REAL-TIME DETECTION OF IOT CYBERSECURITY INTRUSIONS

Baquar Khan[1], Syed Mahmood Ali[2], Mohammed Shamshad[3], Dr.Mohammed Rahmat Ali[4]
[1,2,3]B. E Student, Department of CSE, ISL College of Engineering, India.
[4]Assistant Professor, Department of CSE, ISL College of Engineering, Hyderabad, India.

ABSTRACT: A computer network may be impacted by malicious software, computer viruses, and other hostile attacks. A crucial element of network security is intrusion detection, which is an active defensive system. Traditional intrusion detection systems suffer from problems including poor accuracy, poor detection, a high rate of false positives, and an inability to handle novel forms of intrusions. To address these issues, we propose a deep learning-based novel method to detect cybersecurity vulnerabilities and breaches in cyber-physical systems. The proposed framework contrasts the unsupervised and deep learning-based discriminative approaches. We presents a generative adversarial network to detect cyber threats in IoT-driven IICs networks. The results demonstrate a performance increase in terms of accuracy, reliability, and efficiency in detecting all types of attacks. The output of well-known state-of-the-art DL classifiers achieved the highest true rate (TNR) and highest detection rate (HDR) when detecting the following attacks such as BruteForceXXS, BruteForceWEB, DoS_Hulk_Attack, and DOS_LOIC_HTTP_Attackon the three data sets namely NSL-KDD, KDDCup99, and UNSW-NB15 datasets. It also maintained the confidentiality and integrity of users' and systems' sensitive information during the training and testing phases.

INTRODUCTION

An intrusion detection system (IDS) monitors network traffic in order to spot potentially harmful transactions and promptly notifies users when one is detected. It is software that scans a system or network for nefarious activity or infractions of policies. The next line of defense for a system is comprised of intrusion detection systems (IDS).Through the use of unique attack-specific rules and a range of benign traffic/normal flow patterns, intrusion detection systems are able to differentiate between malicious and benign activities. In order to better identify and install intrusion detection systems (IDSs) that can thwart complex, current cyberattacks, data mining is used in comparison to standard IDS. The increasing number of devices used in IIoT based setups has businesses becoming more concerned about protecting critical infrastructure (CI), particularly Internet Industrial Control Systems (IICs). To detect online assaults against IICSs networks, a number of intrusion detection systems (IDS) have been created and published in the literature. Nonetheless, a large number of the existing IDSs' methods and assessment criteria have some serious shortcomings. Using a deep-autoencoderbased LSTM model/method, we develop an effective IDS for IIoT-powered IICs to solve the problems of low detection rate and high false positive rates (FPR).

LITERATURE SURVEY

Convolutional Neural Network—A Practical Case Study:

https://link.springer.com/chapter/10.1007/978-981-16-7618-5_27

ABSTRACT: The convolutional neural networks had enormous success in the classification of images, and networks such as "AlexNet", "VGG", "Inception" and "ResNet" were references for this purpose. This way, it is intended to verify which networks were more successful in the "Imagenet" dataset challenge. Then, it was verified their success when classifying videos through the "Kinetics400" and "UCF101" datasets and, finally, to conclude if the success in the classification of images can also evidence a possible success in the classification of videos. To this end, the margin of error of the networks mentioned above is compared. The two networks with the lowest margin of error are selected, and these networks are studied to classify videos. Thus, if these networks are successful, they can receive input videos from sensors and accurately identify the human activity present in the video. It should be noted that the networks "ResNet" and "Inception" had very satisfactory success rates, above 70%, showing success in the approach adopted.

Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets:

https://www.mdpi.com/1424-8220/22/10/3744

ABSTRACT: The rapid expansion of Internet of Things (IoT) applications has resulted in a significant rise in network data and a high computational complexity among the diverse linked devices. IoT devices gather important data that helps businesses and individual consumers make vital choices that affect their daily lives. The majority of these Internet of Things devices have poor CPU speeds, little memory, and minimal energy storage. Because these devices lack the capability to run current general-purpose security software, they are thus susceptible to cyber-attacks. IoT networks become inherently risky as a result. By moving sophisticated processing operations from IoT devices to the edge, the multi-access edge computing (MEC) platform has arisen to alleviate these limitations. The majority of connected works now in existence concentrate on identifying the best security ways to safeguard IoT devices. We think greater focus should be on distributed systems that use MEC. Modern network intrusion detection systems (NIDS) and IoT network security procedures are thoroughly reviewed in this study. We have examined the methods that make use of machine learning (ML) techniques and are based on MEC platforms. Additionally, a comparative examination of the assessment criteria, deployment methodologies, and datasets that are publicly accessible that were used in the NIDS design is performed in this research. Lastly, we suggest a MEC-based NIDS architecture for IoT networks.

