**Intrusion Detection System:**

A system called an intrusion detection system (IDS) watches network traffic for unusual activity and issues notifications when it is seen. While an IDS's major duties are anomaly detection and reporting, certain intrusion detection systems are also equipped to respond to suspicious activity or abnormal traffic by blocking traffic coming from suspect Internet Protocol (IP) addresses. In order to catch hackers before they seriously harm a network, intrusion detection systems are employed to identify irregularities. IDSes can either be host-based or network-based. While a network-based intrusion detection system resides on the network, a host-based intrusion detection system is installed on the client computer. Systems for detecting intrusions operate by scanning for indications of previously known attacks or changes from routine behaviour. The protocol and application layers are moved up the stack to look at these alterations or abnormalities. They are capable of accurately detecting things like Domain Name System (DNS) .

**Machine learning:**

Machine learning (ML), a branch of artificial intelligence (AI), is the branch of computational science that is concerned with the analysis and interpretation of patterns and structures in data to enable learning, reasoning, and decision-making without the involvement of a human. Simply defined, machine learning enables users to send massive amounts of data into computer algorithms, which then analyze, recommend, and decide using only the supplied data. The algorithm can use the knowledge to improve its decision-making in the future if any corrections are found. The principal machine learning tasks are:Regression,Classification,Clustering,Transcription,automated translation, Analyzing anomalies, Analyses and sampling, estimation of the probability mass function and probability density.

**How to use Machine learning in Intrusion Detection System:**

Without any labeled dataset, unsupervised learning algorithms can "learn" the typical network pattern and report anomalies. It is particularly prone to false positive alarms yet is able to detect new sorts of intrusions. Thus, just one unsupervised approach, K-means clustering, is covered in the following sections. By introducing a tagged dataset and teaching a supervised machine learning model to distinguish between a normal and an attack packet in the network, we may decrease the false positives. The supervised model can recognize variations of known attacks and handle them skillfully. We'll talk about common supervised methods (Bayes Network, Random Forest, Random Tree, MLP, Decision Table).A system called an intrusion detection system (IDS) watches network traffic for unusual activity and issues notifications when it is seen.While an IDS's major duties are anomaly detection and reporting, certain intrusion detection systems are also equipped to respond to suspicious activity or abnormal traffic by blocking traffic coming from suspect Internet Protocol (IP) addresses.In order to catch hackers before they seriously harm a network, intrusion detection systems are employed to identify irregularities. IDSes can either be host-based or network-based. While a network-based intrusion detection system resides on the network, a host-based intrusion detection system is installed on the client computer.Systems for detecting intrusions operate by scanning for indications of previously known attacks or changes from routine behavior. The protocol and application layers are moved up the stack to look at these alterations or abnormalities. They are capable of accurately detecting things like Domain Name System (DNS) .

**Machine learning:**

Machine learning (ML), a branch of artificial intelligence (AI), is the branch of computational science that is concerned with the analysis and interpretation of patterns and structures in data to enable learning, reasoning, and decision-making without the involvement of a human. Simply defined, machine learning enables users to send massive amounts of data into computer algorithms, which then analyze, recommend, and decide using only the supplied data. The algorithm can use the knowledge to improve its decision-making in the future if any corrections are found.The principal machine learning tasks are:Regression,Classification,Clustering,Transcription,automated translation,Analyzing anomalies,Analyses and sampling,estimation of the probability mass function and probability density.

How to use Machine learning in Intrusion Detection System:

Without any labeled dataset, unsupervised learning algorithms can "learn" the typical network pattern and report anomalies. It is particularly prone to false positive alarms yet is able to detect new sorts of intrusions. Thus, just one unsupervised approach, K-means clustering, is covered in the following sections. By introducing a tagged dataset and teaching a supervised machine learning model to distinguish between a normal and an attack packet in the network, we may decrease the false positives. The supervised model can recognize variations of known attacks and handle them skillfully. We'll talk about common supervised methods (Bayes Network, Random Forest, Random Tree, MLP, Decision Table).