AI DRIVEN THREAT DETECTION

By: Enoch Anbu Arasu Ponnuswamy

Digital technology has increased rapidly and this has led to an outbreak of data and connectivity, transforming the way how individuals and organizations operate. This transformation has resulted in massive benefits but they have brought in vulnerabilities which can be benefitted by malicious actors. Today's cyber threats need innovative approaches to cyber security.

Artificial Intelligence (AI) is primarily used for threat detection in Cyber security. It helps to detect, analyze and respond to cyber threats in a faster way. It is used to detect and prevent cyber threats, such as malware, phishing attacks, and intrusion attempts.

AI provides a simplified process of data analysis, data screening as well as detecting any risks.

EVOLUTION OF THREAT DETECTION

Traditional Methods of Threat Detection

Traditionally, threat detection was done with a focus either on the threat that was detected or in the tools like System Information and Event Management (SIEM) rules, Intrusion Detection System (IDS) rules, Machine Learning Models, User Entity Analytics.

Increasing Incident Surface

Organizations are following various technologies like SaaS applications, IoT devices, Cloud Computing, Remote/Hybrid working etc. due to increase in digital transformation. This helps them to increase their productivity and in turn increase customer experience. This results in an increase in the Incident surface for attackers.

Financial Implications

Organizations that operate with limited resources often find it challenging to allocate funds for efficient cyber security measures. For the ever-evolving threat landscape, it is financially difficult to implement 24x7 threat monitoring and response. This stands as a major challenge in today's competitive business landscape.

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Definitions and Types of Artificial Intelligence Technologies

Machine Learning involves developing algorithms and statistical models enabling computer systems to learn and program themselves from experiences without being explicitly programmed. It involves creating computer systems that can learn and improve on their own by analyzing data and identifying patterns, instead of being programmed to perform a specific task.

Deep Learning is a type of Machine Learning that uses neural networks to imitate the learning process of the human brain. A neural network uses machine learning and AI to teach machines how to process data in a way that is inspired by the human brain. A neural network consists of functional layers. Enclosed in these layers, certain behaviors, tasks, or processes trigger a specific response from the machine. If there are more layers within the neural network, the more expressive and sophisticated the response.

Generative AI refers to deep learning models that consume raw data and generate new outputs that are like but slightly different from the original content, including text, audio, computer code, and images.

How AI Cybersecurity Is Different

An emerging need for creative problem-solving and complex challenges in the workplace indicate that Cyber security protection with Artificial Intelligence will never replace security professionals. A distinct feature of AI is that it can assist human security professionals by analyzing vast amount of data, recognize patterns and create insights on large volume of data. Traditional security processes might take weeks to complete the same.

Traditionally used signature-based detection tools and systems are effective for known threats. They are inadequate for novel or unknown threats. They also result in a lot of false positives and security professional's wasted efforts.

Manual Analysis of security events and event logs are required for traditional cyber security in search of indicators of a potential security breach. This requires more than one security analysts and also consumes extensive amount of time.

AI based cyber security overcomes these limitations and much more. It will have enormous impact on cyber security process and people.

