A Comparative Study of Computing Techniques for Effective Implementation of Green IOT

Divya K S
Assistant Professor
Department of CSE
SNGCE
Kochi, India
divyaks@sngce.ac.in

Dr.Vidhya P M
Associate Professor
Department of CSE
SNGCE
Kochi, India
vidhya@sngce.ac.in

***Abstract*—This paper aims to discuss the computing techniques which will enhance the efficiency of Green Internet of Things (GIoT). IoT or Internet of Things is a concept, which aims to connect billions of devices with each other. The IoT devices sense, collect, and transmit important information from their surroundings. Green IoT envisages to bring down the energy utilization required in the daily IoT connections.**

***Keywords*—Green IoT, Energy utilization, IoT**

I. INTRODUCTION

A numerous amount of sensing devices, processing elements, and communication technologies are involved in the growth and expansion of any IoT based system. Furthermore, the communication devices must be capable of providing an uninterrupted connection for the QoS of the system. Due to IoT, physical objects are seamlessly integrated into the information network where they can become active participants in business processes [1]. Green IoT (Internet of Things) refers to the use of IoT technologies and applications in a manner that minimizes the environmental impact of these systems. As the use of IoT devices and systems grows, it is becoming increasingly important to ensure that these systems are designed and deployed in a way that is sustainable and environmentally responsible. The concept of green IoT involves the use of hardware, software, and networking technologies that are designed to reduce energy consumption, minimize waste, and optimize resource usage. For example, energy-efficient hardware components and communication protocols can be used to minimize the power consumption of IoT devices. Inspired by achieving a sustainable environment for IoT, we first give the overview of green IoT and the computing methods that are used to reduce the excessive usage of energy hungry IoT devices .For the remaining part of this paper, Section II provides the current IoT trends and challenges. Section III reviews the existing approaches for the green IoT. Section IV provides recent literature reviews on the field of Green IoT.

II.

III. IOT TRENDS AND CHALLENGES

IoT has changed the way many applications used to work in the past. It has revolutionized many areas like the Food Supply Chain, Transportation Industry, Smart Cities and Smart Homes. IoT devices are generating huge amounts of data that need to be processed quickly. The emerging 5G connectivity provides faster speed and lower latency for making them ideal for IoT applications that require real- time data transmission and processing. Edge Computing which involves processing data closer to the source rather than in the cloud, can improve the response time and reduce latency. Digital Twins is a virtual representation of a physical object or system that simulates and models. The advancement in IoT helps to optimize processes, predict maintenance needs and improves overall efficiency [2]. Another area which is of increasing trends is the BlockChain technology, which is used to create secure, decentralized IoT networks that are less vulnerable to hacking and other security threats. Wearable IoT devices such as fitness trackers and health bands have the added advantage of IoT connectivity.

As with trends in IoT, it faces challenges as well. There are many challenges posed by the IoT technologies like Security and Privacy challenges as described in [3] and [4] as one of the key areas that experts need to work on in order to gain trust of the users. IoT devices and systems are vulnerable to cyber-attacks, which can lead to data breaches, privacy violations, and system failures. The large number of connected devices and the lack of standard security protocols make IoT security a major challenge.IoT devices and systems often use different communication protocols, making it difficult to connect and exchange data between them. The lack of interoperability hinders the development of large-scale IoT systems and limits their potential.IoT devices generate a huge amount of data, much of which is personal or sensitive. Protecting this data from unauthorized access or misuse is a significant challenge.IoT systems can include millions or even billions of devices, which can be challenging to manage and scale. Developing IoT systems that can scale efficiently and reliably is critical to their success. When it comes to energy efficiency, IoT devices can consume a significant amount of energy, which can contribute to environmental issues such as carbon emissions and climate change. Developing energy-efficient IoT devices and systems is essential to minimize their impact on the environment.

IV. GREEN IOT

Green IoT (Internet of Things) computing techniques are methods used to reduce the environmental impact of IoT devices and systems. Here are some common techniques:

1) Energy-efficient hardware design: Hardware components of IoT devices can be designed to consume less power, which results in lower energy usage and less carbon emissions.

2)Energy-efficient communication protocols: Communication protocols used by IoT devices can be designed to consume less power, which reduces energy usage and carbon emissions.