A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method:

https://www.mdpi.com/1424-8220/22/16/5986

ABSTRACT: Due to the rapid growth in IT technology, digital data have increased availability, creating novel security threats that need immediate attention. An intrusion detection system (IDS) is the most promising solution for preventing malicious intrusions and tracing suspicious network behavioral patterns. Machine learning (ML) methods are widely used in IDS. Due to a limited training dataset, an ML-based IDS generates a higher false detection ratio and encounters data imbalance issues. To deal with the data-imbalance issue, this research develops an efficient hybrid network-based IDS model (HNIDS), which is utilized using the enhanced genetic algorithm and particle swarm optimization(EGA-PSO) and improved random forest (IRF) methods. In the initial phase, the proposed HNIDS utilizes hybrid EGA-PSO methods to enhance the minor data samples and thus produce a balanced data set to learn the sample attributes of small samples more accurately. In the proposed HNIDS, a PSO method improves the vector. GA is enhanced by adding a multi-objective function, which selects the best features and achieves improved fitness outcomes to explore the essential features and helps minimize dimensions, enhance the true positive rate (TPR), and lower the false positive rate (FPR). In the next phase, an IRF eliminates the less significant attributes, incorporates a list of decision trees across each iterative process, supervises the classifier's performance, and prevents overfitting issues. The performance of the proposed method and existing ML methods are tested using the benchmark datasets NSL-KDD. The experimental findings demonstrated that the proposed HNIDS method achieves an accuracy of 98.979% on BCC and 88.149% on MCC for the NSL-KDD dataset, which is far better than the other ML methods i.e., SVM, RF, LR, NB, LDA, and CART.

A tree classifier based network intrusion detection model for Internet of Medical Things:
https://www.sciencedirect.com/science/article/abs/pii/S0045790622004049

ABSTRACT: Healthcare is one of the key areas of prospect for the Internet of Things (IoT). To facilitate better medical services, enormous growth in the field of the Internet of Medical Things (IoMT) is observed recently. Despite the numerous benefits, the cyber threats on connected healthcare devices can compromise privacy and can also cause damage to the health of the concerned patient. The massive demand for IoMT devices with seamless and effective medical facilities for the large-scale population requires a robust secured model to ensure the privacy and safety of patients in this network. However, designing security models for IoMT networks is very challenging. An effort has been made in this work, to design a tree classifier-based network intrusion detection model for IoMT networks. The proposed system effectively reduces the dimension of the input data to speed up the anomaly detection procedure while maintaining a very high accuracy of 94.23%.

A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment:
https://www.sciencedirect.com/science/article/abs/pii/S0045790622004700

ABSTRACT: The rapid expansion of Internet of Things (IoT) applications has resulted in a significant rise in network data and a high computational complexity among the diverse linked devices. IoT devices gather important data that helps businesses and individual consumers make vital choices that affect their daily lives. The majority of these Internet of Things devices have poor CPU speeds, little memory, and minimal energy storage. Because these devices lack the capability to run current general-purpose security software, they are thus susceptible to cyber-attacks. IoT networks become inherently risky as a result. By moving sophisticated processing operations from IoT devices to the edge, the multi-access edge computing (MEC) platform has arisen to alleviate these limitations. The majority of connected works now in existence concentrate on identifying the best security ways to safeguard IoT devices. We think greater focus should be on distributed systems that use MEC. Modern network intrusion detection systems (NIDS) and IoT network security procedures are thoroughly reviewed in this study. We have examined the methods that make use of machine learning (ML) techniques and are based on MEC platforms. Additionally, a comparative examination of the assessment criteria, deployment methodologies, and datasets that are publicly accessible that were used in the NIDS design is performed in this research. Lastly, we suggest a MEC-based NIDS architecture for IoT networks.

