ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/ankit-srivastava/374

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 2 & Iss: 2

Research Article

Use of AI/ML in Data Security

Ankit Srivastava*

Citation: Srivastava A. Use of AI/ML in Data Security. J Artif Intell *Mach Learn & Data Sci 2024*, 2(2), 1724-1726. DOI: doi.org/10.51219/JAIMLD/ankit-srivastava/374

Received: 02 April, 2024; **Accepted:** 18 April, 2024; **Published:** 20 April, 2024

***Corresponding author:** Ankit Srivastava, USA, E-mail: Ankit1985sri@gmail.com

ABSTRACT

AI and Machine Learning (ML) play a crucial role in data security by enabling automated threat detection, anomaly identification and proactive response to potential cyberattacks by analyzing vast amounts of data to identify patterns and behaviors that could indicate malicious activity, significantly improving the speed and accuracy of security measures compared to traditional methods; essentially, AI/ML "learns" from data to identify and prevent threats as they evolve, making it a powerful tool for modern data protection.

Keywords: AI/ML, Data security, Cyber Security

1. Introduction

Artificial Intelligence (AI) improves security by enhancing threat detection, response capabilities and overall cybersecurity measures in the following ways: Advanced Threat Detection and Real-time Monitoring: AI analyzes data for unusual patterns and behaviors, enabling early threat detection. Artificial intelligence (AI) and machine learning (ML) are positively changing industries across the globe and cyber security is no exception. As AI and ML continue to make progress, their impact on cyber security is becoming increasingly vital. However, this impact is a double-edged sword, offering both enhanced security and increased vulnerability.

2. What is AI/ML

High level AI means to mimic the work and intelligence of human through computer and robots. Machine learning is branch of Artificial intelligence which automatically enables machine to learn from experience. AI is the broader concept of enabling a machine or system to sense, reason, act or adapt like a human. ML is an application of AI that allows machines to extract knowledge from data and learn from it autonomously. While artificial intelligence encompasses the idea of a machine that can mimic human intelligence, machine learning does not. Machine learning aims to teach a machine how to perform a specific task and provide accurate results by identifying patterns[1].

3. Benefit of AI/ML

AI reduces human interference so chances of errors is reduced. AI takes the decision based on information gathered on algorithm to take the next step. AI/ML can process huge data in minimal time and extract the relevant information out of it, it can take better decision then human and quickly too. Ai algorithm can be used in identifying human behavior and choices. Which indeed helps in enhancing customer's experience. It also helps in reducing the cost drastically. AI significantly boosts efficiency and productivity by optimizing processes and reducing the time and resources required to complete tasks. It can automate the daily routine task and save time.

4. Role of data in AI

We know that AI is data-dependent. Data is what keeps AI systems running and allows them to learn and predict new information in an improved way over time. Machine learning, a part of artificial intelligence, is used by computer systems to learn from data without being programmed particularly for that. AI systems perform better with different kinds of data[2]. Fist step is to train AI to identify the data, then test the efficiency of algorithm. Next step id to make the real time decision making and improve the algorithm. Data is what keeps AI systems running and allows them to learn and predict new information in an improved way over time. Machine learning, a part of artificial intelligence, is used by computer systems to learn from data without being programmed particularly for that. AI systems perform better with different kinds of data.

5. Data security in AI

Compromised data risks the integrity of AI models and failures in applications such as healthcare or finance can result in severe consequences. AI systems also need to comply with data protection regulations, such as PCI DSS, HIPAA, etc[2]. Data security in AI is very important is some one steels the data then whole model will be compromised. Some one from inside can steel the data and sell it to competitor. There can be multiple type of threats Data poisoning is a serious threat to AI systems. Creating false examples is basically where people play with the training data of AI models. Attackers can easily change the behavior or decision-making process of AI systems by adding fake data points. Another type of attack are which deconstruct the model and change the prediction modeling. Automated malware is AI-powered malware that can execute a targeted attack. It can be used to avoid threat detection as well and improve the effectiveness of infection by identifying optimal time and suitable circumstances to deliver a payload.

AI security vulnerabilities can lead to operational disruptions, impacting business continuity and productivity. In the event of an attack or breach organizations may need to halt operations temporarily to address the issue, resulting in loss of revenue and productivity. Restoring systems and ensuring their security can take time, leading to extended periods of operational downtime and associated financial losses.

