Juni Khyat
(UGC Care Group I Listed Journal)
ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

THE FUTURE OF THE INTERNET OF THINGS

[#1]P.SATYAPRASAD, B. Tech Student, Dept of Civil Engineering,

[#2]V.VIJAY KUMAR, B. Tech Student, Dept of CSE,

SREENIDHI INSTITUTE OF SCIENCE AND TECHNOLOGY,HYD,TS.

ABSTRACT: With the Internet of Things (IOT) gradually evolving as the subsequent phase of the evolution of the Internet, it becomes crucial to recognize the various potential domains for application of IOT, and the research challenges that are associated with these applications. Ranging from smart cities, to health care, smart agriculture, logistics and retail, to even smart living and smart environments IOT is expected to infiltrate into virtually all aspects of daily life. Even though the current IOT enabling technologies have greatly improved in the recent years, there are still numerous problems that require attention. Since the IOT concept ensues from heterogeneous technologies, many research challenges are bound to arise. The fact that IOT is so expansive and affects practically all areas of our lives, makes it a significant research topic for studies in various related fields such as information technology and computer science. Thus, IOT is paving the way for new dimensions of research to be carried out. This paper presents the recent development of IOT technologies and discusses future applications and research challenges.

Keywords—*Internet of Things; IOT applications; IOT challenges; future technologies; smart cities; smart environment; smart agriculture; smart living.*

---

1. INTRODUCTION

Digital world revolutionizes our life styles by incorporating the things and the internet in a more organized and disciplined way. This merger had a great impact on our economy, governance, and industry in terms of efficiently utilizing the resources as well their better organization. One of the main ideas that play a big part in the revolution of the digital world is Internet of things. It was first coined by British Scientist kavin Ashton in 1999 when he was working on item identification with RFID tags in supply chain management in which all operation performed without the involvement of humans. After that many developments have been made in the IOT and it becomes an emerging field for future. By 2020 this technology will become leading technology around the world. In authors predict that by the end of 2020 nearly 212 billion smart objects being deployed in the market. Further machine to machine traffic flow will show enamours increase in the market by 45% till 2020. It will greatly impact on the economic growth in almost all fields of life. Fig depicts the projected market share of different IOT applications domains.

IOT is the combination of two words: The Internet and things. The Internet means connectivity, a thing cover not only electronic devices but also includes living things (animals, human, birds and etc.) and non-living things (clothes, food and etc.) and the word “of” connect these two words to form an IOT. Further IOT gives the concept of ubiquity.

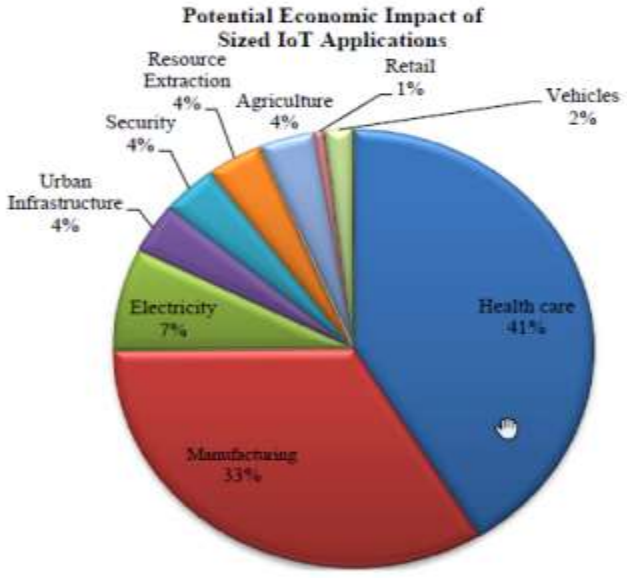

Fig. Projected Market share of different IOT applications domains

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

Due to its diversification, it is important to know what IOT is, defines IOT as "An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data, and resources, reacting and acting in face of situations and changes in the environment"

IOT is a connection of objects that behave intelligently with the situation. Simple objects will become smart in IOT. To fulfil this dream there are some requirements of IOT which are: Dynamic Resource Demand, Real Time Needs, Exponential Growth of Demands, Availability of Application, Data Protection, and Users Privacy, Efficient Power Management, Access to an Open and Inter Operable System and execution of Application Near to end User. These requirements will be managed by the corporation of different technologies like: Radio frequency Identification (RFID), Internet Protocol (IP), Electronic product code, Bar code, Wireless fidelity (Wi-Fi), Near field communication (NFC), Actuators, Wireless sensor network (WSN) and Artificial Intelligence (AI). Further IOT has some aliases like Cyber Physical Systems, Pervasive Computing, Ubiquitous Computing, Machine to Machine Interaction, Human Computer Interaction and Artificial Intelligence.

