NATIONAL WORKSHOP ON DEEP LEARNING FOR CYBER SECURITY

06-07 MARCH 2020

About Society for Electronic Transactions and Security

Society for Electronic Transactions and Security (SETS) was set-up as a premier Research Institution to work in the area of Information Security under the Office of Principal Scientific Advisor to the Government of India. It has established an "Advanced Facility in Information Security and Cryptology (AFISC)" working in the research areas of Information Security as Knowledge Centre focussing on Cryptology, Hardware Security and Network Security to meet the specific long-term and short-term cyber security needs of the Nation. SETS has established a state of the art Side Channel Analysis (SCA) Lab for hardware security; AI-CS Project management group to work on futuristic needs of AI for cybersecurity and also a Walk-in Cyber Security Education & Research (WiCSER) lab to demonstrate indigenously developed solutions to the end users. SETS has developed competencies in the area of Quantum Key Distribution (QKD) and Post Quantum Cryptography.

About the Document

On 6,7 March 2020, SETS organized a National Workshop on Deep Learning for Cyber Security that focussed on the applications of Artificial Intelligence for Cyber Security, industry's take on shaping AI trajectories in security, investigating the robustness and resiliency of AI systems and the rise of Adversarial Learning, its impact. This report is a summary of those discussions, framed around research questions and possible topics for future research directions.

Acknowledgement

We are grateful to Dr. R Chidambaram, Shri. R S Mani, Dr. B Ravindran and eminent speakers from Government R&D (C-DAC, SETS), industry and academia.

Table of Contents

Introduction 4

Artificial Intelligence 5

- Introduction to Neural Networks 5
- Intelligence through Data Integration 6

Artificial Intelligence for Cyber Security 6

- Deep Learning based Face Biometrics 6
- Unsupervised Learning- Auto-Encoders and RBM for Cyber Security 7
- Supervised Learning- RNNs for Cyber Security 8
- IDS Dataset Preparation 8
- Next Gen Malware Detection using Deep Learning Techniques 9
- Mitigating Cyber Attacks through Deep Learning 9
- Similarity Learning using CNN 10
- Machine Learning based DDoS Detection 10
- Evaluation of Side Channel Analysis using Deep Learning 10

Cyber Security for Artificial Intelligence 11

- Privacy Techniques in Machine Learning 11
- Deep Neural networks implementation considerations 11
- Towards Trust worthy Deep Learning 12

Transfer Learning 12

National Strategy on Artificial Intelligence and Cyber Security (AI-CS) 13

Conclusion 13

Annexure 14

Introduction

On 6,7 March 2020, SETS organized a National Workshop on Deep Learning for Cyber Security aimed for security researchers/ penetration testers/ infosec enthusiasts to bridge the gap between Cyber Security and Artificial Intelligence.

The workshop was inaugurated by Dr. R. Chidambaram, Homi Bhabha Professor, BARC ,Former Principal Scientific Adviser to the Government of India and President SETS, Chennai. Dr Ravindran, Professor, Indian Institute of Technology Madras delivered the Key note address. Shri R S Mani, Head, National knowledge Network, NIC, Chennai presented the special address.

Dr R Chidambaram in his Inaugural address stated that information searched on the internet travels through a multitude of servers before it reaches the user. Each server is only adding to the million lines of logs that it maintains and added that the time has come that we look at those logs, gather valuable information that would thwart cyber attacks and strengthen the cyber security measures of our nation.

Shri R S Mani in his special address stated the end user is more conscious of the speed of the internet. Along with the speed is the cost of detectablity of attacks. There has always been a trade-off between the speed and attack detection latency. Denial of Service attacks last a few minutes, even before the user is aware of the attack, the attack has happened. He added that combining the strengths of artificial intelligence (AI) with cyber security, security professionals will have additional resources to defend vulnerable networks and data from cyber attackers.

Prof. Ravindran started his key note address with Turing's vision and was a journey from biological neural network to the present advanced recurrent and attention networks. He also stressed on how RL models learn by a continuous process of receiving rewards and punishments on every action taken, it is able to train systems to respond to unforeseen environments.

Artificial Intelligence

Introduction to Neural Networks

An artificial neural network operates by creating connections between many different processing elements, each analogous to a single neuron in a biological brain. These neurons may be physically constructed or simulated by a digital computer. Each neuron takes many input signals, then, based on an internal weighting system, produces a single output signal that's typically sent as input to another neuron. Non-linearity is achieved using activation functions. The neurons are stacked into layers to reduce the loss function.

A convolutional neural network is a neural network meant to process input stored in arrays. CNNs are often used for processing 2D arrays of images or spectrograms of audio. They are also used frequently for three-dimensional (3D) arrays (videos and volumetric images). Regardless of the dimensionality, CNNs are used where there is spatial or temporal ordering.

