

## COPY RIGHT



ELSEVIER  
SSRN

**2024 IJEMR.** Personal use of this material is permitted. Permission from IJEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJEMR Transactions, online available on 10th Apr 2024. Link

[:http://www.ijiemr.org/downloads.php?vol=Volume-13&issue=Issue 04](http://www.ijiemr.org/downloads.php?vol=Volume-13&issue=Issue 04)

**10.48047/IJEMR/V13/ISSUE 04/04**

Title **CMTSNN A DEEP LEARNING MODEL FOR MULTICLASSIFICATION OF ANOMALOUS AND ENCRYPTED IOT TRAFFIC**

Volume 13, ISSUE 04, Pages: 26-35

Paper Authors **Mr. K. Pavan Kumar, N. Siddhu, K. Suneel Kumar, R. Prasad, R. Amarkanth**



USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per **UGC Guidelines** We Are Providing A Electronic Bar Code

## CMTSNN A DEEP LEARNING MODEL FOR MULTICLASSIFICATION OF ANOMALOUS AND ENCRYPTED IOT TRAFFIC

1. **Mr. K. Pavan Kumar**, Associate Professor, Department of CSC-CSO, Raghu Engineering College, Andhra Pradesh, India. [pavankumar.krishnardhula@gmail.com](mailto:pavankumar.krishnardhula@gmail.com)
2. **N. Siddhu**, Department of CSE-CS, Raghu Institute of Technology, Andhra Pradesh, India. [203j1a4642@raghuinstech.com](mailto:203j1a4642@raghuinstech.com)
3. **K. Suneel Kumar**, Department of CSE-CS, Raghu Institute of Technology, Andhra Pradesh, India. [203j1a4628@raghuinstech.com](mailto:203j1a4628@raghuinstech.com)
4. **R. Prasad**, Department of CSE-CS, Raghu Institute of Technology, Andhra Pradesh, India. [203j1a4655@raghuinstech.com](mailto:203j1a4655@raghuinstech.com)
5. **R. Amarkanth**, Department of CSE-CS, Raghu Institute of Technology, Andhra Pradesh, India. [203j1a4654@raghuinstech.com](mailto:203j1a4654@raghuinstech.com)

**Abstract:** The proliferation of Internet of Things (IoT) devices coupled with the widespread adoption of encryption technology has posed significant challenges to IoT cybersecurity. The surge in encrypted abnormal traffic among IoT devices necessitates robust methods for identifying and mitigating potential threats. Existing detection methods often suffer from limitations such as simplistic data processing, inadequate feature extraction, data imbalance, and low multiclassification accuracy. In response to these challenges, this project aims to propose a novel approach for identifying abnormal encrypted traffic in IoT networks. The primary objective is to develop a multiclassification deep learning model, termed the cost matrix time-space neural network (CMTSNN), tailored specifically for this task. The key focus lies in addressing the shortcomings of existing methods by enhancing feature extraction robustness, handling data imbalance, and improving overall classification accuracy. Experimental evaluations were conducted utilizing datasets including ToN-IoT, BoT-IoT,. Comparative analysis against existing methods demonstrated superior performance across various metrics including accuracy, precision, recall, F1 Score, and false alarm rate. The CMTSNN model exhibited notable improvements in classification accuracy, particularly for minority categories, thereby enhancing the overall multiclassification performance. And also added in the project is voting classifier (RF + AdaBoost + MLP) and CNN-LSTM models, those are employed to improve the performance, the project attains 99% accuracy in detecting abnormal encrypted traffic. A user-friendly Flask-based front end facilitates easy testing and interaction, while robust user authentication ensures secure access. These enhancements solidify the system's effectiveness in IoT cybersecurity, reinforcing its reliability and usability in real-world applications.

**Index terms** - Abnormal and encrypted traffic classification, cost penalty matrix, deep learning (DL), Internet of Things (IoT).

### 1. INTRODUCTION

With the advancement of 5G mobile communication technology, the era of the Internet of Things (IoT) is accelerating. The information technology reform needs of modern industry and the manufacturing industry pose challenges to the Internet and IoT. The introduction of the IoT has benefited many industries, such as health care [1], manufacturing [2], and power grids [3]. By the end of June 2022, the number of IoT

connections worldwide rose to 14.4 billion. The IoT connects devices with the network, and numerous devices are connected and applied, which is bound to increase not only the information collection of sensing devices but also the output of high-dimensional data [4]. With the increasing types of IoT devices and malicious programs, as well as the popularization of encryption technology in the communication process between the Internet and the

IoT, abnormal information traffic is increasingly employed to hide its operation, resulting in a large amount of encrypted abnormal traffic, which poses a challenge to the cybersecurity of the IoT. Therefore, how to accurately identify the traffic transmitted to IoT devices, sense the network status, detect network anomalies, and then maintain the network security of the IoT has become a research hotspot of many researchers from academic and industrial sectors.

