Applications of Artificial Intelligence in Cyber Security

Shreyash Mahadik[1] Prajakta Khatal[2] Shalaka Mahadik[3]
[1,2,3]Student
[1,2,3]Department of Computer Engineering
[1,2,3]MGM'sCET, Navi Mumbai, India

Abstract— The growing and evolving cyber security risk facing global businesses can be stemmed by the integration of AI into security systems. The main focus of this paper is the improvement of cyber security with various uses of artificial intelligence and machine learning. And machine learning can help IT security professionals to achieve cyber hygiene and enforce least privilege environments at scale. The purpose of this paper is to shed light on current trends and applications, in industry and government, at the intersection of artificial intelligence and the security field. In addition to a spotlight on current uses, we also touch on up-and-coming applications and room for innovation.
Key words: Artificial Intelligence, Cyber Security

I. INTRODUCTION

While security as a percentage of IT spend continues to grow at a robust rate, the cost of security violation is growing even faster.

Organizations are spending close to $110 billion on a dizzying array of security products. In fact, it is not uncommon for CISO organizations to have 35 to 45 security products in their environment. However, if you ask chief information security officers how they feel about their security risk, they will express concerns over being highly reveal and unprotected.

Artificial intelligence (AI) and machine learning (ML) can offer IT security professionals a way to enforce good cyber security practices and shrink the attack surface instead of constantly chasing after malevolent activity.

Machine learning techniques such as unrestricted learning and continuous retraining can keep us ahead of the hackers. However, script kiddie aren't resting on their laurels. Let's give our threat researchers the time to creatively think about the next attack vector while enhancing their abilities with machines.

II. ROLE OF AI IN CYBER SECURITY

Evolving technologies and the growing numbers of "always on", "always connected" devices, tools and products are giving the instigators of cyber-threats increased opportunities for access and interference.

With statistics suggesting that assaults on individuals, corporations, and government bodies account for almost $350 billion in lost revenue annually, and some 92% of companies admitting to having been victim to some kind of attack – figures that translate to 20 individuals per second being affected by cyber-crime – countering these threats is a real and ongoing concern, for enterprises.

Security individuals are finding themselves overwhelmed by the multiplicity of attack vectors and tools available to the cyber-criminals, and are increasingly looking to a new ally, in the quest for cyber security: AI Machine learning and artificial intelligence (AI) are being applied more broadly across industries and applications than ever before as computing power, data collection and storage capabilities increase. This vast trove of data is valuable fodder for AI, which can process and analyze everything captured to understand new trends and details.

III. APPLICATIONS OF AI IN CYBER SECURITY

There is lot of buzz around analytics in cyber security. You can look at the use of analytics in cyber security from 3 different perspectives, based on the sources of data on which analytics is being applied, based on machine learning methods being used or based on calculated end results to be achieved.

A. Based on Data Sources

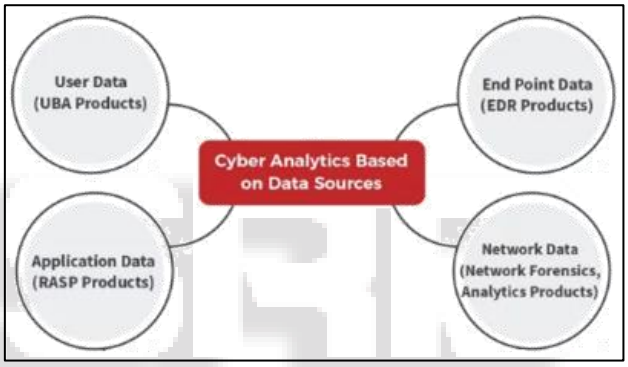

Fig. 1: Cyber Analytics based on Data Sources

If you are more disposed towards logs, security events and data, you may find classifying analytics based on types of data sources more purposeful. In fact, the security companies currently describes analytics mostly from this perspective. See the Figure 1 above.

B. Based on Machine Learning Methods:

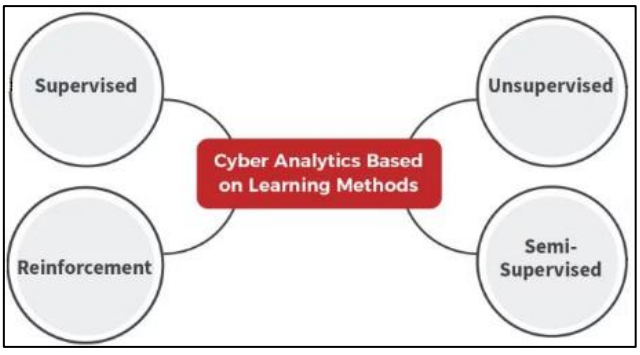

Fig. 2. Cyber Analytics based on Machine Learning methods

There is another method to categorize the machine learning models above, which is supervised learning where machine learns from past data that humans have already labeled as good or bad, attack or false positive, double-dealing or normal data, individually learning where no past labeled data exist or reinforcement learning where machine learns from

All rights reserved by *www.ijsrd.com*

feedback from its longer-term results. Supervised learning will contain classification, regression and deep learning. Unsupervised learning contain clustering, association rules and pattern matching algorithm. Figure 2 illustrates Learning methods.