Proposed System:

We propose a deep learning-based novel method to detect cybersecurity vulnerabilities and breaches in cyber-physical systems. The proposed framework contrasts the unsupervised and deep learning-based (RNN, CNN, and DNN) discriminative approaches. We presents a generative adversarial network(RBN, DBN, DBM., and DA) to detect cyber threats in IoT-driven IICs networks. Tests the performance of the proposed efficient IDS framework on IIoT IICs and exterior networks on the NSLKDD, KDDCup99, and UNSW-NB15 datasets.

SYSTEM ARCHITECTURE:

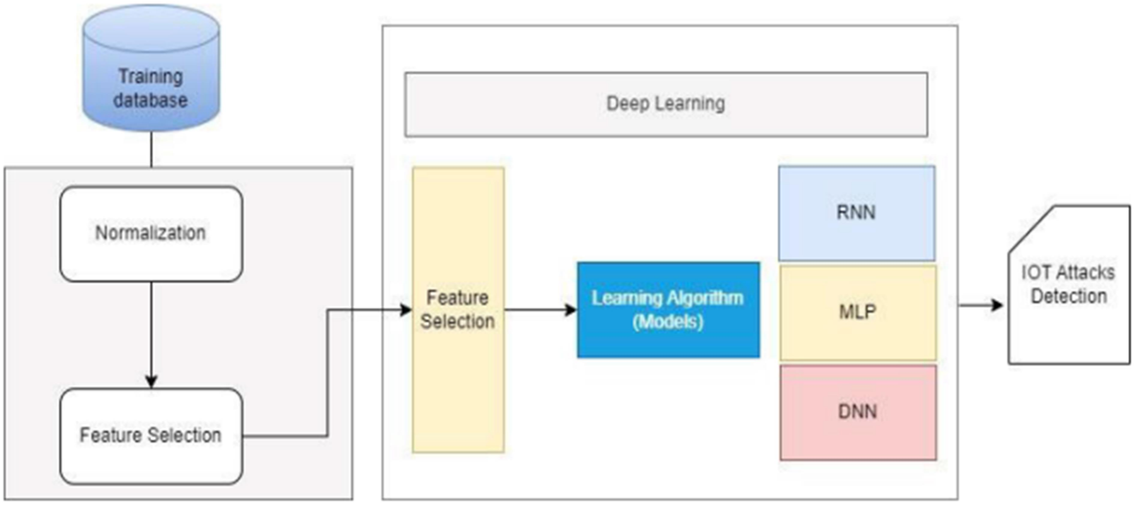
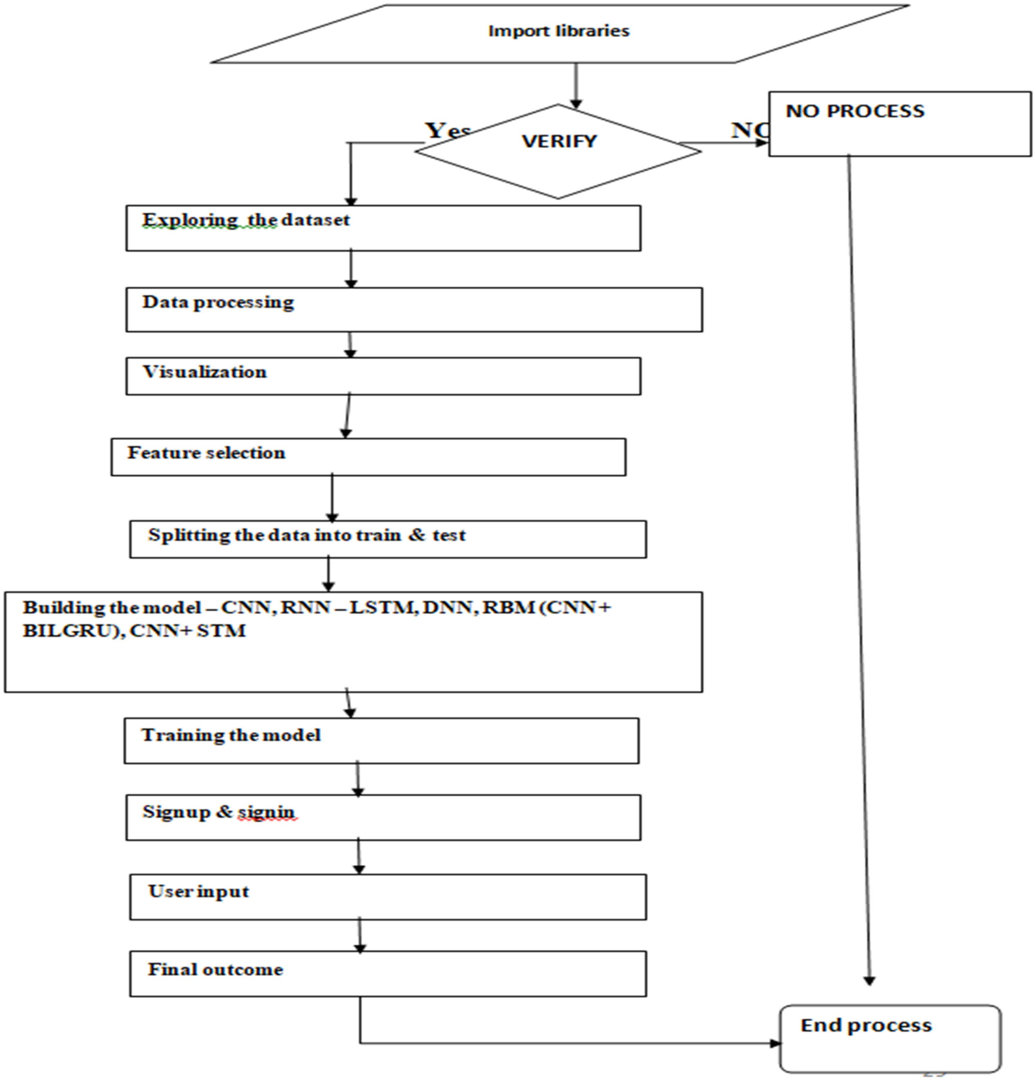


