IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 3, December 2022

Security Challenges in Internet of Things (IoT)

Mr. Ganesh Vithoba Bhojane and Mr. Mohan Anand Parte
Lecturer
Hirwal Education Trust's College of Computer Science and Information Technology, Mahad-Raigad, India
bhojaneganesh746@gmail.com and parttemohan84@gmail.com

Abstract: *The Internet of Things (IoT) is a transformative technology that connects numerous devices and systems to the internet, offering unprecedented convenience and efficiency. However, it also presents numerous security challenges that must be addressed to fully realize it's potential. This research paper examines the unique security challenges posed by IoT devices and networks, identifying common attack vectors such as device tampering, data interception, and distributed denial of service (DDoS) attacks. The root causes of these security challenges include resource constraints, insecure communication protocols, and the massive scale of IoT deployments. To address these challenges, the paper explores existing and emerging security solutions and best practices, such as secure bootstrapping, end-to-end encryption, and regular software updates. It also explores the role of block chain and machine learning in enhancing IoT network and data security. The paper reviews current regulatory and compliance frameworks designed to safeguard IoT ecosystems and user privacy, emphasizing the need for ongoing policy development and international collaboration. The research aims to equip IoT stakeholders with a comprehensive understanding of security challenges in IoT networks, enabling proactive addressing to unlock the full potential of IoT technology while ensuring data confidentiality, integrity, and availability.*

Keywords: Internet of Things (IoT), security challenges, IoT networks, cybersecurity, threat analysis, security solutions, blockchain, machine learning, regulatory frameworks .

REFERENCES

[1] S. Kumar, K. A. Kumar and R. Raman, "Internet of Things Security: Attacks, Solutions, Strengths and Limitations," Detection, and Future Visions: A Systematic Review,"
[2] P. Mann, N. Tyagi, S. Gautam and A. Rana, "Classification of Various Types of Attacks in IoT Environment,"
[3] L. M. Zagi and B. Aziz, "Privacy Attack on IoT: a Systematic Literature Review,"
[4] J. Karande and S. Joshi, "Real-Time Detection of Cyber Attacks on the IoT Devices,"