IOT is expanding its application domain over the globe and covering the different fields like logistics and transportation, Healthcare, smart environments, personal and social, agriculture and schools. In transportation, it includes assisted driving, mobile ticketing and environmental monitoring augmented maps. When we talk about health it includes tracking of patients, identification and authentication, data collection, and sensing. Personal and social aspect covers following applications domain: social networking, Historical queries, losses, and thefts. Figure describes the application domain of IOT Applications.

For example, a car equipped with IOT technology will not only assist the drivers by providing the facility of maps i.e. giving directions and suggesting best routes to reach the destination. Further, it also connects the driver with traffic management system of the city and more importantly informs the driver about the condition of the car by in cooperating with the sensors present in the engine and gives the real-time data to the driver. Apart from that, it will also connect to the manufacturer for feedback about different parts of the car. In that way, it will not only help the driver but also the manufacturer to manufacture the best products. When a fault occurs in any part of the car, information not only distributed to the driver but also to the manufacturer. It will also assist the driver to reach the nearest maintenance shop intelligently and perform the following task automatically: taking an appointment to that shop, checking the availability of worker as well as defected part (in the case of replacement identified by the system). Further, it will also notify other users of that defected part for necessary actions well before time for safe driving. This is the one way the internet of things improves the human life. There are many other scenarios and projects which lead us safe and comfortable life just because of IOT paradigm.

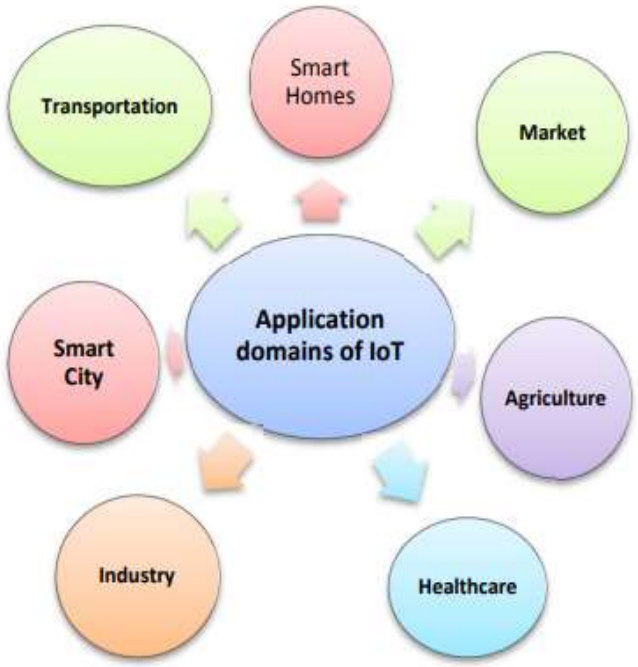

Fig : Application domains of IOT

2. LITERATURE SURVEY

IOT has a multidisciplinary vision to provide its benefit to several domains such as environmental, industrial, public/private, medical, transportation etc. Different researchers have explained the IOT differently with respect to specifc interests and aspects. Te potential and power of IOT can be seen in several application domains. Figure illustrates few of the application domains of IOTs potentials.

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

Various important IOT projects have taken charge over the market in last few years. Some of the important IOT projects that have captured most of the market are shown in Fig. In Fig, a global distribution of these IOT projects is shown among American, European and Asia/Pacific region. It can be seen that American continent are contributing more in the health care and smart supply chain projects whereas contribution of European continent is more in the smart city projects.

