ACADEMIC CV OF NAFIZA TABASSOUM

Email ID: nafisatabassum2016@gmail.com

Academic Profile:
LinkedIn
GitHub
Google Scholar
Mobile Number: +8801886998807

ACADEMIC QUALIFICATIONS

Bachelor of Science in Computer Science and Engineering 2023

Thesis on IoT,Cyber Security, GAN

Ahsanullah University of Science and Technology, Bangladesh

- GPA: 3.376 on the scale of 4.00
- **Last 60 credit hours GPA: 3.501 on the scale of 4.00**

RESEARCH PUBLICATIONS

1. PAPER TITLE: **"Interpretability of Machine Learning Algorithms for News Category Classification Using XAI"**
   Published in: 2024 6th International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT)

Responsibility: Text classification has been a popular research topic for several years. To date, several advanced models have been developed in this field. In today's digital landscape, the proliferation of online news sources necessitates the efficient categorization of user accessibility. To address this situation, machine learning models can be used to automate news category classification based on news headlines and short descriptions. However, we know that machine-learning models act like black boxes. The interpretability of a model provides a clear understanding of how decisions are made, ensuring transparency, and user acceptance. This transparency helps in model validation and effective collaboration between human and computer interactions. Local Interpretable Model-agnostic Explanations (LIME), as an Explainable Artificial Intelligence (XAI) technique, can be implemented to generate interpretable explanations that aid in understanding the reasoning behind specific predictions. Our approach aims not only to predict news categories but also to provide transparent insights into model decisions. Initially, we used Sentence Bidirectional Encoder Representations from Transformers (SBERT) for contextual text embedding purposes, followed by different machine learning models for classification tasks, such as Random Forest (RF), Logistic Regression (LR), Decision Tree (DT), and K-Nearest Neighbors (KNN). Notably, RF achieves exceptional accuracy of 91.48 %, surpassing contemporary benchmarks. Finally, LIME elucidates crucial features guiding classification decisions, facilitating model validation, and fostering human-computer collaboration. This study enriches the evolving discourse on interpretable AI models by providing a robust framework for transparent news classification in an era inundated by information.

2. PAPER TITLE: **"Efficient Feature Selection On Adversarial Botnet"**
   Published in: FedCSIS 2023: 18th Conference on Computer Science and Intelligence Systems

Responsibility: The research paper focuses on enhancing intrusion detection systems (IDS) by using Generative Adversarial Networks (GANs) with efficient feature selection to detect novel malware in real-time. Motivated by the rising sophistication of botnet attacks, the study aims to improve IDS accuracy with fewer features. The methodology involves feature selection using Pearson Correlation, Wrapper, and Mutual Information methods to optimize GAN performance. The results showed that the GAN model, coupled with Mutual Information, delivers high efficacy in accurately detecting malware using minimal but critical features. GAN was used to generate false data and evaluate certain features with Convolutional Neural Networks (CNN). The GAN and CNN combination iteratively optimizes the discriminator's performance, enhancing the model's accuracy.The proposed model was applied on two binary datasets named KDD-99 and CSE-CIC-IDS2018 where the accuracies were 83% and 85%.

3. PAPER TITLE : **"Multiclass Feature Selection Model for Adversarial Attacks in IoT Environment"**
   - **Published In :** IEEE International Conference on E-Business Engineering (ICEBE) 2024

Responsibility : This research addresses the increasing threat of malware attacks in Internet of Things (IoT) networks, which compromises the security and reliability of connected systems. Existing Machine Learning-based Intrusion Detection Systems (IDS) often struggle to handle these threats due to the complex and dispersed nature of IoT malware. To improve IDS effectiveness, we propose a feature selection approach using Generative Adversarial Networks (GAN) to help detect both new and known cyber threats in real-time.The feature selection process involves two steps: (1) reducing features with the Mutual Information (MI) technique to retain the most relevant ones, and (2) refining feature selection using inclusion and exclusion methods based on GAN's discriminator accuracy. We tested this on the CICIOT 2023 dataset which is a multiclass dataset ,focusing on 20 key features for optimal efficiency and accuracy.For modeling, we used a combination of Convolutional Neural Network (CNN) for data generation and preliminary feature evaluation,Mutual Information Classifier to validate the effectiveness of chosen features and Recurrent Neural Network (RNN) with a limited feature set to classify the malware attacks.The result of this work outperform all the existing work close to this despite of using least amount of features only.

