ENCRYPTED AND ABNORMAL TRAFFIC CLASSIFICATION IN IOT USING CMTSNN-BASED DEEP NEURAL NETWORKS

[1] Mutnuri. R. S Kavya Sri, [2] Dr. L. Sumalatha

[1, 2] Jawaharlal Nehru Technological University College of Kakinda (UCEK)

[1] satyasrisharma17@gmail.com, [2] lsumalatha@jntucek.ac.in

Abstract: The extension of the internet of things (IoT), along side the great use of encryption technology, created massive boundaries to the IoT cyber safety. increasing encrypted anomalous conversation from IoT system requires effective strategies to hit upon and clear up feasible risks. Current detection methods often show restrictions, including basic data processing, insufficient extraction of elements, data imbalances and reduced accuracy of multiclass classification. This have a look at seeks to offer an modern approach for detecting unusual encrypted communication inside IoT networks in response to these troubles. the main aim is to create a model of deep learning of multiclassification, which has been known as a cost matrix time–space neural network (CMTSNN), especially for this reason. The primary emphasis is to correct the shortcomings of contemporary methodologies with the aid of resistance to the extraction of elements, manipulate of statistics imbalances and increase the accuracy of the general classification. The experimental evaluation was carried out using data sets such as Ton-Iot and Bot-Iot. The comparative overview of current approaches revealed greater performance across several measures, including "accuracy, precision, recall, score F1 and false alarm frequencies". The CMTSNN has demonstrated large improvements within the type accuracy, specifically in minority classes, which progressed the overall multiclassification performance. studies includes voting models (RF + ADABOOST + MLP) and CNN-LSTM, which might be used to increase performance and achieve 99% accuracy in identifying aberrant encrypted facts. The flask -primarily based front cease increases usability for checking out and interplay, even as strong user verification guarantees safe access. those modifications sell the efficiency of the machine in cyber security IoT and growth its reliability and value in realistic applications.

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

1. INTRODUCTION

With 5G mobile communication technology, IoT age. cutting-edge enterprise and manufacturing need IT transformation that confront the net and IoT. IoT helped health care, manufacturing and energy network [1–3]. the worldwide variety of IoT connections reached 14.4 billion through June 2022. Many gadgets are interconnected and used by IoT, which increases the collection of scanning devices and excessive -dimensional information [4]. With the upward push of

IoT and harmful programs and the recognition of encryption technology in communication with the internet-Im, unusual facts visitors is used to cover its operation, resulting in tons encrypted uncommon operation that threatens cyber safety IoT. for this reason, many academic and company researchers observe the way to reliably become aware of the operation of IoT, network status, hit upon network abnormalities and keep network protection.

The IoT machine needs stable architecture to keep a solid and speedy connection among information and communique technology. unique architectural layers of IoT devices have distinctive vulnerabilities and attack methodologies, and therefore defense mechanisms and detection systems are created at specific stages and angles. After extensive investigation, the techniques of safety and related companies and academic academics of the system of antivirus detection and disturbance are offered. Firewally IoT uses safety gates and routers to block external threats in the internal network. The data source divides the detection systems to the network traffic and based on the host. Detection of abuse and detection of anomaly are detection techniques. The development of the Internet and IoT is fast and the data flows in the network are massive. More innovative and efficient approaches and technologies are needed to solve data security problems. This observe extra exactly identifies and classifies IoT community site visitors with the aid of detecting function differences among normal and peculiar operation, enhancing analysis and detection capacity and speed of community detection, stopping uncommon operation on IoT and developing a safe and reliable surroundings of IoT.

Network intrusion detection is a challenge for classification for IoT cyber safety; It can quickly discover and classify hidden attacks and threats in network data. Recently, many methods of classification of network traffic have appeared, in particular based on the port based on the port [5], the inspection of the payload [6], the “machine learning (ML) and the methods based on deep learning (DL)” [7] based on used technologies. The simplest techniques are based on the port. This method is less accurate due to the fact some dangerous applications use a random port approach or trade community port addresses to save you detection. Detection of a deep packet classifies operation by means of spotting green site visitors hundreds or packets the use of predefined guidelines manually adapted to fit the chains. This technique overcomes the categorization of ports, but it is harder to create reliable comparative criteria and more intensive. However, many attackers use encrypted communication to prevent detection, and the inspection technology cannot identify it.