Fig.5.1.1 System architecture

DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.



IMPLEMENTATION

Algorithms:

CNN: A convolutional neural network (CNN) is a specific type of artificial neural network that uses perceptrons, a machine learning unit algorithm, for supervised learning, to analyze data. CNNs apply to image processing, natural language processing and other kinds of cognitive tasks.

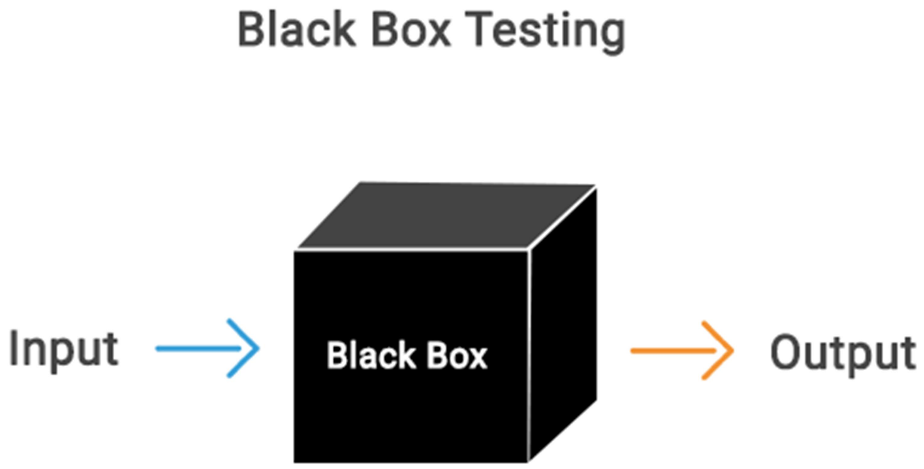
RNN – LSTM: Recurrent Neural Network with Long Short-Term Memory (RNN-LSTM) is a deep learning algorithm designed for sequential data analysis. It overcomes the limitations of traditional RNNs by incorporating LSTM units, which can capture long-range dependencies in data. LSTM units are equipped with memory cells and gates to control the flow of information, preventing the vanishing gradient problem. RNN-LSTM is particularly effective in tasks involving sequential data, such as natural language processing, speech recognition, and time-series forecasting, where it excels at capturing intricate temporal patterns and dependencies.

