JOURNAL OF APPLIED SCIENCE AND SOCIAL SCIENCE
eISSN 2229-3113 pISSN 2229-3205

Volume 15 Issue 12, December 2025
Impact factor: 2019: 4.679 2020: 5.015 2021: 5.436, 2022: 5.242, 2023: 6.995, 2024 7.75

ROLE ARTIFICIAL INTELLIGENCE IN DETECTION AND PREVENTING CYBER-ATTACKS

Begimov O‘ktam Ibragimovich
PhD, associate professor, Alfraganus University, Tashkent, Uzbekistan
Email: uktam1985beg@mail.ru
https://orcid.org/0000-0002-6983-6709
Bo‘riboyev Tolibjon Mirali ugli
Alfraganus University, Tashkent, Uzbekistan
E-mail: buriboevtolib@gamil.com
https://orcid.org/0009-0001-6700-4095

Abstract: The importance of using artificial intelligence (AI) in the field of cybersecurity. Artificial intelligence can play a key role in detecting and preventing cyber attacks , thanks to its ability to quickly analyze large amounts of data and identify anomalies that may indicate a potential threat. AI can also be used to automate routine security-related tasks, freeing up security professionals for more complex tasks.

Keywords: artificial intelligence, machine learning, phishing, traffic, information security.

Introduction.

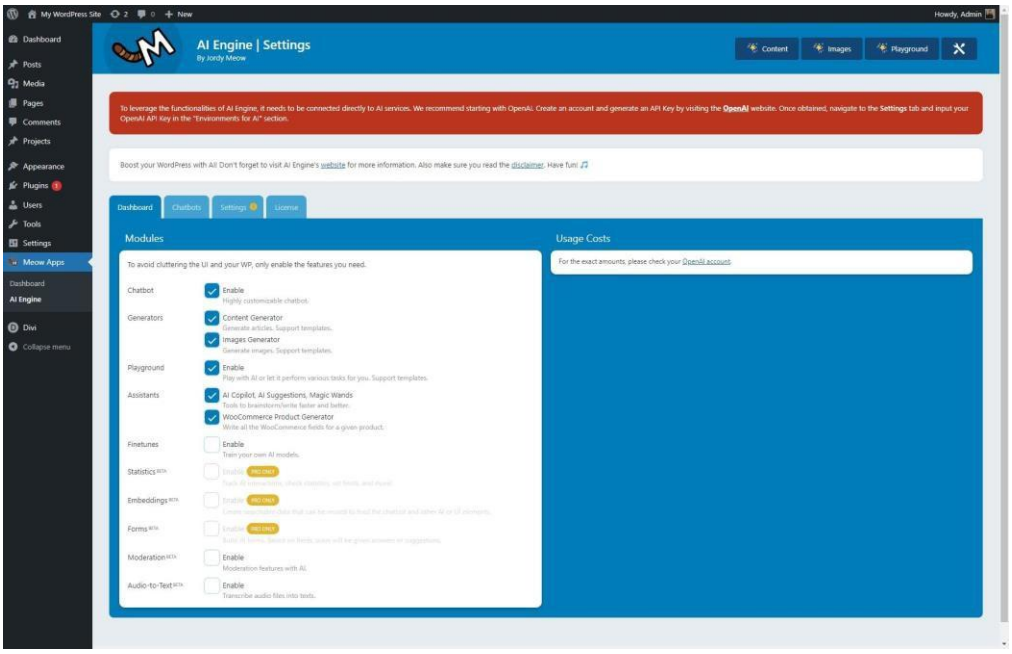
Artificial intelligence (AI) plays a key role in detecting and preventing cyberattacks. AI enables automation of analysis and detection processes. threats, Also accepts instant measures For reflections or Attack prevention. Every year, cyberattacks are becoming more common, both using AI and as a defense mechanism. AI is both revolutionizing industries and harming traditional ones. users And So same huge corporations. Each one from large companies at this time moment is developing mine AI. One from largest players on market AI are companies: INTEL, NVIDIA, IBM, etc. With the rapid growth of digital technologies, cyber-attacks have become more frequent, complex, and damaging. Traditional security systems based on fixed rules and signatures are no longer sufficient to counter modern threats such as zero-day attacks, advanced persistent threats (APTs), and ransomware. Artificial Intelligence (AI) has emerged as a powerful tool in cybersecurity, enabling faster, smarter, and more adaptive detection and prevention of cyber-attacks.
AI can be used to create intrusion detection systems that monitor network traffic and analyze it for suspicious activity. AI is trained based on past cyberattack data. For example, some programs are publicly available, such as Snort,Security.Onion, AIEngine,etc. programs.

JOURNAL OF APPLIED SCIENCE AND SOCIAL SCIENCE
eISSN 2229-3113 pISSN 2229-3205
Volume 15 Issue 12, December 2025
Impact factor: 2019: 4.679 2020: 5.015 2021: 5.436, 2022: 5.242, 2023: 6.995, 2024 7.75

Snort program is currently used by companies such as La Jolla Logic, ARSIEM Corporation, Cyberjin .Security Onion is used such companies How: Sealing Tech, Scientific Research Corporation, Applied Insight, etc. AIEngine is a software AI accelerator created by Qualcomm. The program utilizes hardware and software resources. The program interface is shown below (Fig. 1).

