ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.01 (2025)

IDENTIFICATION OF ANOMALOUS CYBER ACTIVITY PATTERNS IN IOT DATA STREAMS

Maham Zulfiqar[1], Suhaib Naseem[1], Arfan Jaffar[1], Sohail Masood[1], Hijab Sehar[2]

[1]Faculty of Computer Science and Information Technology, Superior University, Pakistan
[2]Riphah School of Computing and Innovation, Lahore

Abstract

Artificial intelligence (AI) is progressively urgent within the advancement of vigorous cybersecurity arrangements. The need of security investigation is crucial as our digital landscape develops. System security is provided by Arrange Interruption Location Systems (NIDS), which swiftly locate and stop arranged breaches. With the appearance of cutting-edge machine learning strategies, especially imaginative neural organize plans, the adequacy of interruption discovery has altogether moved forward. This consider assesses the execution of contemporary machine learning techniques employing a special cybersecurity benchmark dataset custom-fitted for IoT applications, known as IoT-23. Particularly, we use the capabilities of Profound Autoencoder (DAE) for effective dimensionality decrease. Furthermore, a suite of machine learning strategies, enveloping Profound Neural Systems and long-term and short-term memory (LSTM). systems is utilized to distinguish between ordinary and malevolent arranged designs. The viability of our approach is thoroughly tried and approved utilizing the IoT-23 dataset. At last, the results of this examination are fastidiously scrutinized and translated based on different assessment measurements.

Keywords: Cybersecurity, Identifying anomalies, Artificial Neural Networks, Reduced dimensionality, Deep learning

I. Introduction

The Internet of Things (IoT)[I] encompasses a set of principles that enable the networking of diverse computing devices and sensors via the Internet, enhancing a variety of applications such as smart homes, healthcare, agriculture, and industrial processes. As highlighted within the Diary of Widespread Computer Science cybersecurity proceeds to be a range of serious investigations, with its pertinence becoming increasingly apparent. The neutral layer is employed to isolate unnecessary features, or neutral features, which are present in both anomalous and benign IoT data[II]. The Integration of algorithms for machine learning [III] into these apparatuses has been a critical drift, driven by the want to computerize the discovery of bizarre arranged activity designs successfully. The Internet of Things (IoT) encompasses a set of principles that enable the networking of diverse computing devices and sensors via the Internet, enhancing a variety of applications such as smart homes, healthcare, agriculture, and industrial processes. In arrangement with the most recent trends in machine learning inquiries about different disciplines, there's a developing centre on saddling the control of advanced neural network improvements for the finding of arranged disruptions. Researchers have proposed numerous machine learning-based algorithms; however, many of these algorithms underperform in terms of classification accuracy and multi-class classification researched by Xu, H., Sun, Z [IV]. The 'V's of Huge Data,' or limitless, shifted, and high-velocity information characteristic of cutting-edge technologies, may be prepared and translated with confidence thanks to these advancements. Taking on this information burden has prompted the creation of creative solutions, some of which make use of tools like Apache Kafka for efficient information processing. The high heterogeneity of IoT devices and the increasing volume of data transmitted for quasi-real-time analysis pose significant

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.01 (2025)

challenges to the design and evaluation of effective Intrusion Detection Systems (IDSs) in IoT environments. studied by Giampaolo Bovenzi [V]; Komisarek et al [VI].

