogeneous sensor nodes [17]. These nodes spread over a large geographic area to perform a specific task. Networks increases its reliability and performance based on the growth of connected devices is increased. Failures in sensor nodes may cause due to Environment interference, physical damage, or lack of power [18]. This failure should not affect the overall task of the sensor network. This problem is overcome by means of new protocol of WSN and IoT. When a sensor node cannot receive messages from neighbour nodes for a specific period of time, then the sensor node becomes failure and the routing path identify exclusively [19]. When two or more sensor nodes fail in the same area, the problem becomes more complex. The network will get collapse because other set of nodes identify a route to the final destination might not work properly. The data collected by other devices is delivered to the intended destination by means of appropriate routing protocol in dynamic manner [20]. Fault tolerant sensor network identify the redundancy in multi-level of communication system.

Consuming of Energy, very less time delay, high order throughput, quality of connection is varied limited are the policies to route in the network. The algorithm Expected transmission count (ETX) is achieved up to two times better than minimal hop-count in terms of high throughput [21]. Throughput paths on multihop wireless communication is very high for data transmission and also minimizes the expected total number of transmissions of packet in the network. Balanced energy adaptive routing (BEAR) is a new routing technique for IoT networks [22]. BEAR operates in three phases: 1. Sharing of information 2. Neighbour nodes were selected and facilitated by the
successor nodes based on identifying the location of nodes referred as BEAR protocol 3. Transmission of information. The current request response model improves the exchange of data between peer-to-peer systems in a IoT based application by means of Context-aware routing (CAR) [23]. This methodology reduces total wasted time during transmission in network delay and improved the services of network and its bandwidth.

**Challenges faced during Software Development**

Some other important challenges in IoT networks are ‘5V’ (volume, velocity, value, variety, and veracity). The size of the data found is doubled when the challenges incorporated while developing the software. It is expected that it will reach 44 Zetta bytes in the next four years [24]. It is difficult to analyse, process, and store the ‘5V’ of data through traditional technologies. Usage of vast amount of data implements the intelligent algorithms which used to minimize the problems. A IoT Big Data Analysis (IBDA) is a new framework which is introduced in [25]. The sensor and the big data integration accumulate the 5V of information in the IoT field [26]. Hadoop is incorporated in the proposed system to build the system in real environment and spark over Hadoop applications used for data processing which results the proposed system is more efficient and scalable [27].

**Innovative and Multifarious Addictions Challenges**

Human in the loop systems is one of the important issues in real life [28]. In recent years, IoT applications increase rapidly in number and become more advanced. Humans use many of these smart applications. Belongings and individuals will operate synergistically [29]. The latest opportunities introduced in the IoT system were Healthcare, price of the devices with low cost, carriage, etc. Certain works have been considered previously regarding the repeated operation towards humans in IoT applications [30]. However, the IoT resolve any problem occurred between the administrator of the system is intervened for an emergency situation or anything abnormal conditions.

3. **Conclusion**

Different kinds of approaches of IoT are attained by means of energy, scalability, security and its privacy, big data. The things are interconnected to internet with various kinds of applications like sensors, actuators, and other embedded systems. This technology creates more effort on the quality, different lifestyles in our daily life, and the way of behaviour and interaction with the system. Therefore, large-scale devices provide new research challenges and problems. This paper provides a synopsis of the concerns and dares related to its services.

**References**