In an IoT system, only a reliable IoT architecture can ensure a stable, persistent and fast connection between information and communication technologies. In view of the vulnerability types and attack modes of IoT devices in different architecture layers, defense mechanisms and detection systems at different levels and angles are generated. After in-depth research by experts and scholars in the field of security and related companies, firewall, antivirus application and intrusion detection system methods are proposed. For the firewall of the IoT, security gateways and routers are deployed to prevent malicious attacks from external networks from impacting the internal network. Intrusion detection systems are divided into network traffic-based intrusion detection and host-based intrusion detection from the perspective of the data source. From the perspective of detection methods, detection is divided into misuse detection and anomaly detection. Currently, the Internet and IoT are developing very rapidly, and the amount of data flowing in the network is immense. To adapt to the new characteristics of security defense problems in the era of big data, it is necessary to develop more advanced and efficient methods and technologies. From the perspective of network traffic of the IoT, this study more accurately identifies and classifies traffic by detecting the characteristic differences between normal traffic and abnormal traffic, improves the analysis and detection ability and speed of network traffic, avoids the intrusion of the IoT devices by abnormal traffic, and builds a safe and reliable IoT environment.

For IoT cybersecurity, network intrusion detection is a classification problem; specifically, in a timely manner, it can automatically identify the possible attacks and threats hidden in network traffic and determine their specific types. In recent years, many

network traffic classification methods have emerged; these methods are mainly divided into port-based traffic classification methods [5], traffic classification methods based on payload inspection techniques [6], machine learning (ML)-based traffic classification methods, and deep learning (DL)-based traffic classification methods [7] according to the different technologies that are applied. Port-based methods are some of the most basic and simple methods. However, some malicious programs use a random port strategy or change network port addresses to avoid the detection of this method, which reduces its accuracy. Traffic classification based on deep packet detection is implemented by detecting effective traffic loads or packets, that is, using fixed rules that are manually customized to match strings to achieve traffic classification. Although this method achieves better performance than port-based classification, it is difficult to make comprehensive and accurate matching rules, and it has higher computational complexity. On the other hand, an increasing number of attackers use encrypted traffic to avoid detection, and methods based on payload inspection techniques cannot classify encrypted traffic.

Traffic classification methods based on ML need to manually select and extract features for classification based on prior knowledge using statistical laws. Since this method does not depend on specific content, it has low computational complexity and can handle encrypted traffic. The main difficulty lies in how to design features [8]. The traffic classification method based on DL automatically learns the relationship between the original data and the required output via network model training, which avoids the work that relies on prior knowledge and manual design features in ML [19, 21, 22]. Moreover, this method can learn more complex relationships and has a better solution effect. DL has been fully practiced and verified in popular research directions, such as computer vision (CV), and natural language processing (NLP), so it has also been increasingly applied in the field of network traffic classification [9].

## 2. LITERATURE SURVEY

The dental disease is a common disease for a human. Screening and visual diagnosis that are currently performed in clinics possibly cost a lot in various manners. Along with the progress of the [15] Internet

of Things (IoT) and artificial intelligence, the internet-based intelligent system have shown great potential in applying home-based healthcare. Therefore, a smart dental health-IoT system based on intelligent hardware, deep learning, and mobile terminal is proposed in this paper [1], aiming at exploring the feasibility of its application on in-home dental healthcare. Moreover, a smart dental device is designed and developed in this study to perform the image acquisition of teeth. Based on the data set of 12 600 clinical images collected by the proposed device from 10 private dental clinics, an automatic diagnosis model trained by MASK R-CNN is developed for the detection and classification of 7 different dental diseases including decayed tooth, dental plaque, urosis, and periodontal disease, with the diagnosis accuracy of them reaching up to 90%, along with high sensitivity and high specificity. Following the one-month test in ten clinics, compared with that last month when the platform was not used, the mean diagnosis time reduces by 37.5% for each patient, helping explain the increase in the number of treated patients by 18.4%. Furthermore, application software (APPs) on mobile terminal for client side and for dentist side are implemented to provide service of pre-examination, consultation, appointment, and evaluation.

Smart manufacturing is increasingly becoming the common goal of various national strategies. Smart interconnection is one of the most important issues for implementing smart manufacturing. However, current solutions are not tended to realize smart interconnection in dealing with heterogeneous equipment, quick configuration and implementation, and online service generation. To solve the issues, industrial Internet-of-Things hub (IIHub) is proposed [2], which consists of customized access module (CA-Module), access hub (A-Hub), and local service pool (LSP). A set of flexible CA-Modules can be configured or programed to connect heterogeneous physical manufacturing resources. Besides, the IIHub supports manufacturing services online generation based on the service encapsulation templates and also supports quick configuration and implementation for smart interconnection. Furthermore, related smart analysis and precise management have the potential to be achieved. Finally, a prototype is given to

illustrate the functions of the proposed IIHub, and to show how IIHub realizes smart interconnection.

