

# Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application

**B. Narsimha<sup>1</sup>, Ch V Raghavendran<sup>2</sup>, Pannangi Rajyalakshmi<sup>3</sup>, G Kasi Reddy<sup>4</sup>, M. Bhargavi<sup>5</sup> and P. Naresh<sup>6</sup>**

<sup>1</sup>Asso. Prof. & Head, Department of CSE, Holymary Institute of Technology and Science, Hyderabad, India, [prof.narsimha@gmail.com](mailto:prof.narsimha@gmail.com)

<sup>2</sup>Prof., Department of CSE, Aditya College of Engineering and Technology, Surampalem, India, [raghuchv@yahoo.com](mailto:raghuchv@yahoo.com)

<sup>3,4</sup>Asst. Prof., Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India, <sup>3</sup>[pannangiraji@gmail.com](mailto:pannangiraji@gmail.com),

<sup>4</sup>[kasireddy.csegnit@gniindia.org](mailto:kasireddy.csegnit@gniindia.org)

<sup>5</sup>Asst. Prof., Department of CSE, CMR Engineering College, Hyderabad, India, [maddibhargavireddy@gmail.com](mailto:maddibhargavireddy@gmail.com)

<sup>6</sup>Asst. Prof., Department of IT, Guru Nanak Institutions Technical Campus, Hyderabad, India, [pannanginaresh@gmail.com](mailto:pannanginaresh@gmail.com)


\*Correspondence: Pannangi Rajyalakshmi; Email: [pannangiraji@gmail.com](mailto:pannangiraji@gmail.com)

**ABSTRACT-** Cyber security comes with a combination of various security policies, AI techniques, network technologies that work together to protect various computing resources like computing networks, intelligent programs, and sensitive data from attacks. Nowadays, the shift to digital freedom had led to opened many new challenges for financial services. Cybercriminals have found the ability to leverage e- currency exchanges and other financial transactions to perform their fraudulent activities. The unregulated channel makes it essential for banks and financial institutions to deploy advanced AI & ML (DL) techniques to fight cybercrime. This can be implemented by deploying AI & ML (DL) techniques. Customers are experiencing an increase in the fraud-hit rate in financial banking operations. It is difficult to defend against dynamic cyber-attacks using conventional non-dynamic algorithms. Therefore, AI with machine learning techniques has been set up with cyber security to build intelligent models for malware categorization & intelligently sensing the fraud with danger. This paper introduces the cyber security defense mechanism by using artificial intelligence (AI), machine learning (ML)) techniques with the current Feedzai security model to identifying fraudulent banking transaction. We have given a preface to the popular ML & AI model with random forest algorithm and Feedzai's Open ML fraud detection software tool, which provides automatic fraud-recognition to the current intelligent framework for solving Financial Fraud Detection.

**Keywords:** Digital Space, Machine Learning, Deep Learning, Malware Detection Intelligence Sensing Feedzai.

## ARTICLE INFORMATION

**Author(s):** B. Narsimha, Ch V Raghavendran, Pannangi Rajyalakshmi, G Kasi Reddy, M. Bhargavi and P. Naresh

**Special Issue Editor:** Dr. S. Muthubalaji 

**Received:** 11/04/2022; **Accepted:** 29/04/2022; **Published:** 13/05/2022;

**e-ISSN:** 2347-470X;

**Paper Id:** 0322SI-IJEER-2022-04;

**Citation:** 10.37391/IJEER.100206

**Webpage-link:**

<https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100206.html>

This article belongs to the Special Issue on **Intervention of Electrical, Electronics & Communication Engineering in Sustainable Development**

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.



attacks by using different technologies for networking servers, mobile devices, and computing systems.



**Fig. 1:** Cyber Security Sub-Domains

## 1. INTRODUCTION

Today in our day- to- day life, we all are living in a digital age that is interconnected to the digital ecosystems. Cyber-attacks [7] are increasing tremendously and targeting to the digital ecosystems. Cyber security has forced great impact on various critical transactions.

### 1.1 Cyber Security

It is the process of protecting data from various malicious

In this paper, we have given various AI and ML approaches to cyber security [13] and introduced a popular ML&AI model

using random forest algorithm. Fraud detection mechanisms have been implemented using Feedzai's Open ML fraud detection software tool.

