Global Journal on Innovation, Opportunities and Challenges in AAI and Machine Learning
Vol. 4, Issue 1 – 2020
ISSN: 2581-5156

A Data Science-Driven Approach of Machine Learning to Provide Better, Smarter, and Faster Security

Ajit C Vichare[1]
[*]*Principal Solutions Architect, Digital Supply Chain-AI, ML, RPA, Analytics, Author and Thought Leader.*
Correspondence E-mail Id: *editor@eurekajournals.com*

Introduction

Regardless of where we look in the security world today, we'll see the terms machine learning and artificial intelligence (AI). There's been a lot of enthusiasm for machine learning and AI as security merchants and their clients search for better approaches to improve their security stance and battle against progressing cyber-attacks. Machine learning and AI offer incredible approaches in taking care of issues in numerous different aspects of our lives, so it's just natural to attempt to utilize them to make comparative achievements in the field of security.

Tragically, there's a great deal of publicity and deception encompassing what machine learning and AI can do to improve security. In this paper, the author discussed the most basic aspects one has to think about applying machine learning and AI in the organization's security environment. The author also figures out how to perceive the most significant opportunities and difficulties for utilizing machine learning and AI to improve our security team's capacity to quickly recognize and react to cyber-threats.

The Evolving Need for Machine Learning, AI, and Data Science

Machine learning, artificial intelligence, and data science are terms with shifting definitions. For the motivations behind this paper, we've characterized the accompanying terms:

- **Data Science:** "*The discipline of extracting information from data. Data science is a broad field that includes machine learning*".
- **Machine Learning:** "*The science of enabling computers to learn without being explicitly programmed to do so. Machine learning applies statistics and algorithms at scale on large amounts of data. One of the goals for machine learning is to achieve artificial intelligence*".
- **Artificial Intelligence (AI)**: "*The science of enabling a computer to automate something a human would normally do that requires intelligence, analysis, and decision making*".

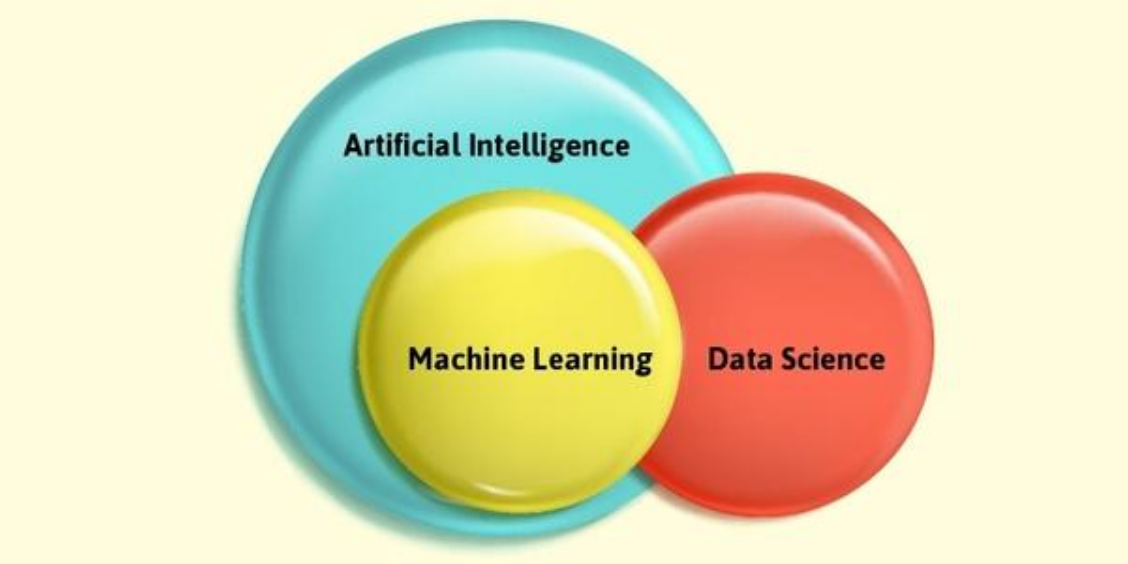

Figure 1.Machine Learning, AI, and Data Science

As the expense of storage has gone down, it has gotten progressively available for data storage needs. The processing power also increasing continuously to about two-fold every year. These advances in innovation have met up to make machine learning accessible and open to use.

