Dr. M. SHOBANA

No:778,judges colony, S.kolathur,Chennai,Tamilnadu.
· 9791196465
Divyashobana.m@gmail.com/ https://www.linkedin.com/in/shobana-manoharan-1a292219/

To secure a promising position that offers both a challenge and a good opportunity for growth

SUMMARY

- Strong Hands on experience in python, Matlab and R programming
- Hands on experience in Tableau visualization tool,
- Good knowledge in python and R data analytics libraries.
- Good knowledge in Matlab image processing packages.
- Have strong hands on experience in Machine Learning ,deep learning techniques, opencv and mediapipe
- Have knowledge in hardware description languages like Verilog and VHDL
- Handled python, computer networks, network security and operating system classes.
- Completed certificate course and undergone training on Java at Cosmosoft Technologies Limited, Chennai.

SKILLS

- Data extraction
- Recommendation System
- Predictive modelling
- Sentiment Analysis
- Mediapipe
- Deep learning
- Hugging face
- Data visualization
- Weka
- Object detection

EXPERIENCE

JUNE 2013 TO APRIL 2017

ASSISTANT PROFESSOR(FULL TIME), KARPAGAM COLLEGE OF ENGINEERING, COIMBATORE

1ST OCTOBER 2019 TO 31ST MARCH 2020

CONSULTANT (PART TIME), DS IT CONSULTANCY

Worked as a developer in an R & D project which is based on data mining required for the construction industry

21ST NOVEMBER 2022 TO 21ST FEBRUARY 2023

SOLUTION PROVIDER (PART TIME), RAPID CANVAS

Completed four Machine learning projects on the rapid canvas platform and they are documented based on the company requirements

20TH MARCH 2023 TO 21TH JUNE 2023

DATA SCIENCE CONSULTANT (REMOTE), TABLELYF QATAR

Worked as a Data science consultant and handled sign language recognition projects

AUGUST 2023 TO PRESENT

WORKFOSTER

Working as a subject matter expert as freelancer

EDUCATION

FEBRUARY 2023
PhD, ANNA UNIVERSITY
Title: "A framework of Data analytics model for classifying attacks in the IoT environment"

JUNE 2013
M.TECH VLSI DESIGN, SASTRA UNIVERSITY
CGPA: 8.1(First class with Distinction)

JUNE 2011
B.TECH COMPUTER SCIENCE , SASTRA UNIVERSITY, CGPA : 7.2

JUNE 2007, HSC: 82.58% (COMPUTER SCIENCE)

JUNE 2005, SSLC :73.9%

PUBLICATION DETAILS

1. **Title:** Efficient method of hiding data by pixel intensity.
Authors: M.Shobana and R.Manikandan.
Journal: International Journal of Engineering and Technology(Scopus indexed).

2. **Title:** A Novel Approach for Hiding Image using Pixel Intensity.
Authors: M.Shobana , P.Gitanjali and R.Manikandan.
Journal: International Review on Computers and Software (Scopus indexed).

3. **Title:** An Approach for Encryption Mechanism for Stego-Image by Using Hexadecimals
Authors: M.Shobana , P.Gitanjali ,S.Raghave and N.Ram kumar.
Conference: National Conference on Information Science & Engineering

4. **Title:** Efficient X-box Mapping in Stego-image Using Four-bit Concatenation
Author: M.Shobana
Journal: International Journal of Electronics and Information Engineering

5. **Title:** An Efficient image Steganography approach using key Compression
Author: M.Shobana
Journal: Journal of Engineering and Interdisciplinary Research

6. **Title:** Class-C chopper based battery operated electric vehicle
Authors: V. Mithya, M. Shobana, R. Suguna, S.Chellaganeshavalli
Journal: International Journal of Applied Engineering Research (Scopus indexed).

7. **Title:** An Efficient Image Steganographic Algorithm Using CMYK Color Model
Author: M.Shobana
Journal: International Journal of Research and Innovations in Science and Technology

8. **Title:** Pixel Value Differencing Method Based on CMYK Color Model
Author: M.Shobana

Journal: International Journal of Electronics and Information Engineering

9.Title: An Efficient botnet Detection Approach for Green IoT Devices using ensemble learning Techniques
Author: M.Shobana , Dr.S.Poonkuzhali
Journal : Journal of green engineering

10**. Title:** A novel approach for detecting IoT Botnet using balanced network traffic attributes
Author: M.Shobana , Dr.S.Poonkuzhali
Journal: Lecturer notes in Computer Science(Springer publication)

11. **Title**: IOT Malware:An analysis of Device Hijacking
Author:M.Shobana, Dr.S.Rathi
Journal: International journal of scientific research in Computer Science,Engineering and Information Technology