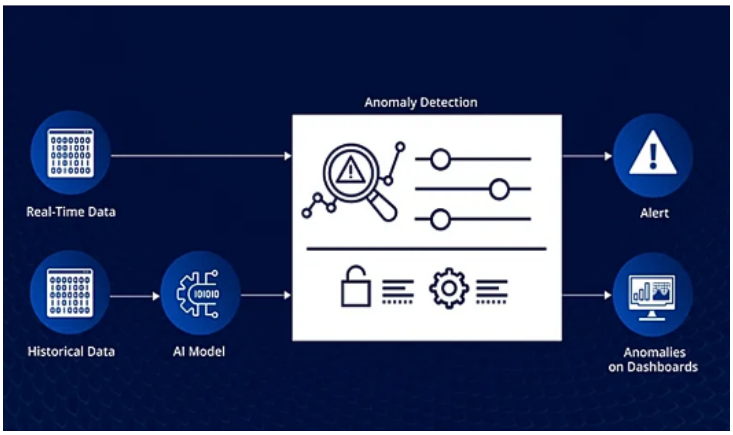
ARTIFICIAL INTELLIGENCE DRIVEN THREAT DETECTION MECHANISMS

Anomaly Detection Using Artificial Intelligence

Anomaly detection refers to identification of items or events that do not follow an expected pattern in a dataset and these are usually non detectable by a human expert.
It aims to find data patterns that deviate from a specified data distribution. It catches an unusual and abnormal behavior of data.

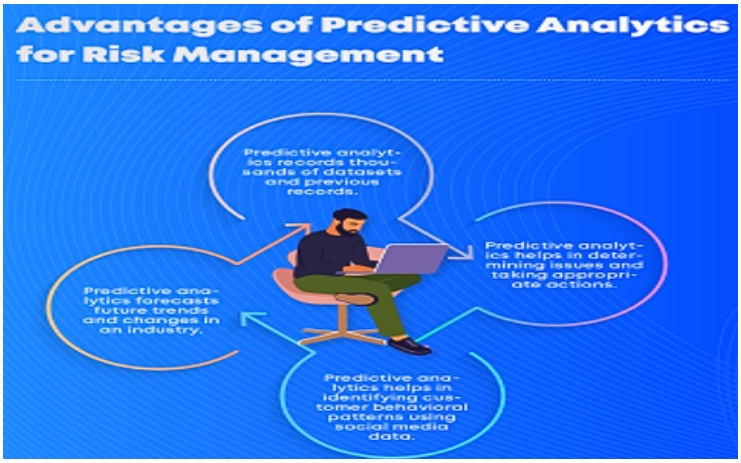
Manual observation and identification of an abnormality is not completely accurate with high data volume. A compelling need for an advanced mechanism in which the identification of the abnormalities from logs can be done in a short amount of time brings out the introduction of artificial intelligence and machine learning capabilities in the picture. Use of AI real time anomaly detection makes it possible in a blink of an eye.

AI based anomaly detection can automatically analyze data and identify abnormalities in the patterns. It enhances accuracy and prevents false triggers. It doesn't require manual intervention to understand anomalies, and this occurs even before the system is affected.



Predictive Analysis for Identifying Potential Threats

By using Predictive Analytics in Cyber security, organizations can proactively detect and respond to cyber threats before they cause significant damage. Predictive analytics uses Machine Learning algorithms, AI models to identify cyber threats before they occur. It uses trends, anomalies and past data to foresee and eliminate risks. This continuous monitoring and analysis of data provides early warning signs of possible attacks.



Organizations must keep in mind that if the data source is limited, AI and ML will not capture all the potential risks. Applying predictive analytics from end to end of the organization improves customer experience by reducing outages.

Behavioral Analysis to Detect Unusual Patterns

Behavioral analysis uses a combination of machine learning, artificial intelligence, big data, and analytics to identify suspicious behavior to identify patterns, trends, anomalies to take appropriate actions. It provides data to identify trends and easily spot outliers, so that potential threats can be easily spotted. Traditionally, organizations identified malicious behaviors using signatures that are related to certain types of known attacks. Cyber attackers are more sophisticated and they develop new methods, procedures that enable them to enter vulnerable environments and they are also not detected by conventional approaches. Behavioral Analytics can also identify root causes, provides insights for future identification of similar attacks.

