4N6 Cyber Resilience Internship

ASSIGNMENT(Set-2)

Artificial Intelligence in Cybersecurity

AI has made some inroads in the cybersecurity sector and several AI vendors claim to have launched products that use AI to help safeguard against cyber threats. At Emerj, we've seen many cybersecurity vendors offering AI and machine learning-based products to help identify and deal with cyber threats. Even the Pentagon created the Joint Artificial Intelligence Center (JAIC) to upgrade to AI-enabled capabilities in their cybersecurity efforts.

In this article, we list out some of the more common use-cases for AI in cybersecurity, where there has been some evidence of real-world business use. Specifically, we cover:

- AI for Network Threat Identification
- AI Email Monitoring
- AI-based Antivirus Software
- AI-based User Behavior Modeling
- AI For Fighting AI Threats

We begin our analysis of AI in the cybersecurity space with an explanation for why AI is such a good fit for cybersecurity.

The Natural Fit for Artificial Intelligence in Cybersecurity

For a business safeguarding their data, network security is critical, and even small data centers might have hundreds of applications running, each of which need to have different security policies enforced. Human experts

might take several days to weeks to fully understand these policies and make sure the security implementation is successful.

Cybersecurity inherently involves repetitiveness and tediousness. This is because identification and assessment of cyberthreats require scouring through large volumes of data and looking for anomalous data points. Companies can use the data collected by their existing rules-based network security software to train AI algorithms towards identifying new cyberthreats.

Understanding the consequences of the attack and the response needed from the company also requires further data analysis. AI algorithms can be trained to take certain predefined steps in the event of an attack and over time can learn what the most ideal response should be through input from cybersecurity subject-matter experts.

Human security experts cannot match the speed and scale at which AI software can accomplish these data analysis tasks. Additionally, AI-based cybersecurity data analysis software can complete the task with consistently higher accuracy than human analysts. Large-scale data analysis and anomaly detection are some of the areas where AI might add value today in cybersecurity.

Many cybersecurity intrusions usually operate over the enterprise network monitoring the data going in and out of the network is one way to detect cybersecurity threats. Monitoring each ‘packet’ of data that is part of the enterprise networks communications is almost impossible for human analysts to monitor accurately.

Machine learning-based software can potentially use multiple techniques such as statistical analysis, keyword matching, and anomaly detection to determine if a given packet of data is different enough from the baseline of data packets used in the training dataset.

All of this seems to indicate that artificial intelligence is now starting to be seen as an effective tool to gain serious advantages against fraudsters and hackers.

AI for Network Threat Identification

Enterprise network security is critical for most companies, and the hardest part about establishing good network cybersecurity processes is understanding all the various elements involved in the network topography.

For human cybersecurity experts, this means time-consuming work in tracking all the communications going in and out of the enterprise network.

Managing the security of these enterprise networks involves identifying which connection requests are legitimate and which are attempting unusual connection behavior, such as sending and receiving large volumes of data or having unusual programs running after connection to an enterprise network.

The challenge for cybersecurity experts lies in identifying which parts of an application, whether on the web, mobile platforms, or applications that are in development or testing, might be malicious. Identifying the malicious applications amongst thousands of similar programs in a large-scale enterprise network requires enormous amounts of time and human experts are not always accurate.

AI-based network security software can potentially monitor all incoming and outgoing network traffic in order to identify any suspicious or out of the ordinary patterns in the traffic data. The data in question here is usually too voluminous for human cybersecurity experts to accurately classify threat incidents.

In a real-world example, the startup ShieldX Networks claims they use AI to speed up the process of identifying which security policies are applicable for each application. In addition, the company claims their software can study the network communications data for each application over a period of time and then generate suggestions for security policy for that application.

Apart from this, in the banking sector AI vendors such as Versive (now acquired by eSentire) offer enterprise cybersecurity AI software that use anomaly detection to identify network security threats. The company claims their software can help financial firms and banks with adversary detection and cybersecurity threat management.

AI vendor Versive (now acquired by eSentire) offers enterprise cybersecurity AI software called the VSE Versive Security Engine, which they claim can help banks and financial institutions analyze large datasets of transactions and cybersecurity-related data using machine learning.