To discover new cyber-attack and to achieve higher fraud detection accuracy existing cyber fraud detection systems are not that much efficient and have faced many difficulties to detect new cyber-attack patterns.

### 1.2 Artificial Intelligence (AI) in Cyber Security

AI is a rapid intensification division for computer science researchers to develop new techniques, and system applications. Using AI techniques, intelligent machines can be design. AI has broad range of application in the areas like manufacturing, agriculture, grid designs, Autonomous Vehicles, Smart Cities. These smart applications are implemented using NLP [6], Chat bots & Speech Recognition, Virtual Assistants, facial recognition, and robotics. AI techniques [8] have been used in the field of cyber security for vulnerability management, breach risk prediction, incident response, exposure of threat, malware monitoring and intrusion detection and prevention etc. Artificial Intelligence techniques are considered to be as a potential solution to the increasing cybercrimes. AI can prevent and detect many abnormalities related to fraud detections.

### 1.3 Machine Learning (ML) in cyber security

Machine learning technology plays a vital role to address various issues of business related large-scale data. Figure 2 describes various development phases of Fraud detection using a Machine Learning model. ML approaches [1] in cyber security uses past fraud data patterns and recognizes them in their future transactions. ML algorithm like Random forest [10] (combinations of decision trees) construct decision trees to classify the data objects. It helps to find fraud traits efficiently than humans.

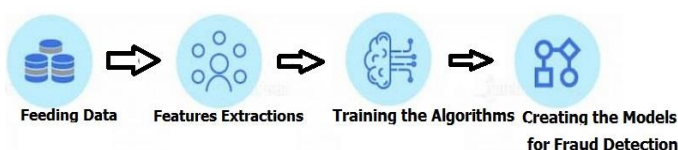


Fig 2: ML Process at Cyber Security

ML is a sub-part of AI. ML approach comes with 3 core category: unsupervised learning, supervised learning, and reinforcement learning. Malware detection and network intrusion detection can be processed more efficiently using ML approaches.

### 1.4 Use of Deep learning (DL)

Deep Learning [2] is sub-branch of ML, which uses Neural Networks (similar to neurons in human being) techniques to simulate human brain like behavior. DL approaches behaves like human being neurons and construct the neural structural design with multifaceted interconnections [11].

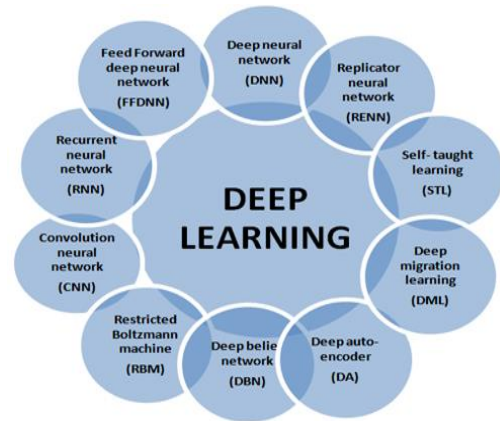


Fig. 3: Deep learning approaches

DL can be subdivided across different types so-called as artificial neural networks (also known as neural nets). The neural nets are critically layered and have names as a CNN (convolutional neural network) typically used for vision (sight / pixel) processing or an RNN (a recurrent neural network) that has time based functionality [5].

## 2. ARTIFICIAL INTELLIGENCE: A NEW TREND OF CYBER SECURITY

AI understand potential vulnerabilities and acts as an accelerator to analyze large scale of business related data and distinguish real from apparent threats.

### 2.1 Applications of Artificial Intelligence to Cyber security

The main goal of the artificial intelligence in cyber security is to detect cyber threats, fraud transits and to reduce the cyber-attacks [14].

AI may often be better and more effective than humans in detecting malicious malware. Automation in Security improves the organization's ability to prevent and detect the damage the-security flaws.

