

# Cyber Security Automation

## Applying AI,ML and DL In Cyber Security & Digital Forensics( Algorithms, Tools and Codes)

**Amrit Chhetri,**

DFIR Expert | AI & Cyber Security Researcher  
Cyber Security Architect & CEI(RCS, Siliguri, West Bengal)  
Certified Forensic Psychologist,  
Associate Technical Editor(4N6)  
Tech Speaker and Forensic Researcher( My Cyber Hubs & Merapps)  
Member Of: DSCI( Individual) & Nasscom Community

# About AMRIT CHHETRI

- **Me:**

- I'm Amrit Chhetri from Darjeeling, West Bengal, India. Currently, based in Siliguri with residence at 3A, 3<sup>Rd</sup> Floor, Medicare Building, Lower Bhanu Nagar, Siliguri-734004, WB, India. I'm CEI(Certified EC-Council Instructor) with following Global Certifications:
  - CSCU, CEH, CHFI, CTIA, CSA, ECSA from EC-Council
  - Certified Smart City Expert from King's University, UK and 100 Plus other Certifications
- Since February 2020, I'm working as **Associate Technical Editor**, Digital Forensics Mentor and Research Lead for Digital Forensics Journal(D4N6)
- Also, I'm DFIR Analysts and Cyber Security and AI Researcher

- **Edge AI Certifications and Research Papers:**

- Udacity-Intel Edge AI IOT Developer Scholarship
- I've presented 4 plus Research Papers in the fields of Forensics with AI, BigData, IOT Security and Cyber Security Architecture

- **Experiences and Projects:**

- 18 Plus Years of Experiences and 7 Years in Cyber Security, Incident Response, VAPT and Digital Forensics
- I was J2EE Developer and BI System Architect/Designer of DSS for APL and Disney World
- I have played the role of BI Evangelist and Pre-Sales Head for BI System\* from OST
- I have worked as Business Intelligence Consultant for national and multi-national companies including HSBC, APL, Disney, Fidelity, LG(India), Fidelity, BOR( currently ICICI), Reliance Power. \* *Top 5 Indian BI System ( by NASSCOM)*

# Certifications and Research Papers:

## Cyber Security Certifications( Of Amrit Chhetri)



## AICTE- STTP Certifications:



## Community Engagements(AIML, Cyber Security & DFIR)



## Instructor/Faculty Development Certifications( C-DAC, EC-Council)



## Vendor Free Certifications



## Speaker Certificates( CII, 4N6, AMITY, THM, CU):



## AI/ML/DL Certifications:

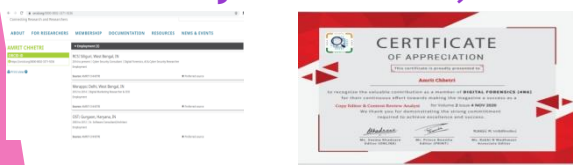


## Mentor Certificates



Press from 4N6>

## Cyber Security Researcher, Forensics Tech Editorial & Articles:



# What Audience Will Learn?

"AI and ML can give businesses a **competitive edge** in information security and data safety. To deal with the Cyber Security threats of the future, businesses need to embrace AI and ML-based tools and security mechanisms"- *Nathan McKinley, Cerdonis Technologies*

## 1. AI Basics

## 2. Secure By Design & Security Automation

## 3. AI In Cyber Security

## 4. AI Models for Cyber Security

## 5. Penetration Testing( Basics)

## 6. ML in Penetration Testing

## 7. AI-Based Security Controls

## 8. Security Audit And Cyber Acts

### Participants will learn:

- \* Cyber Resilience and Artificial Intelligence
- \* Cyber Threat Modeling and Cyber Threat Intelligence
- \* Machine Learning Frameworks
- \* AIML Dev. Platforms-Penetration Testing
- \* Incident Response And Cyber Security
- \* AI-Based Penetration Testing and Security Tools
- \* Designing of AI-Powered Security Controls
- \* Cyber Security Architecture for AI-Based Controls
- \* Adoption of Responsible AI
- \* Information Security Frameworks
- \* **"AI for Security"** Skills Building Strategies

### Scope of AI in Cyber Security (Security Domains):

- ▶ **Threat Modeling** - Enhancing Threat Modeling Procedures
- ▶ **Cyber Threat Intelligence** - Automated and enhanced Information collection and sharing
- ▶ **Risk & Vulnerability Assessment** - Identifications and Analysis of Risks and Vulnerability

# Agendas-AI in Cyber Security:

- Understanding AI & AI
- Scope of AI in Cyber Security
- Threat Modeling And Cyber Threat Intelligence
- Security Strategy & Testing Methodology
- Penetration Testing with AI
- Cyber Insurance and Cyber Economics
- Use Cases of AI In Cyber Security

# Understanding AI Basics

# Understanding Edge AI:

## Artificial Intelligence and Machine Learning

1. AI is an Intelligent System that imitates Human-Intelligence for Learning and completing complex tasks where as Machine Learning is subset of AI where Machine learns from Data and takes decisions. The classification which are not labeled is called Clustering

2. AI Frameworks: TensorFlow, Keras, PyTorch, CoreML, ScikitLearn and Custom Frameworks such as SAP Leonardo AI

## Edge AI:

1. Edge AI is a Intelligent System that runs AI Models locally on Hardware device such as NCS(Intel Neural Compute Stick), Google Edge TPU, Nvidia Jetson Nano and FPGA, without requiring Network connection

2. Edge AI can run on wide range of Systems-Data Center Servers, IOT Devices, FPGA, SCADA/IIOT System



## Benefits of AIML (Standard):

- \* Mathematical Mapping with Security Problems
- \* Automation of CTIA and Cyber Security
- \* Open Source Frameworks
- \* Global Community Support
- \* AIML Upskilling Support & Easy Access

## Benefits of Edge AI (Standard):

- \* Real-Time Decision Capability
- \* Low or Zero-Latency
- \* Automation Cyber Security Cost Analysis
- \* Automation of CSIRT Services(Alerts and warnings, incident handling)
- \* Root Cause Analysis-Cyber Threats & Controls

## Scope of AI in Cyber Security ( Security Domains):

- ▶ **Penetration Testing** - Information Gathering, Exploitation, Security Controls and Audit
- ▶ **Digital Forensics** - SOC and NOC
- ▶ **Incident Response and Incident Management**



# AI Environment for Cyber Security:

## AI Environment:

- \* **Data Scientist Tools** : Jupyter Notebook( on Anaconda Navigator, Kaggle), IBM-SPSS, BigData Analytics
- \* **Neural Network Designing Tools**: Neural Network Designer
- \* **Model Converters** : Intel OpenVINO Toolkit

## Edge AI Hardware:

\* Edge AI can be deployed in low-end Hardware -such as CPU, FPGA, Intel Neural Compute Stick(NCS), etc.Model Converter makes AI Models compatible in the selected Hardware or Platforms. This supports AI Models for Cyber Security in designated devices such IOT Devices.

**Model Converters**: Intel OpenVINO Converter( mo.py), NVIDIA Converter, SDK-based Converter, etc.

## Sample SQL Code :

## Deployment Options for Hardware for Edge AI:

Type	Hardware Specifications
CPU	New CPU Box or Free CPU
External AI Devices	Intel Neural Compute Stick Google Edge TPU FPGA
GPU	
Browser AI	AI-Based Security Plugin Security Models like Cookie
Mobiles AI	AI-Based Security on Apps AI-Based Agent from SIEM, EDR, EPP
Embedded AI	Micro-Controller

## Scope of AI/Edge AI in Cyber Security ( Security Domains):

- ▶ **Secure By Design** ( API Testing) and **Privacy By Design** - AI-Based System Design Patterns or Frameworks
- ▶ **Edge AI on Endpoints or Endpoint Protection**
- ▶ **Card Skimmer Device Detection- ATM Security**



# Edge AI Devices: Edge Computing Security





## Edge Computing and Edge Devices on Security:

**Edge Computing** needs new Architecture of Security but Edge Computing or Edge Devices adds extra Advantages in designing Automated Security Controls too.