Machine learning and AI have become trendy aspects of the security space. Security teams have a critical requirement for increasingly automated techniques for recognizing threats and noxious client conduct—and this need is driving expanded enthusiasm for these domains. Automation is imperative for overpowered security teams. This is on the grounds that avoidance measures are not reliable, and a significant number of the present detection techniques depend on manual investigation and dynamic to discover propelled threats, noxious client conduct, and different serious issues.

Security investigators experience enormous quantities of bogus positives and negatives. The threat surface has expanded exponentially because of the development of cell phones, cloud storage, and the Internet of Things, all of which just increment the number of bogus positives. Security teams are covered in alert exhaustion. They can't stir rapidly enough to stay aware of the movement to be examined, or they basically can't recognize emerging threats. "Unfortunately, more security doesn’t necessarily mean better security. In fact, the current strategy of most organizations, layering on many different technologies is not only proving ineffective, it is overly complex and expensive. The status quo is not sustainable,” says Keith Weiss, head of U.S. software coverage for Morgan Stanley. “Even as companies spend more on security, losses related to cybercrime have nearly doubled in the last five years.” Improving detection implies improving precision and productivity, and that requires making sense of how to make detection innovations more intelligent. That is the place AI and machine learning come into the picture.

Global Journal on Innovation, Opportunities and Challenges in AAI and Machine Learning
Vol. 4, Issue 1 – 2020
ISSN: 2581-5156

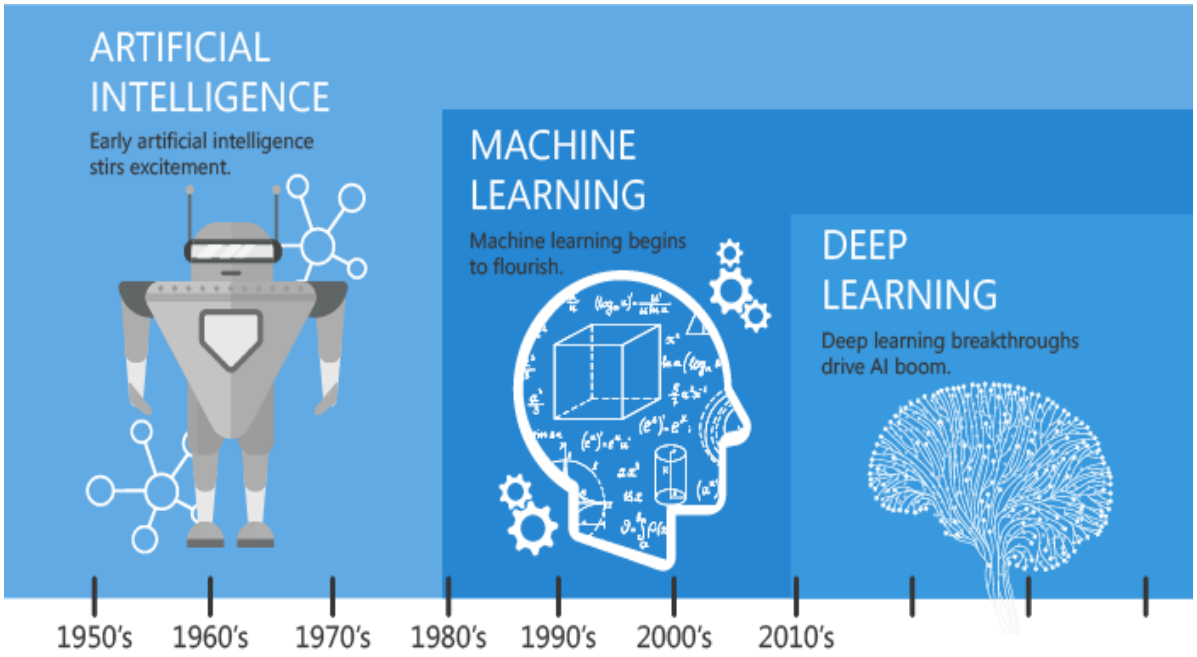

Figure 2.Artificial Intelligence, Machine learning, and Deep Learning

Machine learning offers obviously better abilities than people can convey in perceiving and anticipating specific sorts of patterns. Security advances can utilize machine learning to recognize patterns in their data, empowering them to settle on choices and to assist people with settling on choices quicker and all the more precisely.

