Can AI Be the Answer to Data Protection and Private Security ?

Devolutions

THIS ARTICLE WRITTEN BY PAULINE FARRIS, FREELANCE WRITER AND TRANSLATOR, IS PART OF OUR GUEST BLOG SERIES.

PLEASE CONTACT US IF YOU WOULD LIKE TO BE FEATURED ON OUR BLOG.

AI – The Potential Answer to Enterprise, Government, and Personal Security

The beauty of AI lies in its ability to learn from previous data. And it uses that previous data to make recommendations and predictions.

Financial enterprises and insurance companies are already using AI to make decisions about the risk levels of potential borrowers and customers, and they do so by churning accumulated data from past consumer behavior.

It’s All About Risk

While AI can help identify risk for banks and insurers, there is also great potential for its use in data protection – personal, business and even government. And a great deal of that potential lies in the area of predictive analysis.

Data breaches cost an average of $3.8 million, according to a study by the Ponemon Institute. This of course has meant that large enterprises have been investing heavily in data protection, and at significant cost. In fact, it is estimated that cybersecurity will become a $170 billion-dollar industry by 2020.

AI Bridges a Gaping Hole

While businesses and even governments are investing in systems to gather intelligence data that they will need to identify security risks, they are still relying on human analysts to churn that data and detect threats. It’s not that they can’t do this. It’s that it takes time and there is a shortage of such analysts.

AI Use on a Global Scale

AI has the potential to fill this gap and to fill it better, since AI can gather larger amounts of data and communicate with other AI systems. Working in collaboration, AI systems could eventually create a powerful analytical workforce capable of predicting security threats to data. And when organizations across the globe share the data and predictions their algorithms have analyzed, security wins. The more data that is shared, the better predictive models will become.

AI on an Organizational Scale

Individual businesses face threats to their proprietary data protection, as well as the data of their customers/clients/patients. New AI technologies are now being developed that will collect and analyze employee behaviors and analyze them based upon huge data collections. Such analyses can reveal which employees are more vulnerable to cyberattacks based upon their online behaviors. This, in turn, can inform decisions about selective monitoring, focusing on suspicious emails or URLs that the employees may be accessing through their network computers.

Given that 90% of malware can only insert itself when human interaction is involved, this use of AI can be a significant value for protection.

AI and Personal Security

While AI is currently being piloted and even used by enterprises and governments, there is the potential for personal security too. Consider the following examples:

#1. The exponential increase in the use of IoT devices – whether these are personal wearables or assistants/devices in our homes that control everything from temperature to appliances – leaves us vulnerable to myriad personal security risks. AI is already being used to track our behaviors with these devices and to make recommendations based upon what we do. But at what cost? The more we use IoT, the more vulnerable we are to cyberattacks.

In response, should we consider using AI to analyze and predict when those cyberattacks may be a threat, where they may be coming from, and to alert us to the danger? There may come a day, in fact, where customizable AI algorithms will be available to all of us based upon our online behaviors and activities.

#2. Suppose you were to have a bot that could privately access all of your data and look through your calendar to determine where you might be traveling overseas for business purposes. And suppose that bot could intelligently remove sensitive information/data from your devices based upon the risk threat of where you were going. Not that the data would be gone. It would be accessible through other virtual means, but "unavailable" to others when you're using risky networks.

Here's a more concrete example. Perhaps you have a confidential contract that has been translated and is on your device as you travel to another country. Your AI algorithm knows you need to protect that contract as you enter a questionable virtual environment. And so, it removes it from your device, placing it in a secure environment until you are ready to deliver it to the right recipient.

#3. Alerts and Notifications. AI is already being used by personal investing apps. Your investment behaviors and risk tolerance are being "learned" by that app, so that you can receive alerts, notifications, and recommendations in real time to help you make quick decisions. There is no reason why, in the future, you cannot have a personal AI app that will provide risk alerts when your personal information becomes vulnerable. Further, it will monitor your online behavior and provide predictive analyses to prevent you from engaging in risky behavior.

A Perfect Fit?

While it will take time for data sets to grow and anomalies to be eliminated, AI will continue to develop more knowledge and processing skills. As AI learns to analyze when and how cyberattacks are successful, it will begin to detect conditions under which they occur. And it will then be able to detect and predict public, business, and personal risks before we are ever able to see them. AI and security, indeed, seem to be a perfect match.