3) Cloud-based processing: IoT devices can offload processing tasks to cloud-based servers, which are often more energy-efficient than local devices.

4) Energy-efficient algorithms: IoT systems can use algorithms that are designed to optimize energy usage, reducing the overall carbon footprint of the system.

5) Renewable energy sources: IoT systems can be powered by renewable energy sources such as solar, wind, or hydroelectric power.

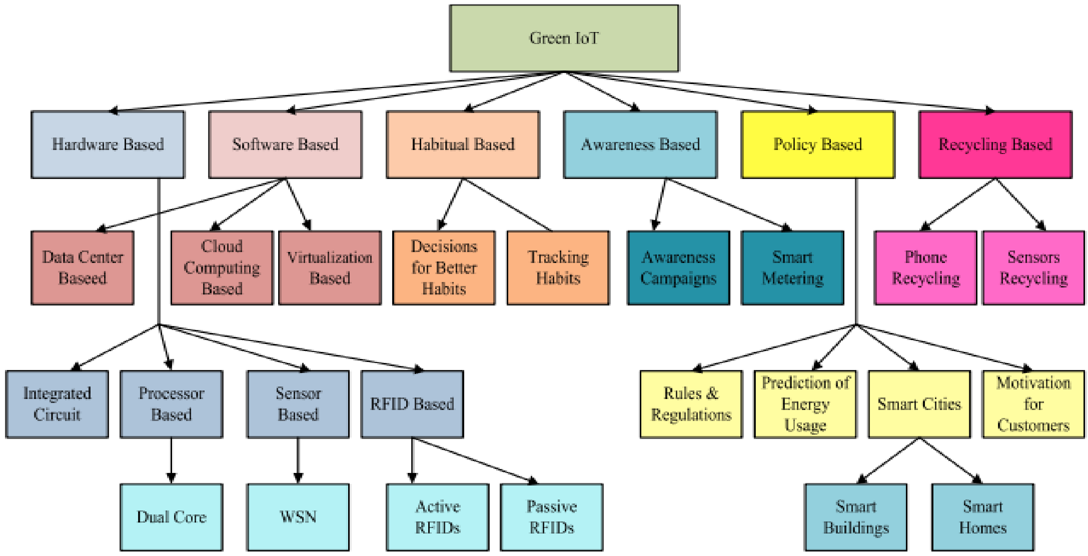
6) Sleep mode: IoT devices can be programmed to enter sleep mode when they are not in use, reducing power consumption and carbon emissions.

7) Dynamic power management: IoT devices can adjust their power consumption based on workload, reducing energy usage and carbon emissions.

Overall, green IoT computing techniques can help reduce the environmental impact of IoT devices and systems while still allowing them to perform their intended functions.

V. COMPUTING TECHNIQUES IN GREEN IOT

In this section, we give a literature review of all the models proposed recently for energy efficient deployment of IoT. A detailed taxonomy is presented in Figure 1. There are many techniques that can be implemented for Green IoT. Hardware based, Software based, Awareness based, Policy based, Recycling based are the major categories



identified for the classification. Green IoT is a very hot research topic in the ICT industry as the

Fig 1. Taxonomy of Green IoT. Source:R. Arshad et al.: Green IoT: An Investigation on Energy Saving Practices for 2020 and Beyond

traditional energy resources are decreasing rapidly and the use of energy is increasing exponentially. An optimal workload distribution framework, in [5] evaluates the workload in different servers on different locations having renewable power generators, by taking into account servers' resource consumption, electricity cost etc. Green Technologies to implement IoT while maintaining QoS across various domains were elaborated in [6] which explicitly focused on the solutions for Green IoT. Data Centre and Cloud Computing and their Green solutions, which are the backbone of an IoT network, were not discussed. Green Machine to Machine (M2M) must be energy efficient transmission power and improved communication protocols within green machine to machine communication. Green Wireless Sensor Network has many sensor nodes having small capacity and limited power. Green WSN can be accomplished by Green routing techniques, Radio Optimization technique and Green Energy
Conservation technique. Techniques like data centers can be vital for attaining an energy efficient IoT network. e-CAB, which is a policy based design, proposed by a researcher in [7] utilizing an Orchestration Agent (OA) in a system based on ClientServer model, that is accountable
for management of data centers. Awareness campaigns are a vital factor in decreasing the
energy consumption but this varies from culture to culture and country to country because you cannot predict or estimate how many people will listen and follow your campaigns. So, Smart Metering Technology can be used to provide homeowners with a real time feedback of their energy consumption from various sources of their homes, offices, buildings and then we can advise them on how to control and minimize their energy consumption based on that real-time data. This can save energy from 3-6% [8].