ADVANTAGES OF ARTIFICIAL INTELLIGENCE DRIVEN THREAT DETECTION

AI has huge benefits in cyber security and has the below advantages:

- **Improved Speed -** AI Cyber security uses machine learning, data analytics and hugely improves speed and accuracy in threat detection.
- **Improved Accuracy -** AI powered cyber security uses machine learning algorithms to identify threats with more accuracy compared to conventional threat detection methods
- **Real-time Threat Detection** - By analyzing vast amounts of data, they can detect anomalies and potential threats long before they can cause significant damage.
- **Automation** - Automation in AI based cyber security is critical for identifying threats in early stages and thereby preventing potential attacks.
- **Adaptability** - AI models adapt to new attacks which make them effective in devising attack strategies. This adaptability reduces the dependence of rule-based systems that becomes outdated.
- **Scalability** - AI based cyber security solutions are scalable which suit them for organizations of all sizes. They handle large volume of data without compromising in the size of human resources.

REAL WORLD APPLICATIONS - LOS ANGELES BASED HOSPITAL

Healthcare facilities have a compelling need to provide a safe and secure environment for patients, staff and visitors. They require protective measures that have all kinds of safety protocols to deal with possible security breaches that threat patients and healthcare workers.

Many hospitals incorporate AI based Cyber security measures with the aim of enhancing patient and personnel safety and optimizing their overall operating efficiency.

Challenge

- Implementing 24/7 monitoring of the entire hospital premises and threat detection amidst security guard shortages.
- Implementing thorough pandemic protective measures.
- Providing solution to workplace violence against healthcare workers (according to National Nurses United, in 2021, 81% of responders admitted experiencing violence either in the form of verbal threats or physical assaults).
- Preventing intrusions through non-entrance doors, other vulnerable areas.
- To increase active shooter preparedness.
- Proactive detection of fire hazards early enough which ensures a timely and more effective response during emergency evacuation.
- Safety of medical equipment, supplies and medication.

Solution

The solution provider created a comprehensive Healthcare Security Suite which aimed at providing a safe and effective risk management which in turn helped the patients and staff to have a safe and comfortable environment that is free from risks and threats.

The solution provider created an AI based software which implemented pandemic protection methods, non-contact thermal screening, and social distancing monitoring, real time people counting with face mask usage detection. It also widely identified firearms and also tracked the gunmen across the connected cameras even though the weapons were hidden.

Benefits

- Streams from multiple cameras helped the security personnel to detect fights, assaults and other threats by analyzing them in real time which prevented workforce violence.
- Slip and fall accidents are identified immediately which alerted the personnel to provide help and support.
- Alerts are sent very quickly when a patient tries to leave their bed, which minimizes the high-risk falls for fragile patients.
- Helps in detecting displeased personnel or fired staff and other individuals that happen to cause an issue all the time.
- Identifies hazardous smoke and fire and send alerts for mitigation.
- Thermal Screening helped in speeding up the process of checking individuals and eased out the concern of the staff and personnel regarding the infection.
- AI based cyber security measures expanded the coverage of the healthcare facility in terms of safety and security. It also reduced the amount of manpower.

CHALLENGES AND CONSIDERATIONS

1. Quality of Data
AI requires high quality data for work effectively. Cyber security data is often found disrupted, incomplete, or outdated, which affects the reliability and accuracy. Cyber criminals can compromise or manipulate AI to generate fake or deceptive data. In order to avoid this, data must be collected, stored and processed in a secure environment and data updating must also be done.

2. Legal and Ethical Issues
Ethical and Legal issues pose a major challenge in the usage of AI in cyber security. Decisions are automated in AI which affects the security, privacy of organizations and individuals. AI systems may not always make fair and transparent decisions and may raise doubts about the accountability of its operators. In order to mitigate this challenge, it is always advisable to follow ethical principles and best practices for AI in cyber security. Compliance of relevant laws and regulations should always be taken care of.

3. Balancing AI And Human Expertise

Lack of trust and adoption is a challenge in using AI in cyber security. Lack of awareness, confidence, fear of losing control, jobs are some of the issues which many stakeholders encounter which which make them reluctant in using AI based cyber security. There is a need for clear and transparent communication in terms of effectiveness, benefits of usage of AI in cyber security to help the stakeholders to involve themselves and reap the benefits.

