Problem Definition Description

Submitted by:

Group Number 26 [Manikanta Desu(203174002), Mayank Seth(203190001), Vivek Rathore(190100138), Ashara Keyur Ashwin(19D100003), Akash Rajendra Gayakwad(190260004)]

The Internet of Things (IoT) paradigm has been rapidly evolving towards making a greater impact on everyday life to large industrial systems. Widespread use of the Internet of Things (IoT) in various domains like smart city, healthcare, supply chain and transportation make IoT a target of potentially malicious attacks which affect smart environment applications and security and privacy are considered key issues in any real-world smart environment based on the IoT model.

The security vulnerabilities in IoT-based systems create security threats that affect smart environment applications and might disrupt the normal functioning of systems. Network based attacks have been increasing over the past years. Network security has to be a high priority to protect against potential attacks. Thus, there is a crucial need for an Intrusion Detection System (IDS) designed for IoT environments to mitigate IoT-related security attacks that exploit some of these security vulnerabilities.