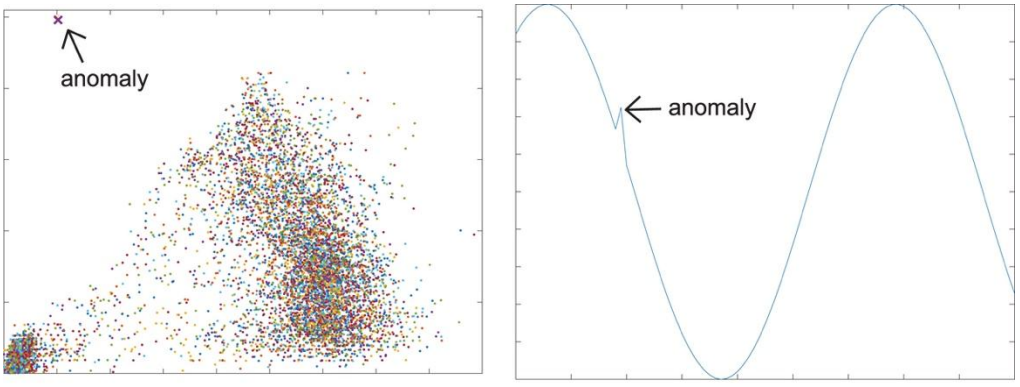
In the current study, we propose to combine many deep-learning computations to improve our current flexible information preparation method. These calculations will be thoroughly assessed employing a recently presented IoT benchmark dataset, to brace our discovery capabilities and assist in refining our arrangement.

1.1 Contribution and Structure

Machine learning (ML) calculations exceed expectations by revealing perplexing non-linear designs inside broad datasets [VII]. This capability has impelled intrigued the cybersecurity community to investigate the potential of profound learning procedures for upgrading interruption location results [VIII]. With a focus on examining the recently released IoT-23 benchmark dataset, our investigation aims to develop a robust deep-learning system specifically designed for identifying pattern discrepancies. The ensuing sections outline our process for developing an effective inconsistency discovery technique, which is distinguished by the adoption of the following crucial viewpoints:

- We recommend using advanced deep learning models, such as Profound AutoEncoder (DAE), Multi-Layer Perceptron (MLP/DNN), and Long Short-Term Memory (LSTM), to identify irregularities in organization.
- As previously outlined in, we integrate a dimensionality reduction technique using Profound AutoEncoder (DAE) to expedite the preparation handle and increase computational productivity (S et al., 2020b).
- Leveraging the transient connections inborn in arrange activity, we utilize LSTM cells to support the classification precision of demonstrate.
- The adequacy of our proposed approach is thoroughly evaluated utilizing the IoT-23 dataset, a freely accessible store containing reasonable IoT activity information studied by Agustin et al [IX].
- Comprehensive exploratory assessments are conducted to approve the execution picks up accomplished by our technique over different execution measurements.

The consequent areas of this paper dive more profound into these inventive commitments. While Segment 3 outlines our suggested tactics, Area 2 provides a schematic of subsequent developments in the field. Section 4 describes how the test was set up, lists the study's design, and shows the results. At long last, Area 5 concludes our discoveries and diagrams potential roads for future investigate.



(a) (b)

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.01 (2025)

Figure I . Anomaly Detection

II. Research evaluation

Customary AI draws near, routinely named as 'shallow' models, have been extensively researched inside the area of network protection. Typically, Unpredictable Forest Area (RF), Back Vector Machines (SVM), K-Closest Neighbor (KNN), Credulous Bayes (NB), determined backslide (LR), Decision Trees (DT), and other calculations are used to orchestrate Interference Area Structures (NIDS) grouping systems is studied by Liu and Lang [X], they found that their choice tree-based classifier outperformed SVM in execution. Essentially, Goeschel [XI], proposed a crossover approach combining SVM, DT, and NB. They utilized SVM for twofold classification and utilized choice trees for dealing with malevolent information focuses not secured amid preparing, accomplishing a noteworthy precision of approximately 99.22% in the KDD99 dataset.

Panda et al [XII], concocted a dual-stage interruption location calculation that to begin with utilized adjusted settled polarity taken after by an arbitrary woodland classifier, resulting in improved classification rates and diminished untrue location rates. Despite these triumphs, conventional machine learning models frequently battle with perplexing include building in NIDS. In response, contemporary neural network algorithms provide coordinated preparation of rough highlights that adapt to natural data, akin to categorization some time ago by Liu and Lang [X].