We can illustrate with some use cases. Spam filtering and phishing detection uses Bayesian techniques for categorizing good versus spam mails. Fraud detection uses neural networks, data mining and decision trees for deciding on frauds. Detecting insider threats like abnormal user access or data ex-filtration uses clustering techniques. Bots can be detected through selective information function use for detecting machine to machine communication patterns. Association analysis can show attacker groups that are using similar attack methods in your network.

C. Based on End Objective of Analytics

Many of the current activity tools and analytics products like EDR and network forensics are good examples of diagnostic and detective analytics. IBM Watson is an example of normative analytics because it pulls together related information from global sources to guide an analyst when handling an incident. User and entity behavior tools can provide prognostic analytics based on past risk behaviors.

If you are concentrated on business results, you may find classifying analytics based on end objectives more purposeful. See Fig 4 below.

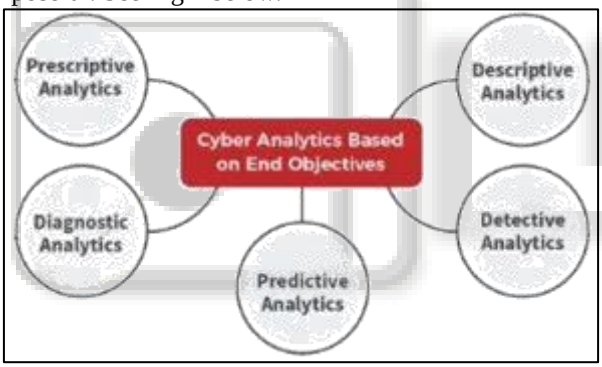

Fig. 3: Cyber Analytics based on End Objectives

AI will minimize false positives. It will augment rules-based detection systems with the machine learning methods of clustering, pattern matching, association rules, and data visualization.

D. Other Applications of AI in Cyber Security Solutions

It is up to human imagination. For the interest of clarity, following application categories can be examined:

1) Spam Filter Applications
2) Network Intrusion Detection and Prevention
3) Fraud detection
4) Credit scoring and next-best offers
5) Botnet Detection
6) Secure User Authentication
7) Cyber security Ratings
8) Hacking Incident Forecasting

E. Applications of AI in Malware Analysis & Detect Attacks

It's achievable to detect a software whether is a Malware or a normal software with artificial intelligence. In order to develop an artificial intelligence application that does malware detection the first thing to do is to determine some typical features. In addition of some unoffending software and some malware to those features, the system is trained.

There are flock of academic researches about detecting cyber-attacks using artificial intelligence. The prosperity rate of those researches varies between 85% and 99%.

In the last few years, in addition to academic researches, some products have been reinforced to detect cyber-attacks with the help of artificial intelligence like Dark Trace. Dark Trace claims to have more than 99% of success rate and it also has a very low rate of false positives.

Dark trace claims to be able to catch network attacks without the use of rules, using Machine Learning techniques that grant real-time detection. They benefit particularly from Unsupervised ML techniques, which grant the ability to catch unknown threats due to the fact that the learning is not based on known datasets, rules, or models, allowing the computer to self-learn patterns of normality and abnormal behaviour.

IV. AI AS CYBER SECURITY TOOL

AI involves computer algorithms, software programs that mimic the human knowledge to learn, interpret patterns and make predictions.

Artificial intelligence should modify computer security tools by speeding up incident responses once malicious software is detected on computer networks. It could help thwart email-delivered ransom ware or buzz botnets that knock out access to websites.

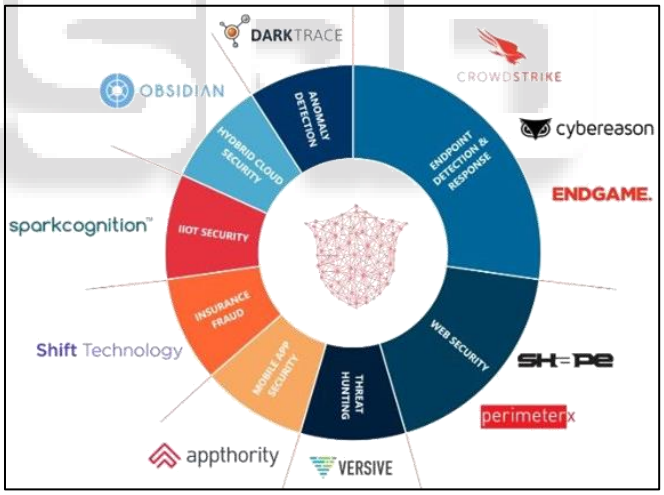

Fig. 4: Cyber Security AI Start-Ups

"There's a possibility for AI to level the playing field," Oltsik said. "One of the impractical uses for AI and machine learning is to automate the response side." Machine learning is the type of AI used most often in cyber security.