## Edge AI Devices:

Edge AI enriches functions of Cyber Security and selection of Hardware for Edge AI is strategic but complex and challenging. "ML is teaching programs to find the malicious part, without us having to list all the factors they've been looking for." - Rick Howard, Chief Security Officer, Palo Alto Networks

## Great Edge AI Devices:

Device	URL/Websites	
Nvidia EGX A100	<a href="https://www.nvidia.com/en-in/data-center/products/egx-edge-computing/">https://www.nvidia.com/en-in/data-center/products/egx-edge-computing/</a>	
Intel Neural Compute Stick 2	<a href="https://www.intel.com/content/www/us/en/products/boards-kits/compute-stick.html">https://www.intel.com/content/www/us/en/products/boards-kits/compute-stick.html</a>	
NVIDIA Jetson Nano	<a href="https://developer.nvidia.com/embedded/jetson-nano-developer-kit">https://developer.nvidia.com/embedded/jetson-nano-developer-kit</a>	
Google Edge TPU	<a href="https://aiyprojects.withgoogle.com/edge-tpu">https://aiyprojects.withgoogle.com/edge-tpu</a>	
FPGA		
Raspberry PI/Adruino		

## Edge AI Powered Security: In Actions:

- ▶ Security of Autonomous System Security
- ▶ Smart-city Monitoring
- ▶ Video Security Analytics

# Edge AI-Based Security-Design Strategies:

## Edge AI Model- Eye Tracking UBEA:

### 1. Gaze Estimation Model

([https://docs.openvinotoolkit.org/latest/\\_models\\_intel\\_gaze\\_estimation\\_adas\\_0002\\_description\\_gaze\\_estimation\\_adas\\_0002.html](https://docs.openvinotoolkit.org/latest/_models_intel_gaze_estimation_adas_0002_description_gaze_estimation_adas_0002.html))

### 2. Face Detection Model

([https://docs.openvinotoolkit.org/latest/\\_models\\_intel\\_face\\_detection\\_adas\\_binary\\_0001\\_description\\_face\\_detection\\_adas\\_binary\\_0001.html](https://docs.openvinotoolkit.org/latest/_models_intel_face_detection_adas_binary_0001_description_face_detection_adas_binary_0001.html))

### 3. Facial Landmarks Detection Model

([https://docs.openvinotoolkit.org/latest/\\_models\\_intel\\_landmarks\\_regression\\_retail\\_0009\\_description\\_landmarks\\_regression\\_retail\\_0009.html](https://docs.openvinotoolkit.org/latest/_models_intel_landmarks_regression_retail_0009_description_landmarks_regression_retail_0009.html))

### 4. Head Pose Estimation

([https://docs.openvinotoolkit.org/latest/\\_models\\_intel\\_head\\_pose\\_estimation\\_adas\\_0001\\_description\\_head\\_pose\\_estimation\\_adas\\_0001.html](https://docs.openvinotoolkit.org/latest/_models_intel_head_pose_estimation_adas_0001_description_head_pose_estimation_adas_0001.html))

## Edge AI in Cyber Security Approaches:

### Types/Models:

1. Purchase - Of AI-Based Security Tools
2. In-House Development

### In-House Development - Platforms:

1. Model Converter and Model Optimizer -Intel OpenVINO Toolkit
2. AIML Frameworks and AI Model - OSS, Community or In-House Development
3. Mater Model Designing Principles
4. MS Threat Modeling Tool - MITRE ATT&CK Navigator, etc
5. Cyber Intelligence Tools- AlienVault OSSIM, Exabeam Analytics

### Security Analytics:

1. Larger Scale - Data Lake
2. Standard SOAR Analytics

## Edge AI on Cyber Security:

Embedded AI for Cyber Security: SCADA, ICS(Industrial Control System), CSP, IIOT

Emerging Cognitive Systems: AI, VR and Mixed Security, XANN Security

Future Scopes : Autonomous System Security, SWARM Intelligence Network, Digital Twins System

### AI-Based Security Tools

***DarkTrace: Cyber AI Platform that secures IT DNA protected and secure***

The background features abstract, overlapping geometric shapes in various shades of pink and purple, creating a modern, tech-oriented aesthetic.

# Scope of Edge AI in Cyber Security plus Threat Modeling And Cyber Threat Intelligence

# Scope Of AI In Cyber Security?

## Applicable Areas:

- \* Threat Modeling And Cyber Threat Intelligence
- \* Risk and Vulnerability Assessment
- \* Penetration Testing
- \* Digital Forensics - SOC and NOC
- \* Incident Response

## Digital Forensics:

- \* Malware Detection - Classification
- \* Malware Feature Extraction
- \* Website Detection and Analysis
- \* Botnet Detection
- \* AI/Edge AI on Fraud Detection
- \* Edge AI on Suspect Identification
- \* Fraud Detection and Analysis
- \* Malicious URL Detection
- \* PIM( Personal Identify Management) Security

## Consideration Essentials:

- ▶ Availability of Cyber Security Policies
- ▶ BIA( Business Impact Analysis)
- ▶ Technological Stacks

- \* Secure By Design ( API Testing)
- \* Edge AI on Endpoints or Endpoint Protection
- \* Card Skimmer Installation Detection - *Computer Vision*
- \* Fast Flux Detection
- \* Cyber Security Controls

## Scopes

- \* Penetration Testing with Machine Learning
- \* Digital Forensic Readiness
- \* IOT Device Reconnaissance
- \* Crime Hotspot Tracking and Geospatial Analysis
- \* Data and Content Security
- \* Security Controls of ICS(Industrial Control Systems) and SCADA
- \* Spam Filter Applications
- \* Secure User Authentication and 2-F
- \* Security Analytics - AI Models and Data Lakes

# Modern Cyber Threats:

## AI-Powered Attacks:

Risk and Vulnerability Assessment is executed to know current Posture of Cyber Security where as Threat Modeling is performed to map Possible Cyber Threat Landscape/Surface Areas. Threat Models are used in CTAI, PenTesting, etc.