12. **Title:** Multichannel based IoT malware detection system using system calls and opcode sequences.
Author: M.Shobana , Dr.S.Poonkuzhali and R.Kishore Kumar
Journal: The international arab journal of Information technology (SCI Indexed)

13.**Title:** A deep transfer learning approach for iot/iiot cyber attack detection using telemetry data
Authors: Dr.S.Poonkuzhali, M.Shobana and J.Jeyalakshmi
Journal: Neural Network World (SCI Indexed)

CONFERENCE ATTENNDED:

- Presented a paper on International Workshop on Artificial Intelligence in the IoT Security Services (AI-IOTS 2020) hosted virtual at Dubai.
- Presented a paper on International Conference on Innovative Trends In Information Technology (ICITIIT-20) at IIIT Kottayam, India.
- Presented a paper on International Conference on Information and Communication Technology for Competitive Strategies (ICTCS-2022) hosted virtual at Jaipur, India.

PROJECT EXPERTISE

PROJECT# 1: PREDICTIVE ANALYTICS TO ENSURE ZERO ACCIDENTS DURING BASE BUILDING CONSTRUCTION IN AEC INDUSTRY

Role : Developer
Tools & Tech Used : Python, Machine Learning Package, Weka and R

Description:

The construction industry has one of the highest rates of fatalities and injuries for workers in America, according to postings by the United States Bureau of Labor Statistics. The OSHA also reports that fall hazards are the leading cause of injury at construction sites. There are roughly 150,000 construction site accident injuries each year according to the Bureau of Labor Statistics. Among these 61% of construction accidents were due to impalement from rebar and

112% due to trenching and excavation works. By analyzing the previous record of severe injury happened at construction site, this project classifies the accidents based on degree on injury, project type, source of injury, environmental factor, and event type. Based on nature of injury and body parts, the remedial solution will be suggested as per OSHA standards.

PROJECT #2: A NOVEL APPROACH TO DETECT IOT MALWARE BY SYSTEM CALLS USING DEEP LEARNING TECHNIQUES

Role : Developer
Tools & Tech Used : Python,Machine and deep learning library packages,NLP packages
Work published in : International Workshop on Artificial Intelligence in the IoT Security Services (AI-IOTS 2020)

Description:

This model focusses on detecting the malware based on their behavior in terms of system calls sequence arise during its execution. The system calls of IoT malware are gathered using Strace tool in Ubuntu. The generated malicious system calls are preprocessed by n-gram techniques to retrieve required features. The extracted system calls were classified into two class i.e normal and malicious sequence using Recurrent neural network(RNN). The efficiency of this deep learning is tested using various performance metrics. The real time IoT malware samples were collected from IOTPOT honeypot which emulates different CPU architecture of IoT devices

PROJECT #3: A NOVEL APPROACH FOR DETECTING IOT BOTNET USING BALANCED NETWORK TRAFFIC ATTRIBUTES

Role : Developer
Tools & Tech Used: Python, Machine learning library packages
Work published in: Lecturer notes in Computer Science (Springer publication)

Description:

Over the evolution of internet technology give rise to the intelligence among tiny objects so called IoT devices. At the same time, this scenario increases the intrusion of malware into the IoT devices eg. Mirai, bashlite. In this project, the class imbalance problem has been identified in the BoT-IoT dataset. This problem is overcome by the random oversampling technique. Then this resultant dataset is further classified into normal and attack traffic using three effective classifier such as Support Vector Machine, Naïve Bayes, and Decision Tree (j48). The performance of this security model is evaluated using quality metrics like Precision, Recall, F-measure, Response time and ROC to identify the best classifier which is apt to detect malware in IoT devices.

PROJECT #4: TOWARDS SECURING WIRELESS INSULIN PUMP SYSTEM USING UNSUPERVISED DEEP LEARNING TECHNIQUE

Role : Developer
Tools & Tech Used : Python, Deep learning library packages

Description:

The existing solutions suggested for IoMT security issues are relies on supervised learning, so this project is heavily based on unsupervised learning to improve the efficiency of the designed security model. In this work, an intrusion detection system has been designed for most significant IoMT device namely Insulin pump system for diabetes treatment using deep learning technique in an unsupervised manner. In this model deep autoencoder has been utilized

to classify the unauthorized insulin value from the legitimate insulin value and this model used insulin logs of several patients as its dataset.

