**Vulnerability and Exploitation Identification in IoT Networks using artificial intelligence and machine learning**

Cyber-attacks have become more widespread and a few attacks have made feature news over the previous decade, focusing on organizations and government organizations. These attacks have caused considerable financial losses and had the option to prevent the activity of governmental organizations. Moreover, since the Internet of Things (IoT) have arisen, the quantity of devices associated with the Internet is expanding quickly and turning out to be obvious objectives for Cyber-attacks. To relieve Cyber-attacks, cyber security analysts intensely rely on Intrusion Detection Systems (IDSs) that can identify maliciously activities by coordinating examples of matching patterns or noticing different activities.

 The proposed research target building up a basically deployable network protection answer for below cyber threats. There are a few issues inside the Cyber security field can be solved by utilizing A.I techniques. For example,

1-Network Intrusion Detection System (IDS):

How to characterize the organizational conduct of the client into normal behavior or attack?

The most effective method to improve the order exactness of the peculiar location is a sort of IDS. For this situation, can apply any AI models (i.e., classifiers) like Artificial Neural Network (ANN), Support Vector Machine (SVM), Decision Tree (DT), or Naive Bayesian Classifier (NBC).

The new exploration papers in this field attempt to upgrade the classifiers by utilizing metaheuristics, for instance, an algorithm used to prepare ANN (i.e., finding loads of the hubs), or finding the ideal boundaries for SVM..

One more examination subject was A.I can be utilized to upgrade IDS, by choosing the most significant highlights in the IDS dataset (i.e., NSL or KDD data set). This issue is called Feature Selection Problem. The element choice essentially relies upon one significant inquiry which is, How to choose the base number of highlights which upgrade the grouping exactness?

2-Email or SMS spam filtering.

The most effective method to order the messages or the SMS text into spam and not spam? In this issue, A.I or AI models can be applied precisely the same as the past issue.

3-Malware recognition issue. Same as the past focuses.

4- Intelligent Anti-virus softwares.