||Jai Sri Gurudev||

Sri Adichunchanagiri Shikshana Trust ®

SJB INSTITUTE OF TECHNOLOGY

No. 67, BGS Health & Education City, Dr. Vishnuvardhan Road, Kengeri, Bengaluru - 560 060

Approved by AICTE - New Delhi.

An Autonomous Institution, Affiliated to Visvesvaraya Technological University, Belagavi,

Accredited by NAAC A+, Accredited by NBA. Certified by ISO 9001-2015

Department of Computer Science & Engineering

Project Phase-2 Presentation on

"Deep Learning Framework to detect Cyber-Attacks in IoT Network"

Guide Name

Mrs. Manjula H S

Assistant Professor

Dept of CSE, SJBIT

Presented by :

Nischitha B [1JB20CS073]

Pallavi R [1JB20CS076]

Preethi V [1JB20CS084]

Rakshith N Magi [1JB20CS092]

TABLE OF CONTENTS

ABSTRACT

* The Internet of Things(IoT) is a network of interrelated devices that connect and exchange data with other IoT devices and the cloud.
* These devices represent a vast attack surface for cyber-attacks.
* With the increase in the IoT devices being connected to the internet the chances of the cyber-attacks have increased .
* Hence the KDD network dataset was used to train the models to detect and classify the attacks.

INTRODUCTION

* The Internet of Things (IoT) is a paradigm that refers to the interconnected network of physical devices and other objects embedded with sensors.
* The connection of IoT devices to the internet has lead to the lack of security as the systems get attacked and the data is lost.
* The ‘Generative Deep Learning to Detect Cyber attacks for the IoT-23 Dataset’ paper has been referred.
* The deep learning methods are effectively used in the detection of the attacks in the IoT devices.

LITERATURE SURVEY

Slno.	AUTHOR	METHOD	ATTACKS ADDRESSED	DATASET	RESULT
1	Shire	Angle-Based Outlier Detection , Principal Component Analysis, Minimum Covariance Determinant , ARIES GAN.	Man In The Middle attacks,Ping Distributed DoS attacks,	Modbus/TCP network flows,DNP3 network flows, operational data	The accuracy of the proposed mechanism reaches 91%.
2	Saharkhizan	Modbus IoT environments, RNN Long-Short-Term-Memory, MENSA model.	TCP SYN DoS attacks, Modbus query flood attacks.	Simoes, CICFlowMeter	Compared to the existing anomaly-based IDS, MENSA addresses efficiently the FP.
3	Shafi	Virtual Honeypot Devices, Markov models,BlackBox IDS	DoS attack,privacy,eavesdropping,backdoor attacks.	IoT testbed	Detects both known and unknown attacks with high detection rates & low false-positive alerts

LITERATURE SURVEY Contd..

4	Shire	DL-based detection method, State Vector Estimator, DL-Based Identification , MENSA	False Data Injection, DoS attacks.	Modbus/TCP,DNP3	MENSA achieves the best performance either for detecting operational anomalies or discriminating the Modbus/TCP and DNP3 cyberattacks
5	Imtiaz Ullah	Transfer learning, RNN, CNN	Replay, Flooding and DoS attacks	BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020,	Proposed binary and multiclass classification models showed high accuracy, precision, recall, and F1 score

PROBLEM STATEMENT

* The aim of our project is to design a framework to detect cyber attacks using Deep-Learning models.

OBJECTIVES

- To implement an efficient network intrusion detection system.
- To implement a multi–class classification to identify different types of attacks.
- To design an intelligent intrusion detection and prevention system.
- To compare various ML algorithms to detect intrusion detection system.

