USING AI TO PROTECT NETWORKS FROM ATTACKS

Mamadalieva Sugdiyona Ilkhomjon qizi
Fergana branch of the Tashkent University of Information Technologies, master's student, Fergana region, Buvayda district, Soy-Buyi street 4
Abdurakhimov Ozodbek Azimjon o'g'li
Fergana branch of the Tashkent University of Information Technologies, student, Namangan region, Namangan district , Kul buyi street 53
Tojidinov Azizbek Ilhomjon o'g'li
Fergana branch of the Tashkent University of Information Technologies, student, Andijon region, Buloqboshi district , Hamkor street 403

Annotation: Network attacks are a growing threat to businesses and organizations of all sizes. Traditional security measures, such as firewalls and intrusion detection systems (IDS), are no longer sufficient to protect against the latest and most sophisticated attacks. Artificial intelligence (AI) offers a promising new approach to network security. AI-based systems can learn from historical data to identify patterns of behavior that are associated with attacks. This allows them to detect new and emerging threats that traditional security measures cannot see.

Keywords: AI, artificial intelligence, network security, network attack detection, anomaly detection, botnet detection, security intelligence, machine learning, deep learning, threat intelligence, cybersecurity.

Introduction

Network attacks are a constant threat to businesses and organizations of all sizes. These attacks can have a devastating impact, causing financial losses, reputational damage, and even disruption to operations. Traditional security measures, such as firewalls and intrusion detection systems (IDS), are no longer sufficient to protect against the latest and most sophisticated attacks. These attacks are often targeted, well-funded, and constantly evolving.

Artificial intelligence (AI) offers a promising new approach to network security. AI-based systems can learn from historical data to identify patterns of behavior that are associated with attacks. This allows them to detect new and emerging threats that traditional security measures cannot see.

Main part

In the network anomaly detection AI can be used to monitor network traffic for unusual patterns of activity that may indicate an attack. As an example, could be mentioned that AI can be used to detect sudden spikes in traffic, unusual patterns of network activity, or anomalous login attempts.

AI can be used in botnet detection and prevention to identify and block botnets, which are networks of compromised computers that can be used to launch attacks. AI can be used to identify botnets by analyzing network traffic patterns, identifying patterns of malicious activity, or detecting unusual communication patterns between devices.

AI can be used in security intelligence to analyze security data from multiple sources, such as network logs, security alerts, and threat intelligence feeds, to identify trends and patterns that may indicate an impending attack. For example, AI can be used to identify new malware strains, emerging attack vectors, or suspicious activity by known threat actors. AI-based security systems are still in their early stages of development, but they have the potential to revolutionize the way that network security is managed. By providing a more proactive and effective approach to detecting and responding to threats, AI can help organizations to better protect their networks and data from attack. The use of AI to protect networks from attacks is still in its early stages, but it has the potential to revolutionize the way that network security is managed. AI-based systems can provide a more proactive and effective approach to network security, helping organizations to detect and respond to threats more quickly and

effectively. We can demonstrate below paragraphs key benefits of using AI to protect networks from attacks.

Improved accuracy and speed of detection: AI-based systems can detect attacks more accurately and quickly than traditional security measures. This is because AI systems can learn from historical data to identify patterns of behavior that are associated with attacks, even if those attacks have not been seen before.

Ability to detect new and emerging threats: AI-based systems can detect new and emerging threats that traditional security measures cannot see. This is because AI systems can learn from new data as it becomes available and adapt their detection models accordingly.

In reduced workload on security analysts, AI-based systems can automate many of the tasks involved in network security, such as monitoring traffic for anomalies, detecting botnets, and analyzing security data. This frees up security analysts to focus on more strategic tasks, such as investigating incidents and responding to threats. Next paragraphs show about challenges of using AI for network attack detection.

1. Data requirements: AI-based systems require large amounts of data to train and operate effectively. This data can be difficult and expensive to collect and maintain.
2. Model training and deployment: Training and deploying AI-based systems can be complex and time-consuming. This is because it is important to ensure that the systems are trained on the right data and that they are deployed correctly in order to be effective.
3. Interpretability and explanatory of AI models: AI models can be complex and difficult to understand. This can make it difficult to interpret the results of the models and to explain to decision-makers why the models are making certain recommendations. According to researcher's point of view future directions of AI-based network security. Developing new AI algorithms and techniques for network security. Researchers are developing new AI algorithms and techniques that can be used to improve the accuracy and speed of network attack detection, as well as the ability to detect new and emerging threats. Using AI to automate security tasks. Researchers are developing new AI-based tools and systems that can automate many of the tasks involved in network security, such as monitoring traffic for anomalies, detecting botnets, and analyzing security data. Making AI-based security systems more interpretable and explainable: Researchers are developing new techniques for making AI-based security systems more interpretable and explainable to decision-makers. This will help decision-makers to understand why the systems are making certain recommendations and to make better decisions about how to respond to threats.

Conclusion

AI is a powerful tool that can be used to protect networks from attacks. AI-based security systems can detect new and emerging threats that traditional security measures cannot see. AI can also be used to automate security tasks and to make security systems more interpretable and explainable to decision-makers.Organizations should consider using AI to protect their networks from attacks. AI-based security systems can help organizations to reduce their risk of being attacked and to better protect their data from theft and loss.

References:

1. Muxtarov, F., & Tojidinov, A. (2023). Tarmoq xavfsizligini url filtirlash bilan yaxshilash. Research and implementation, 1(4), 39-44.
2. Muxtarov, F., & Sadirova, X. (2023). Korxonada axborot xavfsizligini ta'minlashning zamonaviy usullari. Engineering problems and innovations.

3. Muxtarov, F., Turdimatov, M., & Mominova, M. (2023). Umumiy o'rta ta'limga kiberxavfsizlik fanini tizimli isloh qilishning ustuvor yo 'nalishlari. Engineering problems and innovations.
4. E McGaughey, 'Will Robots Automate Your Job Away? Full Employment, Basic Income, and Economic Democracy' (2018) SSRN, part 2(3) Wayback Machine saytida arxivlangan (24-may 2018-yil)..
5. en:George Musser, "en:Artificial Imagination: How machines could learn en:creativity and en:common sense, among other human qualities", *en:Scientific American*, vol. 320, no. 5 (May 2019), pp. 58–63.
6. *Tom Simonite*. „2014 in Computing: Breakthroughs in Artificial Intelligence". *MIT Technology Review* (29-dekabr 2014-yil).
7. Sun, R. & Bookman, L. (eds.), *Computational Architectures: Integrating Neural and Symbolic Processes*. Kluwer Academic Publishers, Needham, MA. 1994.
8. Taylor, Paul, „Insanely Complicated, Hopelessly Inadequate" (review of en:Brian Cantwell Smith, *The Promise of Artificial Intelligence: Reckoning and Judgment*, MIT, 2019, ISBN 978-0262043045, 157 pp.; en:Gary Marcus and Ernest Davis, *Rebooting AI: Building Artificial Intelligence We Can Trust*, Ballantine, 2019, ISBN 978-1524748258, 304 pp.; en:Judea Pearl and Dana Mackenzie, *The Book of Why: The New Science of Cause and Effect*, Penguin, 2019, ISBN 978-0141982410, 418 pp.), *en:London Review of Books*, vol. 43, no. 2 (21-yanvar 2021-yil), pp. 37–39. Paul Taylor writes (s. 39): „Perhaps there is a limit to what a computer can do without knowing that it is manipulating imperfect representations of an external reality."