Versive claims banks NetFlow (network protocol developed by Cisco for collecting IP traffic information and monitoring network traffic), proxy, DNS data (computer network data) as inputs to the Versive Security Engine. The

software can then monitor enterprise networks using anomaly detection to alert human officers in case of deviations in the data that might be similar to events in past cyberthreats.

AI Email Monitoring

Enterprise firms understand the importance of monitoring email communications in order to prevent cybersecurity hacking attempts such as phishing. Machine learning-based monitoring software is now being used to help improve the detection accuracy and the speed of identifying cyberthreats.

Several different AI technologies are being used for this use-case. For instance, some software use computer vision to “view” emails to see if there are features in the email that might be indicative of threats, such as images of a certain size. In other cases, natural language processing is used to read through the text in emails coming in and going out of the organization and identify phrases or patterns in text that are associated with phishing attempts. Using anomaly detection software can help identify if the email’s sender, recipient, body, or attachments are threats.

This use-case again highlights AI’s strengths with large scale data analysis. It is not difficult for a human employee to read through an email and identify suspicious features, but doing so for millions of emails sent and received within large organizations on a day-to-day basis is simply impossible. AI software can instead read through all the incoming and outgoing emails and report the most likely cases of cybersecurity threats to security personnel.

For instance, Tessian claims to provide email monitoring AI software that can help financial firms prevent misdirected emails, prevent data breaches and phishing attacks. The company’s software likely uses natural language processing and anomaly detection in different steps in order to identify which emails are likely cybersecurity threats.

AI-based Antivirus Software

Traditional antivirus software function by scanning files on an enterprise network to see if any of them match the signature of known malware or viruses. The problem with this approach is that it is dependent on security updates for the antivirus software when new viruses are discovered. Additionally, this method makes traditional antivirus software slow in terms

of real-time threat detection and makes deploying a scalable system challenging.

In contrast, AI-based antivirus software in many cases uses anomaly detection to study program behavior. Antivirus systems using AI focus on detecting unusual behavior generated by programs rather than matching signatures of known malware.

While traditional antivirus software works well for threats that have been previously encountered and identified through its public signature, new threats are not easily detected and resolved by these types of software. Steve Grobman, SVP at McAfee claims that most traditional antivirus software can achieve a 90% threat detection rate. The added advantage that AI brings to the table in this use-case is in increasing the threat detection rate to even 95% or above.

Cylance, which was acquired by Blackberry, claims their Smart Antivirus product offering uses AI to predict, detect and respond to cybersecurity threats. The company claims that unlike traditional antivirus software, Cylance's AI-enhanced Smart Antivirus does not need virus signature updates but rather learns to identify patterns that indicate malicious programs from scratch over time.

AI-based User Behavior Modeling

Some types of cybersecurity attacks on enterprise systems can compromise specific users in the organization by taking over their login credentials without their knowledge. Cyberattackers who have stolen a user's credentials can gain access to an enterprise network through technically-legitimate means and are thus hard to detect and stop. AI-based cybersecurity systems can be used to detect a pattern of behavior for particular users in order to identify changes in those patterns. In doing so, they can alert security teams when that pattern is broken.

AI vendors such as Darktrace offer cybersecurity software that they claim uses machine learning to analyze raw network traffic data to understand the baseline of what normal behavior is for each user and device in an organization. Using training datasets and inputs from subject-matter experts, the software learns to identify what constitutes a significant deviation from the normal baseline behavior and immediately alert the organization to cyber threats.

AI For Fighting AI Threats

Companies need to improve the speed at which they detect cyberthreats because hackers are now employing AI to potentially discover points of entry in enterprise networks. Thus, deploying AI software to guard against AI-augmented hacking attempts might become a necessary part of cybersecurity defense protocols in the future.

In the past couple of years, companies around the world have succumbed to cyberthreats and ransomware attacks such as WannaCry and NotPetya. These types of attacks spread rapidly and affect a large number of computers. It's likely that the perpetrators of these types of attacks might use AI technology in the future. The advantage that AI could give these hackers is similar to what AI offers in businesses: rapid scalability.