Categorization of ML -based operation requires the selection and extraction of human elements for the previous classification of knowledge using statistical laws. This approach can handle encrypted communication and has minimal computing costs because it does not rely on content. The most difficult part is the design of the elements [8]. training of the community model routinely learns the connection between the unique information and the necessary output within the get right of entry to classification of DL operation, which eliminates the want for previous understanding and functions of guide layout in ml [19, 21, 22]. With this strategy, it's far higher to analyze and solve a extra complex connection. The DL has been thoroughly carried out and confirmed in prominent research regions along with computer

vision (CV) and natural language processing (NLP) and is consequently used greater inside the categorization of network traffic [9].

2. LITERATURE SURVEY

Dental ailment prevails. clinical screening and visual prognosis can be luxurious. How IoT and AI enhance, internet intelligent systems offer a widespread promise for home health care. on this examine [1], the sensible dental fitness system is designed on intelligent hardware, deep learning and cellular terminal to test its usability to home enamel. This research additionally develops an smart dental system to show tooth. based on 12,600 scientific snap shots collected via the proposed devices from 10 private dental clinics, an automated diagnostic model of the educated R-CNN mask for detecting and classification of 7 dental sicknesses, including a crumbled tooth, dental, uorosis and periodontal disease, up to 90% accuracy, high sensitivity and high specificity. After a one -month test at ten clinics, the common diagnostic time for each affected person decreases via 37.5%, which explains 18.4% increase in treated sufferers. programs about customer and dental cellular terminals permit offerings of initial examination, consultation, appointment and evaluation.

National plans are increasingly preferred by intelligent production. Intelligent connection is essential for intelligent production. Current solutions do not provide intelligent connection with heterogenic devices, quick settings and installation, or create online services. It is proposed to overcome concerns [2]. Flexible CA-blue can combine diverse physical sources. In addition, IIHUB offers the development of online production services using templates of service encapsulation and easy to set and deploy for intelligent connections. In addition, smart analysis and accurate administration may be possible. Finally, the prototype shows how IIHUB achieves intelligent connections and its functionality.

The largest deployment IoT in the world, intelligent network, reduces energy consumption in the city. The intelligent grid generates a large number of sensitive energy data, including the instructions for sending and invoice. To create an strength method based totally on Q-learning cloud servers, they constantly obtain statistics in a simple text, allowing adversaries to apply user information. in this have a look at [3] we offer a light-weight privacy-preserving Q -learning framework (LiPSG) to formulate sensible power management strategy. Lipsg distributes the electrical information of every electricity place into uniformly mystery stocks earlier than sending them to the control center. statistics is continually maintained in random sharing layout at some point of Q-learning calculation to shield statistics privacy. New additive secret sharing protocols implement computer technology. Computer technology is also used to strengthen efficiency. Complex theoretical studies and testing show Lipsg safety and efficiency. Lipsg first presents a universal privacy-based privacy strategy that creates a high-efficiency architecture and minimal performance loss compared to the privacy techniques of intelligent grid protection.

Recent demand for high -speed transfer rates has stimulated research in technologies of new characterization and categorization of network traffic. Their poor treatment prevents network survival, transport engineering, QoS and dynamic access control. Most techniques of operation categorization use a deep packets inspection(DPI) or a port -based classification. considering the fact that extra

communication is encrypted and applications use dynamic ports or ports from different popular programs, such approaches are outdated. This studies [4] indicates a shipping categorization module based on machine learning for community schemes that require real -time transport treatment. The module releases the Naive Bayes algorithm to the independence of attributes in a new manner. The locating suggests that the proposed module is a capacity opportunity in actual time.

This record [5] proposes a far off management technique for strength internet of factors, describes the threshold agent on the edge and internet information Platform InternCafe facts platform, and presents equipment, improve, configuration, tracking, confidentiality measurement and feasibility verification methods.