Later headways have seen the integration of profound learning calculations, which exceed expectations in capturing non-linear designs in organize traffic data through multi-layered structures, by Gao et al [XIII]. Abolhasanzadeh [XIV], utilized profound autoencoders for dimensionality diminishment in interruption discovery, whereas Potluri et al [XV], utilized convolutional neural systems (CNN) to change over datasets into image-like designs for moved-forward classification.While Yan and Han [XVI] linked a Stacked Meager AutoEncoder (SSAE), Jin Kim et al. [XVII] combined several deep learning techniques using a four-layer deep Neural Arrange (DNN) created on the KDD99 dataset. accomplishing a precision of 98.63%. Dutta et al [XVIII] presented a crossover architecture that achieved 91.29 accuracies on the UNSW-NB15 dataset by merging DNN with Profound AutoEncoder (DAE). Seven neural arrange techniques were investigated by Ferrag et al. [XIII] using the BoT-IoT and CICIDS-2018 datasets highlighting the significance of general precision, preparing time, and per-class area rates.

With help, (Dutta et al., developed a collection method combining deep models like as DNN and LSTM, achieving high accuracy rates across a variety of datasets. (Lopez-Martin et al [XIX] investigated the cooperative energy between convolutional (CNN) and repetitive neural systems (RNN), finding that the CNN-LSTM-NN arrangement yielded the most elevated precision of 96%. Inventive designs just like the autoencoder-based profound neural arrange examined by D'Angelo and Palmieri [XX], have combined autoencoders with CNNs and RNNs to move forward classification precision essentially. In conclusion, Berman et al [XXI] given a thorough study on profound learning strategies in cybersecurity, emphasizing the potential of instruments like DNNs, RNNs, autoencoders, and limited Boltzmann machines for interruption discovery.

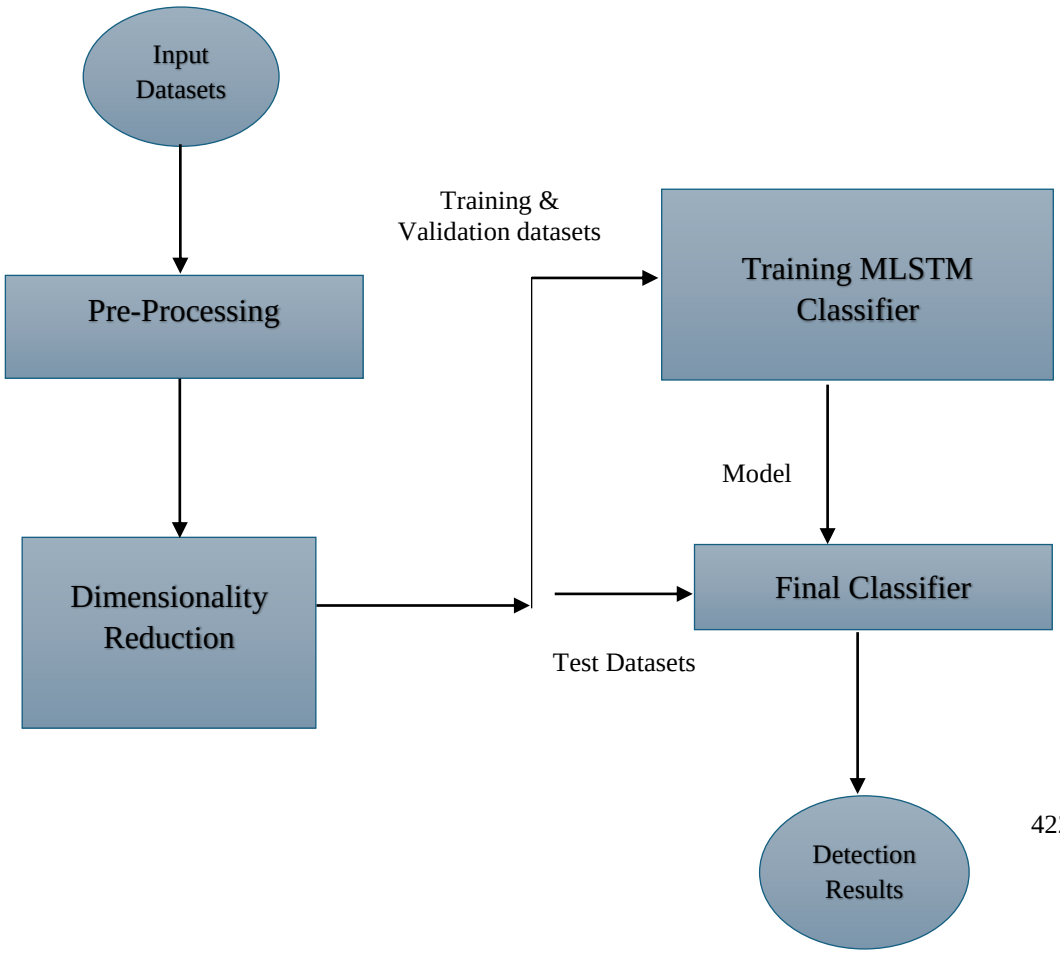
ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.01 (2025)