Cybersecurity Vendor Crowdstrike claims their security software, Falcon Platform, uses AI to guard against such ransomware threats. The software reportedly uses anomaly detection for end-point security in enterprise networks. The video below demonstrates how the software works:

The Future of AI in Cybersecurity

AI-use in cybersecurity systems can still be termed as nascent at the moment. Businesses need to ensure that their systems are being trained with inputs from cybersecurity experts which will make the software better at identifying true cyber attacks with far more accuracy than traditional cybersecurity systems.

Businesses need to understand that these systems are only as good as the data that is being fed to them. AI systems are usually famously touted to be "garbage in, garbage out" systems, and a data-centric approach to AI projects is necessary for continued success.

The one challenge for companies using purely AI-based cybersecurity detection methods is to reduce the number of false-positive detections. This might potentially get easier to do as the software learns what has been tagged as false positive reports. Once a baseline of behavior has been constructed, the algorithms can flag statistically significant deviations as anomalies and alert security analysts that further investigation is required.

Cybersecurity applications are among the most popular AI applications today. This is in large part due to the fact that these applications rely on anomaly detection which machine learning models are very well suited for.

Additionally, most large businesses might already have existing cybersecurity teams, product development budgets and IT infrastructure to handle large amounts of data.

As cyberattacks grow in volume and complexity, artificial intelligence (AI) is helping under-resourced security operations analysts stay ahead of threats. Curating threat intelligence from millions of research papers, blogs and news stories, AI provides instant insights to help you fight through the noise of thousands of daily alerts, drastically reducing response times.

Watch the video to hear Kevin Skapinetz, IBM Security vice president of strategy and design, explain how advanced AI can act as an advisor to analysts, helping them quickly identify and connect the dots between threats

Use cases for AI and ML in cyber security

As cyber attacks get more diverse in nature and targets, it's essential that cyber security staff have the right visibility to determine how to solve vulnerabilities accordingly, and AI can help to come up with problems that its human colleagues can't alone.

"Cyber security resembles a game of chess," said Greg Day, chief security officer EMEA at Palo Alto Networks. "The adversary looks to outmanoeuvre the victim, the victim aims to stop and block the adversary's attack. Data is the king and the ultimate prize.

"In 1996, an AI chess system, Deep Blue, won its first game against world champion, Garry Kasparov. It's become clear that AI can both programmatically think broader, faster and further outside the norms, and that's true of many of its applications in cyber security now too."

With this in mind, we explore particular use cases for AI in cyber security that are in place today.

Working alongside staff
Day went on to expand on how AI can work alongside cyber security staff in order to keep the organisation secure.

"We all know there aren't enough cyber security staff in the market, so AI can help to fill the gap," he said. "Machine learning, a form of AI, can read the input from SoC analysts and transpose it into a database, which becomes ever expanding.

"The next time the SoC analyst enters similar symptoms they are presented with previous similar cases along with the solutions, based on both statistical analysis and the use of neural nets – reducing the human effort.

“If there’s no previous case, the AI can analyse the characteristics of the incident and suggest which SoC engineers would be the strongest team to solve the problem based on past experiences.

“All of this is effectively a bot, an automated process that combines human knowledge with digital learning to give a more effective hybrid solution.”

Battling bots

Mark Greenwood, head of data science at Netacea, delved into the benefits of bots within cyber security, keeping in mind that companies must distinguish good from bad.

“Today, bots make up the majority of all internet traffic,” explained Greenwood. “And most of them are dangerous. From account takeovers using stolen credentials to fake account creation and fraud, they pose a real cyber security threat.

“But businesses can’t fight automated threats with human responses alone. They must employ AI and machine learning if they’re serious about tackling the ‘bot problem’. Why? Because to truly differentiate between good bots (such as search engine scrapers), bad bots and humans, businesses must use AI and machine learning to build a comprehensive understanding of their website traffic.

“It’s necessary to ingest and analyse a vast amount of data and AI makes that possible, while taking a machine learning approach allows cyber security teams to adapt their technology to a constantly shifting landscape.