REQUIREMENTS ANALYSIS

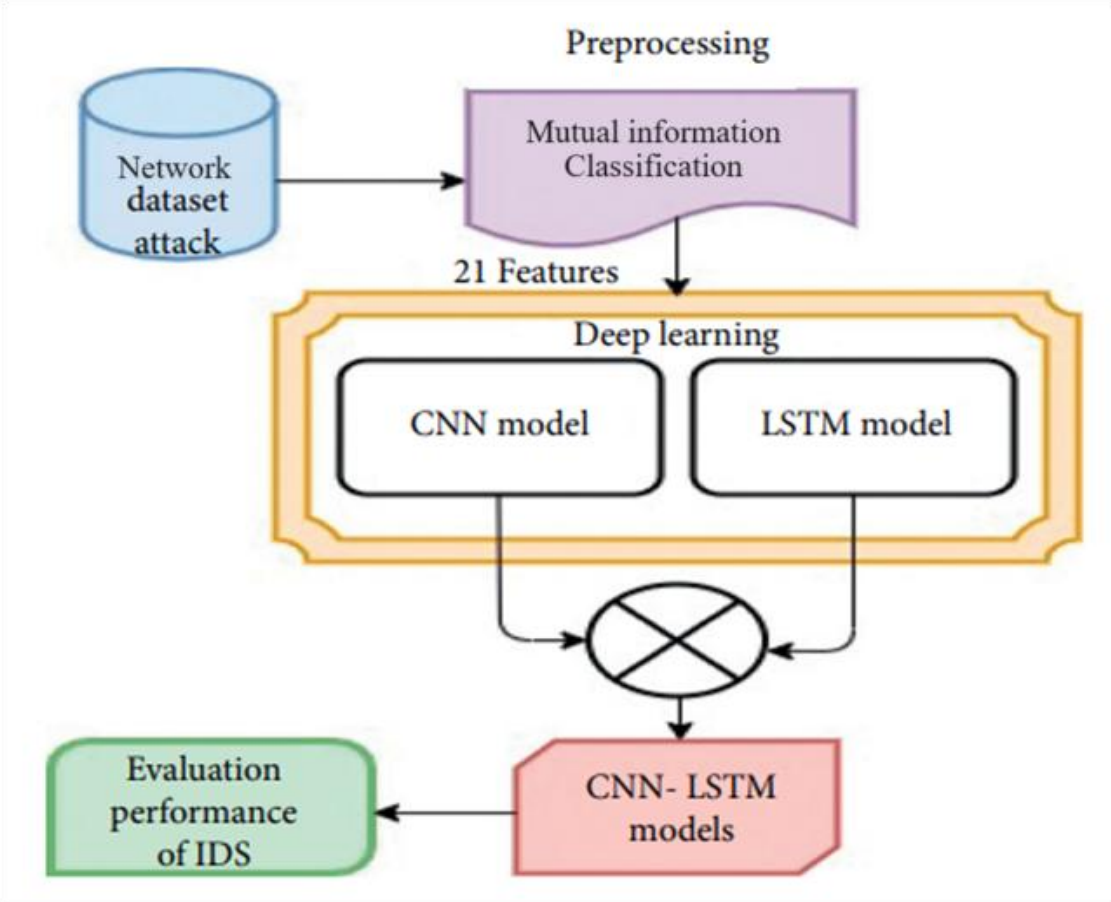
Hardware Requirements

* Processor Type : Intel CORE i5
* Speed : 2.4 GHz
* RAM : 8GB
* Hard Disk : 80GB HDD

