Submission Summary

Conference Name
IEEE International Conference on Emerging Smart Computing and Informatics (ESCI) 2020

Track Name
ESCI2020

Paper ID
266

Paper Title
Survey on anomaly based intrusion detection systems in IoT networks

Abstract
IoT devices are becoming popular day-by-day. Several vulnerabilities in IoT present the need for IoT security. The number of attacks on these devices keep increasing and most of them are slight variations of the previously known attacks, which can bypass the conventional firewall systems.
The existing systems are not suitable for IOT devices as IOT devices have low computational power. Those that use signature-based intrusion detection work only on known patterns and attacks, hence they cannot recognize newer attacks with unknown pattern. Also, many systems use cloud computing, which has a downfall that it needs access to internet at all times and are most often paid.
The following survey discusses a few of the anomaly based intrusion detection systems built to tackle this situation. It shows the different methods used along with their drawbacks or future scope. Also, an anomaly-based detection system has been proposed. It comes into effect when detecting newer attacks, that are not filtered by the firewall. It is capable of handling newer/unknown attacks, which signature based cannot deal with. It would be set up on a local higher powered device rather than on cloud.

Created on
1/13/2020, 9:32:10 PM

Last Modified
1/13/2020, 9:32:10 PM

Authors
Rhishabh Hattarki (Sinhgad College of Engineering, Pune) < rhish9h@gmail.com>
Shruti Houji (Sinhgad College of Engineering, Pune) < shrutihouji98@gmail.com>
M. Dhage (SIT) < mrdhage.scoe@sinhgad.edu>
Sanika Patil (Sinhgad College of Engineering, Pune) < patilsanika02@gmail.com>
Sahil Dixit (Sinhgad College of Engineering, Pune) < sahildxgeneration10@gmail.com>

Primary Subject Area
Cyber Security

Secondary Subject Areas
Iot And Automation

Submission Files
s3r_conference_paper.docx (53.2 Kb, 1/13/2020, 9:31:56 PM)