## AI-Powered Attacks :

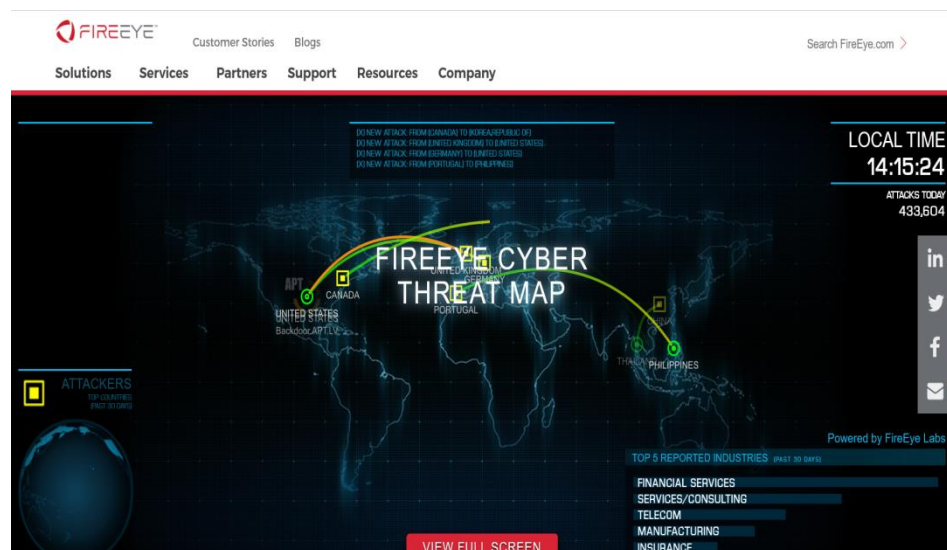
IBM Deep Locker - AI-Based Malware

([https://researcher.watson.ibm.com/researcher/view\\_group.php?id=4354](https://researcher.watson.ibm.com/researcher/view_group.php?id=4354))

## AI-Based Information Gathering:

Deep Exploit and similar

FireEye Cyber Threat Map

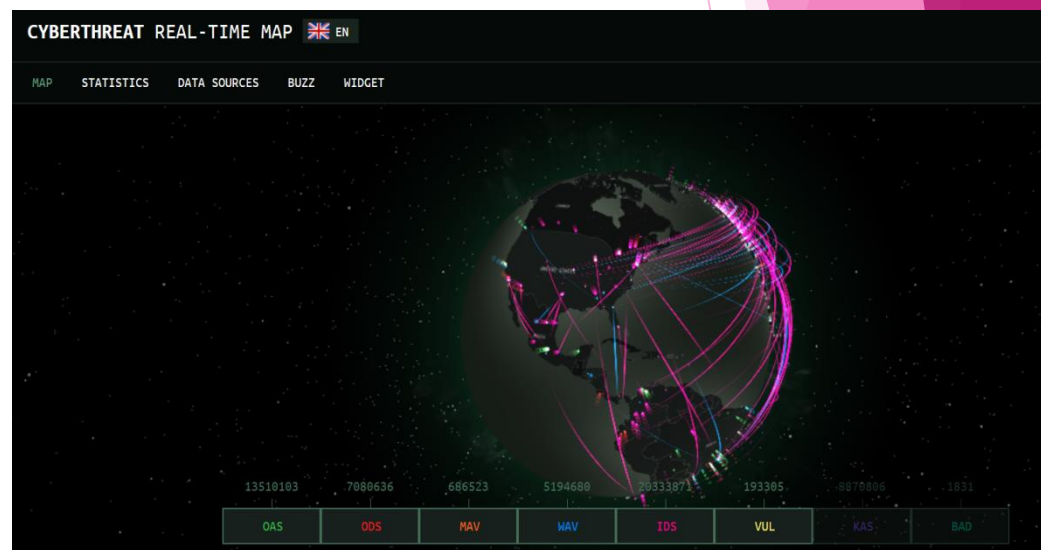


## Top 5 Reported Industries:

(URL: <https://www.fireeye.com/cyber-map/threat-map.html>)

- ▶ Financial Services, Consulting
- ▶ Telecommunication, Manufacturing Insurance

## Kaspersky Cyber Threat Map



## Top 5 Attack Types:

(URL: <https://cybermap.kaspersky.com/>)

- ▶ Botnet Activity Detection(BAD), Vul. Scan
- ▶ On-Demand Scan(ODS), IDS( Intrusion Detection System)

# Cyber Threat Modeling:

## Cyber Threat Modeling:

Cyber Threat Model is structured process that identifies potential Security THREATS & Vulnerabilities, quantify the impacts of those Threats and prioritize Techniques to mitigate attacks and to protect IT systems. "Threat Modeling works to identify, communicate and understand threats and mitigations with the context.." -OWASP . To map the Scope of Edge AI in Security Testing and Control Designing, Threat Modeling allows to cover all possible Cyber Threats in Pre-Engagement Phase.

## MITRE ATT&CK - Threat Modeling for Threat Intelligence and Cyber Security:

MITRE ATT&CK is global repository of adversary Tactics and Techniques based on real-world observations. It is used as Foundation TT on Cyber Threat Modeling in private, public and government sectors, by Cyber Threat Analysts and Researcher, to acquire Cyber Resilience

## Common Use Cases(Categories):

- Detections and Analytics
- Threat Intelligence
- Adversary Emulation and Red Teaming
- Assessment and Security Engineering

## Cyber Threat Modeling Tools: ATT&CK Navigator

Description:

A tool to help navigate, annotate, and visualize ATT&CK for Cyber Security exercises.

Website: <https://mitre-attack.github.io/attack-navigator/enterprise/>

## Adopting Cyber Threat Modeling:

- ▶ Perform Cyber Risk Assessment
- ▶ Evaluate Threat Modeling Frameworks and Tools such as Microsoft Threat Modeling Tool
- ▶ Start with Basic Modeling

# Cyber Threat Intelligence:

## Cyber Threat Intelligence:

Cyber Threat Intelligence( CTI) is Information about Threats and Threat Actors that helps in mitigating Cyber Incidents and Malicious events in IT Ecosystem. It is performed under ICO( Intent, Capability and Opportunity) Triad to know IOC( Indicator Of Compromises). Some of common Techniques of Cyber Threat Intelligence are:

OSINT

HUMINT

SOCIAL ENGINEERING

## Objective of CTI :

Cyber Security Analysts can adopt CTI in IT Security exercises powered/support Machine Learning for

1. Improved Cyber Incident Detection
2. Enhanced and Automated Incident Prevention
3. Automation of Security Operations and Remediation Activities
4. Improved Risk Management
5. To understand Attacks Equations

***Attacks = Motives+ Methods+ Vulnerability***

***Risk = Probability \* Potential ( Risk directional proportionate with Probability)***

## CTI Use Cases/Functions:

1. Alarm, Events and Alerts
2. Incident Response and Malware Analysis
3. Investigation and Mitigation
4. Fusion Analysis and Cyber Threats Collaborations

## Cyber Threat Intelligence Tools :

- ▶ AlientVault USM , IBM X-Force Exchange
- ▶ Threat Connect, ELK( Kinana Dashboard)
- ▶ Splunk Enterprise



# Security Strategy & Testing Methodology

# Security Strategy & Testing Methodology:

## Security Strategy:

- \* Engage with Security Initiative for AI-Based Security Ecosystem
- \* Perform Security Assessment- DSCI CAF
- \* Evaluate AI-Based Tools
- \* Perform Penetration Testing with AI - DSCI CAF with LPT other Methodology
- \* Design AI-Powered Security Controls -Based on Penetration Testing Report
- \* Perform Internal Assessment

### Security Assessment

(Accessing exiting Security Posture and it is also part of Vulnerability Assessment)

### Vulnerability Assessment

(Finding Weakness, misconfiguration and issues  
Phases: Vulnerability Scanning and 2. Vulnerability Analysis)

### Penetration Testing

(Exploiting identified Vulnerabilities to design/device Security Controls  
Stages: Pre-Attack, Attacks and Post-Attacks  
Vulnerabilities and Exploits Mapping for Security Testing:  
Rapid7, Offensive Security, NVDB, etc)

## DevOps in Edge AI-Based Cyber Security :

1. Collaborative Project Management Tool :MS Project 2019
2. Source Code Management : Git, GitHub
3. Project System, Logs Analysis: Nagios, LogRythm
3. Continuous Vulnerability Assessment :Script, Artificial Intelligence, RPA, PenTesting Bots
4. In-Project Upskilling

# Penetration Testing Methodology:

## OSSTM:

Open Source Security Testing Methodology is open standard Methodology and OSSTMM is maintained by Institute of Security and Open Methodologies( ISECOM). "OSSTM covers 10 Security domains-

**Human Security** :Cyber Security Awareness, Training and Security Community Engagement

**Physical Security** : Security of Physical Systems or Devices, Wireless Communications -:Security of WiFi, NFC, Bluetooth, RFID, GSM(Networks)      Data Security - Security against 7 Security sub-domains such Spoofing, Phishing, etc.