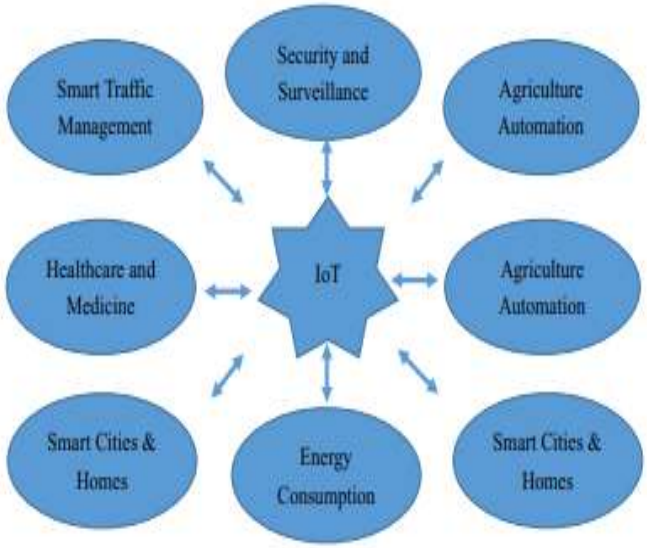

Fig. Some of the potential application domains of IOT

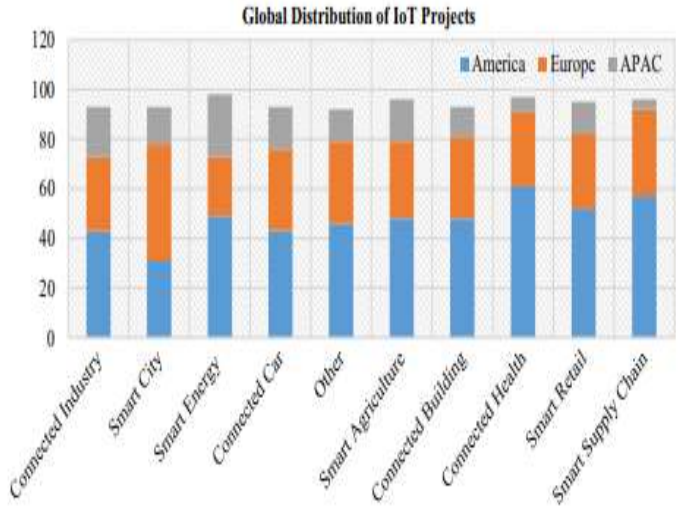

Fig. Global distribution of IOT projects among America (USA, South America and Canada), Europe and APAC (Asia and Pacifc region)

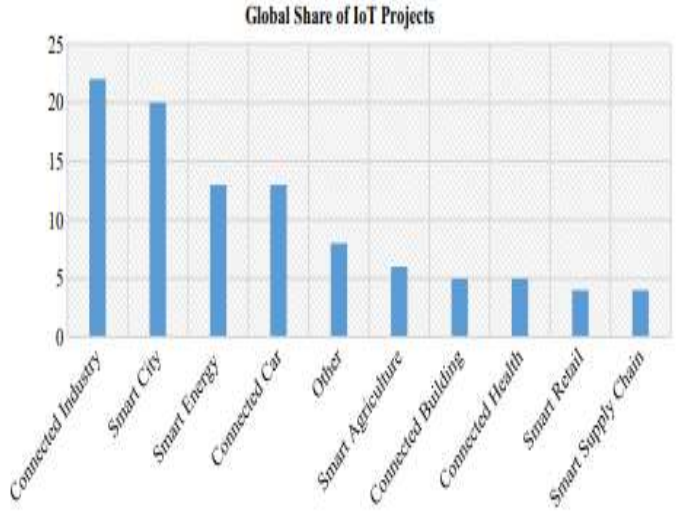

Fig. Global share of IOT projects across the world

Figure , illustrates the global market share of IOT projects worldwide . It is evident that industry, smart city, smart energy and smart vehicle based IOT projects have a big market share in comparison to others.

Smart city is one of the trendy application areas of IOT that incorporates smart homes as well. Smart home consists of IOT enabled home appliances, air-conditioning/heating system, television, audio/video streaming devices, and security systems which are communicating with each other in order to provide best comfort, security and reduced energy consumption. All this communication takes place through IOT based central control unit using Internet. Te concept of smart city gained popularity in the last decade and attracted a lot of research activities. Te smart home business economy is about to cross the 100 billion dollars by 2022. Smart home does not only provide the in-house comfort but also benefits the house owner in cost cutting in several aspects i.e. low energy consumption will results in comparatively lower electricity bill. Besides smart homes, another category that comes within smart city is smart vehicles. Modern cars are equipped with intelligent devices and sensors that control most of the components from the headlights of the car to the engine. Te IOT is committed towards developing a new smart car systems that incorporates wireless communication between car-to-car and car-to-driver to ensure predictive maintenance with comfortable and safe driving experience.

Khajenasiri et al. performed a survey on the IOT solutions for smart energy control to benefit the smart city applications. They stated that at present IOT has been deployed in very few application

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

areas to serve the technology and people. Te scope of IOT is very wide and in near future IOT is able to capture almost all application areas. They mentioned that energy saving is one of the important part of the society and IOT can assist in developing a smart energy control system that will save both energy and money. They described an IOT architecture with respect to smart city concept. Te authors also discussed that one of the challenging task in achieving this is the immaturity of IOT hardware and software. They suggested that these issues must be resolved to ensure a reliable, efficient and user friendly IOT system.