Fig. 1. Interface programs AIEngine

AI is also being used to create intrusion prevention systems that can automatically block suspicious traffic to prevent attacks. This system Maybe analyze behavior users And network



devices, to identify suspicious activity and prevent possible attacks.

AI is used to analyze Big Data and identifying hidden data that could pose potential threats. This allows us to detect and counter new types of cyberattacks that were previously unknown.

To ensure the effective and secure use of AI in cybersecurity, several key considerations must be taken into account. First, data and AI algorithms must be protected from cyberattacks and hacks. Hackers can use malicious algorithms for penetration into the system AI and changes her work, to go around systems protection. That's why necessary strengthen measures to protect AI-based systems and conduct regular vulnerability checks.

Secondly, it‘s necessary to train AI on various types of cyberattacks and threats and use up-to-date data. AI won't be able to effectively detect new types of threats if it hasn't been trained on them. Therefore, it‘s essential to use up-to-date cyberthreat data. And conduct regular education AI, to He could find new types of threats.

Thirdly, ethical and legal issues regarding the use must be taken into account AI V cybersecurity. For example, acceptance decisions on basis AI may lead to a violation of human privacy rights. Hence, the conclusion that it is necessary to develop ethical and legal standards that will regulate the use of AI in cybersecurity.

Finally, it‘s important to remember that AI in cybersecurity cannot completely replace the

JOURNAL OF APPLIED SCIENCE AND SOCIAL SCIENCE
eISSN 2229-3113 pISSN 2229-3205
Volume 15 Issue 12, December 2025
Impact factor: 2019: 4.679 2020: 5.015 2021: 5.436, 2022: 5.242, 2023: 6.995, 2024 7.75

human factor. AI can help automate processes. detection And response on threats, But For acceptance final Security decisions still require human involvement. Therefore, AI should be used as a tool that assists humans, not replaces them. Overcoming cybersecurity challenges using artificial intelligence.

AI systems use machine learning (ML) algorithms to learn normal network behavior and identify anomalies that may indicate cyber-attacks.

- ❖ Detects unusual traffic patterns
- ❖ Identifies insider threats
- ❖ Finds zero-day attacks without predefined signatures

Recently, there has been an increase in AI-based hacking incidents and fraudulent schemes. One of these involves the use of an imitated human voice. It is also used for identification purposes when banking apps request a photo. With cameras, attackers can use method substitutions persons on video got the name “DeepFake”. Yes, there is. some such neural networks DeepFaceLab, Artguru, Facewap And etc. For ordinary user This only entertainment, But When hackers are studying core such AI is already becoming dangerous. Countermeasures are certainly being developed by companies, but it's impossible to track. such hackers quite difficult.For struggle With DeepFake apply Technologies such as blockchain are used because the system is decentralized. Using blockchain, users can create digital fingerprints for their videos to verify their authenticity. However , the technology isn't 100% secure, so there are some attacks against blockchain.For example,such as:Sybils, attack 51%, Attack Routing.

Conclusion.

In conclusion, it should be noted that neural networks have great potential for ensuring computer security. They are improving every year and are becoming increasingly capable of detecting anomalies, recognizing and classifying threat levels, and analyzing user behavior and implementing protective measures. However , it is also important to consider that the level of hacking is increasing, and with each advancement in technology, data protection becomes increasingly difficult. Furthermore, the more AI is accessible to a wider range of users, because With help AI often are happening And attacks on other AI, And are revealed their weaknesses, such as the need for powerful computer stations and a huge amount of computing power. Artificial Intelligence plays a crucial role in detecting and preventing cyber-attacks by providing intelligent, adaptive, and automated security solutions. While challenges remain, the integration of AI into cybersecurity systems is essential to protect modern digital infrastructures.

REFERENCES:

[1] O’.I.Begimov, T.M.Bo‘riboyev / Extracting tagging from exocardiographic images via machine learning algorithmics // Analysis of world scientific views International Scientific Journal Vol 2 Issue 1 IF(Impact Factor)8.2 / 2023

[2] O’.I.Begimov, T.M.Bo‘riboyev / General Theory About the Traditional Methods and Algorithms of Machine Learning // AMERICAN Journal of Public Diplomacy and International

JOURNAL OF APPLIED SCIENCE AND SOCIAL SCIENCE
eISSN 2229-3113 pISSN 2229-3205
Volume 15 Issue 12, December 2025
Impact factor: 2019: 4.679 2020: 5.015 2021: 5.436, 2022: 5.242, 2023: 6.995, 2024 7.75

Studies Volume 02, Issue 04, 2024 ISSN (E):2993-2157.

[3] T.M.Bo‘riboyev / Hetnet tizimi asosida avtonobillaring harakat trafigini boshqarish va tahlil qilish // Nejmettin, 03-06 Ekim 2023 tarihlerinde Erbakan Üniversitesi ve Alfraganus üniversitesi öncülüğünde düzenlenen “ipek Yolunun Ötesinde kongreler dizisi: Bir Yol, Bir Kuşak: Göç, turizm ve ekonomi politik Kongresi (SIRCON 2023)” programına sertifika almak için katıldı. (Sayfa 320-324)

[4] NIST AI 100-2 E2023 Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations https://csrc.nist.gov/pubs/ai/100/2/e2023/final Проверено: 15.07.2024