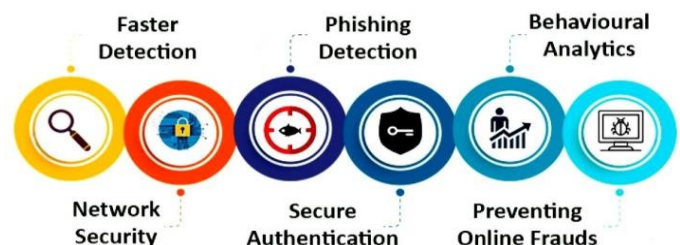
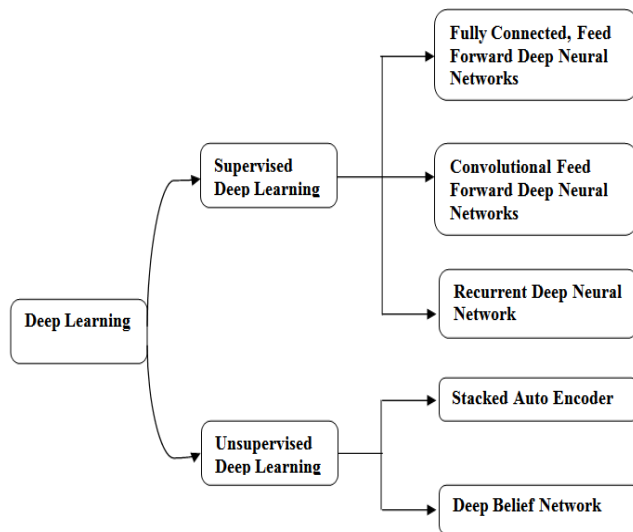


Fig. 4: Applications of AI in Cyber Security

### 2.2 Deep Learning (Sub field of Machine learning): A New trend of Cyber Security

Detecting and preventing organization data from known and unknown cyber security [15] threats is made possible in real-time with the help of deep learning neural network algorithms.

Deep learning-based structures employ in anomaly detections [3] [4].



**Fig. 5:** Deep Learning Categories

### 2.2.1. Supervised Deep learning Model

SL model is a powerful tool to classify data and processing of data is done through machine language. In supervised learning mechanism, we use classified labeled data set. All the input information is labeled as good or bad.

### 2.2.2 Unsupervised Deep Learning Model

It is used to detect anomalous behavior in the cases of small transaction data. This approach incessantly processes the data, analyzes the new data, and updates it based on the new findings. It notices the occurrences of new data patterns and finds whether they are parts of valid or fraudulent operations. Deep learning approach in fraud detection is connected with unsupervised learning algorithms.

### 2.2.3. Reinforcement Deep learning Model

A reinforcement-learning model allows the machines to detect the ideal behavior within a specified context. It frequently learns from the environment, finds the appropriate actions to minimize the risks factor, and maximizes the rewards. A reinforcement feedback signal is used to learn its behavior.

## 2.3. Benefit of Applying Deep Learning to Cyber security

**Raw Data Training:** Capable of training directly from raw data, it can able to detect a new sample with greater levels of accuracy.

**Independent of Human Intervention:** Does not rely on human intervention to perform feature engineering and data manipulation to detect even new and unknown samples.

**Analyze any Type of Data:** The input agnostic development of the algorithm means that Deep Learning can handle any or different types of data

**Non-linear correlations:** Not limited to simple linear correlations, it can analyze multiple levels of complex data patterns.

G. Apruzzese, M. Colajanni, L. Ferretti, and M. Marchetti, in their paper “Addressing adversarial attacks against security systems based on machine learning” explained ml based security system against attacks.

Soleymanzadeh, Raha, Mustafa Aljasim, in their work “Cyberattack and Fraud Detection Using Ensemble Stacking”, used ensemble methods to provide security and explored hoe to detect fraud in banking server data.

## 3. MODELS & METHODOLOGY

### 3.1 Forecast fraud with Machine Learning

Due to the complexity in analyzing the large-scale financial fraud transactions, a mixture of supervised and unsupervised machine learning models are needed.

Two types of machine learning algorithms are used in financial fraud transaction detection: 1.Supervised 2. Unsupervised learning.

In this paper we have introduced the use AI & ML techniques to support Banks for detecting fraud payments, loan fraud using Supervised ML algorithm namely Random Forest.