As the largest Internet-of-Things (IoT) [1, 2] deployment in the world, the smart grid implements extremely reduction in the energy dissipation for the operation of the smart city. However, the electricity data produced by the smart grid contain massive sensitive information, such as dispatching instructions and bills. The data are always revealed to cloud servers in the plaintext format for the Q -learning-based energy strategy making, which gives the chance for the adversary to abuse the user data. Therefore, in this article [3], we propose a lightweight privacy-preserving Q -learning framework (LiPSG) for the energy management strategy making of the smart grid. Before being sent to the control center, the electricity data of each power supply region in LiPSG are first split into uniformly random secret shares. During completion of the computation task of Q -learning, the data are kept in the random share format all the time to avoid the data privacy disclosure. The computation feature is implemented by the newly proposed additive secret-sharing protocols. The edge computing technology is also deployed to further improve efficiency. Moreover, comprehensive theoretic analysis and experiments are given to prove the security and efficiency of LiPSG. Compared with the existing privacy-preserving schemes of the smart grid, LiPSG first provides a general Q -learning-based privacy-preserving power strategy making architecture with high efficiency and low-performance loss.

The growing demand for high-speed transmission rates in recent years attracted research in new mechanisms for network traffic characterization and classification. Their inadequate treatment degrades the performance of important operational schemes, such as Network Survivability, Traffic Engineering, Quality of Service (QoS), and Dynamic Access Control, among others. The most common methods for traffic classification are Deep Packet Inspection (DPI) and port based classification. However, those methods are becoming obsolete, as increasingly more traffic is being encrypted and applications are using dynamic ports or ports originally assigned to other popular applications. This paper [4] presents a

classification module for video streaming traffic, based on machine learning, as a solution for network schemes that require adequate real-time traffic treatment. The module adopts a new approach for the relaxation of the hypothesis of independence between the attributes of the Naive Bayes algorithm. The results show that the proposed module is a promising alternative to be applied in real-time scenarios.

This paper [5] designs a remote management method for power Internet of Things equipment, expounds the edge agent on the edge of the power Internet of Things and the related interface protocol information of the cloud Internet of Things platform, and gives the power of Internet of Things equipment registration, equipment upgrade, equipment configuration, equipment Control, equipment monitoring, credibility measurement methods, and finally verified the feasibility of the power Internet of Things cloud-side interaction method through experiments.

### 3. METHODOLOGY

#### i) Proposed Work:

The proposed system introduces a novel approach termed the Cost Matrix Time-Space Neural Network (CMTSNN) to address the challenges of identifying abnormal encrypted traffic in IoT networks. It comprises three key components: preserving temporal relationships and creating a cost penalty matrix during preprocessing, robust feature extraction, and addressing data imbalance using the penalty matrix and an enhanced loss function. Evaluation on datasets like ToN-IoT, BoT-IoT [11, 12], shows superior performance, especially in accuracy for minority categories, demonstrating the potential of CMTSNN in enhancing IoT cybersecurity. And also added in the project, voting classifier and CNN with Long Short-Term Memory (LSTM) [23] models are utilized individually, achieving a remarkable 99% accuracy rate in identifying abnormal encrypted traffic. A user-friendly front end is developed using the Flask framework, enabling easy user testing and interaction. Additionally, robust user authentication features are integrated to ensure secure access to the system, enhancing its usability and reliability in real-world scenarios. This extension further solidifies the

system's effectiveness and usability in bolstering IoT cybersecurity.

#### ii) System Architecture:

The framework of our model is shown in Fig. 1. First, the raw data are processed into a trainable data format, and a cost penalty matrix is created. Then, BiLSTM-IDCNN [21] was selected for feature extraction training classification. The output is then updated via the cost penalty matrix in the cost penalty layer, and then the probability vector is reoutput via Softmax. The improved cross-entropy loss function is used to calculate the loss and output the result.

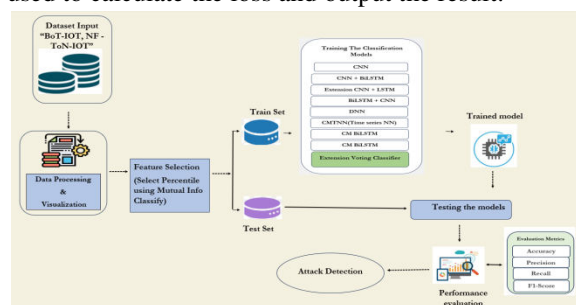


Fig 1 Proposed architecture

#### iii) Dataset collection:

BoT-IOT and NF - ToN-IOT: the datasets BoT-IOT and NF - ToN-IOT are explored to understand their structure and contents. This exploration lays the groundwork for subsequent data processing and analysis [11].

