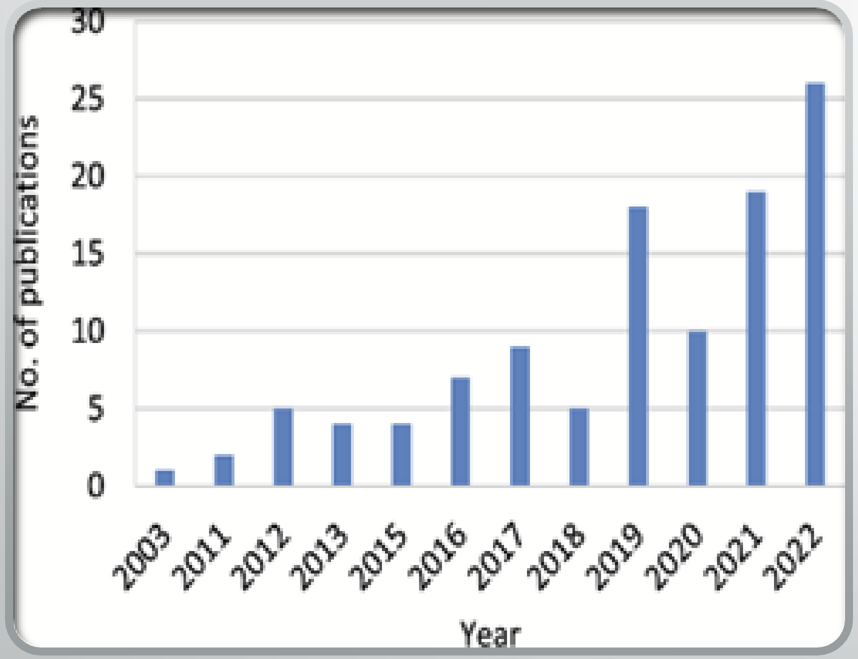
# Artificial Intelligence: The New Tool For Cybersecurity in Finance

By: Michael Reifer, Calvin Basier, and David Oliseh

# Introduction

- The growth of artificial intelligence over the past couple of years has sparked new ideas for cybersecurity.
- AI-driven cyber-attacks in the financial world are becoming a less costly option for criminals.
- Many financial organizations are switching towards the use of AI driven cybersecurity for defense methods. This switch is needed to combat the constant change of attacks in the finance sector.
- This has allowed new methods for criminals or hackers to use AI to attack financial organizations.

# Introduction



- From the new technology more and more publications are being released on how artificial intelligence can be used for cybersecurity in finance.
- In this presentation we will summarize our findings on attack/defense AI-methods used for/against cybersecurity in finance.

# Ai-Based Cyber Attacks Against Finance

- As the world continues to change and Ai is more widely used, the usage of Ai threats increases as well. Despite our advancements in defenses, we must be aware of the attacks as well. Today we'll summarize some of the findings.
- AI Cyber Attacks come in a multitude of different forms the ones I'll be focusing on are:

  Adversarial Attacks On Machine Learning Models

  Ai Social Engineering Attacks

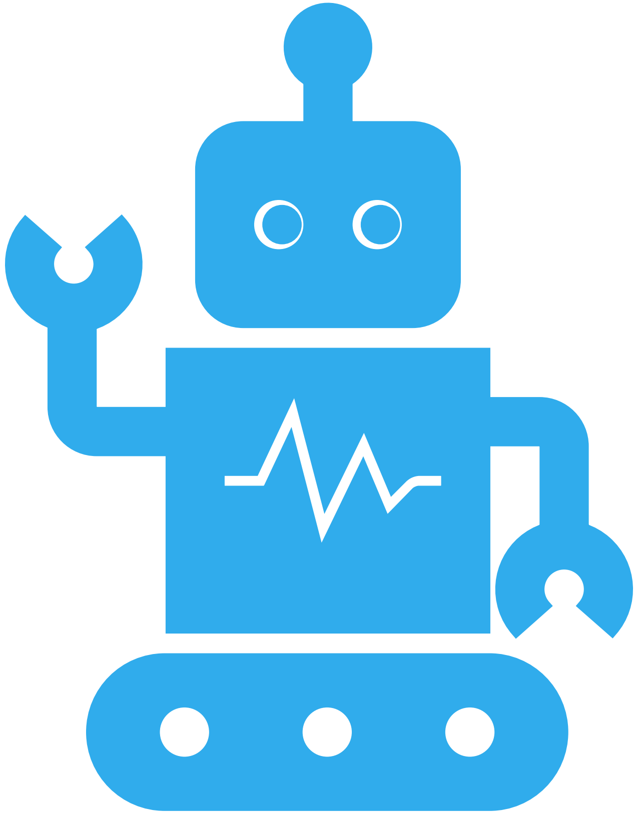
  And Ai-Malware

# Ai-Based Cyber Attacks Against Finance(Cont.)

- **Adversarial Attacks on ML:**
  - ○ Adversarial Machine learning is a subset of machine learning dedicated to attacking models.
  - ○ AML attacks can be categorized as **Poisoning, Evasion, Extraction.**
  - ○ **Poisoning Attacks:** An attack on the machine learning model with the goal of influencing the model in its training phase. This causes the model to learn incorrectly making it develop a bias
  - **Evasion Attacks:** An attack on pre-trained machine learning model where the data is altered to cause misclassifications
  - **Extraction Attacks:** An attack aimed to steal confidential information about the machine learning model.

# Ai-Based Cyber Attacks Against Finance(Cont.)

- Ai-Malware Attacks:
  Malware is malicious software or programs with the intention of altering disrupting and destroying critical components.
- Ai based Malware is emerging utilizing Ai in a variety of different ways
- Self-propagation, Evolution, Etc.
- One method is through code obfuscation via evolutionary Packers. Packers normally conceal malware from anti-viruses and IDS(Intrusion dection systems), by compressing or encrypting malware within code. Evolutionary packers streamline the process by removing the need for packers' software and building in the malware itself evolutionary packers streamline the process.



# Ai-Based Cyber Defense In Finance

# Ai-Based Cyber Defense In Finance

- **ANNs**: They are made up of different biological neural networks that allows them to be able detect credit fraud, risk management and credit scoring. They also have the ability to learn from date and be able to tell potential threats
- **Network intrusion detection using deep learning**: there are different deep learning techniques like convolutional neural networks CNNs and recurrent neural networks RNNs. They are made to be able to identify and detect any network intrusion.
  - **CNNs-** they are mainly used to capture fraud detection and any changes in a transactional data, they are able to look at large data efficiently
  - **RNNs** – these are used to track data that goes back in time like stock prices, they can really help in risk management where companies in finance can use the date to be able to make future decisions

# Ai-Based Cyber Defense In Finance

- **Generative adversarial networks** – they are made up of a generator and also a discriminator network. Regarding finance  they can help make financial data better by being able to contribute to the deep learning techniques
- **XAI based techniques**-  they help understand the AI decision making and be able to predict what the outcomes would be. They are also helpful into identifying the strengths and the weaknesses in the AI

# Conclusion

- AI driven cybersecurity methods help defense by allowing for more automation (this will not remove the needs for humans) in cybersecurity for finance
- AI driven attack methods are harder to combat, and they find specific weaknesses in a financial organization's cybersecurity
- New methods will continue to be developed (on both ends)
- Key take away: is AI is exceptional at detecting Credit card fraud (anomaly detection)