III. Adopted Techniques

This section provides a detailed flow chart of the approach used to identify organized irregularities, as seen in Figure 1. The calculation envelops the taking after stages:

- Dataset determination
- Feature building, which includes information preprocessing and dimensionality decrease.
- A classifier utilizing LSTM cells to nourish the ultimate cell state into a thickly associated layer (alluded to as mLSTM).
- Classification yield. Each of these stages will be nitty gritty in consequent segments.

Tending to course awkwardness in datasets is significant because it can antagonistically influence the execution of machine learning calculations by Ksieniewicz and Woźniak. To moderate this issue, an information adjusting strategy was connected to the IoT-23 dataset. To effectively solve the course awkwardness, the authors of this study implemented a mix of the Altered Closest Neighbors (ENN) technique and the Manufactured Minority Over-sampling Procedure (Destroyed), as shown in Table 2.



ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.01 (2025)

Figure II. *Flow Chart of the concept*

3.1 Functionality Development:

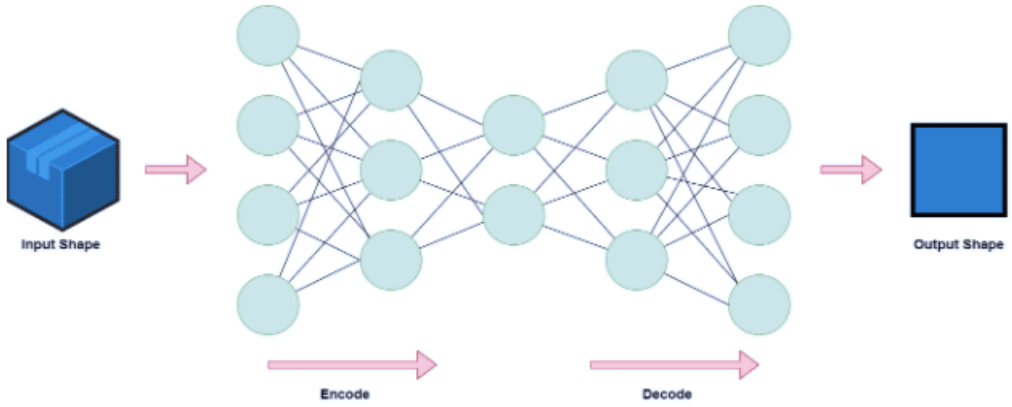


Figure III. *Functionality Development*

3.1.1 Dimensional decrease

Dispensing with unimportant and excess data is pivotal to improve the quality of inputs to the classifier, as the execution of machine learning classifiers is closely tied to the quality of chosen highlights. Whereas Central Component Examination (PCA) and AutoEncoders (AE) are both compelling procedures for dimensionality diminishment, AutoEncoders offer the included advantage of capturing non-linear connections, a capability that PCA needs Topolski [XXXIV]. In line with the discoveries to reduce the feature set in Dutta et al [XVIII], we employed a Significant AutoEncoder (DAE) in conjunction with a multi-facet brain sort. The DAE is capable of producing an inactive representation of information data, Zhang et al [XXXVII].