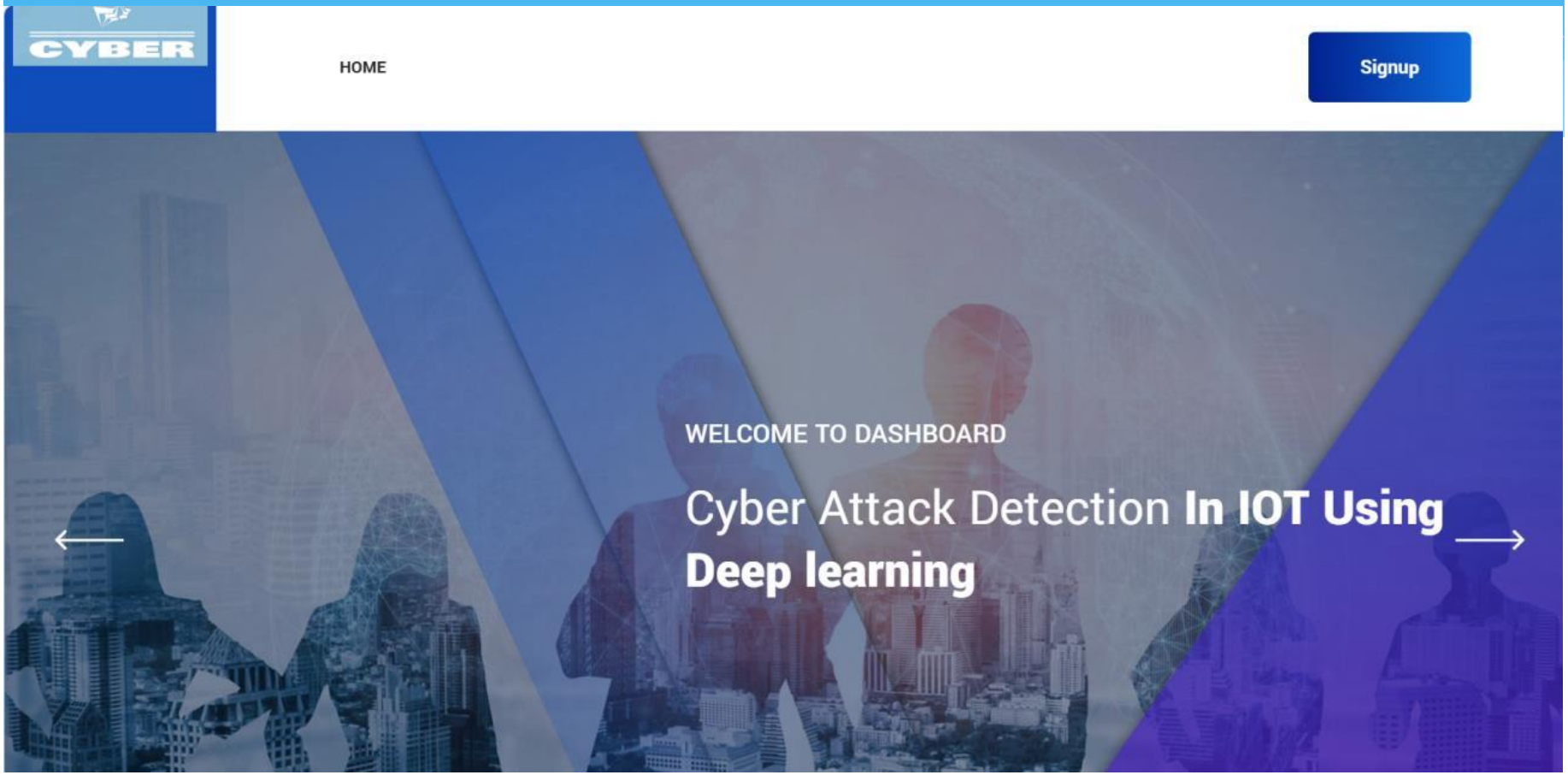
Software Requirements

* Operating System : Windows 64-bit
* Technology : Python
* IDE : PythonIDLE
* Tools : Anaconda
* Python Version : Python 3.6

