LTIMindtree

Artificial Intelligence in Cybersecurity

How AI can help mitigate false negatives and usher in a new era of razor-sharp cybersecurity solutions

Abstract

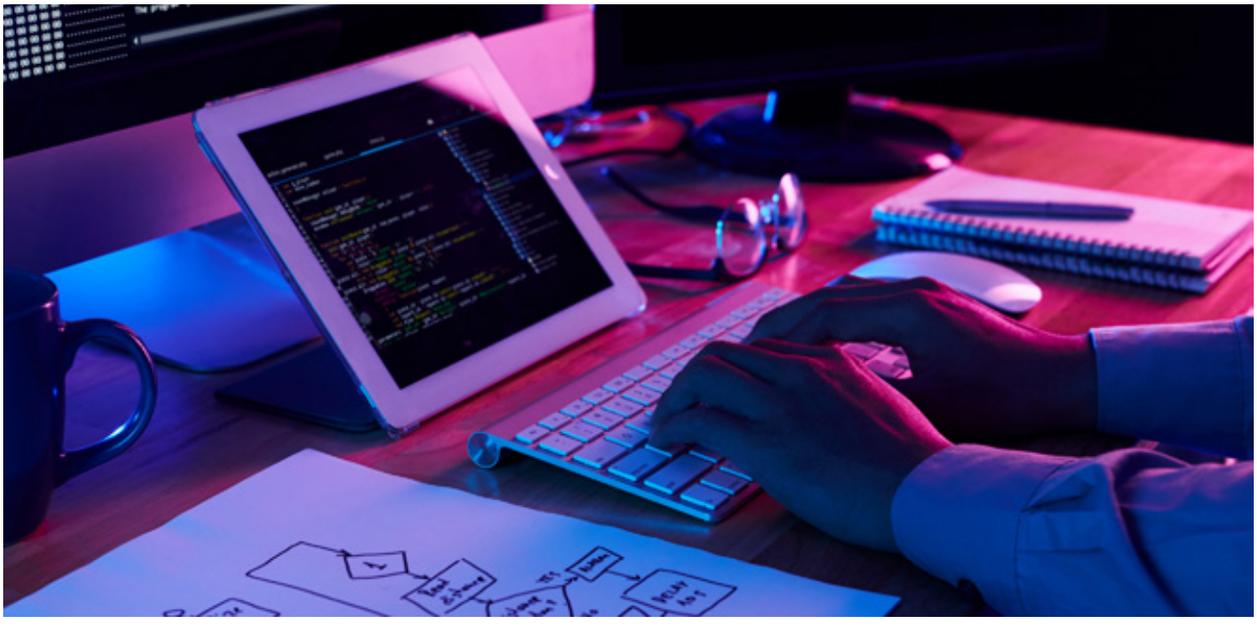
With cyber-crimes expected to cost enterprises trillions of dollars over the next few years, AI's intervention isn't just recommended – it is an urgent imperative. This paper discusses how AI and Analyst Intuition (i.e., AI^2) could help protect networks, enterprise devices, and citizens in the era of Industry 4.0. It also details three pragmatic ways to integrate AI into our security systems.

Table of Contents

Introduction

Artificial intelligence (AI) is no longer a buzzword or a futuristic technology concept, threatening to completely overhaul the world around us. Thanks to advancements in data science and sophisticated computing technologies, AI is helping to make life simpler through automation and data-driven decision-making across various industries. One area where AI's intervention is especially important today is cybersecurity.

Even as growing digital maturity paves the way for sophisticated AI, it also entails an increase in the risks around data security, personal privacy, and system infrastructure. It is estimated that cybercrime will cost enterprises $6 trillion globally by the end of 2021, growing by 15% every year until 2025[1]. This makes it a top priority for enterprises, and if overlooked, could lead to severe and lasting damage. AI is proven to be effective against most cybercrime techniques and could help detect hidden vulnerabilities that are increasingly exploited by cybercriminals. As the volume of attacks increases, these intelligent automated systems could help scale security mechanisms when manual efforts cannot keep up. For this reason, AI in the cybersecurity market is witnessing high demand, projected to reach more than $38 billion by 2026[2]. Several traits make AI ideal for cybersecurity use cases, including its ability to react to previously unknown threats, the speed of action, and the ability to recognize even the smallest changes in the surrounding environment that could signal a larger anomaly.



AI and Security: The Perfect Match

In many ways, AI is suited to security applications like no other use case, owing to its capacity for autonomous, timely, and data-driven decision-making. Combating cybersecurity threats primarily entails anticipating risks, scanning for anomalies, and taking preventive and/or proactive action. This is something AI can do very well.

Understanding the role of AI in cybersecurity

In recent years, hyper-connected workplaces and the growth of cloud and mobile technologies have multiplied existing vulnerabilities in the system. Today, it is possible for malware to spread at lightning speeds, while it is extremely difficult to trace its origin. The Internet of Things (IoT) has added to this challenge by expanding the threat vector. AI can be integrated into existing and new security systems so that its underlying models can be trained on data from historical attacks. Powered by the knowledge of previous errors and vulnerabilities that caused a risk, AI can prevent similar scenarios in the future.

The emergence of AI-based cybersecurity solutions

Across industries, there has been a rise in AI and machine learning (ML) adoption, owing to the proliferation of data and the availability of affordable computing resources. This means that AI now has the robust underlying infrastructure necessary to protect against cyberattacks without concerns around too many false positives, insufficient ROI, and implementation hassles. Enterprises realize that AI-based cybersecurity solutions can save them the cost of employing a highly skilled FTE, which could be better used for generating value.

