Volume 10, Issue 10, October– 2025 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct603

Use of AI in Cybersecurity

Adeeth Seth[1]

[1]The Shriram Millennium School, Noida

Publication Date: 2025/10/17

Abstract: Artificial intelligence (AI) is transforming cybersecurity by enabling systems to identify, anticipate, and respond to online threats more effectively than traditional methods.This article examines key AI applications, including threat prediction, anomaly detection, fraud and phishing prevention, and chatbot-based user support. By analyzing network behavior with machine learning models, AI detects threats in real time and reduces human error. The study shows how businesses can implement AI-driven protections to strengthen risk management and ensure data integrity. As digital threats evolve, AI provides a more adaptive and resilient cybersecurity strategy.

Keywords: *Artificial Intelligence; Cyber Security; Threat Detection; Machine Learning; Phishing.*

How to Cite: Adeeth Seth (2025) Use of AI in Cybersecurity. *International Journal of Innovative Science and Research Technology*, 10(10), 943-945. https://doi.org/10.38124/ijisrt/25oct603

I. INTRODUCTION

Technology plays a very important role in our lives. We communicate with our friends, search for information, avail online services, use the internet for banking, run an entire business & many more. With so much development in technology over the past years, various methods & tactics are planned by hackers to create powerful and "life threatening" cyber attacks. Even with 0.1% of negligence with our cyber security, the hackers get access to your data and misuse it. They can steal your money, damage your reputation. Hence It is very important for everyone to be Cyber safe.

➢ *Types of Cybercrime:*

- Identity Theft: Gaining access to someone else's personal information without their permission. (For example : Hacking into your social media account)
- Psychological Tricks: Hackers play with the mind of the users to trap them in their plan. (For example , you receive an email stating that your bank account KYC needs to be updated , click on the link , this act of sending fraudulent emails is known as phishing)
- Social Media Frauds: If someone gains access to your social media account they can get access to a lot of information like your name , email , password and these days our entire life is on social media and we post regularly , you update on your location on your stories which is very risky as hackers will gain access to all of that information . (For example: Cyber Bullying).
- Mobile Application Frauds: Mobile applications nowadays are not only used for entertainment purposes but for bank transactions too , these applications are prone to cyber attacks.(For Example: You got a message stating that download this app to improve your camera quality,you download it and it downloads some malware in your smartphone to collect all the data)
- Online Banking Frauds: All banking services are shifting online ,users use net banking to fetch their account balance , check their bank statement. Bank servers can get hacked and there can be a data breach. (For example: The bank's server gets hacked and you lose all your money but a person who had set a maximum transaction limit is safe as all of his money wont go)
- Virus Attacks: Nowadays we store a lot of crucial information on our personal computers like passwords , business documents.Virus can enter into your computer through external drives and spread all across your system. (For example: You go to a cyber cafe to get some printouts of your documents, you had stored the files your pen drive and went to the cafe and connected the flash drive to the cyber cafe's computer.The cyber cafe's computer was infected with some virus and as a result the virus is in your flash drive too.)

As we rely on technology a lot ,it's very important for us to keep our data safe from cyber threats.Artificial Intelligence is the key tool in protecting us from these dangers.

➢ *Use of AI in Cybersecurity:*

- Threat Prediction: AI & ML models can be created that can monitor network traffic and analyse patterns to identify potential threats. It can be done by the following steps.

✓ Data Collection: Gather large datasets of network traffic which included normal and malicious activities.
✓ Extraction: Identify and extract the key features that can indicate threats (eg: abnormal login attempts).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct603

- ✓ Model Training: Use machine learning models (eg: Neural Network ,decision trees) to train the model for the given data.
- ✓ Evaluation of the Model: Evaluate the model's accuracy using metrics. Keep on tuning the model to improve its accuracy.

- Use of this Model: A security solution powered by AI keeps an eye on the network traffic of a business. Before any data is compromised, the AI recognizes the unusual login attempts from a foreign IP address , it classifies them as potential danger based on the trends & blocks the IP address.

- Anomaly Detection: AI excels in identifying unusual behaviour that could indicate a cyber threat. AI can flag anomalies in real time allowing for a quick action to reduce potential threats. This detection can be done by the following steps:

- ✓ Data Collection: To determine what normal behaviour is, gather historical data on system activities.
- ✓ Extraction: Feature extraction involves removing characteristics that indicate typical behaviour (such as access patterns and login times).
- ✓ Identification of Anomalies: To teach the model to identify typical behaviour, use unsupervised learning algorithms (such as clustering and autoencoders).
- ✓ Detection: Use the model to watch live data and identify anomalies—differences from the known usual behaviour.