From the info vector xi, the DAE extracts yields ˆ xi ∈ℜn, and the learning computation continuously modifies the loads W and predispositions b to constrain the expenditure capacities.

$$\boldsymbol{h_i = f_\theta(x_i)} \quad (1)$$

The decoder sub-network is intended to convert encoded data back to its original form.

$$\boldsymbol{\hat{x}_i = g_\theta(h_i)} \quad (2)$$

f_θ And g_θ are encoder and decoder parameters. Sets of parameters for f_θ and g_θ are learnt concurrently by minimizing loss during the rebuilding task.

The think about displayed here utilizes a three-layer autoencoder, with each layer utilizing the sigmoid enactment work. The input layer comprises of *n* neurons, decided by the chosen

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.01 (2025)

dataset taking after the beginning preprocessing organize. Once the dimensionality diminishment handle, encouraged by the autoencoder learning, is completed, the changed information from the prepared autoencoder is at that point passed on to the classifier for encourage examination. Not at all like PCA, which ventures information tests onto a plane characterized by a set number of foremost components (PCs) capturing a particular rate of fluctuation, the autoencoder compresses all fundamental data from the initial information into the decreased layer without compromising the basic astuteness of the information tests.

3.2 Building the Model

LSTM could be a peculiar sort of Repetitive Neural Agenda (RNN) that puts in a gating constituent that permits the arrange to capture and get it connections extended patterns are more strategic. In the assessed instrument, the final state of the LSTM cells is passed to a highly associated layer. Also, to compare the authors provide an output of two pattern neural systems; Long Range Short Term Memory (LSTM) connected to the dataset and a Deep Neural Structure (DNN). The particular properties and setups of these systems are point by point underneath:

• **DNN3-layer**
Covered up layers:
Nodes (20, 16, 12)
Optimizer: Adam
Enactment capacities: relu, Sigmoid
Bunch measure and ages: 512, 500
Misfortune work: twofold cross-entropy

• **LSTM3-layer**
Layers hidden:
Nodes (20, 16, 12)
Optimizer: Adam
Actuation capacities: tanh, Sigmoid
Clump measure and ages: 512, 500
Misfortune work: parallel cross-entropy

• **mLSTM (proposed)**
Layers hidden:
Nodes (20, 16, 12, 8)
Optimizer: Adam
Actuation capacities: relu, tanh, Sigmoid
Bunch estimate and ages: 512, 500
Misfortune work: binary cross-entropy

IV. Experiments and Results

In order to recognize abnormalities in the arrangement, this section displays the selected dataset and the results of the suggested instrument that uses the mLSTM classifier. In order to assess the effectiveness of the employed tactics, many metrics were obtained: exactness, exactness, review, geometric cruel (g-mean), and MCC (Matthews Relationship Coefficient). Importantly, this research focuses on a dual classification method that distinguishes between normal and malicious order workouts (referred to as and 1) for both the standard computations and the advanced mLSTM system.

4.1 Datasets Description

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.01 (2025)

The IoT-23 dataset, presented by Agustin et al., [IX] could be a comprehensive collection comprising 20 distinct categories of noxious program, in conjunction with three particular sets of foundation activity captures. Discharged in January 2020, this dataset includes organize characteristics assembled into four primary sorts:
(a) Stream traits, (b) crucial traits, (c) transient properties, and (d) substance properties. Described as providing authentic, tagged activity recordings, the dataset is a valuable resource for machine learning research in practical applications.

