Journal of IoT and Intelligent Solutions
Available online: http://jiotis.com

Vol 1, No. 1, June 2023, pp. 59 - 63

Unleashing The Power of Artificial Intelligence in Cybersecurity

[1*]Mohammed Adnan Ahmed

[1]Faculty of Computer Engineering,
Halic University,
Istanbul, Turkey
**Corresponding Author*: 22092090103@ogr.halic.edu.tr

Article Info

Article history:

Article received on 24 04 2023

Received in revised form 24 04 2023

Keywords:

AI; Cybersecurity; Deep learning

ABSTRACT: The intersection of cybersecurity and artificial intelligence is fascinating, yet heated arena for both hackers and defenders. An examination of the interdependent relationship between AI's capacity to handle data and security protocols uncovers an emergent pattern in cybercrime. As assailants exploit this merger to their advantage with growing frequency, conventional measures can no longer suffice. Thus, devising successful tactics that thwart these sophisticated violations continues to elude businesses and institutions alike. This composition delves into how unifying cybersecurity with AI has opened a new avenues for trespassing systems [1]while underscoring the hazards that mandate proactive actions against evermore polished attacks leveraging the full potential of these technologies.

1. INTRODUCTION

The prevalence of technology in our daily routine has made it an integral facet of modern society. Although tech has undeniably brought us convenience and improved our lives, the same cannot be said about its effects on our online security. Cybercriminals have utilized advanced techniques to carry out attacks with increasing frequency in recent years. One such technique is the use of artificial intelligence (AI) in cybersecurity. [2]The synergy between these two fields provides a promising foundation for both defensive and offensive hacking strategies. By developing intelligent algorithms capable of learning and adapting, hackers can quickly identify system vulnerabilities beyond human capability. However, the malicious utilization of AI- powered tools poses a grave threat because could exploit their capabilities to breach even the most secure computer systems effortlessly. [3]This possibility jeopardizes national security while compromising personal data privacy[4]. Thus, this essay aims to explore how integrating artificial intelligence into cybersecurity creates new possibilities for offensive tactics employed during hacking attempts while delving deep into how these advancements are changing the landscape of cyber warfare significantly.We will examine both advantages offered by this emerging field as well as potential risks associated with it, [5] if we hope to ensure safe computing environments globally, through appropriate.

measures taken worldwide, it is crucial that we address significant threats related to data privacy and national security concerns posed by integrating artificial intelligence with cybersecurity since doing so may encourage hackers' ability to infiltrate any computer system rapidly a revolutionary change that requires immediate attention in today's digital era. These kinds of future risks may be more harmful than nuclear weapons, any cyberattack to hospitals, like cutting electricity or damaging the hospital connections, may cause hundreds of deaths. Also, they can be used for accessing the nuclear weapons of countries and using them against others. This research aims to bring attention to the growing AI without control, which may bring an end to the whole world. The major ethical problem[6] is that hackers may use this kind of system to get into users' critical information such as bank accounts, emails, and so on. Additionally, they may try to launch a cyberattack on censorious government systems, such as national security informations. To avoid such a thing, programmers can use the same system on the government itself. Researchers may ask, "Why should the government try to hack its own system?" The answer is very simple: the AI system will write a report about each bug it finds so they can fix it.These kinds of criminal attacks are game-changing in terms of war. The combination of AI with cybersecurity can be harmful and beneficial to the world. By using it by the right hands, it can help in terms of security, program development, and many others.

2. LECTURE REVIEW

The research on this topic is considered very limited since this project is not yet alive. However, many researchers are afraid of this topic and its consequences. Many researchers conclude that the risks of AI in cybersecurity cannot be predicted, and the ethical use of that tool can be a disaster in terms of criminal attacks. At the same time, it is very important to detect vulnerabilities in protection systems such as firewalls and authentication. Using the system ethically can assist in the protection of user information. Simply put, what happened in the AI playing hide and seek, where the researchers mentioned [7] that the AI could go beyond the codes to develop any essential movement to win the game could also happen in the case of combining it with cyberse- curity, which is a game changer. According to experts in security fields, this combination can change the terms of wars in the coming decades. However, they do not have the necessary techniques to make this combination yet. But in the future, it is very promising to happen. The uses of AI nowadays are expanding. We can see it in the car industry, health, education, and many industrial fields. Too much AI without control may cause a new kind of deep learning where the AI connects with each other to make an attack. This can lead to system shutdowns and uncontrolled self- driving cars. They can even progress a nuclear attack. According to Elon Musk, governments need to make a committee that controls the development of AI around the world. This can reduce the risks and keep experts more familiar with new technologies.