Alavi et al. addressed the urbanization issue in the cities. Te movement of people from rural to urban atmosphere resulting in growing population of the cities. Therefore, there is a need to provide smart solutions for mobility, energy, healthcare and infrastructure. Smart city is one of the important application areas for IOT developers. It explores several issues such as trafc management, air quality management, public safety solutions, smart parking, smart lightning and smart waste collection. They mentioned that IOT is working hard to tackle these challenging issues. Te need for improved smart city infrastructure with growing urbanization has opened the doors for entrepreneurs in the feld of smart city technologies. Te authors concluded that IOT enabled technology is very important for the development of sustainable smart cities.

Another important issue of IOT that requires attention and a lot of research is security and privacy. Weber focused on these issues and suggested that a private organization availing IOT must incorporate data authentication, access control, resilience to attacks and client privacy into their business activities that would be an additional advantage. Weber suggested that in order to define global security and privacy issues, IOT developers must take into account the geographical limitations of the different countries. A generic framework needs to be designed to ft the global needs in terms of privacy and security. It is highly recommended to investigate and recognize the issues and challenges in privacy and security before developing the full fudge working IOT framework.

Fig. Potential IOT application areas for smart cities

Later, Heer et al. came up with a security issue in IP based IOT system. They mentioned that internet is backbone for the communication among devices that takes place in an IOT system. Therefore, security issues in IP based IOT systems are an important concern. In addition, security architecture should be designed considering the life cycle and capabilities of any object in the IOT system. It also includes the involvement of the trusted third party and the security protocols. Te security architecture with scalability potential to serve the small-scale to large-scale things in IOT is highly desirable. Te study pointed out that IOT gave rise to a new way of communication among several things across the network therefore traditional end to end internet protocol are not able to provide required support to this communication. Therefore, new protocols must be designed considering the translations at the gateways to ensure end-to-end security. Moreover, all the layers responsible for communication has their own security issues and requirements. Therefore, satisfying the requirements for one particular layers will leave the system into a vulnerable state and security should be ensured for all the layers.

Authentication and access control is another issue in IOT that needs promising solutions to strengthen the security. Liu et al. brought up a solution to handle authentication and access control. Authentication is very important to verify the communicating parties to prevent the loss of confidential information. Liu et al. provided an authentication scheme based on Elliptic Curve Cryptosystem and verified it on different security threats i.e. eavesdropping, man-in-the-middle

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

attack, key control and replay attack. They claimed that there proposed schemes are able to provide better authentication and access control in IOT based communication. Later, Kothmayr et al. proposed a two-way authentication scheme based of datagram transport layer security (DTLS) for IOT. Te attackers over the internet are always active to steal the secured information. Te proposed approach are able to provide message security, integrity, authenticity and confidentiality, memory overhead and end-to-end latency in the IOT based communication network.

Li et al. proposed a dynamic approach for data centric IOT applications with respect to cloud platforms. Te need of an appropriate device, software configuration and infrastructure requires efficient solutions to support massive amount of IOT applications that are running on cloud platforms. IOT developers and researchers are actively engaged in developing solutions considering both massive platforms and heterogeneous nature of IOT objects and devices. Olivier et al. [19] explained the concept of software defend networking (SDN) based architecture that performs well even if a well-defined architecture is not available. They proposed that SDN based security architecture is more flexible and efficient for IOT.

Luk et al. stated that the main task of a secure sensor network (SSN) is to provide data privacy, protection from replay attacks and authentication. They discussed two popular SSN services namely TinySec and ZigBee. They mentioned that although both the SSN services are efficient and reliable, however, ZigBee is comparatively provides higher security but consumes high energy whereas TinySec consumes low energy but not as highly secured as ZigBee. They proposed another architecture MiniSec to support high security and low energy consumption and demonstrated its performance for the Telos platform.

Yan et al. stated that trust management is an important issue in IOT. Trust management helps people to understand and trust IOT services and applications without worrying about uncertainty issues and risks. They investigated different issues in trust management and discussed its importance with respect to IOT developers and users.

Noura et al. stated the importance of interoperability in IOT as it allows integration of devices, services from different heterogeneous platforms to provide the efcient and reliable service. Several other studies focused on the importance of interoperability and discussed several challenges that interoperability issue is facing in IOT. Kim et al. addressed the issue of climate change and proposed an IOT based ecological monitoring system. They mentioned that existing approaches are time consuming and required a lot of human intervention. Also, a routine visit is required to collect the information from the sensors installed at the site under investigation. Also, some information remained missing which leads to not highly accurate analysis. Therefore, IOT based framework is able to solve this problem and can provide high accuracy in analysis and prediction. Later, Wang et al. shows their concern for domestic waste water treatment. They discussed several deficiencies in the process of waste water treatment and dynamic monitoring system and suggested effective solutions based on IOT. They stated that IOT can be very effective in the waste water treatment and process monitoring.

