International Journal of Intelligent Networks
Volume 3, 2022, Pages 181-187

Security behavior analysis in web of things smart environments using deep belief networks

M. Premkumar [a], S.R. Ashokkumar [b], G. Mohanbabu [a], V. Jeevanantham [c], S. Jayakumar [a]

Show more

Outline | Share | Cite

https://doi.org/10.1016/j.ijin.2022.10.003
Get rights and content

Highlights

- Security in smart environments using Deep Belief Networks.
- Accuracy, detection rate, precision, recall, F1 measure.
- Paper identifies and discusses the significant things of ML for WOT.
- Security analysis was description in details and compare study with many similarly work.

Abstract

The advancements in modern wireless communications enhances the Internet of Things (IoT) which in turns the extensive variety of applications which covers smart home, healthcare, smart energy, and Industrial 4.0. The idea of the Web of Things (WoT) was established to expand the potential of these smart devices. It enables the devices that are connected through a common network. It has played a significant part in connecting all smart devices over the internet, allowing them to share services and resources globally. However, as devices become more connected, they become more exposed to various forms of malicious activities. The DDoS and DoS attacks are the major one that can disrupt the regular operation of network and expose the malicious information. So detecting and preventing the attacks in the WoT is a significant research area. The deep belief networks based intrusion detection system is proposed in this paper to detect the malicious activities like Normal, Botnet, Brute Force, Dos/DDos, Infiltration, PortScan and Web based attacks in WoTs. We examined the proposed method with the CICIDS2017 dataset for training and testing purposes and also achieved the average of 97.8% of accuracy and 97.6% of detection rate.