Interestingly, this isn't a new idea. AI-based cybersecurity solutions can be traced back to early instances such as a project by the New York City Police Department, where a combination of philosophy and organizational management principles with underlying software tools was used for predictive policing. Another example is Zimperium and MobileIron, which helped organizations adopt AI-based anti-malware tools by integrating Zimperium's AI-based threat detection with MobileIron's compliance and security engine.

Envisioning the future

To realize the full potential of AI in cybersecurity, it is important to first understand the unique competencies put forward by machines and human experts. AI can enable threat hunting tools that can protect enterprise networks and end-user devices before they can be classified as threats by human researchers. On the other hand, human efforts are instrumental in shaping the analytical models and learning engines powering AI. The future of cybersecurity, therefore, lies in AI^2 – combining Analyst Intuition with Artificial Intelligence to detect the widest possible variety of attack patterns with greater accuracy. Particularly in the context of Industry 4.0 and IoT, this type of intervention is essential.

Real-World Applications of AI in Cybersecurity

AI replaces the older rules-based approach to enable predictive threat detection and intrusion prevention. This is augmented by the use of Analyst Intuition, as there are minimal false positives and humans can act fast with razor-sharp accuracy. There are three critical ways AI can integrate with enterprise cybersecurity systems:

1. Intrusion detection systems (IDS)

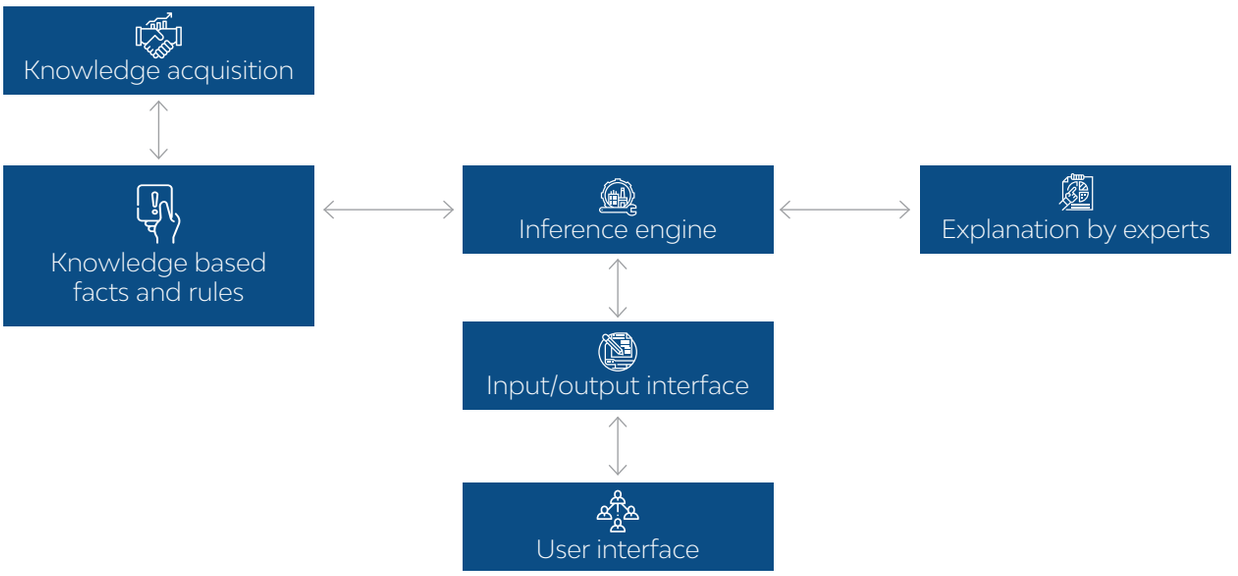
Wireless sensor networks (WSNs) have rapidly evolved in the last few years and are now a pervasive presence in our everyday lives. However, it has also resulted in an uptick in network vulnerability and threats. IDS could potentially address a wide variety of security attacks in WSN, especially when aided by AI. Also, IDS could capture firewall entities and detect malicious connectives at an approximately 95% accuracy rate. This is achieved by monitoring all network events and analyzing them for policy violations or anomalous behavior.

2. Video surveillance security

An AI program could use machine vision to analyze video feeds from a surveillance camera and match it against a database of reference images. Self-learning AI algorithms could improve this further, by delivering a solution that adapts to new imaging inputs, without requiring rules-based intervention. AI can normalize the visual data, classify objects, derive patterns, and recommend actions. Security personnel can then leverage Analyst Intuition to take timely action, but without being constrained by a human attention span. AVATAR by the United States Department of Homeland Security is an example of this approach.

3. Expert System for knowledge-based action

An Expert System is designed to capture the entire range of human knowledge and expertise around a narrowly specified domain in a machine implementable form. The architecture of an expert system is given below:



Expert System

Ideally, it will support AI technologies to make decisions at a level comparable to human experts, along with valid reasoning. As per this diagram, an expert system for cybersecurity requires a program for acquiring facts and rules of the domain (i.e., knowledge acquisition) and the central algorithm, which is the inference engine.

Conclusion

In the era of Industry 4.0, we cannot overstate the importance of maintaining the security and confidentiality of our networks and connected endpoints. The success of AI in cybersecurity hinges on the availability of "good" data, as well as powerful learning models and expert human insights. All these factors are available today, and must together power AI^2, where human knowledge and intuition and machine automation and efficiency both play an equal and compatible role.

References

1. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

2. https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-security-market-220634996.html

About the Author

Vinay Kumar
Software Engineer, LTIMindtree

Vinay Kumar specializes in developing web and iOS applications. In his current role, he works on developing Field Service workflow management applications for a global Elevator company. He holds a bachelor's degree in computer science.

About LTIMindtree

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 82,000 + talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit https://www.ltimindtree.com/.