### 3.2 AI & Machine learning approach for fraud detection in Banking

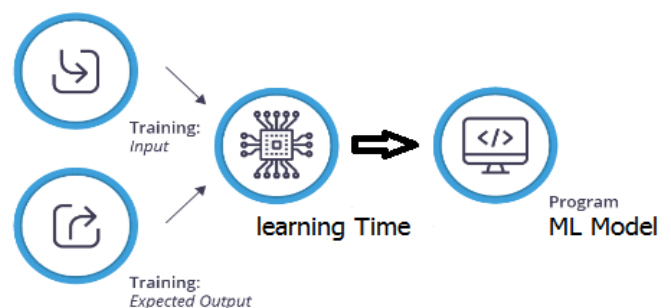
Many financial firms have discarded the use of legacy tools and shifted to the new-age AI & Machine learning solutions for fraud detection [12].

ML algorithms are used to practice millions of data objects quickly and link instances from unrelated datasets to detect suspicious patterns.

#### 3.2.1 Machine Learning process

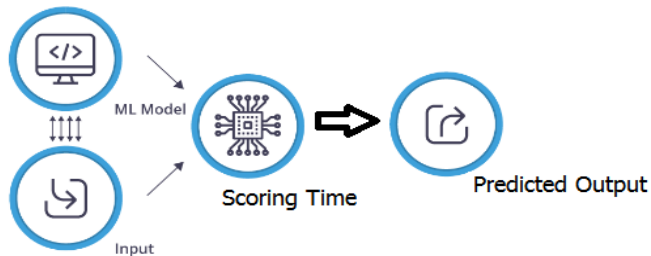
It consists of two main phases:

**Preparation Phase:** Provide input data, the system is trained by labeled data. In training phase labeled data is taken and provided to the system as input. Based on this training data model is developed which is used to generate the expected output for real world input .



**Fig 6:** ML Learning Process (Training Phase)

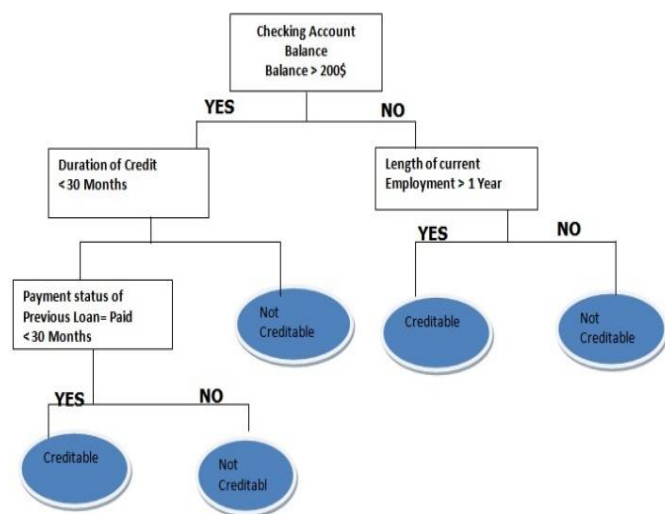
**Evaluation Phase:** We considered attributes that are found in the dataset and computed its features like for a specific account average transaction amount, number of transactions in the past performed in the past.



**Fig. 7: ML Process (Evaluation Phase)**

### 3.3 Supervised method for fraud detection in Banking Sectors using Random Forest Algorithm - Feedzai –AI based Open ML model

Banking Fraud Detection requires [9] a lot of effort as it contains a high risk and impact on reputation. Customer analysis is one of the biggest problems in banking sectors for analyzing the loan defaults or for detecting any fraud transaction, so keeping in mind of all these aspects we used Feedzai model.



**Fig. 8: Loan eligibility checking on credit bases**

The above Figure representation is a tree which decides whether a customer is eligible for loan credit based on conditions such as account balance, duration of credit, payment status.

Random forests algorithms are very simple systems that you can use to set up fraud detection very fast.

### 3.4 Random forest Algorithm

In banking sector random forest algorithm is used mostly for the identification of financial frauds.