The architecture of a CNN consists of three distinct types of layers: convolution layers, pooling layers, and the classification layer. The convolution layers are the core of the CNN. The weights define a convolution kernel applied to the original input, a small window at a time, called the receptive field. The result of applying these filters across the entirety of the input is then passed through a non-linearity, typically an ReLU, and is called a feature map. These convolution kernels, named after the mathematical convolution operation, allow close physical or temporal relationships within the data to be accounted for, and help reduce memory by applying the same kernel across the entirety of the image.

Pooling layers are used to perform non-linear sampling by applying a specific function, such as the maximum, over non-overlapping subsets of the feature map. Besides reducing the size of the

feature maps, and therefore, the memory required, pooling layers also reduce the number of parameters, and therefore, overfitting. These layers are generally inserted periodically in between convolution layers and then fed into a fully connected, traditional DNN

The final layer is the Classification layer that uses the softmax activation function to classify the input into one among the multiple classes.

Intelligence through Data Integration

There a number of important practical/implementation considerations that must be taken into account when training neural networks were discussed. Some of the considerations include:

- Do we need to pre-process the training data? If so, how?
- How may hidden units do we need?
- Are some activation functions better than others?
- How do we choose the initial weights from which. we start the training?
- Should we have different learning rates for the different layers?
- How do we choose the learning rates?
- Do we change the weights after each training pattern, or after the/ whole set?
- How do we avoid flat spots in the error function?
- How do we avoid local minima in the error function?
- When do we stop training?

Artificial Intelligence for Cyber Security

Deep Learning based Face Biometrics

Face biometrics are metrics related to (human) face characteristics that includes Face Verification (match 1 face with other 1 face) and Face Identification (find matching 1 face from n faces in the database).

The methods used for Face Detection both classical techniques like Voila Jones Haar cascade, Histogram of Oriented Gradients and Modern methods like Multi-Task Cascade Convolutional

Networks, Face frontalization and the challenges involved in adopting these techniques were discussed.

Adopting deep learning techniques for malware detection using hash was discussed.

Unsupervised Learning- Auto-Encoders and RBM for Cyber Security

The underlying thread connecting the various unsupervised learning techniques in deep neural networks is the latent variables.

Auto-encoders are a class of unsupervised neural networks in which the network takes as input a vector and tries to match the output to that same vector. By taking the input, changing the dimensionality, and reconstructing the input, one can create a higher or lower dimensionality representation of the data. These types of neural networks are incredibly versatile because they learn compressed data encoding in an unsupervised manner. Additionally, they can be trained one layer at a time, reducing the computational resources required to build an effective model. When the hidden layers have a smaller dimensionality than the input and output layers (Figure 3), the network is used for encoding the data (i.e., feature compression). An autoencoder can be designed to remove noise and be more robust by training an autoencoder to reconstruct the input from a noisy version of the input (Figure 4), called a denoising autoencoder

Restricted Boltzmann Machine (RBM) are two-layer, bipartite, undirected graphical models (data can flow in both directions, rather than just one) that form the building blocks of DBNs.. Similar to autoencoders, RBMs are unsupervised and can be trained one layer at a time. The first layer is the input layer; the second layer is the hidden layer. There are no intra-layer connections (i.e., between nodes in the same layer); however, every node in the input layer is connected to every node in the hidden layer (i.e., full connectivity) connections (i.e., between nodes in the same layer); They have the ability to learn a probability distribution over the set of input. RBMs are used for dimensionality reduction, classification, regression,collaborative filtering, feature learning and topic modelling.

Supervised Learning- RNNs for Cyber Security

Recurrent neural networks (RNN), also known as Auto Associative *or* Feedback Network, belongs to a class of artificial neural networks where connections between units form a directed cycle. This creates an internal state of the network which allows it to exhibit dynamic temporal behavior. Unlike FFNN, RNNs can use their internal memory to process arbitrary sequences of inputs. In RNN the signals travel both forward and backward by introducing loops in the network.

RNNs use feedback loops such as Backpropagation Through Time or BPTT throughout the computational process to loop information back into the network. This connects inputs together and is what enables RNNs to process sequential and temporal data.

Various platforms like Keras, Tensorflow, Pytorch, etc., and other open source frameworks for model development were also discussed.

IDS Dataset Preparation

IDS is the most important defense tools against the sophisticated and ever-growing network attacks. IDS Challenges include Accuracy, False alarm rate & zero day attacks. Data preperation is very important step in the machine learning process. Pre-processing involve Data Cleaning : To deal with missing values and remove unwanted characters from the data and Feature Extraction: analyze and optimize the number of features.

The Benchmark datasets of IDS are the DARPA1998, KDD99, NSL-KDD, UNSW-NB15, CICIDS were discussed.