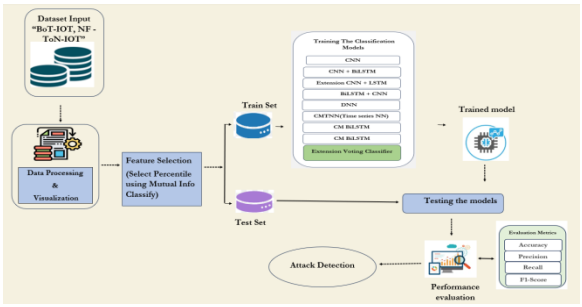
3. METHODOLOGY

i) Proposed Work:

The proposed system represents an innovative methodology called CMTSNN to deal with the difficulties of detecting anamolic encrypted data in IoT networks. It consists of three basic elements: maintaining time references and developing a cost sanction matrix during preliminary processing, effective extraction of elements and alleviating data imbalances by means of a criminal matrix and improved loss function. The assessment of data sets, such as "TON-IOT and Bot-Iot", shows exceptional performance, especially in the accuracy of minority categories, which illustrates the ability of CMTSNN to improve cyber security IoT. In addition, research includes a voting classifier and uses CNN with LSTM, each of which reaches an impressive rate of 99% accuracy in detecting aberrant encrypted data. The front end focused on user is designed using a flask frame that makes it easier to test and interact with users. In addition, strong user authentication mechanisms are included to ensure the system's secure access and thus improve its usability and reliability in practical applications. This improvement increases the efficiency and usefulness of the system in strengthening cyber safety IoT.

ii) System Architecture:

The shape of our model is shown in Fig. 1. first of all, unprocessed statistics are transformed into a format suitable for education and the matrix is determined via cost consequences. in the end, Bilstm-1DCNN became selected for schooling type of characteristic extraction [21]. The output is then revised the usage of the price sanction inside the layer of cost consequences, observed through an output vector of the possibility of Softmax. The stepped forward function of lack of cross entropy is used to calculate the loss and provide the result.



"Fig 1 Proposed architecture"

iii) Dataset collection:

"Bot-Iot and NF- ToN-IoT" it data sets are examined to understand their structure and content. This investigation determines the basis for future processing and analysis of data [11].

	id	dur	proto	service	state	spkts	dpkts	sbytes	dbytes	rate	...	ct_dst_sport_ltm	ct_dst_src_ltm	is_ftp_login	ct_ftp_cmd	ct_flw_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	166666.6608	...	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"

This article uses anomalous data set from "IoT Ton-Iot and Bot-Iot". Two data sets published in 2020 include several forms of aberrant traffic data that have a significant value to identify the multiclasification of anomalous traffic in IoT. "Ton-Iot and Bot-Iot Data Sets were developed by University of New South Wales Canberra Network-Range Laboratory" through the establishment of a network environment in the real world. The replication of the device's software inside the actual environment of the physical network creates standard operation together with new anomalous operation and therefore provides scientists a substantial and different data set of actual anomalous operation concerning IoT. [12] TON-IoT data file includes nine unusual operation categories, including backdoor, injection and scanning. The Bot-IoT data set includes six categories of unusual operation, including DDOS, DOS, operating system and service scan, as well as attacks on keylogging and data leakage. The selected protocol categorizes anomalous DDOS operation and DOS up to 10 different classifications.

	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	63318	52.139.250.253	443	6	91.00	181	165	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 converts unrefined facts to usable facts for companies. information scientists often cope with data processing, which includes series, company, cleaning, verification, analyzes and transformation of statistics into understandable representations which incorporates graphs or posts. information processing can be accomplished through the usage of 3 strategies: manual, mechanical and digital. The goal is to increase the price of facts and make decisions greater green. This allows corporations to reinforce their operations and carry out short strategic selections. In this context, automated data processing technology, consisting of software improvement, are critical. It can rework massive information sets, especially massive statistics, to considerable understanding of quality and selection -making.

v) Feature selection:

The choice of features is the system of figuring out the maximum convertible, non -dundant and applicable characteristics for the improvement of the model. The systematic minimization of the size of statistics sets is crucial, even as the quantity and diversity of records units persist in growth. The number one objective of selecting elements is to increase the overall performance of the predictive model and on the identical time reduce computational prices related to modeling.

the selection of functions, the number one factor of sensible engineering includes identity of the most important traits for getting into the system learning algorithms. the selection strategies are used to lessen the quantity of enter variables by way of eliminating redundant or needless functions, and consequently improves the set to those which can be most suitable for the machine learning model. number one blessings

of selecting capabilities in advance than permitting autonomously to select the gadget getting to know version.

vi) Algorithms:

"CNN (Convolutional Neural Network)": A CNN is a form of deep neural networks which are particularly designed to investigate facts much like grids, consisting of photographs. It uses convolutional layers to autonomically attain hierarchical houses from input statistics, permitting effective capture of patterns and spatial correlations. although CNN is conventionally related to image data, they may be changed for structured information just like a grid, which makes it appropriate for duties in which spatial connection is decisive, inclusive of sequential records or time collection [23, 24].