RESEARCH INTERESTS

1. Machine Learning
2. Deep Learning
3.IoT
4. Generative Adversarial Network (GAN)
5.Natural Language Processing(NLP)
6. eXplainable AI (XAI)
7. Computer Vision

INDUSTRIAL JOB EXPERIENCE

May 2024 – Continue:
Executive SQA Engineer
Enosis Solutions
Dhaka, Bangladesh

Responsibility: My job responsibilities include Manual Tesing, Automation testing of softwares,websites and mobile app.I write intensive test cases by planning a test plan from requirement analysis.I am proficient in test case writing, test case execution,bug reporting through Jira.Communicating efficiently with developers and collaborating with other team memebrs also a cruitial skill of mine.

TEST SCORES

- **International English Language Testing System (IELTS) –** August 2024
  Overall: 7.0 | Listening: 8.0| Reading: 7.0| Writing: 6.0 | Speaking: 7.0

UNDERGRADUATE ACADEMIC PROJECTS AND SKILLS

I. TITLE: **"Automatic Profiling of Gender, Age, and Handedness from Offline Bangla Handwritten Document Images."** Link

Responsibility: Identifying demographic characteristics from handwriting is challenging yet crucial in psychology, historical document interpretation, and forensics. Traditional methods struggle with gender, age, and handedness detection, especially from offline handwriting. This study explores Bangla handwriting using Convolutional Neural Networks (CNNs) with ImageNet pretraining for feature extraction. Remarkable accuracies were achieved: 0.9352 for gender (MobileNetV3), 0.8046 for age (DenseNet121), and 0.7622 for handedness (MobileNetV3). These findings indicate that CNNs outperform traditional models, advancing automated handwriting-based characteristic prediction.

II. PROJECT: **iGraphics Game Development.** GitHub

Responsibility: This is an action-packed treasure hunting game where players battle monsters and gather treasures for an exciting gaming experience. Created in C++ using the iGraphics library, it runs on Visual Studio, delivering thrilling adventures for all.

III. PROJECT: **Employee Management System.** GitHub

Responsibility: This is a Distributed Database Management System project is tailored for a company's employees comprehensive management, handling attendance, personal details,salary details etc .It employs MySQL with PL/SQL language and works on internal quering between two distant devices

IV. PROJECT: **GYM Website Development.** GitHub

Responsibility: This is a Fitness First Gym website, using HTML, CSS, PHP, and Bootstrap 5, provides gym information, membership purchases, and BMI assessment online. It uses MySQL to securely store user details for package purchases, ensuring an organized user information system.

COMPLETED MAJOR COURSES (Bachelor of Science in Computer Science and Engineering)

1. Pattern Recognition with Lab
2. Digital Image Processing with Lab
3. Soft Computing with Lab
4. Numerical Methods with Lab
5. Artificial Intelligence with Lab
6. Computer Networks
7. Database
8. Distributed Database Systems with Lab
9. Formal Languages and Compilers with Lab
10. Computer Graphics with Lab
11. Telecommunication
12. Data Communication
13. Operating System with Lab
14. Microcontroller Based System Design with Lab
15. Mathematical Analysis for Computer Science
16. Digital System Design
17. Algorithms & Data Structures with Lab
18. Computer Architecture

SOFTWARE SKILS

i. Programming skills: C++,JAVA,Python Language
ii. Frameworks: Pytorch and Tensorflow
iii. Libraries: NumPy and Pandas
iv. IDE & Applications: Google Colaboratory, Jupyter Notebook, Codeblocks, Netbeans & LaTeX