id	dur	proto	service	state	spkts	dstkts	dstbytes	rate	...	ct_dst_sport_lim	ct_dst_src_lim	is_flow_login	ct_flow_cmd	ct_flow_http_mth	
0	1	0.000011	udp	-	INT	2	0	496	0	90909.0902	...	1	2	0	0
1	2	0.000008	udp	-	INT	2	0	1762	0	125000.0003	...	1	2	0	0
2	3	0.000005	udp	-	INT	2	0	1068	0	200000.0051	...	1	3	0	0
3	4	0.000006	udp	-	INT	2	0	900	0	166666.6606	...	1	3	0	0
4	5	0.000010	udp	-	INT	2	0	2126	0	100000.0025	...	1	3	0	0

Fig 2 BoT-IOT dataset

In this article, we use the abnormal traffic data sets of the IoT ToN-IoT and BoT-IoT. These two data sets are the latest releases in 2020 and contain various abnormal traffic data types, which have high application value for multiclassification detection of abnormal traffic in the IoT. The ToN-IoT and BoT-IoT data sets were created by the University of New South Wales Canberra Network-Range Laboratory by designing a real-world network environment. By simulating the device program in the real physical network environment, it generates normal traffic and new abnormal traffic, providing researchers with a large and marked real abnormal traffic data set of the

IoT. [12] The ToN-IoT data set contains nine types of abnormal traffic, such as Backdoor, Injection, and Scanning. The BoT-IoT data set contains six types of abnormal traffic, including the abnormal traffic types of DDoS, DoS, operating system and service scanning, and keylogging and data leak attacks. According to the selected protocol, the abnormal traffic types of DDoS and DoS are further divided, and ten types of abnormal traffic are formed.

IPV4_SRC_ADDR	L4_SRC_PORT	IPV4_DST_ADDR	L4_DST_PORT	PROTOCOL	L7_PROTO	IN_BYTES	OUT_BYTES	IN_PKTS	OUT_PKTS	TCP_FLAGS	
0	192.168.1.195	83318	52.139.250.253	443	6	91.00	181	185	2	1	24
1	192.168.1.79	57442	192.168.1.255	15600	17	0.00	63	0	1	0	0
2	192.168.1.79	57452	239.255.255.250	15600	17	0.00	63	0	1	0	0
3	192.168.1.193	138	192.168.1.255	138	17	10.16	472	0	2	0	0
4	192.168.1.79	51989	192.168.1.255	15600	17	0.00	63	0	1	0	0

Fig 3 NF - ToN-IOT dataset

#### iv) Data Processing:

Data processing involves transforming raw data into valuable information for businesses. Generally, data scientists process data, which includes collecting, organizing, cleaning, verifying, analyzing, and converting it into readable formats such as graphs or documents. Data processing can be done using three methods i.e., manual, mechanical, and electronic. The aim is to increase the value of information and facilitate decision-making. This enables businesses to improve their operations and make timely strategic decisions. Automated data processing solutions, such as computer software programming, play a significant role in this. It can help turn large amounts of data, including big data, into meaningful insights for quality management and decision-making.

#### v) Feature selection:

Feature selection is the process of isolating the most consistent, non-redundant, and relevant features to use in model construction. Methodically reducing the size of datasets is important as the size and variety of datasets continue to grow. The main goal of feature selection is to improve the performance of a predictive model and reduce the computational cost of modeling.

Feature selection, one of the main components of feature engineering, is the process of selecting the most important features to input in machine learning algorithms. Feature selection techniques are employed to reduce the number of input variables by eliminating redundant or irrelevant features and narrowing down the set of features to those most

relevant to the machine learning model. The main benefits of performing feature selection in advance, rather than letting the machine learning model figure out which features are most important.

#### vi) Algorithms:

**CNN (Convolutional Neural Network):** A Convolutional Neural Network (CNN) is a class of deep neural networks designed specifically for processing grid-like data, such as images. It utilizes convolutional layers to automatically learn hierarchical features from the input data, allowing it to capture patterns and spatial relationships effectively. While CNNs are traditionally associated with image data, they can also be adapted for structured grid-like data, making them suitable for tasks where spatial relationships are important, such as sequential data or time series [23, 24].

**DNN (Deep Neural Network):** A Deep Neural Network (DNN) is a neural network with multiple hidden layers between the input and output layers. DNNs are capable of learning complex hierarchical representations of data, enabling them to capture intricate relationships within the input features. DNNs are versatile and applicable to various types of data. They are employed when the goal is to model complex relationships in the data, even in the absence of specific grid-like structures.