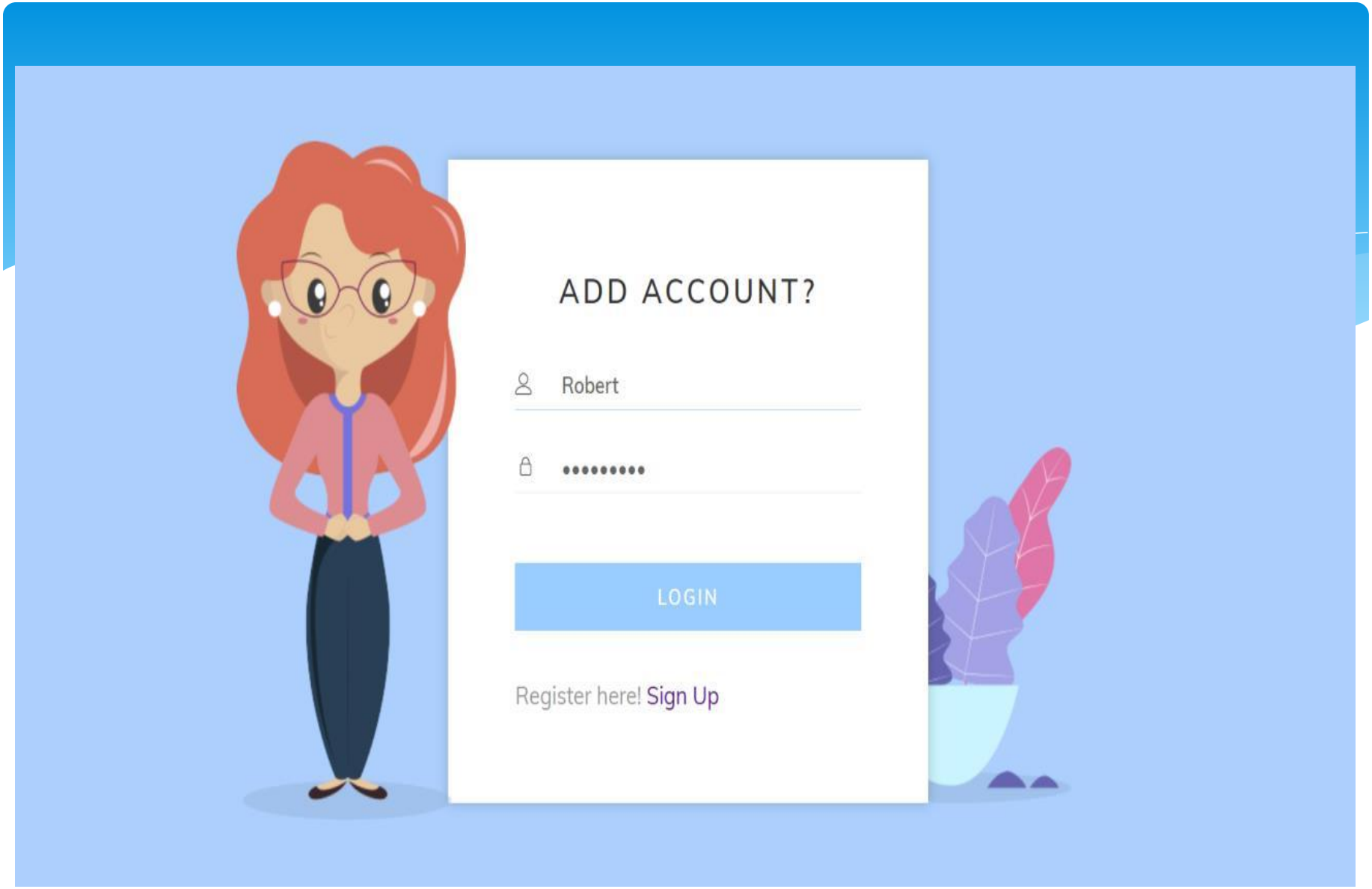
IMPLEMENTATION



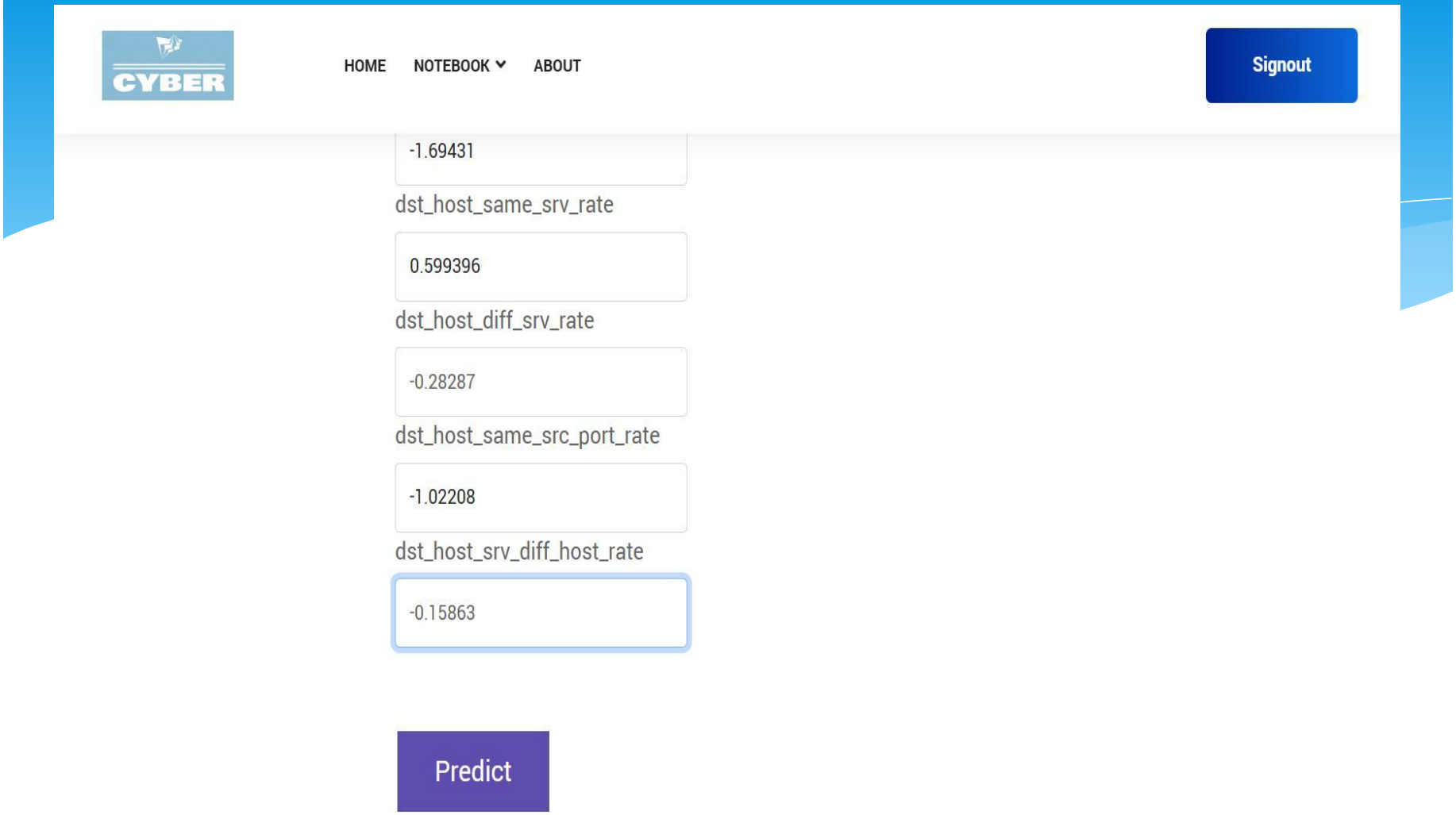
RESULTS



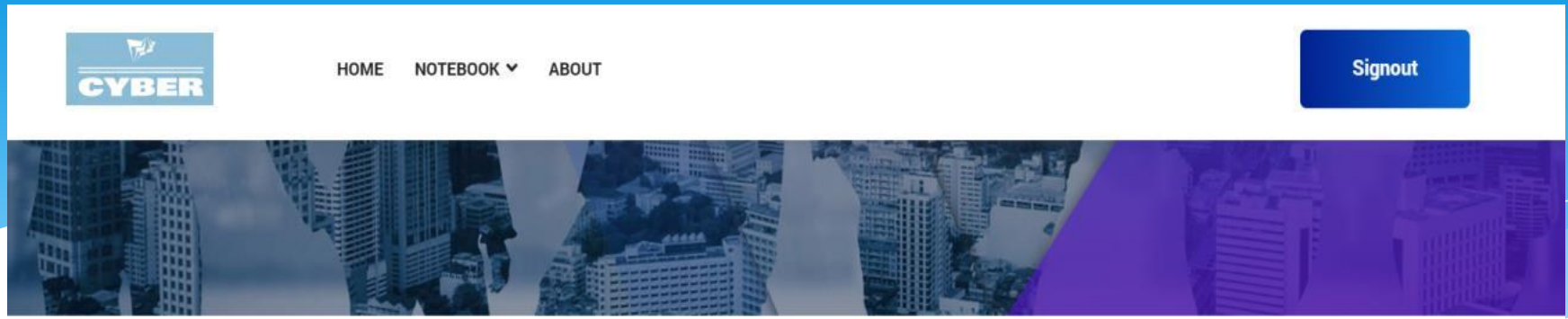
Home Page



Login Page



Prediction Page



Result: **Attack is Detected and its DOS Attack!**

Result Page showing name of attack detected

	ML Model	Accuracy	Precision	Recall	F1-Score
0	CNN	0.989	0.994	0.989	0.991
1	RNN	0.793	1.000	0.793	0.885
2	RBM	0.991	0.993	0.991	0.992
3	DNN	0.994	0.994	0.994	0.994
4	CNN LSTM	1.000	0.993	0.990	0.992

Results of KDDCUP

CONCLUSION

* This project has shown that for a limited set of attacks and IoT devices, it is possible to use generative deep learning methods like mutual information classification and CNN-LSTM to classify attacks with high accuracy.
* We have also used a recent dataset called KDD network attack dataset and implemented baseline models, mutual information classification and CNN-LSTM.
* We also tried randomizing the test set in a way that we can inject new information and the model was able to consider it as an anomaly.
* Our results show that the LSTM based models are more effective at identifying attacks and classifying them.

REFERENCES

[1] B. Alqahtani and B. AlNajrani, ‘‘A study of Internet of Things protocols and communication,’’ in Proc. 2nd Int. Conf. Comput. Inf. Sci. (ICCIS),Oct. 2020, pp. 1–6 doi: 10.1109/ICCIS49240.2020.9257652.

[2] R. Shire, S. Shiaeles, K. Bendiab, B. Ghita, and N. Kolokotronis, “Malware squid: A novel IoT malware traffic analysis framework using convolutional neural network and binary visualization,” in Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Cham, Switzerland:Springer, 2019, pp. 65–76.

[3] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ‘‘DDoS in the IoT: Mirai and other Botnets,’’ Computer, vol. 50, no. 7, pp. 80–84, 2020, doi: 10.1109/MC.2020.201.

REFERENCES Contd..

[4] S. Kwon, H. Yoo, and T. Shon, "IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system," IEEE Access, vol. 8, pp.77572–77586, 2020.

[5] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in Proc. 1st Ed. MCC Workshop Mobile cloud Comput. (MCC), 2012, p. 13.

[11] R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review," Internet Things, vol. 14, Jun. 2021, Art. no. 100365, doi: 10.1016/j.iot.2021.100365.

THANK YOU