DNN: Deep neural networks (DNN) is a class of machine learning algorithms similar to the artificial neural network and aims to mimic the information processing of the brain. DNN shave more than one hidden layer (l) situated between the input and out put layers.

RBM (CNN + BILGRU): RBM (CNN + BILGRU) is a hybrid deep learning algorithm that combines Convolutional Neural Networks (CNN) and Bidirectional Gated Recurrent Units (BILGRU). It's used for tasks like image and text processing. CNN extracts spatial features from data, while BILGRU captures temporal information bidirectionally. This fusion enhances the model's ability to handle complex patterns in both spatial and sequential data.

CNN + LSTM: A CNN processes sequence data by applying sliding convolutional filters to the input. A CNN can learn features from both spatial and time dimensions. An LSTM network processes sequence data by looping over time steps and learning long-term dependencies between time steps.

SYSTEM TESTING



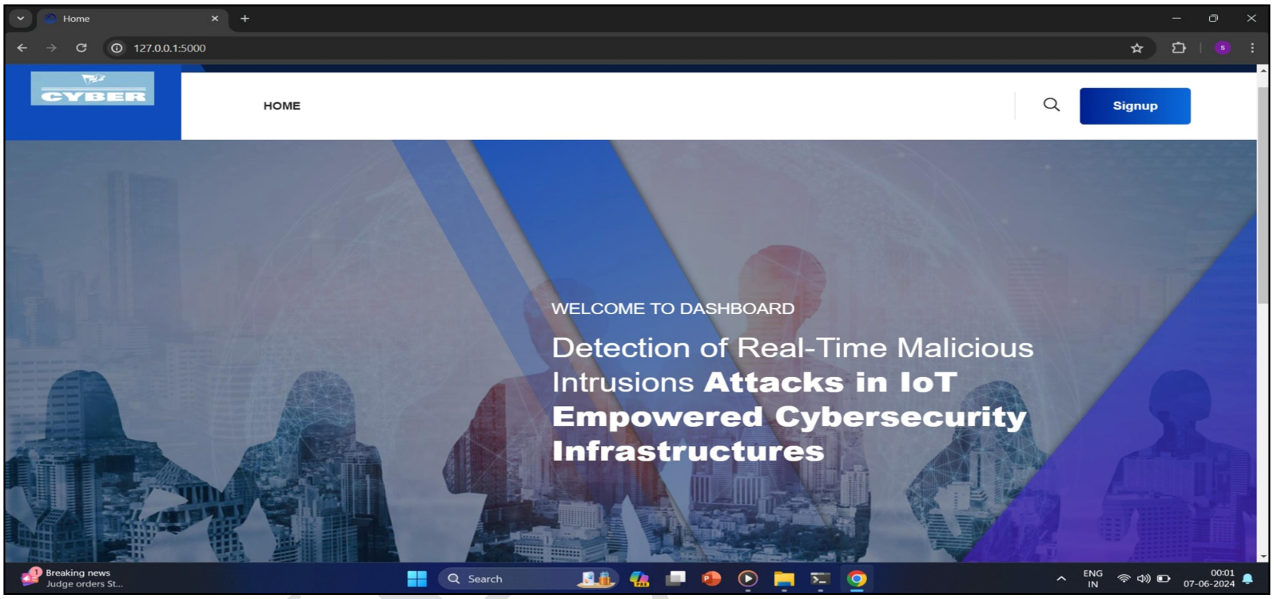
TEST CASES:

S.NO	INPUT	If available	If not available
1	User signup	User get registered into the application	There is no process
2	User signin	User get login into the application	There is no process