Agriculture is one of the important domain around the world. Agriculture depends on several factors i.e. geographical, ecological etc. Qiu et al. stated that technology that is being used for ecosystem control is immature with low intelligence level. They mentioned that it could be a good application area for IOT developers and researchers.

Qiu et al. proposed an intelligent monitoring platform framework for facility agriculture ecosystem based on IOT that consists of four layer mechanism to manage the agriculture ecosystem. Each layer is responsible for specific task and together the framework is able to achieve a better ecosystem with reduced human intervention.

Another important concern around the world is climate change due to global warming. Fang et al. introduced an integrated information system (IIS) that integrates IOT, geo-informatics, cloud computing, global positioning system (GPS), geographical information system (GIS) and e-science in order to provide an effective environmental monitoring and control system. They mentioned that the proposed IIS provides improved data collection, analysis and decision making for climate control. Air pollution is another important concern worldwide. Various tools and techniques are available to air quality measures and control. Cheng et al. proposed Air

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

Cloud which is a cloud based air quality and monitoring system. They deployed Air Cloud and evaluated its performance using 5 months data for the continuous duration of 2 months.

3. FUTURE OF IOT

IOT is gathering enormous popularity all around the world for its huge demand in the field of technology. In IOT objects are present around us in one or another form. This new technology will give rise to Wireless Sensor Network (WSN) for its implementation [43]. As the devices need to be connected ubiquitously for its smart functioning which will eventually increase its demand and usage? looking at its existing demand and potential, we can conclude that it has a great future ahead. Looking at the present scenario of IOT, we wonder what the future technology is going to provide us. Going through an intense research led us say that the devices will make use technology in the most efficient way.

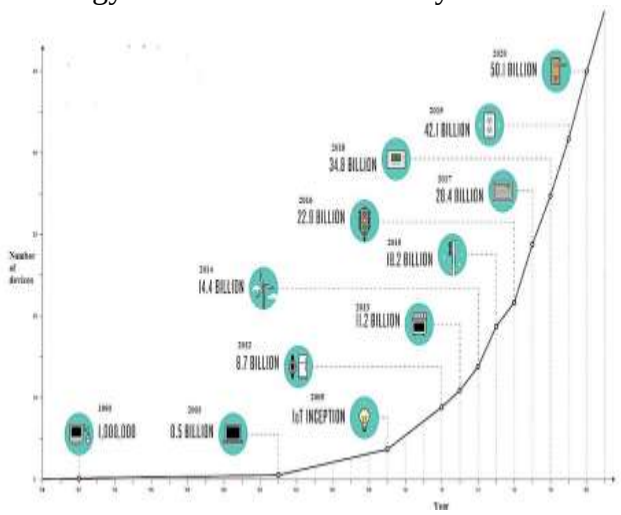

Figure: Growth of IOT devices over years

The above figure 15 shows the rapid growth of IOT devices over years in different sectors. The future seems to be more smart and ubiquitous with the emerging technology. Some of the futuristic predictions made about IOT includes [44]

It has been roughly calculated that by 2025 IOT devices will cross 50 billion. The estimation made by the analytics of IOT shows that in 2016 4.7 billion devices were connected through the internet which may increase to 11.6 billion by 2021 and so on. • The advancement in technology will led to smart city development. The usage of IOT is not limited to people. Now a day companies and cities are adopting the smart technologies very frequently to save more money as well as time [45]. This will result in automated city which can be remotely managed and the data will be collected through IOT devices using various technologies.

- The increasing demand of IOT will give rise to artificial intelligence as the smart devices will collect data and that will be stored at cloud. Machine learning will help the system to understand things without using programming concept [48]. Systems are designed such that data is given priority as it is received which later on make the machine smarter by giving preferences and work on the basis of need of the system.
- More intelligent and secure routers need to be used in case the IOT devices are installed in private places as they are not highly secure. While manufacturing IOT devices the focus is more upon their efficiency and less upon security. Routers need to be secure enough to prevent the connected devices at entry level. So, the manufacturers should look after the different technologies to enhance the security of the system.
- IOT growth will be boosted with the use of 5G network. The 5G(fifth generation) network will enhance the speed as well as efficiency in terms of connecting more smart devices simultaneously. This will also give rise to recent products based on the demand of costumer.
- Security and privacy will also become the area to be concerned about with the arrival of new 5G technology. The devices will be connected within the network through routers which will directly affect them with several attacks. The data will be stored on cloud and make easier for the attackers to aim them.