There are certain criteria that are necessary for building a reliable benchmark dataset. They are as follows:

- Complete Network configuration
- Complete Traffic
- Labelled Dataset
- Feature Set

- Complete Capture
- Available Protocols
- Attack Diversity

Next Gen Malware Detection using Deep Learning Techniques

The traditional malware detection uses hash matching techniques to identify malwares and can be easily evaded using code obfuscation either by shrinking/expanding the code or mutating the code using a polymorphic engine.

Data mining techniques can be employed to detect anomalies at their binary levels. Data Mining on Binary metadata that involves creating a support vector of Boolean values representing whether the binary uses a DLL can be used to detect malwares. Although this technique can be evaded using the Import Address Table patching. Similar Methods include Data Mining on Hex codes, Data mining on Patched Binaries, Data Mining on Behavioral fingerprints can also be evaded. Paladion Network's Next generation Detection and Response system uses multi-variate statistical analysis tools like Mahalanobis distance and neural networks like auto-encoders to effectively combat malwares right at the end points.

Mitigating Cyber Attacks through Deep Learning

The breakout time of cyber intrusion has been steadily decreasing over the years. different tactics and techniques the attackers might use has been categorized and accordingly a plan can be devised to secure the enterprise. MITRE ATT&CK threat model can be leveraged to accomplish the same. Irrespective of elaborate safeguards, attacks are bound to happen. two use cases has been discussed: command and control (C&C) detection and exfiltration and see how Deep learning can be employed to mitigate the damages. For C&C detection, it is modeled to a sequence learning problem and LSTM based modelis leveraged to identify spurious url links. For Exfilteration, anonymous traffic emanating from the enterprise has been studied using a deep Feed forward estimator.

Similarity Learning using CNN

Pre-trained networks like LeNet and Alexnet suffer from a few limitations namely Class Imbalance problem and lack of common embedding for cross-domain examples. Similarity learning is the process of training a metric to compute the similarity between two classes.

Similarity learning has proven itself as a successful set of models for learning useful representations of data. These representations are used to distinguish between available classes. The representations from semantically similar classes will be located nearby, while those of semantically dissimilar classes will be located far apart. Applications of Similarity Learning in Computer Vision include Signature Verification, Face Recognition, Detecting Homoglyph Attacks, and Malware Image Classification Using One-Shot Learning with Siamese Networks.

Machine Learning based DDoS Detection

DDoS has evolved into one of the most serious security threats from the arsenal of both cybercrime gangs and nation-state actors. Some of the considerations discussed are as follows:

- Can we quickly detect attacks?
- Can we differentiate between attacks and flash floods?
- How to mitigate / cope with attacks?
- Post –Mortem analysis

This presentation was the research outcome of the project carried out during the year 2008-2010. It was said that Hidden Markov Models, Naive Bayes Classifier, Support Vector machines have been considered for the DDoS Detection. The detection approach involved a training phase and a Deployment phase. The TCP traffic is separated, smoothened using Laplacian Smoothening followed by classification using Naive Bayes Classifier in the training phase. The modelled is later deployed for TCP traffic Classification.

Evaluation of Side Channel Analysis using Deep Learning

Side Channel Analysis involves capturing additional side-channel information like power consumption/ electromagnetic emanation and Side-channel distinguisher during cryptographic operations

to reveal the secret.

The presentation discussed uses CNN model to perform Side Channel Analysis of GIFT cipher. CNN models can be trained using power traces of from one board and the testing traces can be obtained from a different board to take into account the inter-device variance. The rank function can be evaluated to estimate number of traces required to retrieve the key byte (where the rank converges to zero). Traces misalignment will be taken care by Convolutional network .Data augmentation is useful for the attack, when we have limited traces . The trained CNN model can be used to evaluate the crypto modules by proper automation.

For each trace in the attacking phase, get the probability that the trace belongs to a certain class label. Maximum likelihood principle is used to calculate the set of traces that belongs to a certain key.

Cyber Security for Artificial Intelligence

Privacy Techniques in Machine Learning

Ensuring Privacy of the data and the model during both training and testing phase even when not mandated by current regulations is integral to maintain the power to the people.

Differential privacy is a system for publicly sharing information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals in the dataset. Addition of carefully crafted random noise, Composition of differentially private sub computations and post-processing can be carried out to achieve differential privacy. Adoption of Differenetial Privacy in iOS using the Hadamard Count Mean Sketch has been discussed

Deep Neural networks implementation considerations

Accelerating Deep learning computations can be accelerated through the following considerations

- Training can be in cloud since embedded systems can do limited processing
- Parallelize MAC operations since Convolutions take 90% of the time
- Convolution based on FFT /Matrix Multiplication
- Memory access takes more time than computation
- Cost depends on storage needed on the chip

Embedded deep learning needs lots of research especially for IoT and edge devices Optimizations at hardware level are required. Implementation driven algorithmic innovations need to be carried out.