"DNN (Deep Neural Network)": A DNN is a neural network characterized via many hidden layers positioned between enter and output layers. DNNs can research state-of-the-art hierarchical data representations, letting them perceive deep correlations between input elements. DNNs are customizable and suitable for lots forms of facts. they are used to symbolize complex facts interconnection, even without special configurations of comparable grids.

"BiLSTM + CNN (Bidirectional LSTM + Convolutional Neural Network)": This hybrid model integrates the benefits of Bilstm and CNN. Bilstm captures sequential dependencies in both directions, while CNN emphasizes the extraction of spatial elements, so it is suitable for tasks that include both time and spatial patterns. Suitable for data sets, where it is necessary to capture both sequential dependencies and geographical characteristics such as time series data.

"CNN + BiLSTM (Convolutional Neural Network + Bidirectional LSTM)": Analogious to the preceding combination, however, with the collection reversed. The model first analyzes spatial information the use of CNN after which captures sequential relations via Bi-LSTM. effective, when spatial characteristics are fundamental within the first section of data processing, then calls for the gathering of time relations in sequences [31].

"CM BiLSTM (Cost Matrix Bidirectional LSTM)": The cost matrix is a square matrix in which each file indicates the cost or first-class related to the incorrect category of a selected class. in the category of system learning, throughout the training phase, it is used to allocate different prices for specific types of type errors.

"Bidirectional LSTM (BiLSTM)": Bidirectional LSTM is a form of architecture of the recurrent neural network (RNN). unlike traditional LSTMs that analyze the sequences from the past to the destiny, they examine the Bilstm sequences in each directions - heading for the destiny and the destiny into the past. This two -way processing lets in the model to understand the context and the interdependence from the previous and next components within the series.

CM Bilstm likely consists of the combination of the fee matrix into the education method of Bi-LSTM. The price matrix is probably used to relieve the elegance imbalance for the duration of education by way of allocating distinct sanctions to special lessons. beneficial to strengthen the potential of the version to drive unbalanced magnificence and guarantee fair illustration of all instructions all through schooling.

"CMTNN (Time Series Neural Network)": The cost matrix is a square matrix used within the category obligations of machine learning to offer diverse costs or sanctions for incorrect type of occasions across several training. every element inside the matrix denotes the price of predicting a selected magnificence while the actual elegance differs. This approach could be very powerful in fixing the class imbalance or emphasizing the meaning of accurate identity of sure lessons.

"Time Series Neural Network (TNN)": The neural network of time series is an structure adapted to time series processing facts. it is designed to perceive time correlations and formulas in collection records, which causes them appropriate for programs along with diagnosis, anomaly detection or type within the time collection facts sets.

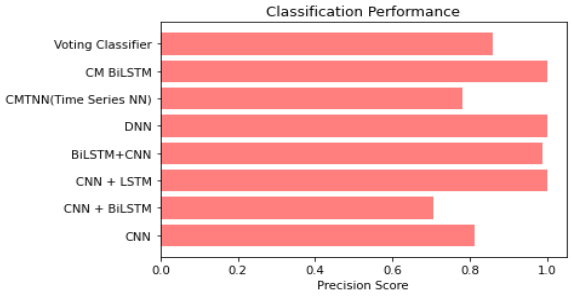
CMTNN suggests a neural network mainly designed for time series facts. Specifics relate to positive systems or methodologies aimed toward successfully taking pictures time relations in collection data. Designed for responsibilities associated with time series evaluation, where it's miles vital to recognize and become aware of time formulation for precise predictions.

4. EXPERIMENTAL RESULTS

Precision: Precision quantifies the percentage of efficiently identified positive cases or samples. Precision is decided by using the components:

"Precision = True positives/ (True positives + False positives) = TP/(TP + FP)"

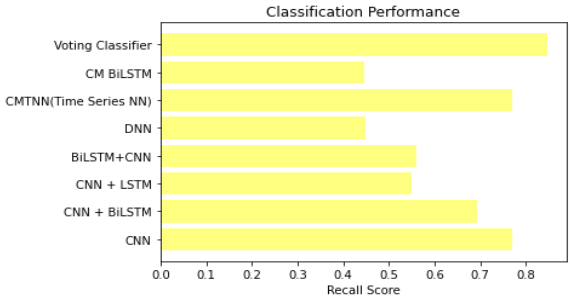
$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$



"Fig 4 Precision comparison graph"

Recall: ML recall assesses a model's potential to choose out all relevant times of a class. It demonstrates a version's efficacy in encapsulating times of a class by using comparing nicely anticipated high satisfactory observations to the general variety of positives.

