Medicon Engineering Themes
Volume 1 Issue 2 November 2021
Editorial Note

# Internet of Everything (IoE): Intelligence, Cognition, Catenate

**Ganesh Khekare***

*Department of Computer Science and Engineering, Parul University, India*

***Corresponding Author:** Ganesh Khekare, Department of Computer Science and Engineering, Parul University, India.

**Received:** October 29, 2021; **Published:** November 08, 2021

Internet of Things (IoT) focuses on physical entities whereas Internet of Everything (IoE) focuses on everything viz., People, Process, Things, Data. IoE intelligently tries to collect and process the data not only from IoT but also from various technologies and even treat people as a node. The IoE is transpiring technology. In the last decade demand for IoE has been increased due to various things like the use of smart devices; increased demand for voice-based services; the concept of smart cities has been evolved; more requirements of processed data in fields of artificial intelligence and machine learning; fog computing, edge computing, deep learning, data analytics, etc. IoE is expected to reach the milestone of 30 billion IoE units at the end of the year 2022. IoE has emerged as a key technology that enables everything to be connected through the internet. As technology is advancing day by day, automation is playing an important role. In every field, IoE is generating a vast amount of data like health systems, traffic systems, smart city monitoring systems, education systems, social networking sites, government organizations, etc. To handle a huge amount of data, a system is required through which it becomes easier to track, analyse, handle, and apply that data in a better way [1].

A huge amount of data is involved in the Internet of Everything. To maintain connectivity, privacy and security is a challenge. To maintain ownership of private data more emphasis on anonymity should be given [2]. As new things are involved in the IoE network dynamic changes are required in the technologies and infrastructure. As technology changes a new IT skill is required. Financial support as well as technically sound people will be the key factor. Standards, interoperability, spectrum and bandwidth constraints, connectivity scaling, reliability, governance, and data localization play a major role. As data is sent throughout the world common governance should be there which will handle cross-border traffic. Whatever data is sent or received is first analysed for the proper format and security threats. This huge amount of data is handled by the regulatory body. Regulation is likely to require a more joined up approach for the Internet of Everything. Likewise, solid law and set of rules can hamper the implementation of IoE e.g., new devices made for health checkups may take a long time to come into the doctor's hands due to a large number of approvals from various agencies like Pre-Qualified Systems (PQS) of World Health Organization. So, cognition and better policymaking are required to make things happen as soon as possible [3].

Scalability, reliability, power requirements, technically skilled human power are the technical challenges as far as IoE is concerned. Scalability is used for the optimum utilization of resources. A large scale of node connectivity managed by IP Networks as IoE consists of billions of nodes. Devices must be reliable to sustain in a complex external environment. Devices like sensors that gather data must provide accurate information. Some objects may require less electricity and some high bandwidth nodes may require a large amount of electricity. A smooth flow of power consumption is required. Proper connectivity to these technical devices must be done. IoT Infrastructure should be cost-efficient. Inadequate technical manpower is an issue for small-scale industries. A special budget is required to train the manpower with updated IT skill sets. Assembly, installation, testing, and maintenance of various devices are still handled by humans [4].

Escalation and extension in IoE devices are focused on compatibility. Compatibility is the technique to send information across applications, devices, or nodes considering 4 different layers - technical; information; people; and at the institute level. Today around 150 protocols are required to connect IoE devices to the cloud system [5]. In large-scale IoE deployment data preservation with se-

curity is the challenge. Anonymity, security, and privacy are all correlated but different in concepts. Anonymity is the act of hiding the original identity of the data. The secured system is not affected by vulnerability attacks or failures. Like, Aadhar card and income tax data in India are very important personal data. Privacy is related to the confidentiality of data. A security threat is not always lead to loss of information to a person, it depends on what data was stolen and how that data is handled and operated. An active attack is more hazardous than a passive attack. Another issue is the identification of nodes, as a vast amount of data is flowing through various heterogeneous networks. The identification of source and destination must be done properly. In short, catenate is required among all the things involved in IOE. Future lies in IoE.

## References

1. Khekare Ganesh., et al. "Analysis of Internet of Things Based on Characteristics, Functionalities, and Challenges". International Journal of Hyper connectivity and the Internet of Things (IJHIoT) 5.1 (2021): 44-62.
2. G Khekare and P Verma. "Design of Automatic Key Finder for Search Engine Optimization in Internet of Everything". 2020 IEEE 1st International Conference for Convergence in Engineering (ICCE) (2020): 464-468.
3. Khekare G and Verma P. "Prophetic Probe of Accidents in Indian Smart Cities Using Machine Learning". Data Engineering and Intelligent Computing (2021): 181-189.
4. Khekare Ganesh., et al. "The Optimal Path Finding Algorithm Based on Reinforcement Learning". International Journal of Software Science and Computational Intelligence (IJSSCI) 12.4 (2020): 1-18.
5. Suvidh P Gohane., et al. "Design and Development of New Architecture for Reconfiguration and Processing of Automation Industrial Control System". International Journal of Scientific & Engineering Research 6.4 (2015): 1293-1299.

**Volume 1 Issue 2 November 2021**