IOT NETWORK IN FUTURE

This part explains a deep understanding about the IOT network in coming future. The given figure below describes different components in the network and how they are interconnected. The working of each component is explained further.

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

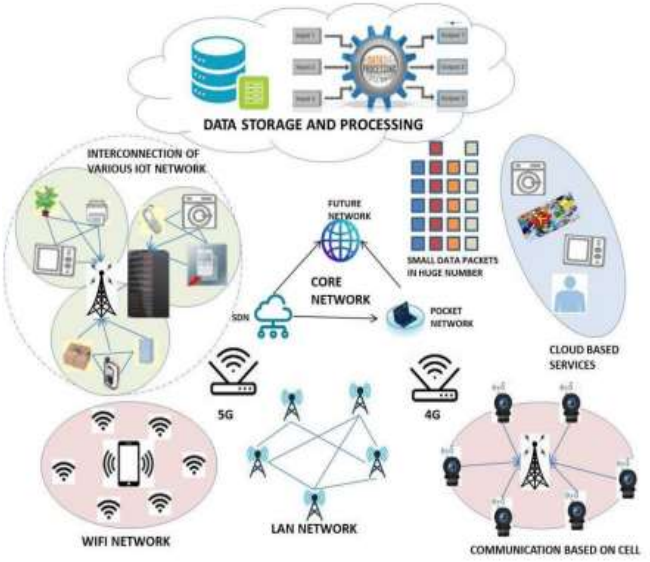

Figure: Future IOT Network

The above architecture uses the concept of SDN(Software Defined Network) which is a prominent architecture in network [49]. It supervises the network control directly rather than using the forwarding concept [50]. The working of SDN is done through different layers mostly infrastructure/physical, control/middle and the application layer [51-53][57].

All the network devices required within is connected at the infrastructure layer which includes the routers, switching equipments etc.

- At the control layer the different mechanism works regarding providing essential protocols required for the network.
- Open flow plays a vital role here by providing the specification required for the network devices and controllers within the network.
- Application layer is basically concerned with the data regarding statistics, state, and the topology of the network.

The use of SDN makes the working of devices smoother. And the use of Open flow protocol provides the controller and network devices to communicate with each other [55][48]. It helps in multiple packets simultaneously within the network and improves the quality of service being provided [54]. And the fastest growing 5G technology in the future provides a high speed communication within the architecture [55]. The IOT provides association such that everything can be tracked individually and easily. The most important right in such network is the privacy of an individual. It provides a trustable environment which should not have any negative impact over society. Technology should be standardized for better performance by reducing barriers [56].

4. RESEARCH CHALLENGES

For all the above potential applications of IOT, there has to be proper feasibility into the different domains to ascertain the success of some applications and their functionality. As with any other form of technology or innovation, IOT has its challenges and implications that must be sorted out to enable mass adoption. Even though the current IOT enabling technologies have greatly improved in the recent years, there are still numerous problems that require attention, hence paving the way for new dimensions of research to be carried out. Since the IOT concept ensues from heterogeneous technologies that are used in sensing, collecting, action, processing, inferring, transmitting, notifying, managing, and storing of data, a lot of research challenges are bound to arise. These research challenges that require attention have consequently spanned different research areas [14].

PRIVACY AND SECURITY

Owing to the fact that IOT has become a vital element as regards the future of the internet with its increased usage, it necessitates a need to adequately address security and trust functions. Researchers are aware of the weaknesses which presently exist in many IOT devices. Furthermore, the foundation of IOT is laid on the existing wireless sensor networks (WSN), IOT thus architecturally inherits the same privacy and security issues WSN possesses [3, 15]. Various attacks and weaknesses on IOT systems prove that there is indeed a need for wide ranging security designs which will protect data and systems from end to end. Many attacks generally exploit weaknesses in specific devices thereby gaining access into their systems and consequently making secure devices vulnerable [16, 17] . This security gap further motivates comprehensive security solutions that consist of research that is efficient in applied cryptography for data and system security, non-cryptographic security techniques as well as frameworks that assist developers to come up with safe systems on devices that are heterogeneous.