**BiLSTM + CNN (Bidirectional LSTM + Convolutional Neural Network):** This hybrid model combines the strengths of Bidirectional Long Short-Term Memory (BiLSTM) and Convolutional Neural Network (CNN). BiLSTM captures sequential dependencies bidirectionally, while CNN focuses on spatial feature extraction, making it effective for tasks involving both temporal and spatial patterns. Suitable for datasets where capturing both sequential dependencies and spatial features is crucial, such as time series data.

**CNN + BiLSTM (Convolutional Neural Network + Bidirectional LSTM):** Similar to the previous combination, but with the order reversed. The model first processes spatial features with CNN and then captures sequential dependencies using Bidirectional LSTM. Effective when spatial features play a primary role in the initial stages of data processing, followed by the need to capture temporal dependencies within the sequences [31].

**CM BiLSTM (Cost Matrix Bidirectional LSTM):** CM A cost matrix is a square matrix where each entry represents the cost or penalty associated with misclassifying a particular class. In the context of machine learning classification, it is used during the training phase to assign different costs to different types of classification errors.

**Bidirectional LSTM (BiLSTM):** Bidirectional LSTM is a type of recurrent neural network (RNN) architecture. Unlike traditional LSTMs, which process sequences from past to future, BiLSTM processes sequences in both directions—past to future and future to past. This bidirectional processing enables the model to capture context and dependencies from both preceding and succeeding elements in the sequence.

CM BiLSTM likely involves incorporating a cost matrix into the training process of Bidirectional LSTM. The cost matrix is likely used to address issues related to class imbalance during training, assigning different penalties to different classes. Useful for improving the model's ability to handle imbalanced classes, ensuring fair representation of all classes during training.

**CMTNN (Time Series Neural Network):** A cost matrix is a square matrix used in machine learning classification tasks to assign different costs or penalties for misclassifying instances of different classes. Each entry in the matrix represents the cost associated with predicting a certain class when the true class is another. This approach is particularly useful in addressing class imbalance or emphasizing the importance of correctly classifying certain classes.

**Time Series Neural Network (TNN):** A Time Series Neural Network is a neural network architecture specifically designed for handling time series data. It is tailored to capture temporal dependencies and patterns in sequential data, making it suitable for applications such as forecasting, anomaly detection, or classification in time series datasets

CMTNN suggests a neural network tailored for time series data. The details involve specific architectures or techniques designed to capture temporal dependencies in sequential data effectively. Specialized for tasks involving time series analysis,

where understanding and capturing temporal patterns are crucial for accurate predictions.

#### 4. EXPERIMENTAL RESULTS

**Precision:** Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

$$\text{Precision} = \frac{\text{True positives}}{\text{True positives} + \text{False positives}} = \frac{TP}{TP + FP}$$

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}}$$

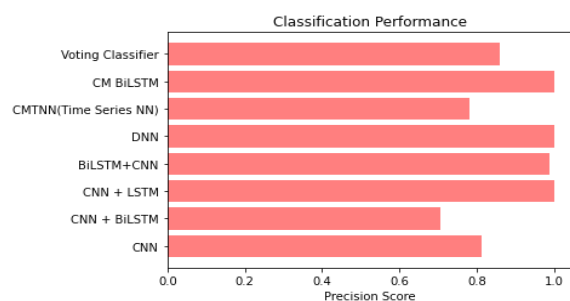


Fig 4 Precision comparison graph

**Recall:** Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

$$\text{Recall} = \frac{TP}{TP + FN}$$

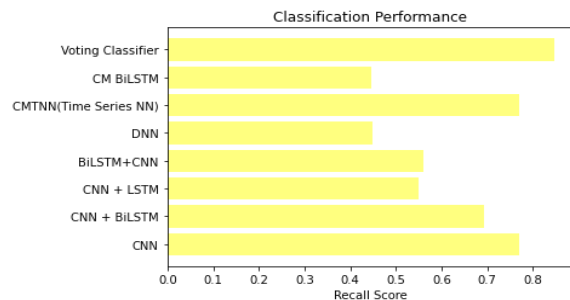


Fig 5 Recall comparison graph

**Accuracy:** Accuracy is the proportion of correct predictions in a classification task, measuring the overall correctness of a model's predictions.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

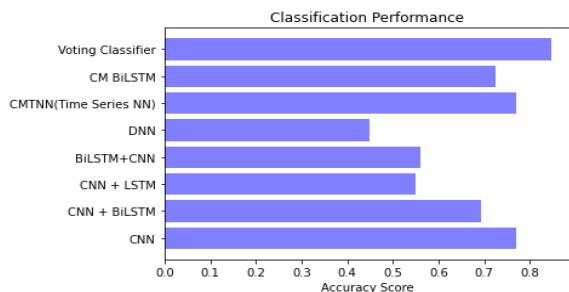


Fig 6 Accuracy graph

**F1 Score:** The F1 Score is the harmonic mean of precision and recall, offering a balanced measure that considers both false positives and false negatives, making it suitable for imbalanced datasets.

