TEAM CICADA

PREVENT & DETECT CYBER ATTACKS

~ Pranav Vinod Patil
~ Sanidhya Singh
~ Dhruv Gupta

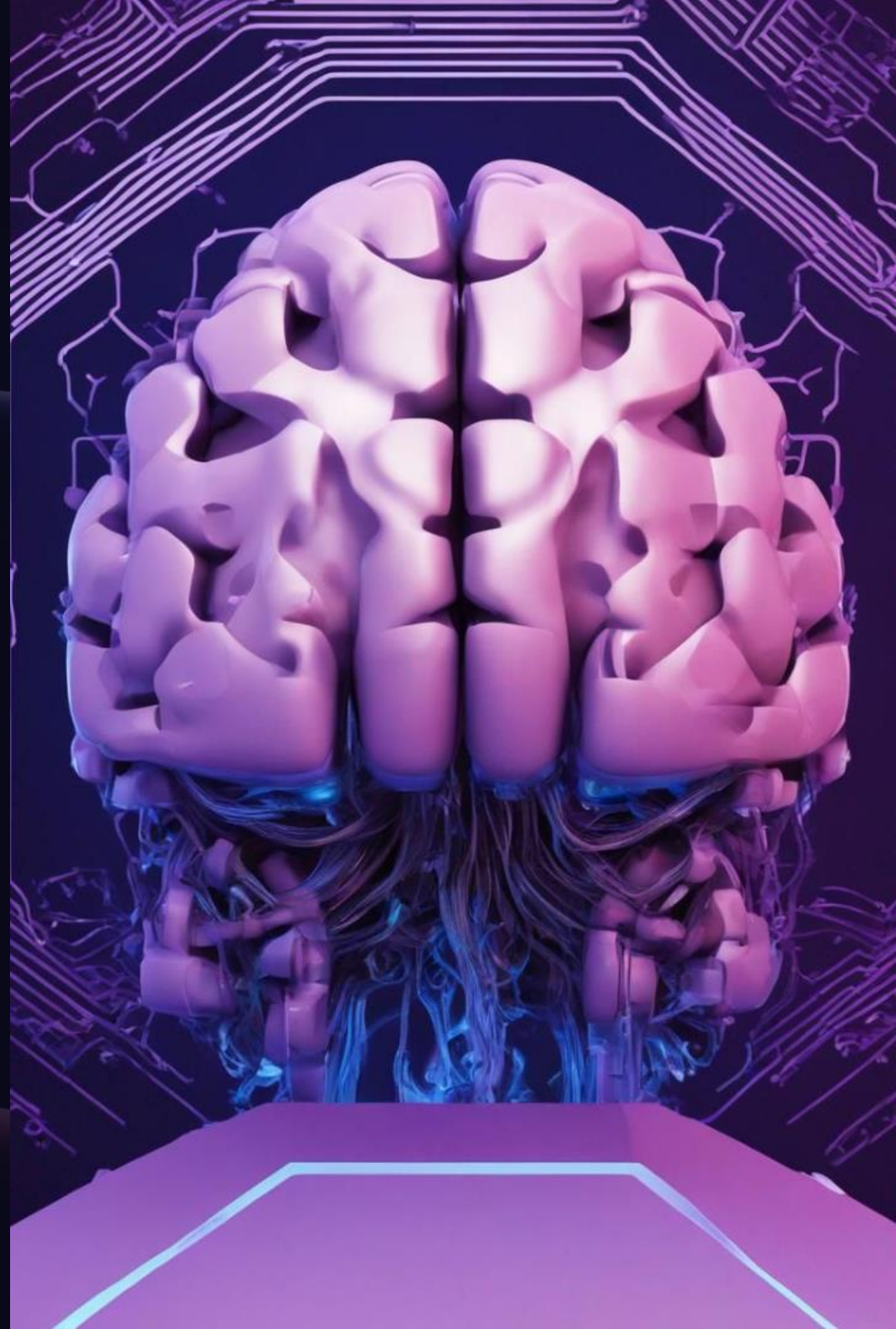
Artificial Intelligence & Machine Learning

- **AI (Artificial Intelligence) :** Artificial Intelligence is the simulation of intelligence processes by machines, encompassing tasks like learning, and decision-making.

- **ML (Machine Learning) :** Machine Learning is a subset of AI enabling computers to learn and improve from experience without explicitly programmed.

- Understanding the basic principles, applications, and implications of AI and ML is crucial for any sector seeking to stay ahead in the digital revolution. This initial exploration will lay the groundwork for grasping how these technologies intersect with and profoundly impact the field of cybersecurity.

~ CICADA



Semblance of AI & ML in Cyber Security

Defensive Strategies

- AI and ML technologies enable real-time threat detection and response.
- They analyze network traffic and user behavior for anomalies.
- Anomalous activity triggers immediate actions like traffic blocking or device quarantine.