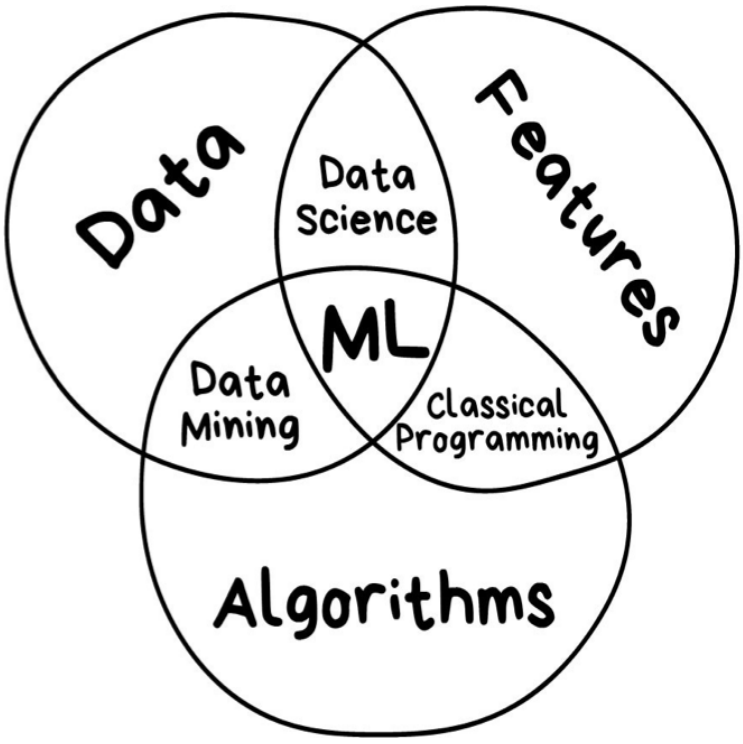

Figure 3.Machine Learning for Cybersecurity

With machine learning, security advances can likewise move past principles-based methodologies that require earlier information on known patterns. For instance, security advancements utilizing machine learning can get familiar with the run of the typical patterns of movement inside a networking environment condition to perceive pattern deviations. These departures are potentially demonstrative of threats and distinguish these threats prior to the Cyber Attack Lifecycle. This could forestall numerous incidents and decrease the effect of others by halting them sooner.

According to research done by the National Science and Technology Council (NSTC): "Utilizing AI may help keep up the quick reaction required to recognize and respond to the scene of ever-developing digital threats. There are numerous opportunities for AI, and explicitly, machine learning frameworks, to help adapt to the sheer unpredictability of the cyberspace and bolster successful human decision making in light of cyberattacks."

The viability of machine learning depends on approaching huge arrangements of top-notch, rich, organized data capturing network activities over various endpoints. The old expression "trash in/trash out" impeccably clarifies this circumstance. On the off chance that machine learning algorithms ingest data sets that aren't precise, clear, efficient, and extensive, they're not going to deliver the ideal outcomes. As such, on the grounds that there are machine learning algorithms set up doesn't really mean what they realize is astute and helpful. In the event that you show algorithms inappropriate exercises, they will convey inappropriate answers.

The Hype and the Reality about Machine Learning in Organization's Security

Ideally, machine learning would be the silver shot for vanquishing your organization's security challenges. It would empower the full automation of security tasks, wiping out the requirement for human contribution. It would realize what each client, framework, and the application does in fantastic detail, empowering quick identification and handling of client pantomime, noxious expectation, and different issues.

Figure 4.Machine Learning and Cyber Security

Applying AI to security by means of machine learning is every now and again introduced as a simple solution. It's most certainly not. As opposed to numerous merchants' cases, no product can do this viably today. Furthermore, it will probably take extensive time and advancement to achieve. Consider the similarities between a SOC that recognizes and reacts to security episodes and a misrepresentation office that utilizes extortion investigation strategies to distinguish and react to credit card misuse. Despite the fact that investigation and recognizable proof might be robotized, people are as yet required to react and recover (e.g., choosing an issue is a bogus constructive, speaking with the affected individuals, and planning activities with different organizations). The present security products can't completely mechanize the SOC and totally kill the requirement for security investigators, incident responders, and other SOC staff.

There is a gigantic measure of significant worth in applying machine learning to settling security challenges. Accomplishing AI would altogether diminish the everyday work performed by exceptionally skilled and generously compensated individuals. It would likewise make the occurrence reaction a lot quicker, powerful, effective, and precise. In any case, rather than making progress toward the unreasonable objective of having AI today, we have to make incremental progress. For example, applying machine learning pattern acknowledgment to consequently connect a threat model from about a month and a half back to a comparable one today is a practical objective.