3	Enter input for prediction	Prediction result displayed	There is no process

RESULTS

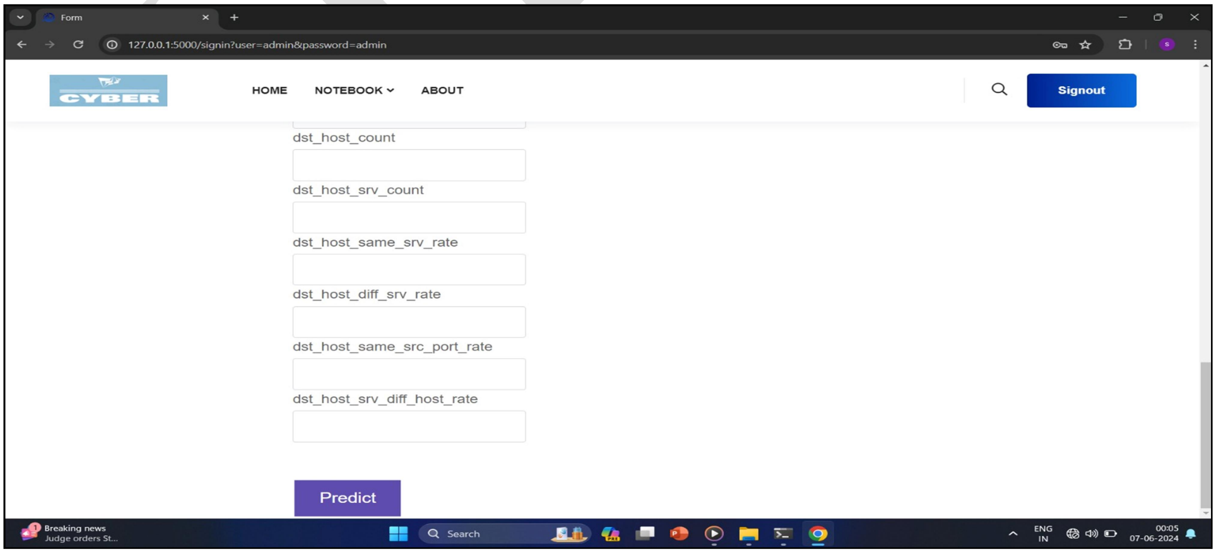
SCREENS:



WELCOME TO DASHBOARD

Detection of Real-Time Malicious Intrusions **Attacks in IoT Empowered Cybersecurity Infrastructures**

Fig 2: Login Page.



dst_host_count

dst_host_srv_count

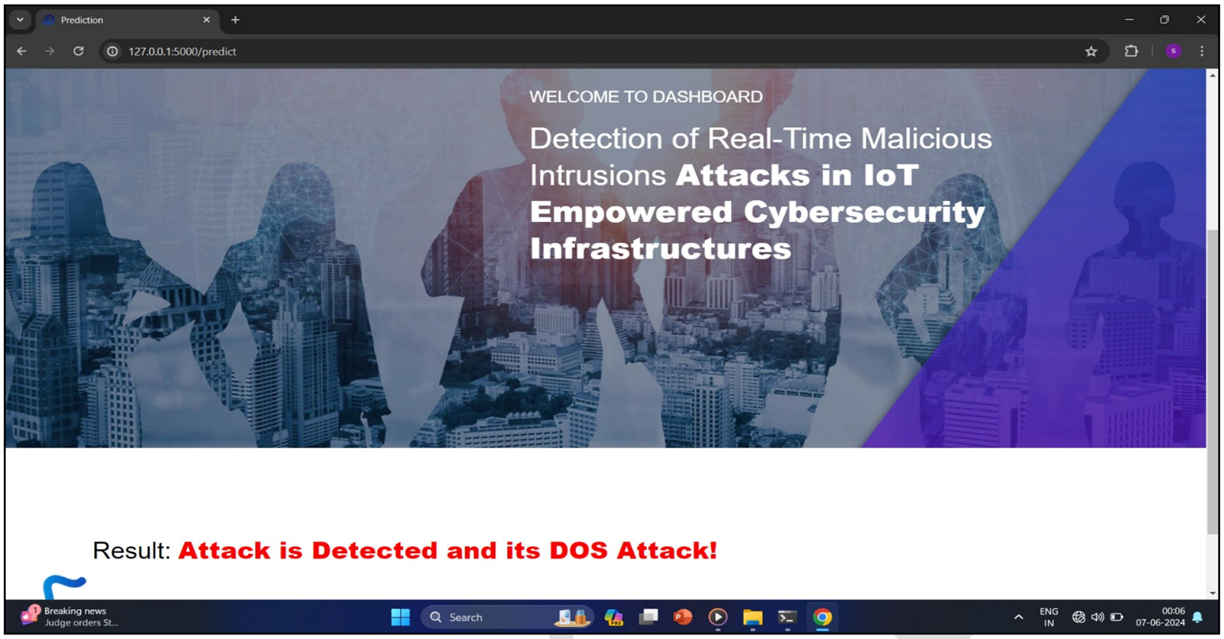
dst_host_same_srv_rate

dst_host_diff_srv_rate

dst_host_same_src_port_rate

dst_host_srv_diff_host_rate

Fig 3: Entering Values for Prediction.



