Veeramreddy Jyothsna and Koneti Munivara Prasad proposed an Anomaly-Based IDS to develop generic meta-heuristic scale for both known and unknown attacks with a high

detection rate and low false alarm rate by adopting efficient feature optimization

techniques using a benchmark NSL-KDD dataset. Though existing intrusion detection

techniques address the latest types of attacks like DoS, Probe, U2R, and R2L,

reducing false alarm rate is a challenging issue with high classification accuracy.

Nabila Farnaaz∗ and M. A. Jabbar propsed Random Forest Modeling for Network Intrusion Detection System to detect four types of attack like DOS, probe, U2R and R2L.10 cross validation are applied for classification and feature selection on the data set to reduce dimensionality and to remove redundant and irrelevant features using NSL KDD data set. However, evolutionary computation needs to be applied as a feature selection measure to further improve accuracy of the classifier.

Mohamed Faisal Elrawy, Ali Ismail Awad and Hesham F.A. Hamed proposed an IDS for IOT based smart environments to mitigate IoT-related security attacks that exploit some of these security vulnerabilities. This article presents a comprehensive survey of the latest IDSs designed for the IoT model, with a focus on the corresponding methods, features, and mechanisms and also provides deep insight into the IoT architecture, emerging security vulnerabilities, and their relation to the layers of the IoT architecture. However there is a need for a powerful and lightweight system with a suitable placement strategy that does not adversely affect the

Integrity of the IoT environment.

S.Suganthi proposed an IDS in IOT devicesto detect the security loopholes arising out of the information exchange technologies in Internet of Things and also learn the various security attacks and approaches to mitigate those attacks**.** However it is difficult toachieve a reliable connection between the individual nodes in IoT due to the nodes constantly changing.

Luis Miguel Torres, Eduardo Maga˜na, Mikel Izal and Daniel Morato proposed an anomaly-based IDS for IEEE 802.11 networks introducing a wireless IDS called S2WIDS. It is an anomaly based system that implements a multidisciplinary approach to detect the most common attacks in wireless environments and it may be able to fight some of the new threats that might arise in the future.However, additional information about the AP might be useful to detect threats such as Rogue Aps.