**Random Forest algorithm for training the dataset.**

The process of training the dataset encloses *importing the RandomForestClassifier* class from the *sklearn.ensemble* library.

```
## Fitting Decision Tree classifier to the training set
From sklearn.ensemble import RandomForestClassifier
Classifier= RandomForestClassifier (n_estimators=50,
criterion="entropy")
classifier.fit (p_train, q_train)
```

Criterion is the function used for analyzing the accuracy of the split.

*n\_estimators* is used for selecting the required number of trees used in the Random Forest for overfitting.

1. Select N arbitrary tuples from dataset (D).
2. Construct a decision tree using information from D
3. Select the trees count from algorithm, do 1 and 2
4. For classification problem, each tree forecast the type of record belongs to.
5. The category was assigned to new record

**For predicting the training test we have choose set result**

```
y_pred= classifier.predict(x_test)
```

### 3.5 Feedzai's Anomaly Detection

We have considered Feedzai Software tool for banking fraud anomaly detections. Feedzai is one of the main intelligent platforms to solve financial crime. It is a powerful AI based anomaly detection scheme, which recognizes and stops the banking fraud transaction. Fraud transactions are assessed utilizing AI models to distinguish designs that are not clear to the natural eye.

#### Procedure:

*Step 1:* First, take the client unique exchange data and study the client profile and exchanges practices.

*Step 2:* In the following stage, outer information focuses are added and Feedzai's information affiliation further improves the data.

*Step 3:* By using machine learning models studies the transactions risk factor and detects financial crime patterns.

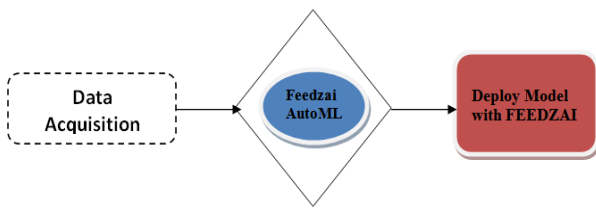
By using the random forest model risk or fraud transactions is detected

Furthermore governs like either exception discovery approach utilizing detachment woodland method or abnormality location utilizing the neural auto encoder can be utilized to adjust the choice to endorse, reject or survey. At the point when the outcome or a choice is clear, white-box clarification measure gives clear documentation.

#### 3.5.1 Fraud Detection using Feedzai's-AI based Open ML Engine

Feedzai is an Open ML software Engine is used to build customized machine learning models for fraud detections.





**Fig. 9:** Feedzai's AI based Open ML fraud detection system

### 3.6 Modules: Generic Python

The openml-generic-python module is the most powerful approach which contains a provider to load Python code that conforms to a simple API.

```

<dependency>
<groupId>com.feedzai</groupId>
<artifactId>openml-generic-python</artifactId>
<version>0.2.1</version>
</dependency>
  
```

Scikit-learn : The implementation in the openml-scikit module adds support for models built with scikit-learn.

```

<dependency>
<groupId>com.feedzai</groupId>
<artifactId>openml-scikit</artifactId>
<version>0.2.1</version>
</dependency>
  
```

### 3.7. OpenML generic Python model

This module contains an OpenML for loading custom code that implements Feedzai's Python API.

Imports a model with path '/random-forest-v1' to the Feedzai platform using this provider, assuming a 'classifier.py' file within it:

The code must contain a "Classifier" class with two methods:

```

# score the instance and return an array with the probability
for each of the classes
def getClassDistribution(self, instance):
    raise NotImplementedError("This must be implemented by a
concrete adapter.")
  
```

# return the predicted class

```

def classify(self, instance):
    raise NotImplementedError("This must be implemented by a
concrete adapter.")
  
```

Building Module: Command to build the model: mvn clean install

Environment supported: Python 3.6 with

```

* numpy
* scipy
* jep (this requires JAVA_HOME to be configured)
* scikit-learn (for the scikit provider)
  
```

## 4. RESULTS AND DISCUSSION

Implementation of machine learning model using Python with Feedzai open ML-AI based software system.

We used Jupiter and Python for training the model.

### 4.1 Steps for Integrate the model into Feedzai open ML Engine

*Step1:* customer original transaction information taken into the Feedzai ML engine

*Step2:* Prepare the data set

In this model we have taken a data set historical transaction.csv file with some columns that are very common for the fraud detection use cases

Timestamp, Amount, Entry mode, Card present,

Fraud target Column (Which states of a transaction is fraudulent or not?)