There is a need for more research to be conducted on cryptographic security services that have the capability to operate on resource constrained IOT devices. This would enable different skilled users to securely use and deploy IOT systems regardless of the inadequate user interfaces that are available

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

with almost all IOT devices. In addition to the protection and security aspects of the IOT, additional areas like confidentiality in communication, trustworthiness, and authenticity of communication parties, and message integrity, and supplementary safety requirements should also be incorporated. These may include features like being able to prevent communication of various parties. As an example, in business transactions, smart objects must be prevented from facilitating competitors' access to confidential information in the devices and thus using this information maliciously.

PROCESSING, ANALYSIS AND MANAGEMENT OF DATA

The procedure for processing, analysis and data management is tremendously challenging because of the heterogeneous nature of IOT, and the large scale of data collected, particularly in this era of Big Data [18]. Currently, most systems utilize centralized systems in offloading data and carrying out computationally intensive tasks on an international cloud platform. Nevertheless, there is a constant concern about conventional cloud architectures not being effective in terms of transferring the massive volumes of data that are produced and consumed by IOT enabled devices and to be able further support the accompanying computational load and simultaneously meet timing constraints [19]. Most systems are therefore relying on current solutions such as mobile cloud computing and fog computing which are both based on edge processing, to mitigate this challenge.

Another research direction as regards data management is applying Information Centric Networking (ICN) in the IOT. Since these information centric systems offer support in the efficient content retrieval and access to services, they appear to be quite valuable not just in accessing but also transferring as well as managing generated content and its transmission. This solution, however, brings about various challenges such as; how to extend the ICN paradigm competently over the fixed network edge, how to take in IOTs static and mobile devices as well as how to apportion the functionality of ICN on resource constrained devices [19].

Data analysis and its context not only plays a crucial role in the success of IOT, it also poses major challenges. Once data has been collected it has to be used intelligently in order to achieve smart IOT functions. Accordingly, the development of machine learning methods and artificial intelligence algorithms, resultant from neural works, genetic algorithms, evolutionary algorithms, and many other artificial intelligence systems are essential in achieving automated decision making.

MONITORING AND SENSING

Even if technologies concerned with monitoring and sensing have made tremendous progress, they are constantly evolving particularly focusing on the energy efficiency and form aspect. Sensors and tags are normally expected to be active constantly in order to obtain instantaneous data, this aspect makes it essential for energy efficiency especially in lifetime extension. Simultaneously, new advances in nanotechnology/biotechnology and miniaturization have allowed the development of actuators and sensors at the Nanoscale.

M2M (MACHINE TO MACHINE) COMMUNICATION AND COMMUNICATION PROTOCOLS

While there are already existing IOT oriented communication protocols like Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT), there is still no standard for an open IOT. Although all objects require connectivity, it is not necessary for every object to be made internet capable since they only need to have a certain capability to place their data on a particular gateway. Additionally, there are a lot of options in terms of suitable wireless technologies such as LoRa, IEEE 802.15.4, and Bluetooth even though it is not clear whether these available wireless technologies have the needed capacity to continue covering the extensive range of IOT connectivity henceforth.

The communication protocols for devices are the driving force in actualizing IOT applications, and they form the main support of data flow between sensors and the physical objects or outer world. While various MAC protocols have been projected for several domains with Frequency Division Multiple Access, Time Division Multiple Access and Carrier Sense Multiple Access (FDMA, TDMA and CSMA) for low traffic efficiency that is collision free, more circuitry in nodes are required respectively. The main objectives of the transport layer include guaranteeing an end-to-end reliability as well as performing end-to-end control of congestion. In

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

this aspect, most protocols are unable to cooperate appropriate end to end reliability [20].

BLOCKCHAIN OF THINGS (BCOT): FUSION OF BLOCKCHAINAND INTERNET OF THINGS

Similar to IOT, BLOCKCHAIN technologies have also gained tremendous popularity since its introduction in 2018. Even though BLOCKCHAIN was first implemented as an underlying technology of Bitcoin cryptocurrency, it is now being used in multifaceted nonmonetary applications [21]. Miraz argues that both IOT and BLOCKCHAIN can strengthen each other, in a reciprocal manner, by eliminating their respective inherent architectural limitations [22]. The underlying technology of IOT is WSN. Therefore, analogous to WSN, IOT also suffers from security and privacy issues. On the contrary, the primary reasons for BLOCKCHAIN's implementation trend in nonmonetary applications is due to its inbuilt security, immutability, trust and transparency. These attributes are powered by BLOCKCHAIN's consensus approach and utilization of Distributed Ledger Technologies (DLTs) which require extensive dependency on participating nodes. Therefore, the fusion of these two technologies BLOCKCHAIN and Internet of Things (IOT) conceives a new notion i.e. the BLOCKCHAIN of Things (BCoT) where BLOCKCHAIN strengthens IOT by providing extra layer of security while the "things" of IOT can serve as participating nodes for BLOCKCHAIN ecosystems [22]. Thus, BLOCKCHAIN enabled IOT ecosystems will provide enhanced overall security [23] as well as benefit from each other.