PROJECT #5: A DEEP TRANSFER LEARNING APPROACH FOR IOT/IIOT CYBER ATTACK DETECTION USING TELEMETRY DATA

Role : Developer

Tools & Tech Used : Python, Deep learning library packages

Description:

In this project, deep transfer learning technique has been adapted for GRU. Each model is trained using dataset belongs to one source IoT device (source domain) and this trained model is used to classify the malicious traffic in another dataset belongs to some other IoT device (target domain). This approach is used for binary classification. These three models have been evaluated using IoT/IIoT telemetry dataset called as TON_IOT which comprises the sensor data generated from the seven different types of IoT devices.

PROJECT #6: COPY PASTE IMAGE FORGERY DETECTION USING DEEP LEARNING ALONG WITH ERROR LEVEL ANALYSIS

Role : Developer

Tools & Tech Used : Python, Deep learning library packages for images

Description:

The versatile improvement of the digital domain, make digital things to altered or forged by the attacker especially image format is easily prone to forgery attacks. Out of the most forged attack approach, copy and paste forgery attack is considered to be highly threating attack. Hence in this work is about IFD (image forgery detection) for copy and paste attack has been proposed using deep learning technique such as convolutional autoencoder for classification along with preprocessing technique such as ELA (Error level analysis). This model has been evaluated and tested using MICC-F220 dataset to achieve high performance. Accuracy, precision, recall, and F1-measure are some of the quality metrics used to evaluate the proposed forgery detection model.

PROJECT #7: AN EFFICIENT MEDICAL IMAGE FORGERY DETECTION USING DEEP LEARNING BASED ON UNET REDUCED FEATURES

Role : Developer

Tools & Tech Used : Python, Deep learning library packages for Images

Description:

The design of tampering detection model for the medical images such as CT scan, MRI scan has been proposed in this work. Here, the deep learning techniques based on significant features has been deployed for the purpose of discriminating fake CT scan from the genuine scan. These significant features were extracted by the efficient variant of CNN called Unet architecture. The base deep learning model used in this work are CNN and Inception model. This designed model is trained and evaluated using the lung CT scan tampering dataset namely “Deepfakes”. In this dataset, the fake scan was generated by the attacker by injecting the fake cancer or by removing the original cancer. Finally, the comparative analysis has been carried out between DL models with and without feature extraction step. The performance of the DL model is quantified in terms of accuracy, precision, recall and F1-measure.

PROJECT #8: COLLABORATIVE -BASED TRAVELS RECOMMENDATION SYSTEM USING DEEP AUTOENCODER FOR INDIAN TOURISM

Role : Developer
Tools & Tech Used : Python, Deep learning library packages

Description:

In this project, deep auto encoder utilized for predicting the user rating to make recommendation for tourist about a particular tourist site. The designed recommendation system is evaluated and tested using two datasets consists of user reviews for two different eccentric location which is extracted from a well-known traveler's website namely trip advisor. The first dataset comprises the user review and its rating score for various places located in Jaipur, India whereas second dataset based on various places across Europe available in Kaggle repository. The performance of the proposed model is measured in terms of Root mean square error (RMSE).

PROJECT #9: DESIGN OF SMART TOURISM SYSTEMS TO FORECAST FOREIGN TOURIST ARRIVAL RATE USING DEEP LEARNING TECHNIQUES

Role : Developer
Tools & Tech Used : Python, Deep learning library packages

Description:

This project focuses on design and development of smart tourism systems using data analytics tools and techniques for forecasting the rate for foreign tourist arrivals to a particular destination using various deep learning techniques such RNN, LSTM-RNN, GRU-RNN, CNN and DNN. The detailed comparative study of these aforementioned techniques has been done to find out the suitable deep learning technique to forecast the foreign tourist arrivals per year. Furthermore, yearly trend analysis has been carried out for the significant parameters such as Domestic tourism, tourism contribution to GDP, Foreign Exchange Earnings, Government expenditure to tourism using visualization techniques.

PROJECT #10: UNSUPERVISED SENTIMENT CLASSIFICATION FOR HOTEL REVIEW RATING USING LSTM AUTOENCODER

Role : Developer
Tools & Tech Used : Python, Deep learning library packages

Description:

In this work, hotel online reviews are considered for sentiment classification to identify positive and negative reviews in the provided dataset. This objective is achieved by the implementation of LSTM autoencoder or Text autoencoder in an unsupervised way. The proposed model is trained and evaluated using the dataset of 51,5000 customer reviews of the hotels across the region of Europe. The performance of the deep learning technique is measured in terms of various quality metrics such as accuracy, precision, recall and F1-Score.

DECLARATION:

I do hereby confirm that the information furnished above is true to the best of my knowledge and belief.

Place: Chennai (M.Shobana)