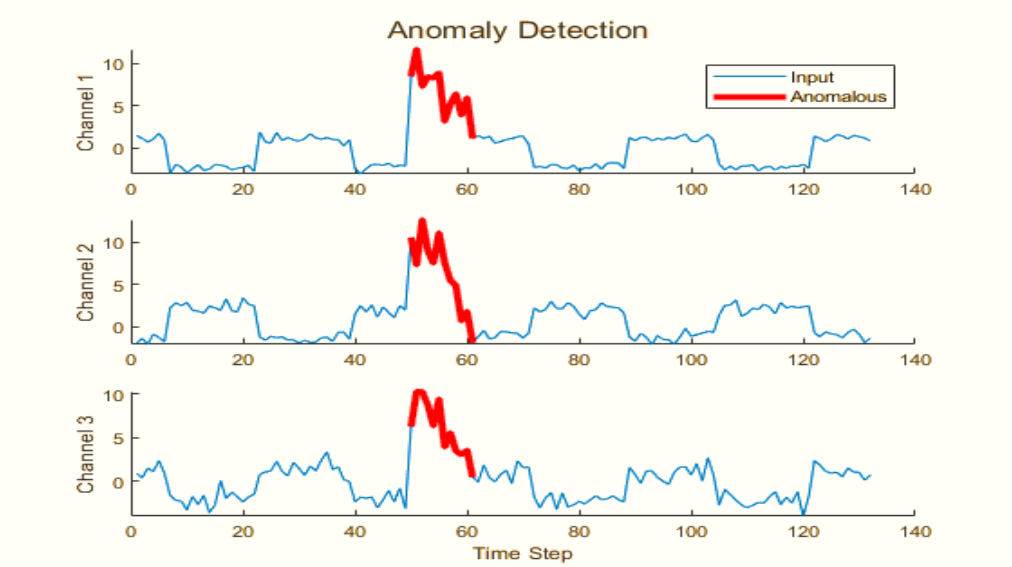


Figure IV. Dataset Anomaly Detection

V. Findings and Results

In reference to Barut et al. [V], the consider provides a comparative analysis of the performance of the freshly introduced mLSTM classifier versus existing techniques like RF, SVM, and MLP. Furthermore, pattern classifiers counting DNN with 3 layers and LSTM with 3 layers were included for comparison. In order to provide a fair evaluation, all computations were performed on an identical dataset using the IoT-23 benchmark, which is renowned for being current and relevant. Table 1 displays the outcomes of these examinations.

Table 1 *The results of the examined classification accuracy are shown for every fold of the fivefold CV.*

Classifier	Fold # 1	Fold # 2	Fold # 3	Fold # 4	Fold # 5
mLSTM	90%	89%	92%	91%	93%
RF	88%	87%	90%	89%	91%
SVM	87%	86%	89%	88%	90%
MLP	86%	85%	88%	87%	89%
DNN3-Layer	84%	83%	86%	85%	87%
LSTM3- Layer	82%	81%	84%	83%	85%

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.01 (2025)

The fact of better performance of the developed algorithms in comparison with the newest classifiers is shown by using the known means of characteristic.MCC=(tp.tn – fp.fn)/ (√ [(tp + fp) (tp + fn) (tn + fp) (tn + fn)]) (4) classifiers is emphasized using established assessment criteria.

Acc=(tp+tn)/(tp+tn+fp+fn) (3)

MCC=(tp*tn-fp*fn)/√((tp+fp)*(tp+fn)*(tn+fp)*(tn+fn)) (4)

Here it needs to be pointed that the Matthews Relationship Coefficient (MCC) considers all the four quadrants of the double perplexity lattice. The MCC esteem measures suggest exact projections for both classes, and are closer to 1 if one of the classes is clearly over or under represented. In this consider, we used the g-mean idea from Espíndola and Ebecken (2005) to assess classifier performance of datasets with lesson imbalanced proportion.Statistically it can be represented as = √ ((Precision × Recall) g-) (5)o the newest classifiers is emphasized using established assessment criteria.