## EC-Council LPT Penetration Testing Methodology:

LPT Penetration Testing Methodology is another well researched and well-outlined Penetration Testing Methodology. This is really IDEAL for AI-based Penetration Testing

Phase LPT Penetration Testing :

Pre-Engagement -> Information Gathering -> Vulnerability Assessment -> Exploitation-> Report Writing-> Information Control Designing

## Cyber Kill Chain Method :

CKC(Cyber Kill Chain) is an well accepted and effective way to know/illustrate how adversaries or attack the systems. It helps in Identification and prevention of Malicious Intrusion Activities and can be considered as one of Penetration Testing Methodology.

Phases of Cyber Kill Chain: :

1. Reconnaissance : Information Gathering to probe weak points or vulnerability
2. Weaponization : Creates a deliverable and Malicious Payload
3. Delivery : Sends Weaponized bundle to victim using Email, USB , Botnets
4. Exploitation : Exploits Vulnerability by executing code
5. Installation : Installs Malware on target system
6. Command and Controls: Creates CnC Channel to communicate and pass data back and forth
7. Actions and Objectives: Performs Actions to achieve INTENDED goals

## SANS Testing Methodology: Testing Methodology from SANS

# Penetration Testing with AI (Intelligent Security System)

# AI for Security-Labs:

## AI for Security- Offensive Vs. Defensive :

**Offensive Site of AI/Attacks by AI:** \* AI Voice Attack \* Information Gathering \* Social Engineering ...

**Defensive Site of AI/Attacks by AI:** \* PenTesting \* Malware Analysis \* Automation \* Threat Monitoring( DarkTrace)

## Edge AI Model Learning Techniques:

1. Supervised      2. Unsupervised   3. Semi-Supervised   4. Reinforcement   5. Deep Reinforcement Learning

## Machine Learning Frameworks for Cyber Security:

### 1. On-Premise :

1. TensorFlow 2. Keras 3. PyTorch 4. CoreML

### 2. Machine learning as a service (MLaaS) :

Amazon AWS Machine Learning

Google Machine Learning

Azure Machine Learning

Kaggle Machine Learning

## Components of Edge AI for Cyber Security:

### 1. Models

### 2. Edge AI Platforms

1. TensorFlow, TensorFlow Lite

2. OpenVINO Toolkit

3. Intel VTune Amplifi

### 3. Datasets/Pipes/Video Streams -Data Lake

## Malware Analysis using Edge AI: Steps and Research Scope

1. Prepare Datasets 2. Make Edge AI Environment Ready - OpenVINO , NVIDIA SDK

3. Run Model Optimizer and Model Converter 4. Deploy on Edge Device on Lab Env. - FPGA, Intel Neural Computer Stick

5. Install on selected Computer - to analyze and protect from Malware

## Intel OpenVINO (Preparing Edge AI for Cyber Security Labs. - On Linux):

1. Install Ubuntu 20.04 LTS

2. Install Pre-requisites

3. Install OpenVINO Tools for Linux

4. Installation Steps

GitHub Project URL:

5. Model Conversion

## Intel OpenVINO (Preparing Edge AI for Cyber Security Labs. - On Windows)

1. Install Windows 10 ( 64-Bits)

2. Install Pre-requisites

3. Get and install IntelOpenVINO Tools 2020

4. Model Conversion ( Short Video with Audio)

## Labs Testing Demos:

1. Number Plate Detection - Physical

Security

# Penetration Testing using AML:

## Purchase Vs. Build- Penetration Testing Tools:

- \* Purchase : Expensive but ready-to-used
- \* In-House Development: Lengthener but effective for Modern Cyber Attacks

## Edge AI Model Learning Techniques:

1. Supervised
2. Unsupervised
3. Semi-Supervised
4. Reinforcement
5. Deep Reinforcement Learning

## Key Considerations:

1. All Systems Considerations -Data, UI, Network
2. Security by Design or Security Automation Practice
3. Appropriate Security Frameworks AML Solutions
  - \* DSCI CAF for Security Assessment
  - \* NIST 800-160( System Security Engineering ) for Machine Learning Models
  - \* Security Guidelines/Frameworks -from SEBI, TRAI, CERT-IN
  - \* Cyber Threat Modeling and Cyber Threat Intelligence
4. Standards of Penetration Testing Report
5. Pre-PenTesting Security Assessment( or Audit)
6. Security Assessment Tools:
  1. Nessus
  2. OpenAudit
  3. NS Auditor and more
7. Evaluation of :
  1. Cloud Vs. On-Premises Solutions - Edge AI
  2. Machine Learning As-A Service with Edge AI

## AI for AI: Securing AI Systems:

1. Standard Practice -Information Gathering
2. Vulnerability Assessment- Nessus
3. System Exploitation-Maintaining Access
  - \* Static Analysis of IR(OpenVINO .xml and bin)
  - \* Dynamic Code Analysis of AI Model-Eclipse Debugger, Code Review Platforms
4. Encrypted AI Models
5. DevOps for Cyber Security Practices

## Designing AI-Powered Security Controls :

1. Know the Security Goals well
2. Include Solutions in Trends
  1. SOC/NOC
  2. Sanboxing
  3. NGFW( with AI)
3. Adopt Standard Practices:
  1. Secure By Design
  2. Multi-Layer Secure Design
4. Initiate Internal Researches - Edge AI for Cyber Security

## AI-Penetration Testing Tools:

1. **MIT AI 2:** Cyber Attack Prediction, useful in Cyber Threat Modeling, CTI
2. **Deep Exploit :** Information Gathering, Explorations, Pos-Exploitations, etc.  
(Website: [https://github.com/130-bbr-bbq/machine\\_learning\\_security/wiki/deep-exploit](https://github.com/130-bbr-bbq/machine_learning_security/wiki/deep-exploit))
2. **Deep Code:** Symantec Code Analysis  
(<https://www.deepcode.ai/>)

# Use Case of Edge AI in Cyber Security: 13

## AI-Based Anti-Virus: BlackBerry Cylance:

- \* Next Gen Anti-Virus with built-in EDR powered by Edge AI-Based
- \* Core Functions by Edge at Edge
- \* Website: <https://www.cylance.com/en-us/index.html>

## AI-Based Anti-Virus: Virus Total

- \* Online Anti-Virus solution with Built-In AI
- \* Detects by File, Hashes and URL

## AI-Based Enterprise DNA Security : DarkTrace

- \* Self-Learning AI for Cyber AI that protects Enterprise DNA through AUTONOMOUS RESPONSE
- \* AXA IT's Network Security by DarkTrace

## Intelligent UBEA(UEBA (User And Entity Behavior Analytics): Exabeam Analytics

- \* Intelligent Security System with Video Analytics

## Physical Security: Artificial Intelligence Based Human Efface Detection (ABHD):

- \* The criminal Registration & Identification Systems
- \* Developed for LEA and Police Offices in India