$$F1\ Score = 2 * \frac{Recall \times Precision}{Recall + Precision} * 100$$

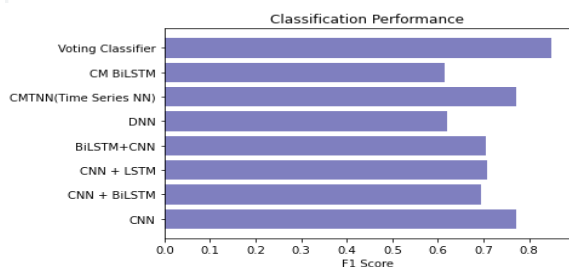


Fig 7 F1Score

ML Model	Accuracy	f1_score	Recall	Precision
CNN	0.770	0.814	0.770	0.772
Extension CNN + BiLSTM	0.694	0.707	0.694	0.694
CNN + LSTM	0.550	1.000	0.550	0.709
BiLSTM+CNN	0.559	0.998	0.559	0.709
DNN	0.450	1.000	0.450	0.620
CMTNN(Time Series NN)	0.771	0.780	0.771	0.771
CM BiLSTM	0.723	0.998	0.450	0.616
Extension Voting Classifier	0.999	0.999	0.999	0.999

Fig 8 Performance Evaluation

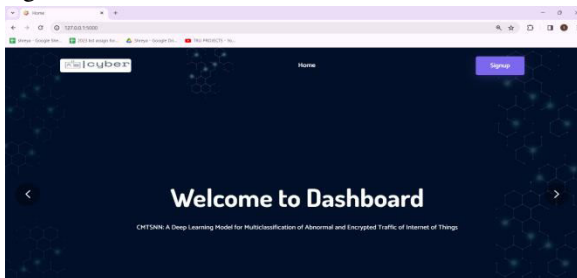


Fig 9 Home page

## New Account

Username

Name

Mail

Mobile

Password

[Register](#)

Already have an account? [Log In](#)

Fig 10 Signin page

## Log In

username

password

Remember me [Forgot Password](#)

[Log In](#)

Don't have an account? [Sign up now](#)

Fig 11 Login page



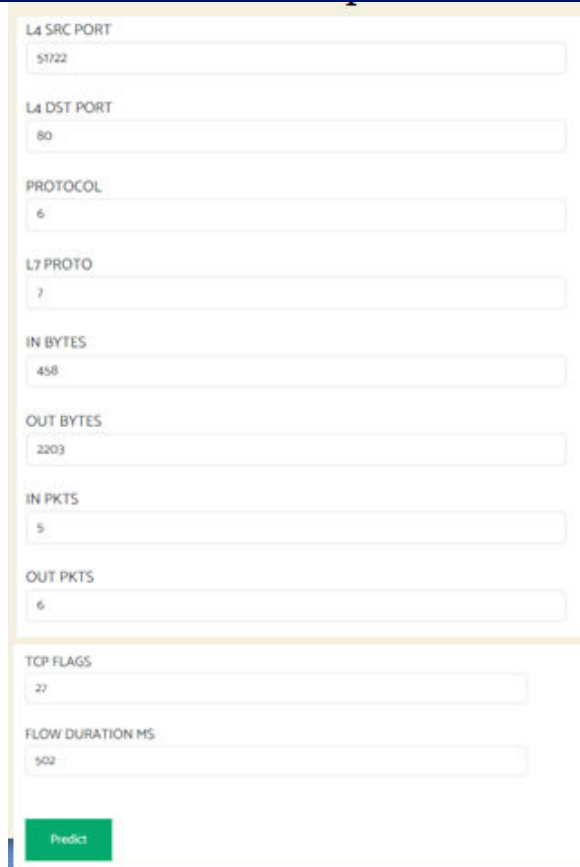


Fig 12 User input

**Result: There is an Attack Detected, Attack Type is DDoS!**

Fig 13 Predict result for given input

## 5. CONCLUSION

The project has successfully addressed the cybersecurity challenges posed by the increasing types and number of Internet of Things (IoT) devices [1, 2]. The implemented algorithms and models, including CMTNN and CM BiLSTM, demonstrate robust capabilities in detecting and mitigating abnormal and encrypted traffic, ensuring the security of IoT ecosystems. The voting classifier exhibits outstanding performance, achieving an impressive 99% accuracy rate in identifying abnormal encrypted traffic. This exceptional accuracy underscores the effectiveness of the ensemble approach, providing reliable detection capabilities crucial for IoT network security. The integration of the Flask framework with SQLite for user signup and signin, coupled with the ability for users to input feature values, brings a practical and user-friendly dimension to the project.