3. METHODOLGY

In recent times, the world of cybersecurity has been experiencing a surge in interest regarding the integration of artificial intelligence (AI) and hacking techniques. To dive further into this subject, researchers combed through an array of valuable educational resources to gather data on how AI can be utilized for cyber exploitation. The initial stage focused on identifying and scrutinizing different AI algorithms that have the potential to breach security measures. [8], [9]Following this, extensive research was carried out on various modes of attack that could be executed through these algorithms. Subsequently, knowledge about these methods brought attention to the importance of creating an optimal defense system capable of shielding against new AI-based cyber threats. The way of combination can conculuded as: 1-Machine Learning Algorithms: Machine learning algorithms can be used to review through a huge amount of data and identify patterns that may show the presence of an issue or weakness. 2-Automated testing technologies can be used to simulate millions of tests in a short amount of time. These tools can scan the system for known openness and identify any new weekness during development. 3- Static analysis tools can be used to scan the system's source code and find a possible weakness

This can be done during development or ongoing security monitoring. 4-Intrusion Detection Systems: can be used to monitor the system for strange activities that could indicate a hacking attempt. 5- Security Information and Event Management Systems: systems can be used to analyze security event records from different sources, including firewall, and servers.The major problem is that this method re- quires a high GPU and RAM because the system will try thou- sands of tests in one minute and report the results independently, in addition, it may take a very long time that can extend into days or even months because the AI will be learning from each test it did.

4. RESULTS

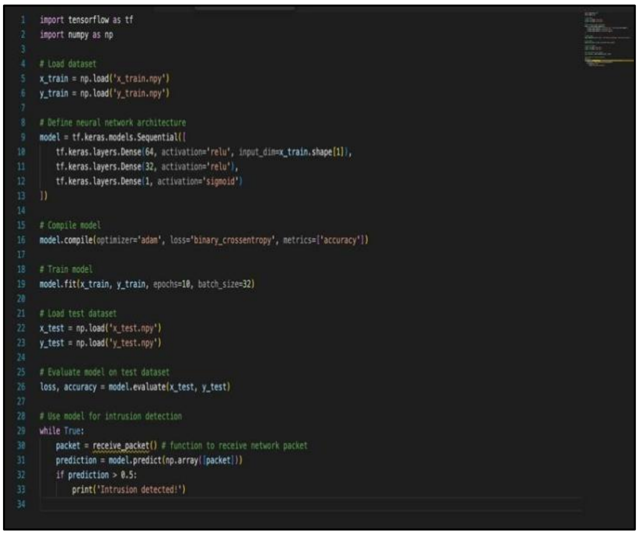
The union between cybersecurity and artificial intelligence has opened new possibilities for malicious hackers to exploit even the most secure computer systems. This development poses a significant threatto data privacy and national security, as advanced AI-based hacking techniques could potentially bypass traditional security measures [10]and gain unauthorized access to sensitive information. In this context, swift response times in cyberspace hold utmost importance because many types of data require prompt interpretation and decision-making. According to a recent study [11]artificial intelligence can play a critical role in effectively managing massive amounts of data. However, such infrastructure also presents significant threats since it provides attackers with additional tools for exploiting IT systems.The application of machine learning algorithms enables automated processes that assist cybercriminals with cracking passwords or circumventing authentication protocols used within computer networks. Therefore, without proper safeguards against advanced attack vectors utilizing machine learning capabilities on powerful hardware could lead malicious actors down paths previously considered unfeasible until recently; ultimately rendering current defensive frameworks ineffective when faced with novel approaches employed by adversaries operating under anonymity via online channels. Thus, securing our system from external intrusion requires constant monitoring by trained professionals who have the capacity to detect any unusual patterns in networktraffic or identify new types of attack vectors being utilized by nefarious agents attempting breach enterprise perimeter defenses leveraging artificially intelligent technologies like neural nets deep convolutional models supervised generative adversarial networks amongst others. Therefore, we must remain vigilant over our IT infrastructure, keeping watchful eyes out for any suspicious activities or patterns indicative of malicious intent from externalactors seeking unauthorized access to sensitive information. In conclusion, the integration of artificial intelligence with cybersecurity can lead to a significant shift in hacking techniques, hence raising serious concerns about data privacy and national security. While AI/ML presents numerous benefits, they are also highly susceptible to deliberate attacks that could make these systems ineffective.