Offensive Threats

- Cybercriminals leverage AI and ML for advanced attack strategies.
- Machine learning algorithms analyze vast datasets to pinpoint vulnerabilities.
- Weak passwords, unpatched software, and other security flaws are targeted.

Regulatory Compliance

- AI and ML aid organizations in achieving regulatory compliance.
- They enhance data protection through precise measures.
- Automated identification and classification of sensitive data are enabled.

The Intersection of AI/ML and Cyber Security

1

Threat Predictive Analytics

By analyzing data and trends, AI/ML models can predict potential cyber attacks and attacks and vulnerabilities, allowing organizations to implement proactive security proactive security measures to prevent breaches.

2

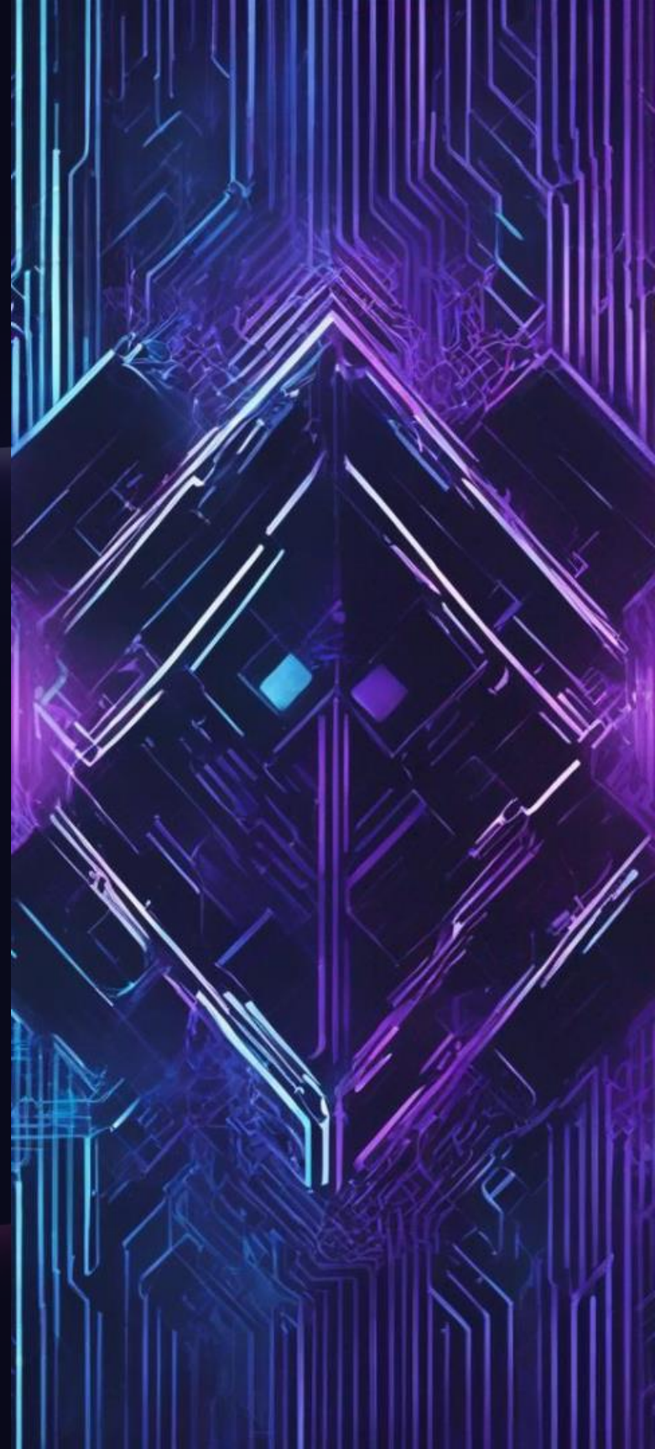
User Authentication and Access Control

ML algorithms can enhance user authentication mechanisms by analyzing behavioral analyzing behavioral biometrics, such as typing patterns and mouse movements, to movements, to verify user identities more accurately.

3

Adaptive Security Measures

ML-powered security systems have the capability to adapt and evolve in response to response to changing cyber threats. By continuously learning from new data and data and feedback, ML models can dynamically adjust security policies and response and response mechanisms to mitigate emerging risks effectively.