Today, machine learning is very useful in threat detection by learning the patterns of ordinary activities and perceiving inconsistencies: the presentation or forecast of another pattern, an adjustment in a current pattern, or the expulsion of a pattern. Given the sheer volume of activities happening in the present frameworks and applications, machine learning's pattern recognition and prescient abilities have become staggeringly significant.

There is an inadequacy to machine learning, be that as it may. Alone, it comes up short on the comprehension of security setting to perceive the significance or irrelevance of every inconsistency. Machine learning can recognize that a client is acting in an atypical way; however atypical conduct isn't really fortunate or unfortunate. For instance, a client interfacing with a server just because maybe an abnormality, however, is it a malevolent demonstration?

In business analytics and different fields, machine learning functions admirably all alone because it sees peculiarity free data and needs no extra setting to anticipate patterns. In the security field, there are numerous kindhearted oddities, so the capacity to recognize inconsistencies, while significant, can't in any way, shape, or form give the entire clarification of what's occurred and empower precise forecasts of what will occur.

To successfully identify threats, you have to utilize the right algorithm for that threat type. The remainder of your devices gives the security setting and pertinence. A SIEM

arrangement can coordinate and connect data from numerous apparatuses, for example, asset management systems, human resources (HR) systems, vulnerability scanners, and identity management solutions, etc. At the point when utilized together, machine learning and different instruments create the hazard data expected to organize human activities. Without prioritization, there are such a significant number of peculiarities that it's difficult to look at them all and discover the genuinely significant ones.

Applying Machine Learning to Security

Machine learning can give numerous likely opportunities to improve your security operations, for example:

Threat Detection

- **Threat Forecast and Detection:** Dissecting peculiar movement so as to perceive developing threats so they can be halted before aggressors accomplish their expected outcomes
- **Risk Management:** Observing and analyzing client movement, resource substance and configurations, network connections, and other resource ascribes to make and keep up powerful hazard profiles for all endeavor resources
- **Vulnerability Information Prioritization:** Utilizing learned data about the organization's advantages and the vulnerabilities being effectively misused to organize their moderation
- **Threat Intelligence Curation:** Refining the data inside threat intelligence feeds to improve quality

Threat Response and Recovery

- **Event and Incident Investigation and Response:** Evaluating and analyzing data on occasions and incidents so as to recognize following stages and compose the incident reaction procedures and work process, for example, choosing and actualizing the suitable incident playbook
- **Forensics:** Enhancing existing crime scene investigation data by recognizing extra data liable to be connected and possibly worth examining
- **Deception and Misdirection:** Learning about the current condition and creating smart strategies for beguiling and misleading attackers so they won't achieve their objectives

Conclusion

Machine learning offers a lot of guarantee in improving security by enormously reducing human exertion and bringing down an opportunity to distinguish, react to, and recuperate from occurrences. Following are the few major challenges in effectively utilizing machine learning for security purpose:

- Giving machine learning real-time access to enormous sets of top-notch, rich organized data including all security-related occasions from all through the endeavor
- Providing machine learning with the logical data important to comprehend the significance and importance of each observed movement and recognized inconsistency
- Performing directed learning with extensive sets of excellent preparing data to instruct the machine on which activities are acceptable and which are awful

On the off chance that your organization is struggling to remain in front of cyber threats because of a lack of assets and the expenses of wasteful and manual work processes, machine learning could be a useful innovation for you. Machine learning could permit your analysts to concentrate on the issues that require instinct and inventiveness. It could likewise help your security activities scale as threats keep on developing.

At the point when utilized viably, machine learning could support your team:

- Detect shrouded threats and limit false positives
- Accelerate incident response
- Streamline SOC operations to lessen mean chance to distinguish and react to threats

References

1. Web Reference: http://www.morganstanley.com/ideas/cybersecurity-needs-new-paradigm.
2. Web Reference: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.
3. Tadapaneni, Narendra Rao. (2020). Artificial Intelligence Security and Its Countermeasures, *International Journal of Advanced Research in Computer Science & Technology* (2347-8446). 8. 10-12.
4. Web Reference: https://go.forrester.com/wpcontent/uploads/Forrester_Predictions_2017_Artificial_Intelligence_Will_Drive_The_Insights_Revolution.pdf.

Author Profile

Ajit C Vichare
Principal Solutions Architect, Digital Supply Chain-AI, ML, RPA, Analytics, Author and Thought Leader

Published on: 29th-May-2020