5. DISCUSION

The impact of artificial intelligence AI on cybersecurity is significant, as it poses a threat to data privacy and national security. Hackers can employ AI technology to breach computer systems, even the most secure ones. By using AI-powered tools for network scanning or pass- word cracking, hackers automate various tasks involved in breaching systems. With this capability in their arsenal, they execute these actions with extreme speed and precision. Unlike humans,[9] AI-driven tools can learn from past attacks which makes them more sophisticated over time. They also possess an innate capability of identifying system vulnerabilities faster than manual detection would allow. The swiftness with which these cyber criminals operate presents a serious challenge as they can go undetected for extended periods. This type of threat is new since attackers employing such tactics far surpass traditional defense strategies in terms of their capabilities. If critical infrastructure like financial institutions or power grids become targets, the outcomes could be catastrophic. To prevent malicious use by individuals or groups, future research must focus on developing techniques that detect and mitigate cyber threats posed by AI- driven cyberattacks before they happen. Policymakers should also consider drafting legislation aimed at regulating these types of technologies before irreparable harm occurs not only to individuals but larger sectors of society's economy.

6. SIMILER EXPEREMENT

A group of scientists created a game called hide and seek[12],[13] where two AI teams, red and blue, compete to win. In the beginning the game was normal, and they were learning their first moves. After millions of tries, interesting things began to happen, and both teams started to make moves that weren't included in their [14]programming codes, such as jumping through walls or using the angle of the map to get rid of materials that could help the other team. Scientists were shocked by the [15]results and decided to change the map over and over, but the AI kept finding bugs in their codes and using them to win the game. From this experiment, we can conclude that if AI is combined with cybersecurity, there isn't any system that's totally safe because the AI will keep trying to find bugs to hack that system. The dangerous thing is that the AI not only tries to find bugs in the code but also uses the non-written code feature to get its desire. Like what happened in the game when the blue team got rid of the red team's essential objects by throwing them out from the angle of the map. [16]This is what we call deep learning. What is deep learning? Deep learning is part of machine learning that analysis massive amount of data in few seconds[9], using network and especial algorithm for that.



```python
import tensorflow as tf
import numpy as np

# Load dataset
x_train = np.load('x_train.npy')
y_train = np.load('y_train.npy')

# Define neural network architecture
model = tf.keras.models.Sequential([
    tf.keras.layers.Dense(64, activation='relu', input_dim=x_train.shape[1]),
    tf.keras.layers.Dense(32, activation='relu'),
    tf.keras.layers.Dense(1, activation='sigmoid')
])

# Compile model
model.compile(optimizer='adam', loss='binary_crossentropy', metrics=['accuracy'])

# Train model
model.fit(x_train, y_train, epochs=10, batch_size=32)

# Load test dataset
x_test = np.load('x_test.npy')
y_test = np.load('y_test.npy')

# Evaluate model on test dataset
loss, accuracy = model.evaluate(x_test, y_test)

# Use model for intrusion detection
while True:
    packet = receive_packet() # function to receive network packet
    prediction = model.predict(np.array([packet]))
    if prediction > 0.5:
        print('Intrusion detected!')
```

Figure 1: Basic Python code that uses an AI algorithm for intrusion detection in a network.

7. CONCLUSION

The amalgamation of artificial intelligence with cybersecurity has opened up a new era of hacking. Cybercriminals can now leverage AI algorithms to exploit weaknesses in computer systems that were formerly undiscovered or challenging to use. The fallout from such attacks could be catastrophic since they have the potential to steal sensitive information or interrupt essential services. Throughout this composition, we have meticulously examined the possible benefits and dangers associated with integrating AI into cybersecurity. Researchers have seen how AI aids in detecting threats more promptly than conventional methods but also how malicious actors may utilize it to avoid detection and commission sophisticated attacks. Going forward, companies must allocate resources towards advanced security measures that incorporate human expertise along- side machine learning capabilities for all encompassing protection against cyber threats. Relying solely on one approach is inadequate; instead, we require a comprehensive strategy that leverages the strengths of each method. In conclusion, blending AI with cybersecurity presents opportunities and challenges equally. To reap its benefits while minimizing risks effectively requires careful deliberation from individuals as well as society at large through sustained research efforts. As technology continues advancing at an unprecedented pace, it's our responsibility not only to maximize gains but also ensure responsible us age.