V. FUTURE OF AI IN CYBER SECURITY

We've never faced more varied and far-reaching cyber-attacks than we have today. What's worse is that these attacks are becoming more common, more sophisticated, and more impactful. When you add a drop cyber security workforce into the mix, the outlook isn't great.

However, AI systems can help resolve some of those problems and ultimately give your business an advantage when facing a cyber-attack.

All rights reserved by *www.ijsrd.com*

Cyber security solutions that depend on AI can use existing data to handle new generations of malware and cyber security attacks.

The IT market has, a tendency to quickly assimilate buzz words pushed by marketing departments. During the last years, technologies such as Big Data, Cloud Computing, Artificial Intelligence, etc., have been repeated again and again in multiple forums, in many cases without a clear understanding of their significance or their application to solving real problems effectively. It's a known fact that when humans don't completely understand a technology, two kinds of effects usually occur: either the technology is irrationally rejected (e.g. new operating systems) or, if it's properly marketed, it's assumed to be the silver bullet capable of solving every problem (Artificial Intelligence). It usually takes some time, even years, for the dust to settle down and for the market to realize the true potential of it.

The irruption of ML in in Cyber Security is forcing a paradigm shift from proactive rule-based prevention, to reactive real-time detection. Security threats have become so varied, different and smart, that traditional techniques, based on rules inferred from known attacks that stop the attack before it happens, don't seem to be a viable approach anymore. Many attacks escape these mechanisms and cause tremendous damage that can't be stopped once it has started. ML aims at identifying attacks in real-time, with little to no human interaction and stopping them before they provoke serious harm.

VI. Conclusion

We can conclude that Artificial Intelligence is not being used nowadays, as it's expected to be, to solve Network or Cyber Security problems in general. For now, only Machine Learning, a branch of AI, is being successfully applied to solve a small part of the problems. Supervised ML has delivered a number of interesting practical solutions, however, there is ongoing research, particularly towards the utilization of Unsupervised ML, as the ultimate goal is to reduce human interaction as much as possible when detecting threats. The only viable way to evolve Security and get AI closer to what it's expected to deliver is to keep investigating and find new techniques capable of providing context, expertise and enhanced data visualization, as well as achieving a tighter integration with Data Science techniques and ML-enhanced data analytics.

For cyber security, AI can analyze huge amounts of data, help right systems and software's to make decision and bring huge reductions in attacks & anomalies in much faster way. Since it can work in 24×7 without rest so humans can't beat the same. AI will allow automated software testing to find and kill bugs before they ship to prevent any banking opportunities on loopholes.

Cyber security is NOT just an information technology department or people in same department problem or responsibility. It is the job of every employee and even customers of the company. As per google search engine identities are being stolen online every 4 seconds 24/7. So what are we doing, how can we protect it. GDPR makes it even more relevant. There are organization; which has affected by the cyber-attacks, or about to suffer and may have suffered but don't know. To find better answers on this we need AI techniques to get over this. Understanding the Relationship between AI and Cybersecurity that is essential need for all is the key to success in business today.

References

[1] Harini M Rajan, Dharani S, "ARTIFICIAL INTELLIGENCE IN CYBER SECURITY – AN INVESTIGATION (PDF)", Vol.04, September 2017.
[2] Selma Dilek, Hüseyin Çakır and Mustafa Aydın "APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNIQUES TO COMBATING CYBER CRIMES: A REVIEW", Vol.06, 1, January 2015.
[3] Enn Tyugu, "Artificial Intelligence in Cyber Defense", Vol.01, January 2011.
[4] Jennifer Robinson, "Artificial Intelligence for Cyber Security". Vol.01, February 2018.
[5] Alberto Perez Veiga, "Applications of Artificial Intelligence (AI) to Network Security", Vol.04, March 2018.
[6] Arockia Panimalar, Giri Pai, Salman Khan, "ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY", Vol.05, March 2018.
[7] Amit Rajbanshi, Shuvam Bhimrajka, C. K. Raina, "Artificial Intelligence in Cyber Security", Vol.02, June 2017.
[8] Alice Silde, "ARTIFICIAL INTELLIGENCE ON THE HORIZON OF CYBER SECURITY", Vol.01, October 2017.
[9] Ranjeev Mittu & William F. Lawless, "Human Factors in Cybersecurity and the Role for AI", Vol.02, February 2015.
[10] Staffan Truvé, "Machine Learning in Cyber Security: Age of the Centaurs", Vol.01, September 2013.
[11] Swapnil Ramesh Kumbhar, "An Overview on Use of Artificial Intelligence Techniques in Effective Security Management", Vol. 2, September 2014.
[12] Carl E. Landwehr, "Cybersecurity & Artificial Intelligence", Vol.01, April 2007.

All rights reserved by *www.ijsrd.com*