A Programming Language named EPDL was designed to help the non-experts to write energy policies for a smart environment like IoT. Many processing tools were introduced in EPDL but addition of new features and possibly an extensive library of functions should be added to make it more robust [9]. Many energy utilization models in IoT concentrate on hardware modifications but classification of objects in an IoT system can help it to make a green network. RFID is an important part of IoT so, enhancement of an active RFID was discussed in [10] and development of passive RFID in Wireless Identification and Sensing Platform (WISP) can lead to a more energy efficient system in IoT discussed in [11].

VI. CONCLUSION

The impact of IoT on the economy is going to be paramount and it is predicted to revolutionize the entire ICT industry. The need of research for a generic architecture, recyclable material and policy making to achieve Green IoT has been highlighted. IoT can undoubtedly change the course of technological advancements in the world if focused and dedicated work is put in the right direction. In this paper we tried to include some of the key trends and challenges in IoT and how the transformation from IoT to Green IoT is possible.

.

REFERENCES

[1] *Bandyopadhyay, D.; Sen, J. Internet of Things: Applications and Challenges in Technology and Standardization. Wirel. Pers. Commun. 2011, 58, 49–69.*

[2] *D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, ''Internet of Things: Vision, applications and research challenges,'' Ad Hoc Netw., vol. 10, no. 7, pp. 1497–1516, Sep. 2012.*

[3] *D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, ''Internet of Things: Vision, applications and research challenges,'' Ad Hoc Netw.,vol. 10, no. 7, pp. 1497–1516, Sep. 2012.*

[4] *R. H. Weber, ''Internet of Things—New security and privacy challenges,'' Comput. Law Secur. Rev., vol. 26, no. 1, pp. 23–30, 2010. [13] D. Singh, G. Tripathi, and A. J. Jara, ''A survey of Internet-of-Things: Future vision, architecture, challenges and services,'' in Proc. IEEE World Forum Internet Things, Mar. 2014, pp. 287–292.*

[5] *M. Ghamkhari and H. Mohsenian-Rad, ''Optimal integration of renewable energy resources in data centers with behind-the-meter renewable generators,'' in Proc. IEEE Int. Conf. Commun., Jun. 2012, pp. 3340–3344*

[6] *A. Kiourti, C. Lee, and J. L. Volakis, ''Fabrication of textile antennas and circuits with 0.1 mm precision,'' IEEE Antennas Wireless Propag. Lett.,vol. 15, pp. 151–153, 2015*

[7] *C. Peoples, G. Parr, S. McClean, B. Scotney, and P. Morrow, ''Performance evaluation of green data center management supporting sustainable growth of the Internet of Things,'' Simul. Model. Pract. Theory, vol.34, pp. 221–242, May 2013.*

[8] *C. McKerracher and J. Torriti, ''Energy consumption feedback in perspective: Integrating Australian data to meta-analyses on in-home displays,'' Energy Efficiency, vol. 6, no. 2, pp. 387–405, 2013.*

[9] *] X. Peng, M. Bessho, N. Koshizuka, and K. Sakamura, ''EPDL: Supporting context-based energy control policy design in IoT-enabled smart buildings: Programming the physical world with EPDL,'' in Proc. IEEE Int. Conf. Data Sci. Data Intensive Syst., Dec. 2015, pp. 297–303.*

[10] *R. H. Weber, ''Internet of Things—New security and privacy challenges,'' Comput. Law Secur. Rev., vol. 26, no. 1, pp. 23–30, 2010.*

[11] *Bilge L., Dumitras T. Before we knew it: An empirical study of zero-day attacks in the real world; Proceedings of the 2012 A.C.M. Conference on Computer and Communications Security; Raleigh, NC, U.S.A. 16–18 October 2012; New York, NY, U.S.A.: A.C.M.; 2012. pp. 833–844. [Google Scholar] [Reflist]*