6. AI in Cyber security

AI for cybersecurity uses AI to analyze and correlate event and cyberthreat data across multiple sources, turning it into clear and actionable insights that security professionals use for further investigation, response and reporting. If a cyberattack meets certain criteria defined by the security team, AI can automate the response and isolate the affected assets. Generative AI takes this one step further by producing original natural language text, images and other content based on patterns in existing data. Benefit that a cybersecurity AI assistant brings to a CISO is improved access to timely information and actionable insights, which leads to enhanced situational awareness. Remember the last time you asked your team for specific analysis or insight and how incredibly frustrating it was to wait weeks before you got the answers you were looking for. AI assistants streamline data collection, analysis and reporting, ensuring that the CISO has a clear, real-time view of the organization's security posture and can make the right decisions in a timely manner[3].

In light of the growing emphasis on data privacy regulations and ethical considerations surrounding AI, overlooking the security aspects of AI can have severe legal consequences. Failure to comply with data privacy laws, for example, may result in substantial fines and protracted legal battles[5].

AI systems are composed of algorithms and vast datasets, which inherently make them vulnerable to risks. Key components of AI systems include:

6.1. Data Layer: The data layer refers to the datasets used for training and testing the AI. This data can come from various sources and is often preprocessed and cleaned before use.

6.2. Algorithm Layer: Machine learning algorithms are applied to learn from the data on this layer. Techniques involved include regression, classification, clustering or neural networks in the case of deep learning.

6.3. Computation Layer: This layer refers to the hardware and software infrastructure that runs the AI algorithms, often requiring high-performance processors or GPUs for complex computations.

6.4. Application Layer: Most of us think only of this layer - where the outputs of the AI system are used.

7. 3 Key Strategies for AI Vulnerability Management

7.1. AI model and data security: Organizations must secure both AI training data and the model. This includes the model's algorithms, parameters and other components of AI architecture. Because the model is a digital file, it can also be corrupted or stolen. Attackers who gain access to these files can easily compromise model functionality and bypass any security infrastructure you've invested in to protect it.

7.2. AI anomaly detection: Network security tools often have continuous monitoring features that scan and alert for anomalies indicating an intrusion. Similarly organizations must implement detection systems for finding deviations in AI systems. This can be difficult, considering the black box approach typical of some AI models. Additionally, determining suspicious behavior is often complex. For example, an AI user who repeats a prompt dozens of times could be an attacker trying to manipulate outputs or a valid user simply testing system performance.

7.3. Incident response planning: It's important to build an incident response plan for AI-specific risks. As part of the plan, thoroughly brief employees on response measures, especially those deviating from traditional cybersecurity protocols and clearly define roles and responsibilities.

7.4. Planning for AI-specific risks: Determine what qualifies as an AI security incident for your enterprise and investigate how your AI systems could be compromised based on each use case. Researching common AI risk scenarios in your industry or niche will also help you anticipate how an incident may unfold and which response measures will be effective. For example, if your organization is a prime target for customer data breaches, consider how adversaries may execute prompt-based attacks to steal information[4].

8. Conclusion

Cybersecurity AI assistant might seem like a pricey addition, but the value it delivers can far outweigh the cost. For CISOs, the assistant's ability to provide real-time insights, reduce decision-making delays and optimize risk management can prevent costly breaches and regulatory penalties, easily saving millions annually. For vulnerability and exposure management leaders, AI assistants are the only way to scale their teams and keep up with the explosion of the attack surface. IT professionals' benefit from automation that saves time, reduces workloads and minimizes errors, translating into significant cost savings and improved security outcomes. AI model security or artificial intelligence security, protects AI systems from cyberattacks. AI systems are increasingly used in many industries, including healthcare, finance and transportation and are therefore targets for cyberattacks.

9. References

1. https://cloud.google.com/learn/artificial-intelligence-vs-machine-learning
2. SentinelOne, September 30, 2024.
3. Artificial Intelligence, Cybersecurity AI Assistant, Cybersecurity Risk Management, Cybersecurity Strategy.
4. outshift.cisco.com/blog/ai-system-security-strategies
5. Chris Konrad, Global Cyber, July 12 2023.