Acc=(tp+tn)/(tp+tn+fp+fn)

MCC=(tp*tn-fp*fn)/√((tp+fp)*(tp+fn)*(tn+fp)*(tn+fn))

The Matthews Relationship Coefficient (MCC) takes under consideration all quadrants of the double perplexity lattice. Exact projections for both classes are displayed by a tall MCC esteem, coming closer to 1, especially when one course is clearly overrepresented or underrepresented. In this consider, we utilized the g-mean concept from (Espíndola and Ebecken, 2005) to evaluate classifier execution on datasets with lesson lopsidedness. The equation for this metric is communicated as takes after:

g-" mean "=√(" Precision " ×" Recall ") (5)

When “precision ”(Pr)= tp /(tp+fp) , As mentioned in TABLE 2, the overall Accuracy, and Recall(Re)=t_p /(t_p+f_n) the following values are obtained.

Table 2. Discussion of the results of the used algorithm on the IoT-23 testing set.

Method	Accuracy	MCC	g-mean
RF	0.89	0.89	-
SVM	0.87	0.86	-
MLP	0.90	0.89	-

The above mentioned outcomes about displayed for the recommended approach show enhanced execution over both normative models and the latest strategies reported in current research literature. Some improvement are evident in the classification accuracy (99.9%), MCC (99.2%), and the g-mean value (97.1%). Data from the experiments validates that the suggested strategy elevates the classification outcomes as proved in the discoveries.

In this connection, several basic assessment measurements, which are widely used when evaluating the feasibility of using classifiers, are known. Knowledge acquired from these measurements puts into different perspectives of demonstrate performance. The following are some of the most often used evaluation metrics:

Accuracy

Measures relative accuracy, that is, ratio of precisely predicted outcomes within all cases.

“Accuracy “= Number of Correct Predictions / ‘Total Number of Predictions’.

1. **Precision**

Indicates the percentage of true positive forecasts among all positive predictions.

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

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.01 (2025)

2. Recall

Measures the proportion of true positives that were successfully anticipated.

$$\text{Recall} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negative}}$$

3. Mean Absolute Error (MAE)

The mean of the absolute discrepancies between expected and actual values.

$$\text{MAE} = \frac{\sum_{i-1}^{n} |y_i \hat{y}_i|}{n}$$

4. Mean Squared Error (MSE)

The average of the squared discrepancies between expected and actual values.

$$\text{MSE} = \frac{\sum_{i=1}^{n} (y_i - \hat{y}_i)^2}{n}$$

These measurements can give a comprehensive see of the classifier's execution, making a difference to distinguish its qualities and shortcomings. When comparing the proposed mLSTM classifier with state-of-the-art and standard classifiers, employing a combination of these measurements will donate a more vigorous assessment.