“By looking at behavioural patterns, businesses will get answers to the questions ‘what does an average user journey look like’ and ‘what does a risky unusual journey look like’. From here, we can unpick the intent of their website traffic, getting and staying ahead of the bad bots.”

Endpoint protection

When considering certain aspects of cyber security that can benefit from the technology, Tim Brown, vice-president of security architecture at SolarWinds says that AI can play a role in protecting endpoints. This is becoming ever the more important as the amount of remote devices used for work rises.

“By following best practice advice and staying current with patches and other updates, an organisation can be reactive and protect against threats,” said Brown. “But AI may give IT and security professionals an advantage against cyber criminals.

“Antivirus (AV) versus AI-driven endpoint protection is one such example; AV solutions often work based on signatures, and it’s necessary to keep up with signature definitions to stay protected against the latest threats. This can be a problem if virus definitions fall behind, either because of a failure to update or a lack of knowledge from the AV vendor. If a new, previously unseen ransomware strain is used to attack a business, signature protection won’t be able to catch it.

“AI-driven endpoint protection takes a different tack, by establishing a baseline of behaviour for the endpoint through a repeated training process. If something out of

the ordinary occurs, AI can flag it and take action — whether that's sending a notification to a technician or even reverting to a safe state after a ransomware attack. This provides proactive protection against threats, rather than waiting for signature updates.

"The AI model has proven itself to be more effective than traditional AV. For many of the small/midsize companies an MSP serves, the cost of AI-driven endpoint protection is typically for a small number of devices and therefore should be of less concern. The other thing to consider is how much cleaning up costs after infection — if AI-driven solutions help to avoid potential infection, it can pay for itself by avoiding clean-up costs and in turn, creating higher customer satisfaction."

Machine learning versus SMS scams

With more employees working from home, and possibly using their personal devices to complete tasks and collaborate with colleagues more often, it's important to be wary of scams that are afoot within text messages.

"With malicious actors recently diversifying their attack vectors, using Covid-19 as bait in SMS phishing scams, organisations are under a lot of pressure to bolster their defences," said Brian Foster, senior vice-president of product management at MobileIron.

"To protect devices and data from these advanced attacks, the use of machine learning in mobile threat defence (MTD) and other forms of managed threat detection continues to evolve as a highly effective security approach.

"Machine learning models can be trained to instantly identify and protect against potentially harmful activity, including unknown and zero-day threats that other solutions can't detect in time. Just as important, when machine learning-based MTD is deployed through a unified endpoint management (UEM) platform, it can augment the foundational security provided by UEM to support a layered enterprise mobile security strategy.

"Machine learning is a powerful, yet unobtrusive, technology that continually monitors application and user behaviour over time so it can identify the difference between normal and abnormal behaviour. Targeted attacks usually produce a very subtle change in the device and most of them are invisible to a human analyst. Sometimes detection is only possible by correlating thousands of device parameters through machine learning."

Hurdles to overcome

These use cases and more demonstrate the viability of AI and cyber security staff effectively uniting. However, Mike MacIntyre, vice-president of product at Panaseer, believes that the space still has hurdles to overcome in order for this to really come to fruition.

"AI certainly has a lot of promise but as an industry we must be clear that its currently not a silver bullet that will alleviate all cyber security challenges and address the skills shortage," said MacIntyre. "This is because AI is currently just a term applied to a small subset of machine learning techniques. Much of the hype

surrounding AI comes from how enterprise security products have adopted the term and the misconception (willful or otherwise) about what constitutes AI.

“The algorithms embedded in many modern security products could, at best, be called narrow, or weak, AI; they perform highly specialised tasks in a single, narrow field and have been trained on large volumes of data, specific to a single domain. This is a far cry from general, or strong, AI, which is a system that can perform any generalised task and answer questions across multiple domains. Who knows how far away such a system is (there is much debate ranging from the next decade to never), but no CISO should be factoring such a tool in to their three-to-five year strategy.

“Another key hurdle that is hindering the effectiveness of AI is the problem of data integrity. There is no point deploying an AI product if you can’t get access to the relevant data feeds or aren’t willing to install something on your network. The future for security is data-driven, but we are a long way from AI products following through on the promises of their marketing hype.”