WELCOME TO DASHBOARD

Detection of Real-Time Malicious Intrusions **Attacks in IoT Empowered Cybersecurity Infrastructures**

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

Fig 4: Result.

CONCLUSION

This paper discusses the involving challenges and limitations in previous studies, which have been investigating how to use deep learning in the early detection and eradication of cyber threats. We employs deep learning techniques for cyber-attack malware detection, such as identification and discriminative. However, we summarized the seven approaches, i.e., deep learning (RNN, CNN, and DNN) and generative models/methods (RBN, DBN, DBM., and DA). In addition, our investigation focuses on accuracy and provided dictionaries in the research field. The experimentation of our work demonstrates IDS and Cybersecurity attacks, which are detected successfully using a collaborative technological environment. Also, we have investigated to find which DL techniques performed better among the others. According to this analysis, the use of deep learning methods increases the investigational rate of classification intrusion while providing a robust performance of state-of-the-art supervised systems. In this scenario, a part of future work, this study extended to include advanced deep learning methods and transfer learning approaches. Moreover, the robustness of the supervised system is validated using IDS training. Thus, when designing a newfangled Intrusion Detection System (IDS), the properties can be used in the real-time system to detect internal and external intruders and their malicious behaviors.

11. REFERENCES

[1] Y. LeCun, Y. Bengio, and G. Hinton, ‘‘Deep learning,’’ Nature, vol. 521, no. 7553, pp. 436–444, 2015.

[2] A. Krizhevsky, I. Sutskever, and G. E. Hinton, ‘‘ImageNet classification with deep convolutional neural networks,’’ Commun. ACM, vol. 60, no. 2, pp. 84–90, Jun. 2017.

[3] M. K. Islam, M. S. Ali, M. M. Ali, M. F. Haque, A. A. Das, M. M. Hossain, D. S. Duranta, and M. A. Rahman, ‘‘Melanoma skin lesions classification using deep convolutional neural network with transfer learning,’’ in Proc. 1st Int. Conf. Artif. Intell. Data Analytics (CAIDA), Apr. 2021.

[4] A. Ahmim, M. Derdour, and M. A. Ferrag, ‘‘An intrusion detection system based on combining probability predictions of a tree of classifiers,’’ Int. J. Commun. Syst., vol. 31, no. 9, p. e3547, Jun. 2018.

[5] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, ‘‘A novel hierarchical intrusion detection system based on decision tree and rules-based models,’’ in Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS), May 2019, pp. 228–233.

[6] Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay,” *Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes*”, International Journal of Intelligent Systems and Applications in Engineering, ISSN no: 2147-6799 IJISAE,Vol 12 issue 3, 2024, Nov 2023

[7] Md. Zainlabuddin, "*Wearable sensor-based edge computing framework for cardiac arrhythmia detection and acute stroke prediction*”, Journal of Sensor, Volume2023.

[8] Md. Zainlabuddin, "*Security Enhancement in Data Propagation for Wireless Network*”, Journal of Sensor, ISSN: 2237-0722 Vol. 11 No. 4 (2021).

[9] Dr MD Zainlabuddin, "*CLUSTER BASED MOBILITY MANAGEMENT ALGORITHMS FOR WIRELESS MESH NETWORKS*”, Journal of Research Administration, ISSN:1539-1590 | E-ISSN:2573-7104 , Vol. 5 No. 2, (2023)

[10] Vaishnavi Lakadaram, " Content Management of Website Using Full Stack Technologies”, Industrial Engineering Journal, ISSN: 0970-2555 Volume 15 Issue 11 October 2022

[11] Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ,” *Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution*”, International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526

[12] Ijteba Sultana, Mohd Abdul Bari and Sanjay,” *Impact of Intermediate per Nodes on the QoS Provision in Wireless Infrastructure less Networks*”, Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021

[13] M.A.Bari, Sunjay Kalkal, Shahanawaj Ahamad," *A Comparative Study and Performance Analysis of Routing Algorithms*”, in 3rd International Conference ICCIDM, Springer - 978- 981-10-3874-7_3 Dec (2016)