- Use of this Model: AI examines how users behave on a business network. When an employee's account unexpectedly tries to access private data at strange times, the AI detects this behaviour as unusual and initiates additional research.

- Fraud Detection: Artificial Intelligence plays a major role in fraud detection specifically in finance. Artificial Intelligence can detect suspicious activity and notify relevant authorities by examining transaction patterns. Detection of Fraud can be done by the following steps:

- ✓ Data Collection: Gather transactional data, including both authentic and fraudulent transactions.
- ✓ Feature Engineering: Create features that help differentiate between legitimate and fraudulent transactions, such as transaction amount, frequency, location, and time of day.
- ✓ Model Training: Supervised learning algorithms (eg: logistic regression neural networks) to train the model on the labelled data, ensuring that the model can differentiate between legitimate and fraudulent transactions.
- ✓ Evaluation of the Model: Evaluate the model's accuracy using metrics , after that deploy it to monitor transactions in real time.

- Use of this Model: AI is used by an online banking platform to track transactions. In order to stop any fraud, the AI highlights an unexpectedly large transaction from a user's account that differs from their typical spending habits.

- Phishing Detection: Phishing attempts can be identified by AI techniques that scan emails and messages. Artificial Intelligence can stop phishing assaults by examining language trends and cross-referencing them with pre-existing phishing templates. It can be done by the following steps:

- ✓ Data Collection: Compile a dataset of emails that have been classified as phishing or legitimate, then normalise and remove invalid characters to clean up the text data.
- ✓ Extraction: To extract features from the email text, such as word frequency and sentiment analysis, use natural language processing (NLP) techniques.
- ✓ Model Training: Utilise machine learning techniques (such as recurrent neural networks and support vector machines) to train the model on the labelled data.
- ✓ Evaluation of the Model: Analyse the model's performance and make adjustments to increase its phishing email detection accuracy.

- Use of this Model: Emails that are scanned by an AI-based email filter are blocked from reaching the user's inbox because it recognises phishing attempts based on established phishing templates and suspicious language patterns.

- AI Cybersecurity Chatbot: An AI Cybersecurity Chatbot assists users by providing real-time guidance on resolving cybersecurity issues. By leveraging data on criminal activities and best practices, it helps users identify and respond to threats like phishing attempts, ensuring safer online interaction. It can be created by the following steps:

- ✓ Data Collection: Compile a thorough dataset of cybersecurity issues, fixes, and best practices from a variety of sources, including knowledge bases, security forums, and incident reports. To make sure the data is correct and relevant, clean and preprocess it.
- ✓ Extraction: NLP approaches can be used to identify important patterns and information in the dataset. This entails being aware of the background of various cybersecurity problems and the accompanying fixes.
- ✓ Model Training: Using the information that was retrieved, train a conversational AI model. Transformers (e.g., GPT, BERT) are examples of advanced NLP models that can be used for this. The model must be able to comprehend user inquiries, recognise the problem, and offer pertinent advice.
- ✓ Integration: Install the trained chatbot and include it into user interfaces (such as mobile apps and web chat). In order to ensure that the chatbot stays effective over time, include continuous learning methods to refresh its knowledge base with new cybersecurity threats and solutions.

- Use of this Model: A user receives a suspicious email and contacts the AI chatbot for help. The user types,"I got an email from my bank asking for my account details. Is this

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct603

a scam?" The chatbot analyzes the email details, identifies it as a phishing attempt, and responds,"This email looks like a phishing attempt. Do not click any links or provide information. Report it to your bank and mark it as spam."

II. CONCLUSION

In summary, the application of artificial intelligence (AI) to cybersecurity has revolutionised the field and greatly improved our capacity to identify, stop, and neutralise online threats. Artificial intelligence (AI) is a vital weapon in the battle against cybercrime because of its capacity to analyse enormous volumes of data, spot anomalies, automate responses, and continuously learn from new threats. Organisations may proactively protect sensitive data, secure their systems, and lessen the risk of cyberattacks by utilising AI-driven solutions. AI will play a more and more important role in cybersecurity as cyber threats continue to change, helping us to stay one step ahead of hostile actors and preserve the integrity and security of our digital environments.

REFERENCES

[1]. https://cybercrime.gov.in/
[2]. https://appinventiv.com/
[3]. https://www.forbes.com/
[4]. https://aibusiness.com/
[5]. https://www.datamation.com/