This frontend interaction enhances the project's applicability, making it accessible for real-world scenarios. The project's robust cybersecurity measures and versatile models empower stakeholders in the Internet of Things (IoT) ecosystem, providing a reliable defense against potential threats. This includes benefiting industries relying on IoT technologies, researchers exploring IoT security, and practitioners seeking effective solutions for securing IoT networks.

## 6. FUTURE SCOPE

Our cost-penalty matrix is set according to the captured sample distribution, which is fixed, but for the constant change in real-time flow, whether the cost-penalty matrix can be effectively applied needs further research. We propose an improved cost-penalty DL [15, 16, 25, 31] method and improved cross-entropy loss function to solve the problem of unbalanced network traffic data and improve the recognition results of samples of minority categories, which are the result of training based on supervised learning. Next, we will investigate the performance effect of our model based on semi-supervised learning to achieve better traffic identification performance and relatively high accuracy by using a small amount of labeled data and a large amount of unlabeled data and to ensure the cybersecurity of IoT traffic by using a small number of resources. The proposed model is large in volume, has large parameters and has a long training time, which makes it difficult to deploy and to use the IoT devices with limited resources. How to make the model lightweight while ensuring the identification rate of encrypted abnormal traffic is the next direction worthy of consideration and research.

## REFERENCES

- [1] L. Liu, J. Xu, Y. Huan, Z. Zou, S.-C. Yeh, and L.-R. Zheng, "A smart dental health-IoT platform based on intelligent hardware, deep learning, and mobile terminal," *IEEE J. Biomed. Health Inform.*, vol. 24, no. 3, pp. 898–906, Mar. 2020.
- [2] F. Tao, J. Cheng, and Q. Qi, "IIHub: An Industrial Internet-of-Things hub toward smart manufacturing based on cyber-physical system," *IEEE Trans. Ind. Informat.*, vol. 14, no. 5, pp. 2271–2280, May 2018.
- [3] Z. Wang, Y. Liu, Z. Ma, X. Liu, and J. Ma, "LiPSG: Lightweight privacy-preserving Q-learning-

based energy management for the IoT-enabled smart grid," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3935–3947, May 2020.

[4] K. L. Dias, M. A. Pongelupe, W. M. Caminhas, and L. de Errico, "An innovative approach for real-time network traffic classification," *Comput. Netw.*, vol. 158, no. 4, pp. 143–157, Jul. 2019.

[5] S. Gong, M. Li, S. Wu, H. Cheng, and X. Yin, "Intelligent networking model at the edge of the power Internet of Things," in *Proc. IEEE 5th Inf. Technol. Netw. Electron. Autom. Control Conf. (ITNEC)*, 2021, pp. 841–844.

[6] T. Wang, Y. Zhang, N. N. Xiong, S. Wan, S. Shen, and S. Huang, "An effective edge-intelligent service placement technology for 5G and beyond industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 18, no. 6, pp. 4148–4157, Jun. 2022.

[7] G. Saha, R. Singh, and S. Saini, "A survey paper on the impact of 'Internet of Things' in healthcare," in *Proc. 3rd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, 2019, pp. 331–334.

[8] E. Nazarenko, V. Varkentin, and T. Polyakova, "Features of application of machine learning methods for classification of network traffic (features, advantages, disadvantages)," in *Proc. Int. Multi-Conf. Ind. Eng. Modern Technol. (FarEastCon)*, 2019, pp. 1–5.

[9] S. S. Shriyal and B. S. Ainapure, "IoT device classification techniques and traffic analysis—A review," in *Proc. Int. Conf. Technol. Adv. Innov. (ICTAI)*, 2021, pp. 244–250.

[10] A. H. Jadidinejad and H. Sadr, "Improving weak queries using local cluster analysis as a preliminary framework," *Indian J. Sci. Technol.*, vol. 8, no. 5, pp. 495–510, 2019.

[11] T. M. Booi, I. Chiscop, E. Meeuwissen, N. Moustafa, and F. T. H. D. Hartog, "ToN\_IoT: The role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion data sets," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 485–496, Jan. 2022.

[12] N. Koroniotis, N. Moustafa, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Gener. Comput. Syst.*, vol. 100, no. 2, pp. 779–796, 2019.

[13] G. D. Gil, A. H. Lashkari, M. Mamun, and A. A. Ghorbani, "Characterization of encrypted and VPN traffic using time-related features," in *Proc. 2nd Int. Conf. Inf. Syst. Security Privacy (ICISSP)*, 2016, pp. 407–414.

[14] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. de Albuquerque, "Internet of Things: A survey on machine learning based intrusion detection approaches," *Comput. Netw.*, vol. 151, no. 9, pp. 147–157, 2019.

[15] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," *J. Netw. Comput. Appl.*, vol. 169, no. 6, pp. 102–107, 2020.

[16] G. Dogan, "ProTru: A provenance-based trust architecture for wireless sensor networks," *Int. J. Netw. Manag.*, vol. 26, no. 2, pp. 131–151, 2016.