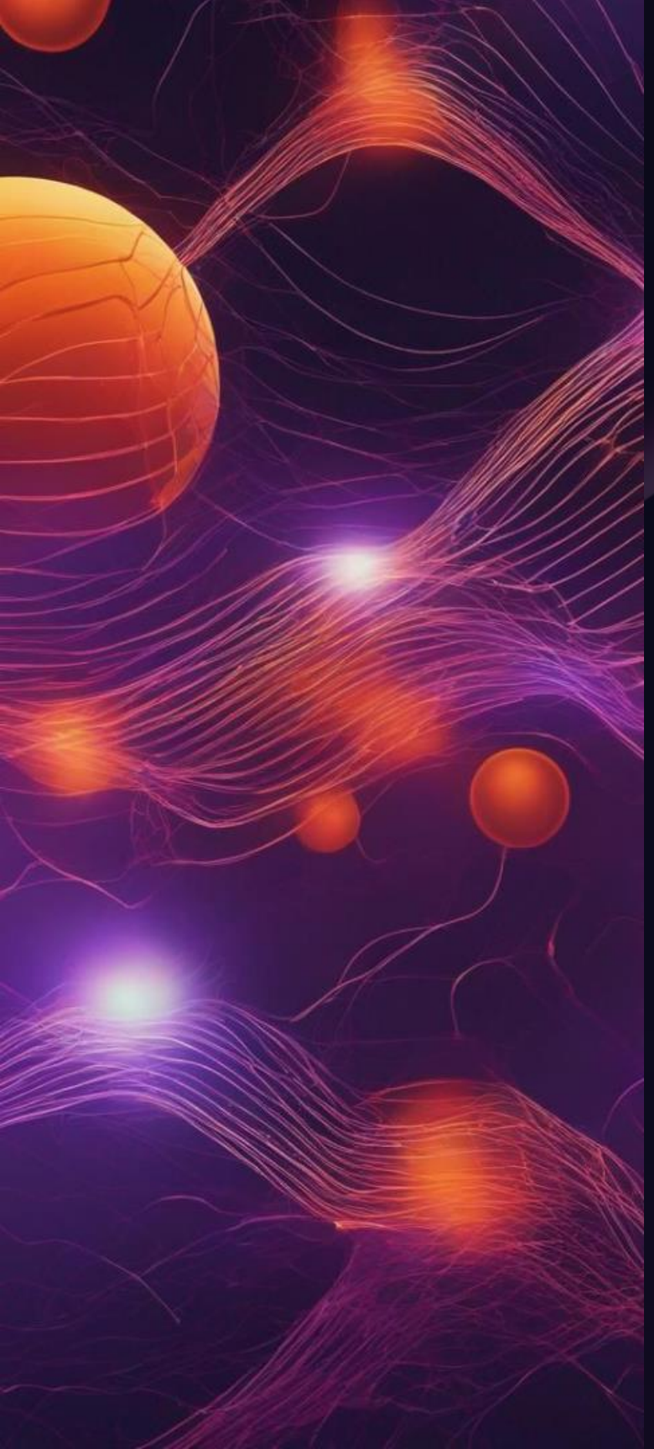
Anti-Phishing Machine Learning Model

1 Email Content Analysis

Anti-phishing ML models can analyze analyze the content of emails to identify identify phishing attempts. They examine various factors such as language, tone, and formatting to distinguish between legitimate and and malicious emails. By learning from from historical phishing attempts, these these models can detect suspicious suspicious patterns or keywords commonly used in phishing emails. emails.

2 URL Analysis

ML models can analyze URLs embedded embedded in emails to determine their their legitimacy. They evaluate factors factors such as domain reputation, URL URL structure, and redirects to identify identify phishing links. By leveraging leveraging features extracted from URLs URLs and historical data on known phishing websites, these models can can accurately classify URLs as safe or or malicious.



Deep Fake Forgery Detection Machine Learning Model

1 Multimodal Analysis

Deepfake forgery detection ML models employ multimodal analysis techniques to analyze various aspects. By examining multiple modalities simultaneously, this model can identify inconsistencies or anomalies that may indicate the presence of a deepfake.

2 Motion Analysis

ML algorithms analyze motion dynamics and patterns within videos videos to detect irregularities or unnatural movements that are characteristic of deepfake manipulation, enabling the identification of forged video content. content.

Challenges and Limitations of ML in Cyber Security

Adversarial Attacks

ML models used in cybersecurity are susceptible to adversarial attacks, where malicious actors intentionally manipulate input data to deceive or evade detection

Data Quality and Bias

In cybersecurity, obtaining labeled training data for ML models can be challenging due to the scarcity of real-world attack samples and the need to ensure data privacy and confidentiality.

Interpretability and Explainability

In cybersecurity, the lack of interpretability can hinder trust and understanding of ML-based security solutions, limiting their adoption in critical applications where explainability is essential for decision-making and accountability.

Use Cases and Examples of ML in Cyber Security

Malware Detection	ML algorithms are widely used to detect and classify classify malware based on characteristics such as file as file attributes, behavior patterns, and network network activity.
Phishing Detection	ML-driven email filters analyze patterns to effectively block phishing attempts before they they reach the user's inbox.
Malware Classification	ML classifies malware types based on code analysis, enabling quicker containment and remediation efforts.

BIBLOGRAPGY

ANTI-PHISHING ML MODEL

DEEP FAKE DETECTION ML MODEL

Google Drive