REFERENCES, *IEEE*

[1] D. Lee, D. Kim, C. Lee, M. K. Ahn, and W. Lee, “ICSTASY: An Integrated Cybersecurity Training System for Military Personnel,” IEEE Access, vol. 10, pp. 62232–62246, 2022, doi: 10.1109/ACCESS.2022.3182383.

[2] I. H. Sarker, M. H. Furhad, and R. Nowrozy, “AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions,” SN Comput Sci, vol. 2, no. 3, p. 173, 2021, doi: 10.1007/s42979-021-00557-0.

[3] M. N. Al-Suqri and M. Gillani, “A Comparative Analysis of Information and Artificial Intelligence Toward National Security,” IEEE Access, vol. 10, pp. 64420–64434, 2022, doi: 10.1109/ACCESS.2022.3183642.

[4] X. Li and T. Zhang, “An exploration on artificial intelligence application: From security, privacy and ethic perspective,” in 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), 2017, pp. 416–420. doi: 10.1109/ICCCBDA.2017.7951949.

[5] B. Marshall et al., “Cross-jurisdictional criminal activity networks to support border and transportation security,” in Proceedings. The 7th International IEEE Conference on Intelligent Transportation Sys- tems (IEEE Cat. No.04TH8749), 2004, pp. 100– 105. doi: 10.1109/ITSC.2004.1398879.

[6] P. Timmers, “Ethics of AI and Cybersecurity When Sovereignty is at Stake,” Minds Mach (Dordr), vol. 29, no. 4, pp. 635–645, 2019, doi: 10.1007/s11023-019-09508-4.

[7] “OpenAI, ‘GPT-4 Technical Report,’ 2023.” Accessed: Apr. 26, 2023. [Online]. Available: https://cdn.openai.com/papers/gpt-4.pdf.

[8] A. Sedik et al., “Deep Learning Modalities for Biometric Alteration Detection in 5G Networks-Based Secure Smart Cities,” IEEE Access, vol. 9, pp. 94780–94788, 2021, doi: 10.1109/ACCESS.2021.3088341.

[9] S. Mubarak, M. H. Habaebi, M. R. Islam, and S. Khan, “ICS Cyber Attack Detection with Ensemble Machine Learning and DPI using Cyber-kit Datasets,” in 2021 8th International Conference on Computer and Communication Engineering (ICCCE), 2021, pp. 349–354. doi: 10.1109/ICCCE50029.2021.9467162.

[10] C. T. Holzer and J. E. Lerums, “The ethics of hacking back,” in 2016 IEEE Symposium on Technologies for Homeland Security (HST), 2016, pp. 1–6. doi: 10.1109/THS.2016.7568877.

[11] J. Burton and S. R. Soare, “Understanding the Strategic Implications of the Weaponization of Artifi- cial

Intelligence,” in 2019 11th International Con- ference on Cyber Conflict (CyCon), 2019, pp. 1–17. doi: 10.23919/CYCON.2019.8756866.

[12] E. Strickland, “AI agents play hide-and-seek: An OpenAI project demonstrated ‘emergent behavior’ by AI players - [News],” IEEE Spectr, vol. 56, no. 11, pp. 6–7, 2019, doi: 10.1109/MSPEC.2019.8889898.

[13] “Hide and Seek Game Code.” https://github.com/acatelan/HideAndSeek (accessed Apr. 26, 2023).

[14] A. Cenkner, V. Bulitko, M. Spetch, E. Legge, C. G. Anderson, and M. Brown, “Passing a Hide-and-Seek Third-Person Turing Test,” IEEE Trans Comput Intell AI Games, vol. 6, no. 1, pp. 18–30, 2014, doi: 10.1109/TCIAIG.2013.2275162.

[15] D. Goularas and S. Kamis, “Evaluation of Deep Learning Techniques in Sentiment Analysis from Twitter Data,” in 2019 International Conference on Deep Learning and Machine Learning in Emerging Applications (Deep-ML), 2019, pp. 12–17. doi: 10.1109/Deep-ML.2019.00011.