**CYBERATTACKS IN IOT NETWORKS**

**ABSTRACT**

The rapid growth of the Internet of Things (IoT) has attracted more attention from cybercriminals than ever before. The increasing number of cyber-attacks on IoT devices and communication networks supports this claim. If left undetected for an extended period, attacks on IoT can lead to severe service interruptions, financial loss, and pose a threat to identity protection. Real-time intrusion detection on IoT devices is crucial for ensuring the reliability, security, and profitability of IoT-enabled services. An intelligent system has been developed using a four-layer deep Fully Connected (FC) model as a communication protocol-independent system to reduce deployment complexities. The proposed system has demonstrated reliable performance in simulated and real intrusion scenarios during experimental performance analysis. It effectively detects Blackhole, Distributed Denial of Service, Opportunistic Service, Sinkhole, and Workhole attacks with good accuracy. The consequences are severe, from financial losses to reputational damage. Securing IoT networks is crucial, requiring robust authentication, encryption, and intrusion detection. Regular software updates, vulnerability assessments, and employee education are essential. The future of IoT depends on prioritizing cybersecurity to prevent devastating attacks. Proactive measures can mitigate risks and ensure the integrity of IoT networks.

Guide Sign: 41110666:K.Abhinav

Suji Helen 41110668:K.Charan Sai