INTEROPERABILITY

Traditionally as regards the internet, interoperability has always been and continues to be a basic fundamental value because the initial prerequisite in Internet connectivity necessitates that "connected" systems have the ability to "speak a similar language" in terms of encodings and protocols. Currently, various industries use a variety of standards in supporting their applications. Due to the large quantities and types of data, as well as heterogeneous devices, using standard interfaces in such diverse entities is very important and even more significant for applications which support cross organizational, in addition to a wide range of system limitations. Therefore, the IOT systems are meant towards being designed to handle even higher degrees of interoperability [24].

5. CONCLUSION

The Internet of Things is playing an active role in our everyday life, and its applications are fabulous and countless. Projections for the impact of IOT on the Internet and economy are impressive, with some anticipating as many as 100 billion connected IOT devices and a global economic impact of more than $11 trillion by 2025. The best part of Internet of Things is that they are bringing the quality of life to human beings, operational efficiency and handles the situations where human being intervention is not at all possible. At the same time, however, the Internet of Things raises significant challenges that could stand in the way of realizing its potential benefits.

In the future, we need to focus more on Internet of Things in terms of development, deployment, architectural, global level standardization, and ethical issues. We also need to concentrate on challenges associated with IOT in order for the potential benefits for individuals, society, and the economy to be realized.

REFERENCES

M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A Review on Internet of Things (IOT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)", in 2015 Internet Technologies and Applications (ITA), pp. 219– 224, Sep. 2015, DOI: 10.1109/ITechA.2015.7317398.

P. J. Ryan and R. B. Watson, "Research Challenges for the Internet of Things: What Role Can OR Play?," Systems, vol. 5, no. 1, pp. 1–34, 2017.

M. Miraz, M. Ali, P. Excell, and R. Picking, "Internet of Nano-Things, Things and Everything: Future Growth Trends", Future Internet, vol. 10, no. 8, p. 68, 2018, DOI: 10.3390/fi10080068.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IOT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.

Guo, B., Zhang, D., Wang, Z., Yu, Z., & Zhou, X. (2013). Opportunistic IOT: Exploring the harmonious interaction between human and the

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

internet of things. Journal of Network and Computer Applications, 36(6), 1531-1539.

S.-I. Hou, S.-A. R. Charlery, and K. Roberson, ―Systematic literature review of Internet interventions across health behaviours,‖ Health Psychology and Behavioral Medicine: Open Access Journal, vol. 2, no. 1, pp. 455-481, 2014.

G. Nunberg, ―The advent of the Internet,‖ 2012.

E. A. Kosmatos, N. D. Tselikas, and A. C. Boucouvalas, ―Integrating RFIDs and smart objects into a unified Internet of things architecture,‖

Zhang, B., Mor, N., Kolb, J., Chan, D.S., Lutz, K., Allman, E., Wawrzynek, J., Lee, E. and Kubiatowicz, J., 2015. The cloud is not enough: Saving IOT from the cloud. In 7th {USENIX} Workshop on Hot Topics in Cloud Computing (HotCloud 15).

Munir, A., Kansakar, P. and Khan, S.U., 2017. IFCIOT: Integrated Fog Cloud IOT: A novel architectural paradigm for the future Internet of Things. IEEE Consumer Electronics Magazine, 6(3), pp.74-82.

Sfar AR, Zied C, Challal Y. A systematic and cognitive vision for IOT security: a case study of military live simulation and security challenges. In: Proc. 2017 international conference on smart, monitored and controlled cities (SM2C), Sfax, Tunisia, 17–19 Feb. 2017. https://doi.org/10.1109/sm2c.2017.8071828.

Gatsis K, Pappas GJ. Wireless control for the IOT: power spectrum and security challenges. In: Proc. 2017 IEEE/ACM second international conference on internet-of-things design and implementation (IOTDI), Pittsburg, PA, USA, 18–21 April 2017. INSPEC Accession Number: 16964293.

S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IOT): A Literature Review," J. Comput. Commun., vol. 3, no. 3, pp. 164–173, 2015.

U. S. Profile, "T H E D I G I T AL U N I V E R S E I N 2 0 2 0 : B i g D a t a , Bigger Digital Shadows , and Biggest Growth in the Far East — United States," pp. 1– 7, 2013.