In recent years, especially with the developments in IoT technologies, the number of people and applications using the internet is constantly increasing. Internet usage is increasing according to Data Reportal data, which provides information about internet usage in the world. Also, according to DataReportal data, 1 million people of internet users are added every day. The distribution of internet usage by years according to Datareportal data is given in Fig. 1. [1].

Increasing internet usage has also brought many security gaps. Many technologies such as firewall, data encryption, user authentication are used to prevent these security gaps. These security mechanisms prevent many types of attacks. However, these security technologies cannot perform in-depth packet analysis. For this reason, they cannot reach the desired level of attack detection. Intrusion Prevention System (IPS) and IDS systems have been developed to complement the shortcomings of these security mechanisms. These systems can perform deeper data analysis compared to other security systems thanks to their algorithms such as machine learning, deep learning, and artificial intelligence.

While IPS systems work as both intrusion detection and prevention mechanisms, IDS systems are used only for intrusion detection and analysis [2–4]. In this study, we focused on IDS systems.