## Malware Analysis using Edge AI - Resources

1. **Books:** Mastering Machine Learning for Penetration Testing , Chiheb Chebbi \* GrayHat Python
2. **Vendor Courses:** \* Intel Data Center To Edge AI - from Intel Academy  
\* AI Foundation from Nasscom - <https://skillup.online/courses/course-v1:NASSCOM+FOUNDAI100+2019/about> ,
3. **Research Papers:**  
Deep Reinforcement Learning: <https://arxiv.org/pdf/1602.01783.pdf>

## Upskilling for Edge AI In Cyber Security:

- \* Engage with AIML Community - GitHub, Facebook, etc.
- \* Acquire Global Security Certifications -
- \* Register for Online Courses from Universities -Cyber Security ...
- \* Engage with Vendor Specific Initiatives- Webinars, Courses, Challenges
- \* Refer Great Books in Cyber Security
- \* Prepare towards to extremes
  - \* NIST 800-160
  - \* Embedded AI for Cyber Security
  - \* Organize Challenges in “Edge AI for Cyber Resilience” Theme



# Impacts Of QML(Q Machine Learning):

## Impact Of Quantum Machine Learning:

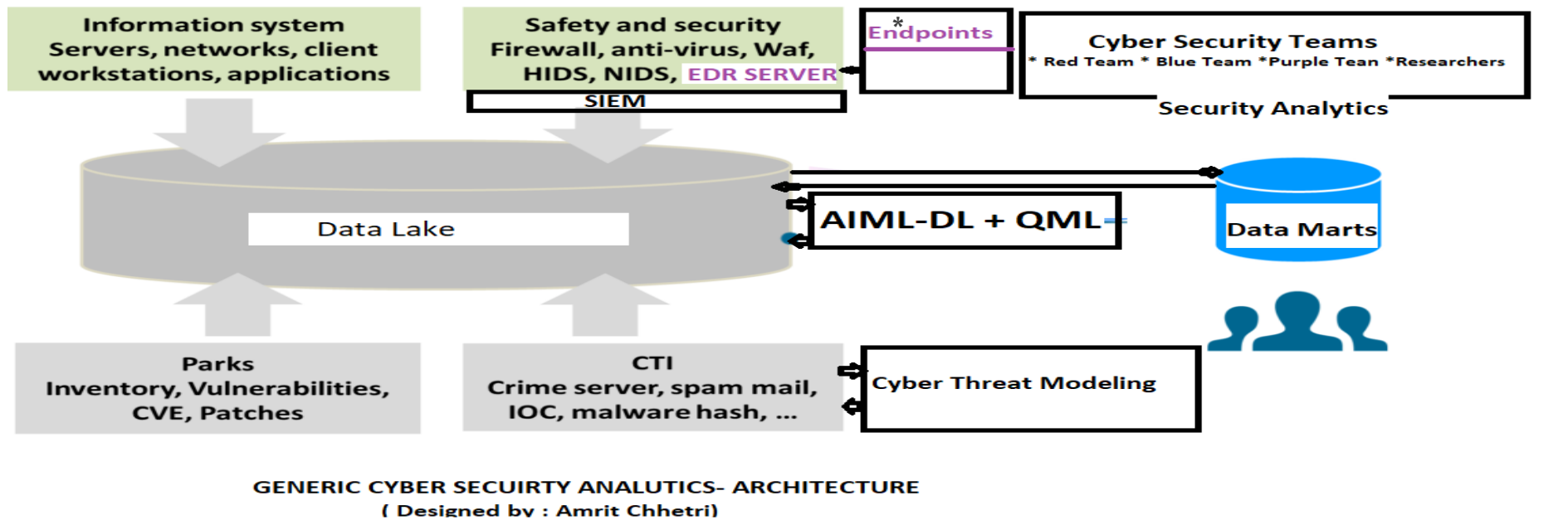
- \* Enhanced Classical AI-Based Cyber Security Assessment, Testing and Security Controls
- \* Adding Quantum Computation in Cyber Security Analytics
- \* Enhancement on TensorFlow Extended (TFX) large Scale Solution
- \* Projected TensorFlow Embedded with QML in Sanboxing

## QML In AI-Based Security

- \* API & GUI Testing, Sandboxing, CTIA
- \* Malware Detection

## QML API/Platforms:

- \* TensorFlow Quantum
- \* PennyLane



## Security Analytics and Genx System Synchronization :

### 1. AI-Based Solution/Product:

- \* Cloud-Based Machine Learning
- \* Microservice-compatible Security System Design
- \* Open-ended Architecture for AI

### 2. Standard Frameworks- NIST System Security

## Model, Edge & Algorithm Evaluation:

- \* Q CNN - Anomaly Detection
- \* Blockchain SWARM Intelligence - for own Security
- \* Edge Computing and Edge in Security Design

# Q & A

*Edge AI In Cyber Security* Masterclass Session: 50 Minutes  
Duration: 10 Minutes

# Machine Learning Environment

( On Anaconda Navigator, PyCharm, Docker, OpenVINO Toolkit & Google Colab )

# Agendas:

1. Install and configure Anaconda Environment
2. Install and configure PyCharm Environment
3. Install and configure OpenVINO Environment
4. Install and configure Colab Environment
5. Install and configure Docker Environment - GPU Support
6. How Be Champion ML System Analyst for Cyber Security
7. How Be Champion ML System Analyst for Cyber Security

## Malware Analysis using Edge AI: Steps and Research Scope

1. Prepare Datasets
2. Make Edge AI Environment Ready - OpenVINO , NVIDIA SDK
3. Run Model Optimizer and Model Converter
4. Deploy on Edge Device on Lab Env. - FPGA, Intel Neural Computer Stick
5. Install on selected Computer - to analyze and protect from Malware

# Install and configure Anaconda Environment:

## Python Installation:

1. Get right version of Installer, Python 3.8 from <https://www.python.org/downloads/release/python-386/>
2. Install with default option
3. Run > python -V to know the version

```
Command Prompt
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\LENOVO>python -V
Python 3.7.6

C:\Users\LENOVO>
```

## Python Features/ Characteristics:

1. Interpreted Programming Language with OOP
2. Easy write and supported by ML Frameworks
3. Cross-Device support, more at <https://www.geeksforgeeks.org/python-features/>

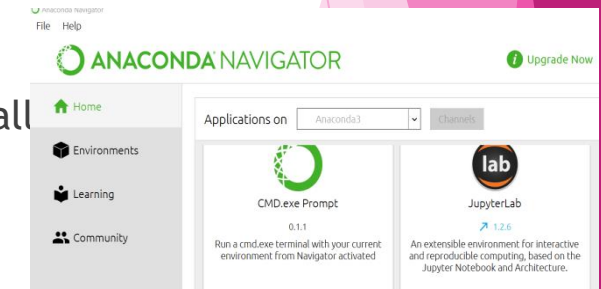
## Anaconda Installation:

1. Get right version of Installer, from <https://www.anaconda.com/products/individual>
2. Install with default option
3. Start Jupyter Notebook and run simple Python Code(file reading)

Ref. : <https://jupyter-notebook-beginner-guide.readthedocs.io/en/latest/install>

## Anaconda Features/ Characteristics:

1. Cross-Framework support - TensorFlow, PyTorch, Keras ..
2. Reliable
3. Integrated multiple IDEs - Jupyter Notebook, PyCharm, ..