FUTURE OF ARTIFICIAL INTELLIGENCE IN THREAT DETECTION

The role of AI in cyber security is set to become even more pivotal as we move forward into digital age. The increase in volume of data demands the use of intelligent, automated systems capable of quick and accurate threat detection and response. AI might become core part of cyber security strategies. Advancement in AI systems will enhance predictive analysis, which makes it possible to anticipate a wider range of cyber-attacks and proactive response. In coming years, the role of AI in cyber security has an opportunity for substantial growth. With increasing cyber-attacks, there is a need for advanced tools and technologies. AI provides powerful set of tools that addresses the present challenges and provides a roadmap for future cyber security strategies.
There will be a need for stronger AI driven defense mechanisms to counterattack AI based cyber-attacks in future. Taking the privacy concerns into account, there will be more demand in terms of ethical AI and a need for clear policies for data collection and processing.

CONCLUSION

Artificial Intelligence and Cyber security have become inseparable components and are characterized by both promises and challenges in the never ending battle against cyber threats. AI has a proven ability to analyze huge volume of data, detect anomalies, and provide real-time threat intelligence. This has helped the organizations to safeguard their digital assets. It is equally important to note AI's limitations and ethical concerns. Hence it is crucial to address them during deployment. The decision about whether to adopt AI based solutions for cyber security lies with the organizations themselves.

In conclusion, with the massive evolution of digital world, the union of AI and cyber security plays a pivotal role in safeguarding individuals, organizations and the whole society. The future of AI in cyber security is filled with both enhanced capabilities and new challenges. It provides a promise of unparalleled protection capabilities, but also demands a proactive and informed approach to manage potential risks and pitfalls.

References

1 (Source: https://www.researchgate.net/publication/372343707 AI_Artificial_Intelligence_Cybersecurity)
2 (Image Source: https://towardsdatascience.com/is-the-future-of-cyber-security-in-the-hands-of-artificial-intelligence-ai-1-2b4bd8384329)
3 (Source: https://www.sophos.com/en-us/cybersecurity-explained/ai-in-cybersecurity)
4 (Source: C. H. Park, "Anomaly Pattern Detection on Data Streams," 2018 IEEE International Conference on Big Data and Smart Computing (BigComp)
5 (https://www.algomox.com/resources/blog/ai-anomaly-detection/)
6 (Image Source: https://medium.com/predict/ai-anomaly-detection-safeguarding-systems-and-data-1327aebe6e1e)
7 (Source: https://www.researchgate.net/publication/375715292_Title_The_Role_of_Artificial_Intelligence_in_Predictive_Cybersecurity_Analytics)
8 Image Source : https://www.bluent.net/blog/predictive-analytics-for-risk-management/)
9 (Source: A. Y. Iskhakov, M. V. Mamchenko and S. P. Khripunov, "Enhanced User Authentication Algorithm Based on Behavioral Analytics in Web-Based Cyberphysical Systems," 2023 International Russian Smart Industry Conference (SmartIndustryCon), Sochi, Russian Federation, 2023
10 Image Source: https://www.authenticid.com/glossary/behavioral-analytics/)
11 (Source: https://www.researchgate.net/publication/377726525_Scalability_and_Resource_Efficiency_of_Next-Gen_AI-_Based_Firewalls_A_Case_Study_on_Cloud_Environments
12 https://www.researchgate.net/publication/375671883_AI_and_Cybersecurity_An_Ever-Evolving_Landscape)
13 (Source:https://www.linkedin.com/advice/3/what-biggest-obstacles-using-ai-cybersecurity-tt68f#:~:text=Data%20quality%20is%20a%20paramount,a%20more%20secure%20digital%20landscape.)
14 (Source: https://www.linkedin.com/pulse/future-ai-cyber-security-comprehensive-guide-crowemackay-hkige/)
15 (Source: https://www.researchgate.net/publication/375671883_AI_and_Cybersecurity_An_Ever-Evolving_Landscape)