[14] Mohammed Rahmat Ali,: BIOMETRIC: AN e-AUTHENTICATION SYSTEM TRENDS AND FUTURE APLLICATION”, International Journal of Scientific Research in Engineering (IJSRE), Volume1, Issue 7, July 2017

[15] Mohammed Rahmat Ali,: BYOD.... A systematic approach for analyzing and visualizing the type of data and information breaches with cyber security”, NEUROQUANTOLOGY, Volume20, Issue 15, November 2022

[16] Mohammed Rahmat Ali, Computer Forensics -An Introduction of New Face to the Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-453 – 456, Volume: 5 Issue: 7

[17] Mohammed Rahmat Ali, Digital Forensics and Artificial Intelligence ...A Study, International Journal of Innovative Science and Research Technology, ISSN:2456-2165, Volume: 5 Issue:12.

[18] Mohammed Rahmat Ali, Usage of Technology in Small and Medium Scale Business, International Journal of Advanced Research in Science & Technology (IJARST), ISSN:2581-9429, Volume: 7 Issue:1, July 2020.

[19] Mohammed Rahmat Ali, Internet of Things (IOT) Basics - An Introduction to the New Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-32-36, Volume: 5 Issue: 10

[20] Mohammed Rahmat Ali, Internet of things (IOT) and information retrieval: an introduction, International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume: 7 Issue: 4, October 2017.

[21] Mohammed Rahmat Ali, How Internet of Things (IOT) Will Affect the Future - A Study, International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-424874 – 77, Volume: 3 Issue: 10, October 2017.

[22] Mohammed Rahmat Ali, ECO Friendly Advancements in computer Science Engineering and Technology, International Journal on Scientific Research in Engineering(IJSRE), Volume: 1 Issue: 1, January 2017

[23] Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay, "*Routing Quality of Service for Multipath Manets, International Journal of Intelligent Systems and Applications in Engineering"*, JISAE, ISSN:2147-6799, 2024, 12(5s), 08–16;

[24] Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46

[25] Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto) Elsevier SCI Oct : 021

[26] Syed Shehriyar Ali, Mohammed Sarfaraz Shaikh, Syed Safi Uddin, Dr. Mohammed Abdul Bari, "Saas Product Comparison and Reviews Using Nlp", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022

[27] Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6

[28] .A.Bari& Shahanawaj Ahamad, "Managing Knowledge in Development of Agile Software", in International Journal of Advanced Computer Science & Applications (IJACSA), ISSN: 2156-5570, Vol: 2, No: 4, pp: 72-76, New York, U.S.A., April 2011

[29] Imreena Ali (Ph.D), Naila Fathima, Prof. P.V.Sudha ,"Deep Learning for Large-Scale Traffic-Sign Detection and Recognition", Journal of Chemical Health Risks, ISSN:2251-6727/ JCHR (2023) 13(3), 1238-1253

[30] Imreena, Mohammed Ahmed Hussain, Mohammed Waseem Akram" An Automatic Advisor for Refactoring Software Clones Based on Machine Learning", Mathematical Statistician and Engineering ApplicationsVol. 72 No. 1 (2023)

[31] Mrs Imreena Ali Rubeena,Qudsiya Fatima Fatimunisa "Pay as You Decrypt Using FEPOD Scheme and Blockchain", Mathematical Statistician and Engineering Applications: https://doi.org/10.17762/msea.v72i1.2369 Vol. 72 No. 1 (2023)

[32] Imreena Ali , Vishnuvardhan, B.Sudhakar," Proficient Caching Intended For Virtual Machines In Cloud Computing", International Journal Of Reviews On Recent Electronics And Computer Science , ISSN 2321-5461,IJRRECS/October 2013/Volume-1/Issue-6/1481-1486

[33] Heena Yasmin, A Systematic Approach for Authentic and Integrity of Dissemination Data in Networks by Using Secure DiDrip, INTERNATIONAL JOURNAL OF PROFESSIONAL ENGINEERING STUDIES, Volume VI /Issue 5 / SEP 2016

[34] Heena Yasmin, Cyber-Attack Detection in a Network, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)

[35] Heena Yasmin, Emerging Continuous Integration Continuous Delivery (CI/CD) For Small Teams, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)