## Important Point on Jupyter Notebook:

1. Select right Environment under “**Application On**”
2. Organize Program Files using by creating function-specific **folders**
5. Add comments/remarks and Study Notes using “**markdown**” option

# Install and configure Anaconda-2:

## TensorFlow for Jupyter Notebook (Using Conda Prompt):

1. Create TensorFlow Python Environment > `conda create --name TensorFlow2X`
2. Activate Environment > `conda activate PyTorch`
3. Install TensorFlow > `conda install Tensorflow`

## TensorFlow for Jupyter Notebook (Using ! Option):

1. Start Jupyter Notebook with right "Application on"
2. Add Command Cell and write:  
`!pip install --upgrade pip , !pip install numpy , !  
pip install pandas , !pip install tensorflow`

## Keras for Jupyter Notebook:

1. Start Jupyter Notebook with right "Application on"
2. Add Command Cell and write:  
`!pip install keras`

Reference: [https://keras.io/getting\\_started/intro\\_to\\_keras\\_for\\_researchers/](https://keras.io/getting_started/intro_to_keras_for_researchers/)

## PyTorch for Jupyter Notebook (Using Conda Prompt):

1. Start conda prompt ( run Admin Mode)
2. Create environment> `conda create --name PyTorch`
3. Activate PyTorch > `conda activate PyTorch`
4. Install PyTorch> `pip3 install torch==1.7.1+cpu torchvision==0.8.2+cpu torchaudio===0.7.2 -f`

[https://download.pytorch.org/whl/torch\\_stable.html](https://download.pytorch.org/whl/torch_stable.html)

## PyTorch for Jupyter Notebook (Using ! Option):

1. Start Jupyter Notebook with right "Application on"
2. Add Command Cell and write:  
`!pip install torch  
!pip install torch==1.7.1+cpu torchvision==0.8.2+cpu torchaudio===0.7.2 -f`

[https://download.pytorch.org/whl/torch\\_stable.html](https://download.pytorch.org/whl/torch_stable.html)

# Install and configure Pycharm Environment:

## Python Installation:

1. Get right version of Installer, Python 3.8 from <https://www.python.org/>
2. Install with default option
3. Run > python -V to know the version

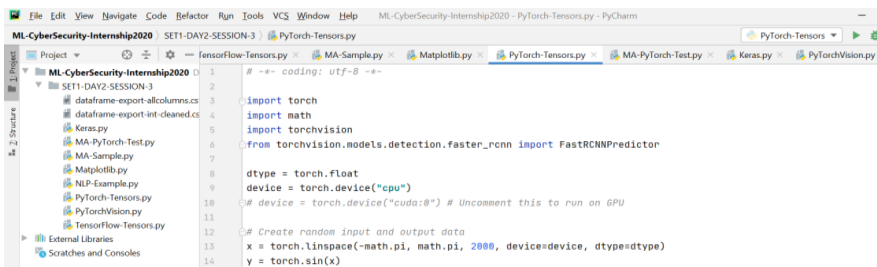
## Pycharm Installation:

1. Get right version of Installer, from <https://www.jetbrains.com/pycharm/download/#section=windows>
2. Install with default option
3. Start PyCharm IDE and write sample code

Ref: <https://www.jetbrains.com/pycharm/download/#section=windows>

## Pycharm Features/ Characteristics:

1. Supports all DevOps functionality - GitHub, Monitoring,
2. Easy to use
3. Availability of all great Add-ons



## Best Practices of Using Pycharm:

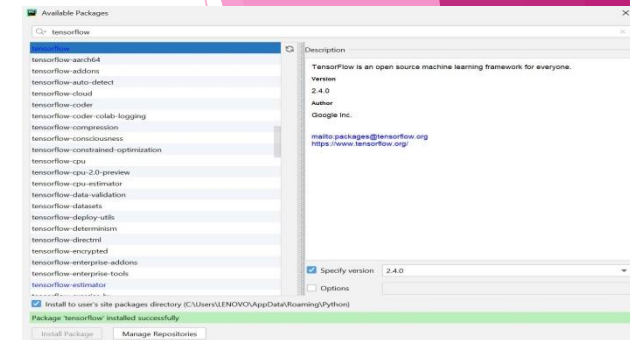
1. Maintain Project specific to one Business/Project requirements
2. Always use Debug Function to debug the code



# Install and configure PyCharm-2:

## TensorFlow with PyCharm IDE -Installation -Steps:

1. Create a Project folder "ML-CyberSecurity-Internship2020" in Base Folder
2. Start PyCharm and select newly created folder
3. Click on File-> ML-CyberSecurity-Internship2020 -> Search TensorFlow module and install
4. Create new folder "SET1-DAY2-SESSION-3"
5. Write TensorFlow Code to display Tensors on TensorFlow



## Keras with PyCharm IDE -Installation -Steps:

1. Start PyCharm and select newly created folder
2. Click on File-> ML-CyberSecurity-Internship2020 -> Select Keras
3. Create new folder "SET1-DAY2-SESSION-3"
4. Write TensorFlow Code to display Tensors on Keras

## PyTorch with PyCharm IDE -Installation -Steps:

1. Start PyCharm and select newly created folder
2. Click on File-> ML-CyberSecurity-Internship2020 -> Select Pytorch
3. Create new folder "SET1-DAY2-SESSION-3"
4. Write TensorFlow Code to display Tensors on Pytorch

## Gensim with PyCharm IDE -Installation -Steps:

- 1 Start PyCharm and select newly created folder
2. Click on File-> ML-CyberSecurity-Internship2020 -> Select gensim
3. Create new folder "SET1-DAY2-SESSION-3"
4. Write TensorFlow Code to Distinct work using gensim

# Install and configure OpenVINO Environment:

## OpenVINO Tools Installation -Windows:

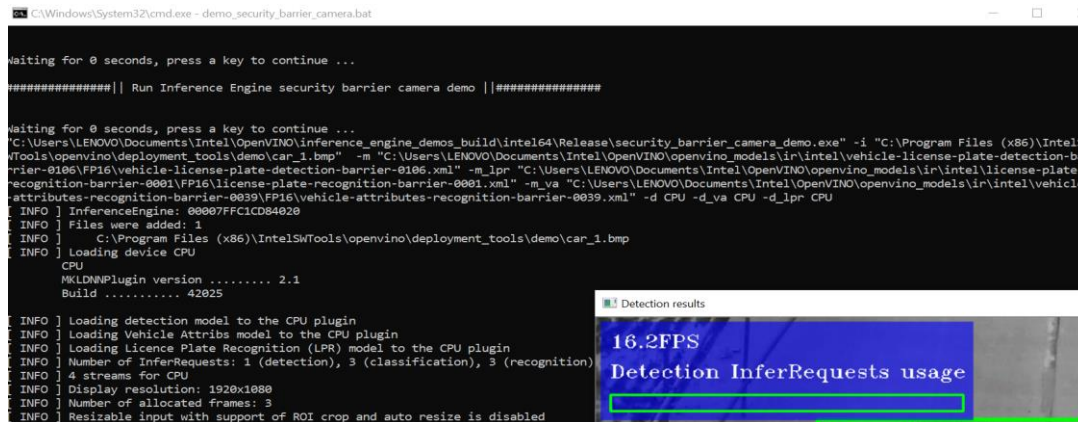
1. Download and install MS Visual Studio/Express Studio from <https://visualstudio.microsoft.com/>
2. Install Windows SDK
3. Get OpenVINO Toolkit 2020 from <> and install

<https://software.intel.com/content/www/us/en/develop/tools/openvino-toolkit.html>

References: <https://github.com/amritchhetrib78/People-Counter-App-At-The-Edge1.0>