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

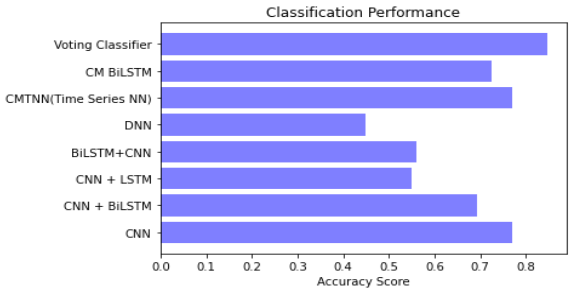


"Fig 5 Recall comparison graph"

Accuracy: A test capacity towards create a proper difference between healthy & sick cases is a measure of accuracy. We can determine accuracy of a test through calculating proportion of cases undergoing

proper positivity & genuine negative. It is possible towards express this mathematically:

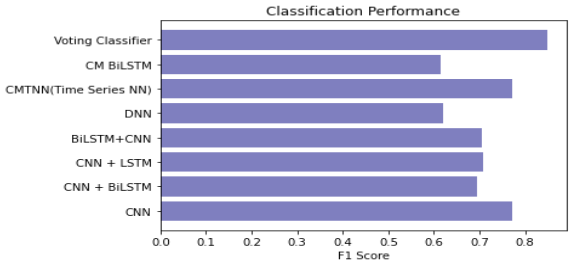
$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$



"Fig 6 Accuracy graph"

F1 Score: The accuracy of a system ML of model is classed the usage of the F1 score. Integrating the precision and recall metrics of the model. The accuracy metric quantifies the frequency of proper predictions made through a model at some level inside the dataset.

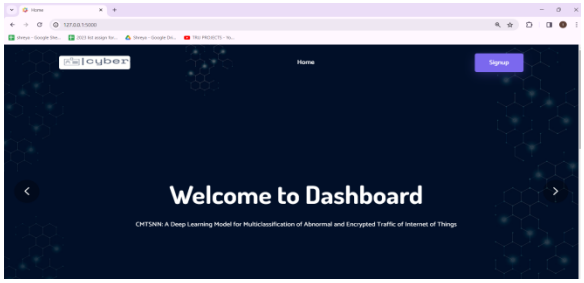
$$\text{F1 Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$



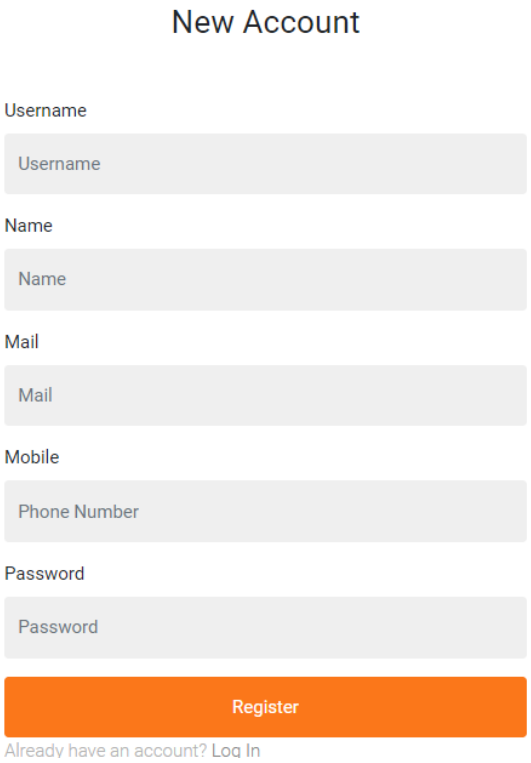
"Fig 7 F1Score"

