Machine learning can help cyber experts in rectifying threats easily

Cybersecurity is the most vital part of any company. It helps make sure that their data is safe and secure. With an increasing demand for artificial intelligence and machine learning these technologies are also transforming the cybersecurity space. Machine learning has many applications in Cybersecurity such as identifying cyber threats, combating cybercrime, and improving available antivirus software using AI capabilities. So, let's see what are the applications of machine learning in cybersecurity.

1 Identifying the Cyber Threats

As cybersecurity plays a critical role in finding out if any cyber threats have entered the systems. The most difficult task of cybersecurity is finding out if the connection requests into the system if any suspicious activities such as sending or receiving data can also lead to the threat. This is where machine learning can help in providing a lot of help to professionals in detecting cyber threats. A cyber threat identification system that is powered by AI can also be used to keep an eye on incoming calls and monitoring systems.

2 AI-Based Antivirus Software

Before using any system, it is highly recommended to install Antivirus as it protects the system from scanning any new files on the network if they might match with any malware signature. Antivirus software which

is integrated with machine learning can identify any kind of virus and thereby alert the user about it.

3 User Behaviour Modelling

There might be some cyber threats that can attack a company and steal the login credentials of any of its users. This can create a lot of issues of stealing data without anyone knowing. Machine learning algorithms can be trained to identify the behaviour of each user such as their login and logout patterns and can alert the cybersecurity team if there are any issues.

4 Combating AI Threats

As many hackers are taking advantage of the technology, machine learning can be used to find the holes where cybersecurity issues are detected. Companies need to use machine learning for cybersecurity purposes too. This can also become a standard protocol for defending against cyberattacks.

5 Monitoring Emails

It is vital to keep an eye on the official Email accounts of the employees to prevent any kind of cyberattacks. For instance, phishing attacks are commonly caused through emails to employees and asking them for any sensitive content. Cybersecurity software along with machine learning can be used to avoid these kinds of attacks. Natural language processing can also be used to scan emails for any suspicious behaviours.

6 To Analyse Mobile Endpoints

Machine learning is already going mainstream on mobile devices and is also driving voice-based experiences on mobile assistants. So using machine learning, one can identify and analyse threats against mobile endpoints while the enterprise is seeing a chance to protect the growing number of mobile devices.

7 Enhances Human Analysis

Machine learning in cybersecurity can help humans to detect malicious attacks, endpoint protection, analyse the network, and vulnerability assessments. Through this, humans can decide on things better by bringing out ways and means to find the solutions to the problems.

8 To Automate Tasks

The main benefit of machine learning is to automate repetitive tasks that can enable staff to focus on even more important work. There are a few cybersecurity tasks that can be automated with the help of machine learning. By incorporating ML into the tasks, organizations can accomplish tasks faster and better.

9 WebShell

WebShell is a piece of code that is maliciously loaded into a website to provide access to make modifications on the Webroot of the server. This allows attackers to gain access to the database. Machine learning can help in detecting the normal shopping cart behaviour and the model can be trained to differentiate between normal and malicious behaviour.

10 Network Risk Scoring

Machine learning can be used to analyse previous cyber-attack datasets and determine what areas of the network are mostly involved in particular attacks. This can help in scoring the attack with respect to a given network area.