An examination of the authentication methods employed by the Internet of Things

Shabana Mohammad[1,a)] ,Dr. Kadapa Sagar[2] and V.Thirupathi[3]

[1] *Sumathi Reddy Institute of Technology for Women, Warangal, Telangana, India.*
[2]*Professor, Dept. of CSE, CBIT, Hyderabad, Telangana, India.*
[3]*School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India.*

[a)] Corresponding author: mdshabana.r@gmail.com

Abstract: Security is among the major obstacles to the Internet of Things' (IoT) development in the modern day. The IoT is a promising technology. As a result of device resource limitations counter security methods more difficult to build and execute. Many eavesdropper attacks might put authentication at risk and launch further assaults against IoT devices. A strong authentication system is thus required in order to fend off all known attack vectors. This paper evaluates lightweight authentication systems on a number of security-related criteria and covers current research on the subject. The paper also lists a number of open research questions about the effectiveness of IoT authentication techniques. Additionally, the paper analyses potential authentication options.

Keywords: Protocol, Security, Lightweight, Internet of Things, Authentication

INTRODUCTION

Due to the variety of applications, it may be used for, the Internet of Things has recently become a popular area of study. IoT aims to seamlessly integrate digital and physical items into a single, overarching network, ushering in a new age of the Internet that is intelligent and self-sufficient. Energy management, scalability, interoperability, and security are only a few of the problems caused by the Internet's explosive rise in linked objects. In terms of the success of IoT, security is the primary worry, which has an impact on other sector difficulties. Considering a complicated ecosystem and resource-constrained IoT devices, it is considerably more difficult than other difficulties. Tiny Internet of Things (IoT) devices typically have a small amount of main memory and processing power, and they are powered mostly by batteries. And it's a difficult challenge to create a security mechanism that can fit into these small gadgets. As a consequence, several IoT security research solutions have been put out that deal with key management, user authentication, device authentication, user access control, privacy preservation, and identity management.