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

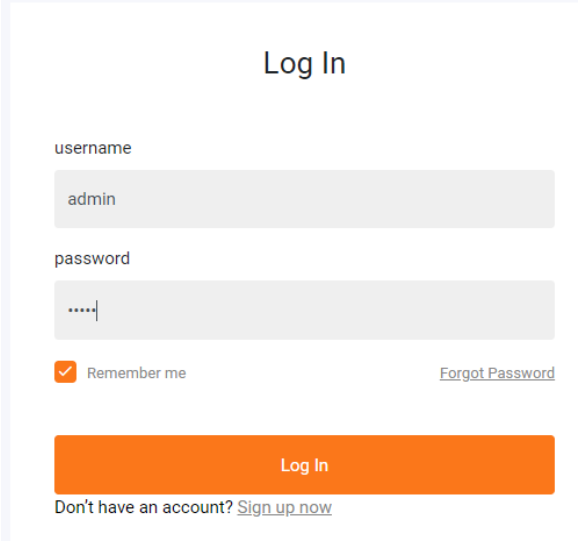
"Fig 8 Performance Evaluation"



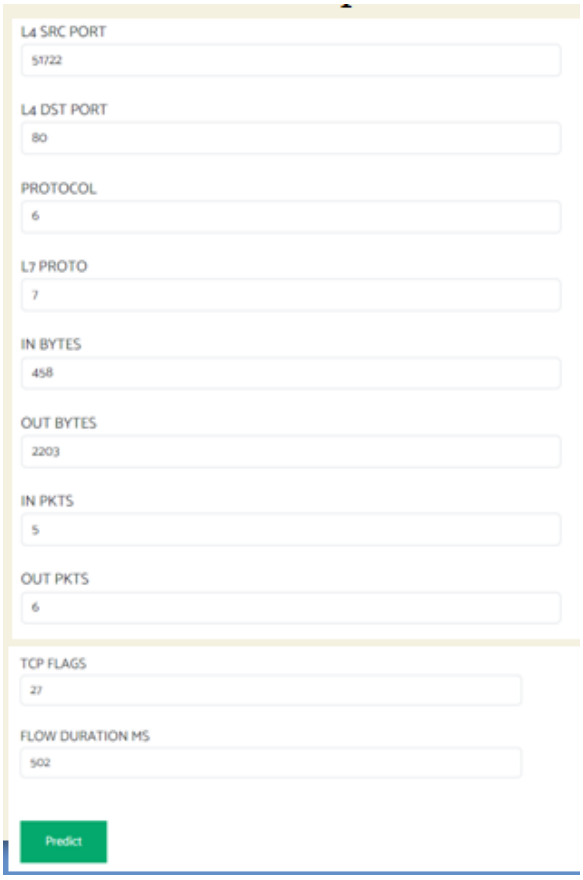
"Fig 9 Home page"



"Fig 10 Signin page"



"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 effectively solved problems with cyber security, which represents a growing diversity and amount of devices of the IoT [1, 2]. Set algorithms and models such as CMTNN and CM Bilstm show a strong knowledge of identification and alleviation of anomalous and encrypted traffic, and therefore the IoT environment is secured. The voting classifier shows exceptional performance with a remarkable accuracy of 99% in detection of anomalic encrypted operation. This remarkable accuracy emphasizes the efficiency of the file method and offers reliable detection capabilities necessary to secure the IoT network. The amalgamation of the SQLite flask frame for registration and verification of users, together with the provision of users to enter the function values, introduces a pragmatic and user -focused aspect into the project. This frontend interactivity improves project relevance, so it is suitable for practical applications. Strong cyber safety protocols and project adaptable models allow players to ecosystem of the IoT and ensure reliable protection against possible attacks. This includes companies depending on IoT technology, scientists investigate the security of the Internet of Things and experts who make effective IoT network protection solutions.

6. FUTURE SCOPE

Matrix of the cost of the penalty is determined on the basis of a fixed distribution of obtained samples; However, its practical use in connection with constant changes in real -time flow requires further research. Introducing an increased approach of deep cost learning and the optimized function of loss of cross entropy to solve the problem of unbalanced network

data and to increase the results of the sampling of minority categories derived from the subordinate training. Subsequently, we will explore the impact of the performance of our model using polluting learning to increase the efficiency of operation identification and achieve considerable accuracy through minimal marked data and extensive unmarked data, while ensuring cyber security of IoT operation with limited resources. The proposed model is of considerable size, has several parameters and requires an extensive training time, complicates its deployment and use on IoT facilities limited to resources. Model optimization for light performance while maintaining the encrypted anomalous operation is a promising way for exploration and study.

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 5Gand-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. Booij, 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 learningbased 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. Leivadeas, "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. Gacanin, "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.