Towards Trust worthy Deep Learning

With the rapid progress and successes in a broad spectrum of applications, Deep Learning is being applied in many safety-critical applications. However, Deep Neural Networks have been found vulnerable to well-designed perturbed samples, called adversarial examples. Such an adversary can cause Deep Learning to make mistakes in predictions. The vulnerability to adversarial examples becomes one of the major risks for applying deep neural networks in mission-critical applications.

the details of recent findings of adversarial attacks on deep learning, counter measures and defence methods has been discussed. Further, the evaluation methods of robustness of defences to adversarial examples have been discussed.

Transfer Learning

Growing concerns of Cyber-attacks and ever-increasing threat canvass, has led the researchers across the globe to look at new ways of addressing challenges posed by the cyber-attacks. Artificial Intelligence and ANNs encompassing ML/ DL algorithms have been considered widely by the researchers in different domains.

Transfer learning is a machine learning method where a model developed for a task is reused as the starting point for a model on a second task. Transfer learning saves training time, increases the performance of neural networks, and does not need a lot of data. .

The four different approaches in the implementation of Transfer Learning are:

- Instance-transfer, where some labelled data in the source domain is reweighted for use in the target domain.
- Feature-representation-transfer, where the model finds a good feature representation that decreases the difference between source and target domains.
- Parameter-transfer, where shared parameters between the source and target domain models are discovered and used for transfer learning.

- Relational-knowledge-transfer, where relational knowledge is built between source and target domains, and data are non-identically distributed as well as represented by multiple relations.

Some of the Cyber Security problems that can be addressed using Transfer namely personalized spam filtering, Intrusion Detection Systems were also discussed.

National Strategy on Artificial Intelligence and Cyber Security (AI-CS)

Artificial Intelligence (AI) and Machine Learning (ML) are rapidly advancing technologies and many applications ranging from machine translation to medical image analysis are being built and demonstrated. In addition, AI and ML technologies can contribute to improving cyber security defense capability to protect from ever- growing sophisticated cyber -threats. While AI is enabling more automated defense systems, it is simultaneously enabling more sophisticated attacks.

Many advanced countries have come out with discussion papers and plan to address the impact of AI/ML in their national economies. There have been efforts to introduce AI within their departments in an effort to develop effective strategies against cyber-attacks. It is imperative for us to build self-reliance in Technology development in "Cyber Security Tools using AI/ML and building secured AI/ML systems and applications" for protecting our ICT systems including critical infrastructure. A brief survey of initiatives on AI-CS by international institutions, and by SETS on AI-CS Project Management Unit (PMU) was presented.

Conclusion

This workshop witnessed the presence of eminent speakers from R&Ds, Industry and academia where each presented their recommendations and suggestion to address threats and strengthening cyber security posture not only as individuals but also a nation. This report presents the SETS perspective of sessions happened at the National Workshop on Deep Learning for Cyber Security. It was communicated that R&D, Industries and academia work collaboratively to outrun Adversarial-AI Counterparts.

Annexure

The title of the talk along with the respective speaker has been tabulated below:

Title of the talk	Speaker
Inaugural Address	Dr R Chidambaram Homi Bhabha Professor, BARC
Special Address	Shri R S Mani Head, National knowledge Network NIC, Chennai
Key Note Address	Prof. Ravindran Balaraman IIT-Madras
Cybersecurity and Deep Learning – Intelligence through Data Integration	Prof. Arun Balaji Buduru IIIT-Delhi
An Introduction: Artificial Neural Networks to Convolutional Neural Networks	Prof. Shahina SSN College of Engineering
Towards trustworthy deep learning – Attacks, Defenses and Evaluation	Shri Ramesh Naidu Laveti, C-DAC, Bangalore
Next-Gen Malware Detection and Response using AI and ML	Shri Amarnath Chatterjee, Paladion Networks
Similarity Learning using CNN	Ms S Irene , C-DAC, Chennai
Privacy Techniques in Machine Learning	Dr. Prem Laxman Das, SETS, Chennai
Machine Learning based DDoS Detection and Mitigation	Ms. A. Suganya, SETS, Chennai
Applications of ML in Cyber Security	Mr.Thiruppathi, SETS, Chennai
National Strategy on Artificial Intelligence and Cyber Security (AI-CS)	Shri R Pitchiah SETS, Chennai

Transfer Learning for Cyber Security	Dr. N. Sarat Chandra Babu SETS, Chennai
Supervised Learning- Recurrent Neural networks for Cyber Security	Ms.Eswari Devi N SETS, Chennai
Unsupervised Learning - Auto Encoders and RBMs for Cybersecurity	Ms. Samyuktha M SETS, Chennai