*Step 3:* Train the model

**Train Model**

```

In | : train_data = data[data.timestamp <= split_point]
      test_data = data[data.timestamp > split_point]

      train_features = train_data.drop(['timestamp', 'fraud_target'], axis=1)
      train_labels = train_data['fraud_target']

      test_features = test_data.drop(['timestamp', 'fraud_target'], axis=1)
      test_labels = test_data['fraud_target']

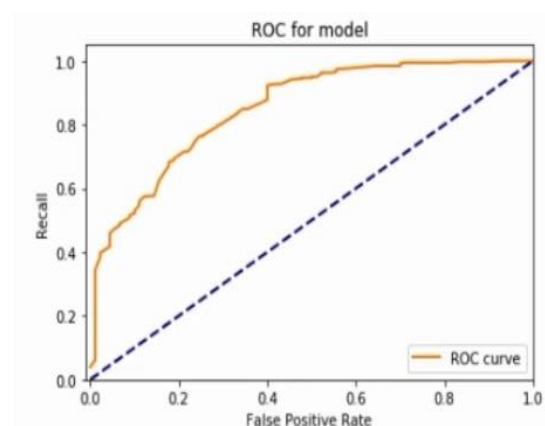
      # Random forest classifier
      #classifier = RandomForestClassifier(n_estimators=30, max_depth=5, criterion='entropy', verbose=1, n_jobs=7, bootstrap=
      # Gradient Boosting classifier
      classifier = GradientBoostingClassifier(n_estimators=3)

      #train
      classifier.fit(train_features, train_labels)
  
```

**Fig. 10:** Screen of Train the model

*Step 4:* Evaluate the performance of the model  
(What models are considered for evaluating the performance?)

Evaluate the data set and generates a rock curve.



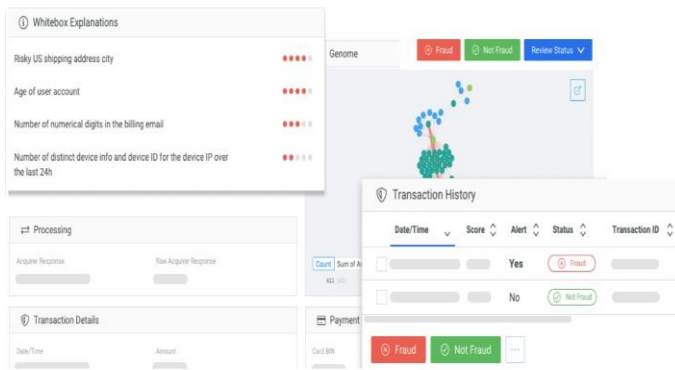
**Fig. 11:** Screen Evaluate the performance of the model

For integrating the model into the Feedzai runtime engine go to the transaction scoring workflow.

*Step 5:* Configure the fraud model external scoring service to integrate with the model that you just trained.

**Step 6:** Save the workflow publish the result. The application is published and the model is now in production.

**Step 7:** Listing all the transactions  
Case manager in the workflow lists all the transactions that are being scored by the model that are just put into production.



**Fig. 12:** Screen Transaction of fraud and not fraud

**Risk analysis:** Based on the transaction score, fraud alerts are identified from the convenient list.  
If something looks suspicious flag alerts

**Table.1 Models with performance**

Model	Frauds Detection Rate	Accuracy
KNN	38.62	78.23%
Naïve bayes	38.46	76.74%
Random forest	42.65	82.94%

## 5. CONCLUSION

The paper we have examined the cyber security defense mechanism by using artificial intelligence (AI), machine (ML)) techniques with the current Feedzai security model to identifying fraudulent banking transaction. Summary of usage of AI and its related technologies (ML & DL), in cyber security is examined. On the other hand, presented applications of Artificial Intelligence related technologies (ML&DL) to cyber security, and have analyzed the benefit of applying deep learning to cyber security and finally deployed a latest financial fraud detection technique using supervised machine learning random forest algorithm and implemented the experiment based on data set historical transactions CSV file. An experimental result shows financial firms can detect fraud and identify genuine transactions in real time using feedzai's software open ML tool with greater accuracy. In future, there will be several topics for integration of cyber security and AI technologies can be building for Novel and special AI algorithms.