## Running OpenVINO Sample:

1. Go to C:\Program Files (x86)\IntelSWTools\openvino\deployment\_tools\demo
2. Run demo\_security\_barrier\_camera.bat to detect text from pictures of Car



```
C:\Windows\System32\cmd.exe - demo_security_barrier_camera.bat

waiting for 0 seconds, press a key to continue ...

#####|| Run Inference Engine security barrier camera demo ||#####

waiting for 0 seconds, press a key to continue ...

C:\Users\LENOVO\Documents\Intel\OpenVINO\inference_engine_demos_build\intel64\Release\security_barrier_camera_demo.exe" -i "C:\Program Files (x86)\IntelS
WTools\openvino\deployment_tools\demo\car_1.bmp" -m "C:\Users\LENOVO\Documents\Intel\OpenVINO\openvino_models\ir\intel\vehicle-license-plate-detection-ba
rrier-0106\FP16\vehicle-license-plate-detection-barrier-0106.xml" -m_lpr "C:\Users\LENOVO\Documents\Intel\OpenVINO\openvino_models\ir\intel\license-plate-
recognition-barrier-0001\FP16\license-plate-recognition-barrier-0001.xml" -m_va "C:\Users\LENOVO\Documents\Intel\OpenVINO\openvino_models\ir\intel\vehicle
-attributes-recognition-barrier-0039\FP16\vehicle-attributes-recognition-barrier-0039.xml" -d CPU -d_va CPU -d_lpr CPU
[ INFO ] InferenceEngine: 00007FFC1CD84020
[ INFO ] Files were added: 1
[ INFO ] C:\Program Files (x86)\IntelSWTools\openvino\deployment_tools\demo\car_1.bmp
[ INFO ] Loading device CPU
CPU
MKLDNNPlugin version ..... 2.1
Build ..... 42025
[ INFO ] Loading detection model to the CPU plugin
[ INFO ] Loading Vehicle Attribs model to the CPU plugin
[ INFO ] Loading licence Plate Recognition (LPR) model to the CPU plugin
[ INFO ] Number of InferRequests: 1 (detection), 3 (classification), 3 (recognition)
[ INFO ] 4 streams for CPU
[ INFO ] Display resolution: 1920x1080
[ INFO ] Number of allocated frames: 3
[ INFO ] Resizable input with support of ROI crop and auto resize is disabled
```

## Malware Analysis using Edge AI: Steps and Research Scope

1. Prepare Datasets
2. Make Edge AI Environment Ready - OpenVINO , NVIDIA SDK
3. Run Model Optimizer and Model Converter
4. Deploy on Edge Device on Lab Env. - FPGA, Intel Neural Computer Stick
5. Install on selected Computer - to analyze and protect from Malware

# Install and configure Colab Environment:

## TensorFlow Environment Google Colab :

1. Open Google Colab and create new Jupyter Notebook at <https://colab.research.google.com/notebooks/intro.ipynb>
2. Write simple code to test:

```
import tensorflow as tf
a = tf.constant(1)
b = tf.constant(2)
c = tf.add(a, b)
with tf.Session() as tfsession:
    print(tfsession.run(c))
```

## Executing Linear Regression:

- 1 Create another Colab
3. Open Linear Regression from [https://colab.research.google.com/notebooks/mlcc/first\\_steps\\_with\\_tensor\\_flow.ipynb](https://colab.research.google.com/notebooks/mlcc/first_steps_with_tensor_flow.ipynb)



## Resources on Google Colab:

1. Working with Google Colab( TensorFlow):
2. Working with Google Colab( PyTorch):

# Install and configure Docker Environment:

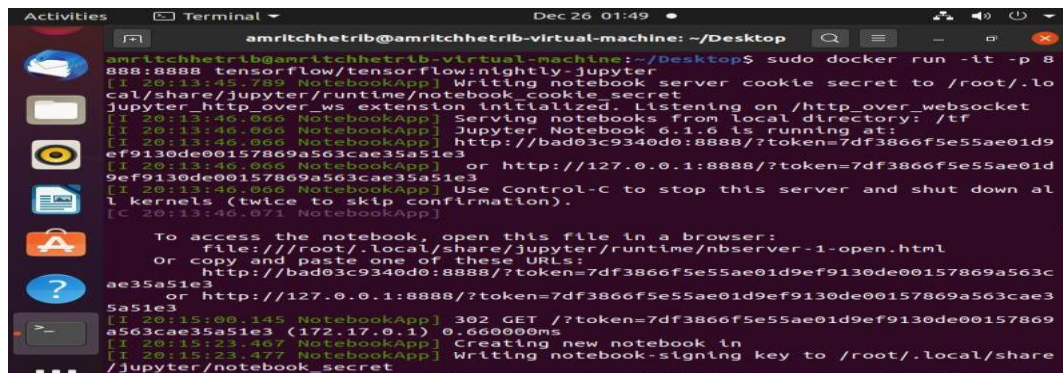
## Preparing Docker environment:

1. Get and configure Ubuntu 16.05 using VMWare Player
2. Update/Upgrade Ubuntu: \$update and upgrade \$sudo apt-get install update
3. Install Docker: \$ apt-get install docker

## Installing TensorFlow Docker:

1. Pull Docker for TensorFlow docker pull tensorflow/tensorflow
2. Run TensorFlow Docker with GPU support: docker pull tensorflow/tensorflow:latest-gpu-jupyter
3. Access Jupyter Notebook with URL displayed on startup ( <http://127.0.0.1:8888/tonken> ...)
4. Explore all Examples and their explanation ....

Reference : <https://www.tensorflow.org/install/docker>



```
amritchhetrib@amritchhetrib-virtual-machine: ~/Desktop
amritchhetrib@amritchhetrib-virtual-machine:~/Desktop$ sudo docker run -it -p 8888:8888 tensorflow/tensorflow:latest-gpu-jupyter
[I 20:13:45.789 NotebookApp] Writing notebook server cookie secret to /root/.local/share/jupyter/runtime/notebook_cookie_secret
Jupyter HTTP over WS extension initialized. Listening on /http_over_websocket
[I 20:13:46.066 NotebookApp] Serving notebooks from local directory: /tr
[I 20:13:46.066 NotebookApp] Jupyter Notebook 6.1.0 is running at:
[I 20:13:46.066 NotebookApp] http://bad03c9340d0:8888/?token=7df3866f5e55ae01d9ef9130de00157869a563cae35a51e3
or http://127.0.0.1:8888/?token=7df3866f5e55ae01d9ef9130de00157869a563cae35a51e3
[I 20:13:46.066 NotebookApp] Use Control-C to stop this server and shut down all kernels (twice to skip confirmation).
[C 20:13:46.071 NotebookApp]

To access the notebook, open this file in a browser:
file:///root/.local/share/jupyter/runtime/nbserver-1-open.html
Or copy and paste one of these URLs:
http://bad03c9340d0:8888/?token=7df3866f5e55ae01d9ef9130de00157869a563cae35a51e3
or http://127.0.0.1:8888/?token=7df3866f5e55ae01d9ef9130de00157869a563cae35a51e3
[I 20:15:00.145 NotebookApp] 302 GET /?token=7df3866f5e55ae01d9ef9130de00157869a563cae35a51e3 (172.17.0.1) 0.660000ms
[I 20:15:23.467 NotebookApp] Creating new notebook in
[I 20:15:23.477 NotebookApp] Writing notebook-signing key to /root/.local/share/jupyter/notebook_secret
```

## References:

1. Docker Installation Guide( Digital Ocean):
2. Working with Jupyter Notebook( TensorFlow GPU) :

# Code Examples:

## Understanding Linear Regression with Example:

1. Linear Regression Explanation : Works based on historical data
2. Mathematics/Algebra/Formulae :  $y = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots$  ( Polynomial LR)
3. Usage/Applicable Areas : Price/Rate Prediction, Population Growth Rate, etc.
4. Sample Code :

[https://colab.research.google.com/notebooks/mlcc/first\\_steps\\_with\\_tensor\\_flow.ipyn](https://colab.research.google.com/notebooks/mlcc/first_steps_with_tensor_flow.ipyn)

- 1 Access Google Colab and
2. Open Linear Regression Example
5. Analyze the outputs and go through code and try to write similar one on own!!!

