IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

Sensors in IOT

Ishmeet Kaur Bhatti[1], Piyush Belsare[2], Vaishnavi Watpade[3], Amey Bhargave[4], Dipali Gharate[5]
Guru Gobind Singh Polytechnic, Nashik, Maharashtra, India[1,2,3,4]
Xaviers college of Engineering, Mahim, Maharashtra, India[5]
ishmeetkaurbhatti6@gmail.com, piyushbelsare19@gmail.com, dipaligharate7876@gmail.com
vaishnaviwatpade12@gmail.com, ameybhargave@gmail.com

Abstract: *The Internet of Things (IoT) paradigm refers to the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with servers, centralized systems, and/or other connected devices based on a variety of communication infrastructures. IoT data collected from different sensors, nodes and collectors are transferred to the cloud over the internet. IoT devices are used by consumers, healthcare, and businesses as well as by the governments. It is being forecast that 31 billion IoT devices will be deployed all over the world by the year 2022. As the use of IoT devices is increasing every moment several IoT vulnerabilities are introduced. The results and analysis indicate that massive deployment of IoT with an integration of new technologies are introducing new security challenges in IoT paradigm.*

Keywords: Sensor, Iot, temperature, signal.

REFERENCES

[1]. 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.2017.8071 8 28.

[2]. 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.

[3]. Zhou J, Cap Z, Dong X, Vasilakos AV. Security and privacy for cloud- based IoT: challenges. IEEE Commun Mag. 2017;55(1):26–33. https://doi.org/10.1109/MCOM.2017.1 6003 63CM.

[4]. Sfar AR, Natalizio E, Challal Y, Chtourou Z. A roadmap for security challenges in the internet of things. Digit Commun Netw. 2018;4(1):118–37.

[5]. Minoli D, Sohraby K, Kouns J. IoT security (IoTSec) considerations, requirements, and architectures. In: Proc. 14th IEEE annual consumer communications & networking conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017. https ://doi.org/10.1109/ccnc.2017.798 32 71.