## REFERENCES

- [1] Abeshu A, Chilamkurti N, 2018. Deep learning: the frontier for distributed attack detection in fog-to-things computing. *IEEE Commun Mag*, 56(2):169-175, <https://doi.org/10.1109/MCOM.2018.1700332>
- [2] Akhtar N, Mian A, 2018. Threat of adversarial attacks on deep learning in computer vision: a survey. *IEEE Access*, 6:14410-14430.
- [3] B. Biggio, I. Corona, D. Maiorca, B. Nelson, N. Srndic, P. Laskov, G. Giacinto, and F. Roli, "Evasion attacks against machine learning at test time," 2017, arXiv:1708.06131. [Online]. Available: <http://arxiv.org/abs/1708.06131>
- [4] Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam, "A Deep Learning Approach for Network Intrusion Detection System," *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2018.
- [5] G. Apruzzese, M. Colajanni, L. Ferretti, and M. Marchetti, "Addressing adversarial attacks against security systems based on machine learning," in *Proc. 11th Int. Conf. Cyber Conflict (CyCon)*, May 2019, pp. 1-18.
- [6] Wookhyun Jung, Sangwon Kim., Sangyong Choi, "Deep Learning for Zero-day Flash Malware Detection," *IEEE security*, 2017.
- [7] J. Gardiner and S. Nagaraja, "on the security of machine learning in malware c&c detection: A survey," *ACM Comput. Surv.*, vol. 49, no. 3, pp. 59:1-59:39, 2016.
- [8] G. Li, P. Zhu, J. Li, Z. Yang, N. Cao, and Z. Chen, "Security matters: A survey on adversarial machine learning," 2018, arXiv:1810.07339. [Online]. Available: <http://arxiv.org/abs/1810.07339>
- [9] Soleymanzadeh, Raha, Mustafa Aljasim, Muhammad W. Qadeer, and Rasha Kashef. 2022. "Cyberattack and Fraud Detection Using Ensemble Stacking" *AI 3*, no. 1: 22-36. <https://doi.org/10.3390/ai3010002>.
- [10] N. Martins, J. M. Cruz, T. Cruz and P. Henriques Abreu, "Adversarial Machine Learning Applied to Intrusion and Malware Scenarios: A Systematic Review," in *IEEE Access*, vol. 8, pp. 35403-35419, 2020, doi: 10.1109/ACCESS.2020.2974752.
- [11] H. Wang et al., "Deep Learning-Based Interval State Estimation of AC Smart Grids Against Sparse Cyber Attacks," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4766-4778, Nov. 2018, doi: 10.1109/TII.2018.2804669.
- [12] W. Xue, H. Wang, T. Wu, J. Peng and Y. Liu, "An Ensembled ELMS Based Defense Mechanism Against Cyber Attack on Power Systems," 2019 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), 2019, pp. 1-5, doi: 10.1109/APPEEC45492.2019.8994549.
- [13] X. Yuan, P. He, Q. Zhu, and X. Li, "Adversarial examples: Attacks and defenses for deep learning," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 9, pp. 2805-2824, Sep. 2019.
- [14] H. Amrouch, P. Krishnamurthy, N. Patel, J. Henkel, R. Karri and F. Khorrami, "Special session: emerging (Un-)reliability based security threats and mitigations for embedded systems," 2017 International Conference on Compilers, Architectures and Synthesis For Embedded Systems (CASES), 2017, pp. 1-10, doi: 10.1145/3125501.3125529.
- [15] C. Whyte, "Problems of Poison: New Paradigms and "Agreed" Competition in the Era of AI-Enabled Cyber Operations," 2020 12th International Conference on Cyber Conflict (CyCon), 2020, pp. 215-232, doi: 10.23919/CyCon49761.2020.9131717.



© 2022 by B. Narsimha, Ch V Raghavendran, Pannangi Rajyalakshmi, G Kasi Reddy, M. Bhargavi and P. Nares. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).