Abstract

Authentication forms the gateway to any secure system. Together with integrity, confidentiality and authorization it helps in preventing any sort of intrusions into the system. Up until a few years back password based authentication was the most common form of authentication to any secure network. But with the advent of more sophisticated technologies this form of authentication although still widely used has become insecure. Furthermore, with the rise of ‘Internet of Things’ where the number of devices would grow manifold it would be infeasible for user to remember innumerable passwords.

Therefore, it’s important to address this concern by devising ways in which multiple forms of authentication would be required to gain access to any smart devices and at the same time its usability would be high. In this paper, a methodology is discussed as to what kind of authentication mechanisms could be deployed in internet of things (IOT).


Index Terms

Computer Science  Security
Keywords

Data integrity, authentication, multi factor authentication, internet of things (IOT), authorization, confidentiality, usability, speed, efficiency, memorability, learnability, voice based authentication, facial recognition, fingerprint recognition, location based authentication