[17] A. Hameed, J. Violos, and A. Leivadreas, "A deep learning approach for IoT traffic multi-classification in a smart-city scenario," *IEEE Access*, vol. 10, pp. 21193–21210, 2022.

[18] M. A. Lawa, R. A. Shaikh, and S. R. Hassan, "Security analysis of network anomalies mitigation schemes in IoT networks," *IEEE Access*, vol. 5, pp. 522–535, 2020.

[19] Y. Li and J. Li, "MultiClassifier: A combination of DPI and ML for application-layer classification in SDN," in *Proc. 2nd IEEE Int. Conf. Syst. Informat. (ICSAI)*, 2014, pp. 682–686.

[20] N. Moustafa, B. Turnbull, and K.-K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4815–4830, Jun. 2019.

[21] P. Maniriho, L. J. Mahoro, E. Niyigaba, Z. Bizimana, and T. Ahmad, "Detecting intrusions in computer network traffic with machine learning," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 3, pp. 433–445, 2020.

[22] W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, "End-to-end encrypted traffic classification with one-dimensional convolution neural networks," in *Proc. IEEE Int. Conf. Intell. Security Informat. (ISI)*, 2019, pp. 43–48.

[23] X. Tong, X. Tan, L. Chen, J. Yang, and Q. Zheng, "BFSN: A novel method of encrypted traffic classification based on bidirectional flow sequence

network,” in Proc. 3rd Int. Conf. Hot Inf.-Centric Netw. (HotICN), 2020, pp. 160–165.

[24] R. Zhao et al., “A novel intrusion detection method based on lightweight neural network for Internet of Things,” *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9960–9972, Jun. 2022.

[25] S. I. Popoola, B. Adebisi, and H. Gacanan, “Hybrid deep learning for botnet attack detection in the Internet-of-Things networks,” *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4944–4956, Mar. 2021.

[26] C. Ma, X. Du, and L. Cao, “Analysis of multi-types of flow features based on hybrid neural network for improving network anomaly detection,” *IEEE Access*, vol. 7, pp. 148363–148380, 2019.

[27] M. Lopez-Martin, B. Carro, and J. Lloret, “Network traffic classifier with convolutional and recurrent neural networks for Internet of Things,” *IEEE Access*, vol. 5, pp. 18042–18050, 2017.

[28] P. Wang, S. Li, F. Ye, Z. Wang, and M. Zhang, “PacketCGAN: Exploratory study of class imbalance for encrypted traffic classification using CGAN,” in Proc. IEEE Int. Conf. Commun., Dublin, Ireland, 2020, pp. 1–7.

[29] X. Zhang, T. Ge, and Z. Chen, “Automatic modulation recognition of communication signals based on instantaneous statistical characteristics and SVM classifier,” in Proc. IEEE Asia-Pacific Conf. Antennas Propag. (APCAP), 2018, pp. 344–346.

[30] N. Zhou, Q. Wang, and J. Zhou, “IoT unbalanced traffic classification system based on Focal\_Attention\_LSTM,” in Proc. IEEE 5th Inf. Technol. Netw. Electron. Autom. Control Conf. (ITNEC), 2021, pp. 899–903.

[31] A. Telikani, A. H. Gandomi, K.-K. R. Choo, and J. Shen, “A costsensitive deep learning-based approach for network traffic classification,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 1, pp. 661–670, Mar. 2022.

[32] M. Lotfollahi, M. J. Siavoshani, and R. S. H. Zade, “Deep packet: A novel approach for encrypted traffic classification using deep learning,” *Soft Comput.*, vol. 24, no. 3, pp. 1999–2012, 2019.

[33] B. Yang and D. Liu, “Research on network traffic identification based on machine learning and deep packet inspection,” in Proc. IEEE 3rd Inf. Technol. Netw., Electron. Autom. Control Conf. (ITNEC), 2019, pp. 1887–1891.

[34] P. Khandait, N. Hubballi, and B. Mazumdar, “Efficient keyword matching for deep packet inspection based network traffic classification,” in Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS), 2020, pp. 567–570.

[35] T. Rezvy, Y. Lu, and T. Zebin, “An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks,” in Proc. 53rd Annu. Conf. Inf. Sci. Syst. (CISS), 2019, pp. 1–6.

[36] W. Choukri, H. Lamaazi, and N. Benamar, “Abnormal network traffic detection using deep learning models in IoT environment,” in Proc. 3rd IEEE Middle East North Africa Commun. Conf. (MENACOMM), 2021, pp. 98–103.

[37] X. Wang, Y. Liu, and W. Su, “Real-time classification method of network traffic based on parallelized CNN,” in Proc. IEEE Int. Conf. Power, Intell. Comput. Syst. (ICPICS), 2020, pp. 92–97.