# Applications of AI in Cybersecurity

Setareh Ghafouri Gharavi

Riipen Project

The Lady Instructor

The cybersecurity industry is grappling with an ongoing personnel shortage, with an estimated 3.4 million unfilled cybersecurity positions globally (FieldEffect). This shortage creates a critical vulnerability in the defense of sensitive systems, as cybersecurity tasks become increasingly complex. Artificial Intelligence (AI) has emerged as a potential solution, offering scalable, automated tools to address the growing workload. AI's ability to sift through vast amounts of data, identify patterns, and respond to emerging threats could revolutionize the way organizations approach cybersecurity. This report examines how AI is transforming cybersecurity by addressing the talent shortage, improving defensive security measures, and enhancing the detection and prevention of attacks.

The demand for skilled cybersecurity professionals continues to rise, driven by the increasing frequency and sophistication of cyberattacks. According to FieldEffect, there is a need for millions of additional professionals to fill all kinds of roles in cybersecurity. Despite this, the talent pool remains insufficient, which leaves critical systems vulnerable to attacks. This situation is exacerbated by the high turnover rate in the industry and the difficulty in recruiting individuals with the required expertise (STIGroup). As a result, organizations are turning to AI to bridge this gap. AI can assist by handling repetitive, resource-intensive tasks and providing support for decision-making, allowing human experts to focus on higher-level strategic work.

AI’s role in defensive cybersecurity is pivotal. Unlike offensive security, which involves actively identifying vulnerabilities and testing systems for weaknesses, defensive security focuses on preventing, detecting, and mitigating potential threats. AI excels in this domain due to its ability to process vast amounts of data and detect subtle patterns that might be overlooked by humans. While AI excels at handling

data and can be used to scan massive databases to detect issues, it is not as effective at synthesis, which is required for offensive security. This often calls for nonstandard ways to break through defensive security measures that may not be available through data for an AI to access. As such, it is best to keep its use to defensive security where it excels.

There are several noteworthy use cases of AI in cybersecurity, including network intrusion and anomaly detection, identifying unusual user behavior or communication through various channels, such as phishing attempts or sabotage by authorized users with access to critical data and tools. AI can also help keep up to date with cybersecurity news to identify and anticipate emerging threats, as well as automate routine security tasks, such as log analysis.

Using machine learning algorithms, AI can detect anomalous activities within a network. Malicious actors often attempt to infiltrate networks by connecting through unauthorized IP addresses, aiming to access resources or sensitive information they shouldn’t have. By training an AI model on historical data, classifying activities as either normal or anomalous, the system can learn to identify future behaviors as suspicious or legitimate. This allows AI to continuously monitor network traffic and flag any irregular activity. Furthermore, AI can go beyond detection by automatically blocking any suspicious IP or network actor without requiring human intervention. This proactive approach mitigates potential threats before they can cause damage, as AI can operate in real-time to monitor and immediately respond to suspicious activity, provided sufficient resources are allocated.

In addition, AI can be employed to identify suspicious users or behaviors, particularly in cases of insider threats (CISA). For instance, disgruntled employees may use their privileges to access sensitive company data or launch attacks from

within the organization. AI can detect unusual spikes in user activity or identify when a user accesses files or systems outside their typical scope, flagging such behaviors as anomalous. By training a machine learning model on historical user data, the AI can learn what constitutes normal behavior for a particular role, department, or even specific individuals. This allows the system to make informed judgments and flag deviations as potential security threats, enabling organizations to respond to insider risks before significant damage occurs.

Outside the context of internal malicious activity, AI can be leveraged to detect and prevent dangerous communications, including social engineering attempts from external sources. One of the most common strategies in social engineering is phishing scams, where attackers send text messages or emails disguised as legitimate requests, such as password reset notifications. These messages often prompt users to open malicious links or input sensitive data, which can compromise both the user and the organization. Even a single employee falling for a phishing scam can expose an entire company to significant risk. This makes phishing one of the most pervasive and dangerous cybersecurity threats.

Another critical application of AI in cybersecurity is staying up to date with emerging threats. As cybersecurity evolves, it becomes an ongoing arms race between attackers and defenders. While defenders patch known vulnerabilities, attackers continuously develop new methods to exploit unaddressed weaknesses, including bugs and vulnerabilities in the latest software. AI can assist in preventing the exploitation of these new vulnerabilities by constantly monitoring security news outlets, forums, and even the dark web for up-to-date information on potential threats. By analyzing this real-time data, AI can help predict and prepare for new

attack strategies before they become widespread, allowing organizations to proactively mitigate risks as emerging threats are identified.

In addition, AI can automate routine security tasks, significantly reducing the time and effort required by human personnel. Manual processes are often time-consuming and prone to errors, particularly when dealing with large volumes of data. AI can handle these tasks quickly, efficiently, and without the risk of human mistake. For example, AI can analyze security logs to identify anomalous activity or trace the source of malicious behavior. It can also scan for vulnerabilities in software, immediately applying patches when bugs or security weaknesses are detected, ensuring that systems remain secure without delay.

In cybersecurity, different types of machine learning algorithms can be employed. Supervised learning involves training models on labeled datasets, where each data point is assigned a specific label or class. For example, in a task like image classification, the model would be trained to categorize an image as either containing a “dog” or a “cat” (Sailpoint). In cybersecurity, this can be used to label activities as “anomalous” or “non-anomalous,” which is very useful in many cases. Supervised learning techniques include decision trees, which classify instances by evaluating each feature step by step until reaching a final decision. This decision-making process is then applied to all instances for classification. Random Forest, an enhancement of decision trees, improves accuracy by combining the results of multiple decision trees, making the final classification more reliable (GeeksforGeeks).

In conclusion, AI is transforming the landscape of cybersecurity by providing innovative solutions to address the growing challenges of the digital age. From enhancing the detection of network intrusions and anomalies to identifying insider

threats and combating phishing scams, AI's ability to process vast amounts of data in real time enables quicker, more accurate responses to security threats. Furthermore, AI's role in keeping up with emerging vulnerabilities and automating routine security tasks enhances overall efficiency and minimizes human error. As cyber threats continue to evolve, AI will remain a crucial tool in defending against both traditional and novel attack methods, helping organizations stay one step ahead in the ongoing battle to protect sensitive information and infrastructure.

Works Cited

*Defining insider threats: CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

Effect, F. (2024, May 29). *Overcoming the cybersecurity talent shortage in 2025*. Field Effect. https://fieldeffect.com/blog/overcoming-the-cybersecurity-talent-shortage

GeeksforGeeks. (2025, January 16). *Random forest algorithm in machine learning*. GeeksforGeeks. https://www.geeksforgeeks.org/random-forest-algorithm-in-machine-learning/

GeeksforGeeks. (2025, February 4). *Decision tree in machine learning | Introduction & example*. GeeksforGeeks. https://www.geeksforgeeks.org/decision-tree-introduction-example/

*Machine learning (ML) in cybersecurity - article*. SailPoint. (n.d.). https://www.sailpoint.com/identity-library/how-ai-and-machine-learning-are-improving-cybersecurity

Stig.net. (n.d.). https://stig.net/the-state-of-us-cybersecurity-employment-analyzing-growth-demand-and-retention-challenges/