## Insider Threat Analysis on PyCharm:

1. Open ML-CyberSecurity-Internship2020 Project
2. Create new file called ATA-Sample.py
3. Execute code from

<https://towardsdatascience.com/insider-threat-detection-with-ai-using-tensorflow-and-rapidminer-studio-a7d341a021ba>

4. Analyze the outputs and go through code and try to write similar one on own!!!

## References:

1. Mathematics of Machine Learning:
2. Deep Learning Models for Cyber Security

# Machine Learning with Java Frameworks

## References:

1. Mathematics of Machine Learning:
2. Deep Learning Models for Cyber Security

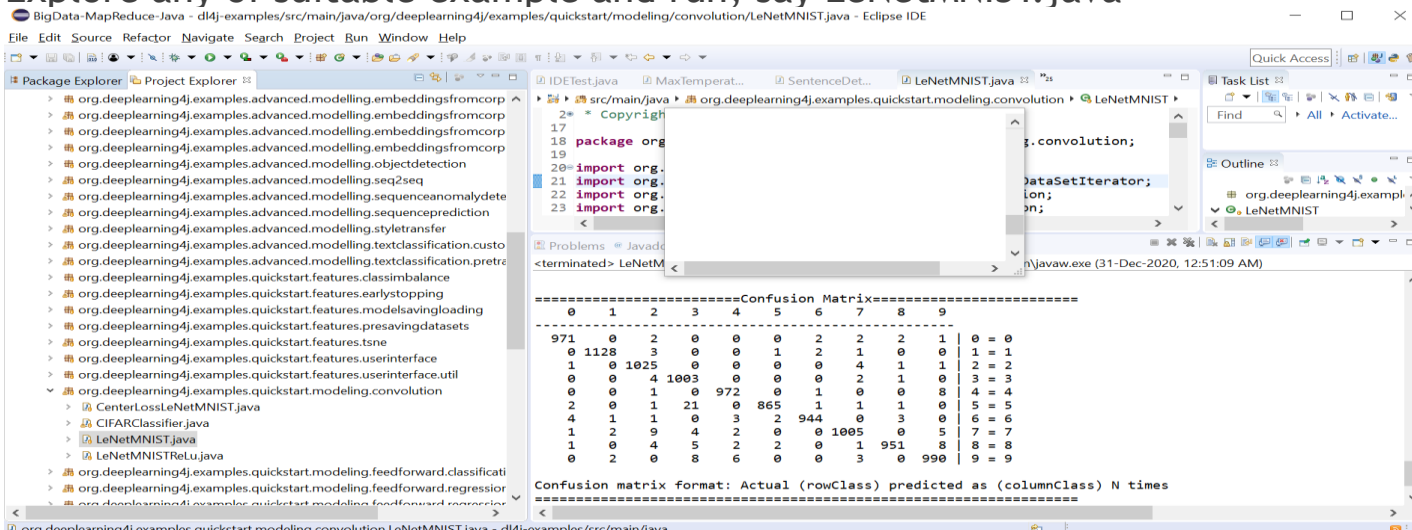
# Machine Learning with Deeplearning4j:

## About Deeplearning4j:

1. Deep Learning Java Framework from supported by Eclipse Foundation
2. Supports Apache Maven-based build and deployment
4. Decent and Quality Examples

## Steps to Configure:

1. Download Eclipse ( 2018 Edition) and also configure Apache Maven
2. Cloned Deeplearning4j repository, git clone <url>
4. Build using maven ,
5. Open Eclipse and import dl4j-examples
6. Explore any of suitable example and run, say LeNetMNIST.java



The screenshot shows the Eclipse IDE interface. The Package Explorer on the left lists the project structure, including 'org.deeplearning4j.examples.quickstart.modeling.convolution'. The main editor displays the 'LeNetMNIST.java' file, which contains Java code for training a LeNet model. The console at the bottom shows the output of the program, including a confusion matrix and the text 'Confusion matrix format: Actual (rowClass) predicted as (columnClass) N times'.

```
=====Confusion Matrix=====
 0  1  2  3  4  5  6  7  8  9
-----
971 0  2  0  0  0  2  2  2  1 | 0 = 0
0 1128 3  0  0  1  2  1  0  0 | 1 = 1
1  0 1025 0  0  0  0  4  1  1 | 2 = 2
0  0  4 1003 0  0  0  2  1  0 | 3 = 3
0  0  1  0 972 0  1  0  0  8 | 4 = 4
2  0  1  21 0 865 1  1  1  0 | 5 = 5
4  1  1  0  3  2 944 0  3  0 | 6 = 6
1  2  9  4  2  0  0 1005 0  5 | 7 = 7
1  0  4  5  2  2  0  1 951 8 | 8 = 8
0  2  0  8  6  0  0  3  0 990 | 9 = 9
```

Confusion matrix format: Actual (rowClass) predicted as (columnClass) N times

## Machine Learning with Java:

1. Books :
2. Research Paper:



# How Be Champion ML System Analyst for Cyber Security:

## Quick to be ML System Analyst:

- Upskill System Design Skills
- Be inside Application Security, Zero Day Architecture and Micro-Architecture
- Get Deep Learning Tools on Local Environment:
  - PyCharm with TensorFlow, PyTorch and needed Frameworks
  - TensorFlow Docker, Machine Learning Based Predictive Analytics
    - IBM SPSS , Rapid Miner Studio , SAS Analytics
  - Understand Whole Of a Model – **MAMCTIMP**
    - **Model** Name and DevOps Configuration : Linear Regression,
    - **Algorithm** Description : Works based on historical data
    - **Mathematics/Statistics** of Models:  $y=a_0+a_1x+a_2x^2+a_3x^3+\dots$  ( Polynomial LR)
    - **Codes** Of Model , **Training** Model , **Inferences**
    - **MLOps** and Deployment , **Performance** Tuning and Optimizaton

## Rules Of 2 Hours/Day :

- Pledge for **Coding Challenge** - 1 Hour/Day:
  - Advanced Python , Pandas and NumPy, PyTorch, Intel OpenVINO Toolkit
  - TensorFlow, TensorFlow Lite, TensorFlow JS and **CoreML**
- Read/Apply **Mathematics of Machine Learning/Deep Learning**- 30 Minutes
- Understand 2 Algorithms/Day – 30 minutes
- Engage With **Machine Learning Communities, Research Forums/Journals**

## Acquire Global Certification during Internship :

- Digital Forensics Upskilling: CHFI, GFCA, CCNP Security, ECIH and CTIA - Send Queries at [amrit.chhetrib@rosefinch.in](mailto:amrit.chhetrib@rosefinch.in) - Amrit Chhetri is a CEI for EC-Council Courses
- Machine Learning Developer : MS AI-900( MCQ, 2 Hours), TensorFlow Developer Certificate( PyCharm-Based, 5 Hours)

# Open Networking

Twitter: <http://twitter.com/AmritChhetriB>  
Facebook: <http://facebook.com/AmritChhetriB>

**THANK YOU ALL**