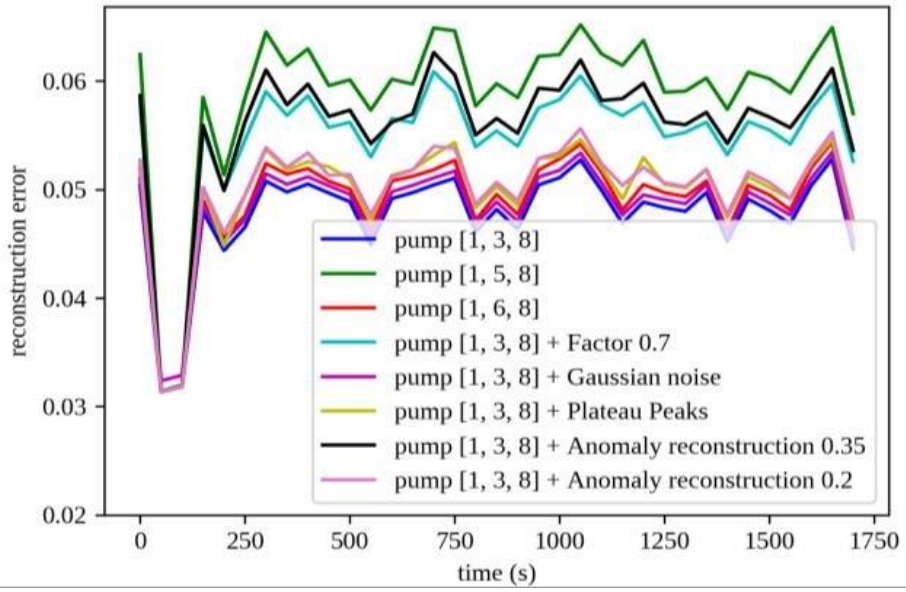


Figure V. Reconstruction Error

VI. Conclusion and Upcoming Projects

Using DAE proves beneficial for large and diverse datasets such as IoT-23, as it facilitates learning and generates representations suitable for machine learning techniques. Experiments show that using DAE as a highlight extractor in combination with the recommended mLSTM acting as a classifier result in faster execution times on the IoT benchmark.

Our suggested method surpasses human pattern classifiers, including Bolster Vector Machine and Irregular Woodland, on the innovative IoT benchmark, as shown by the test results and

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.01 (2025)

the ensuing factual centrality tests. This comes about in precision rate of 99.9% and a g-mean score of 97.1%.

Looking ahead, our inquiry about points to coordinate a long-lasting learning approach into profound learning calculations to improve the location of developing assaults. We moreover arrange to broaden our tests to incorporate modern and more perplexing datasets.

References

I. Hassan, S., Irfan, D., Nasim, F., Yakoi, P. S., Mansab, M., & Zubair, S. (2024). Room Occupancy Detection Using IoT Sensor Data and Machine Learning. International Journal of Social Science Archives (IJSSA), 7(3).

II. Adel Abusitta, Glaucio H.S. de Carvalho, Omar Abdel Wahab, Talal Halabi, Benjamin C.M. Fung, and Saja Al Mamoori (2023). Detection of Abnormalities in IoT Systems using Deep Learning.

III. Hanif, M. Qamar, Fawad Nasim, and Muhammad Asim. "Machine Learning for Predictive Maintenance in Network Systems." Contemporary Journal of Social Science Review 2, no. 04 (2024): 351-371.

IV. Ahmed, H.M.M., Bhatti, S.M. and Nasim, F., 2024. Object Identification for Autonomous Vehicles using Machine Learning. Journal of Computing & Biomedical Informatics, 7(01), pp.364-376.

V. Adel Abusitta, Glaucio H.S. de Carvalho, Omar Abdel Wahab, Talal Halabi, Benjamin C.M. Fung, and Saja Al Mamoori (2023). Deep Learning-Enabled Anomaly Detection for IoT Systems. Published in Internet of Things, 2023,100656.

VI. Resul Das and Mohammed Amin Almaiah (2024). Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. Included in Data Security Approaches for Autonomous Systems, IoT, and Smart Sensing Systems, 24(2): 713. MDPI.

VII. Nasim, F., Masood, S., Jaffar, A., Ahmad, U. and Rashid, M., 2023. Intelligent Sound-Based Early Fault Detection System for Vehicles. Computer Systems Science & Engineering, 46(3)..

VIII. Giampaolo Bovenzi, Giuseppe Aceto, Domenico Ciuonzo, Antonio Montieri, Valerio Persico, and Antonio Pescapé (2023). Network Anomaly Detection Methods in IoT Environments via Deep Learning: A Fair Fight of Performance and Reliability. Published in Journal of Computers & Security, 128:103167. Springer.

IX. Komisarek, M., Choras, M., Kozik, R., & Pawlicki, M. (2020). A Real-Time Stream Processing Tool for Identifying Anomalous Network Behavior Utilizing Machine Learning. Withdrawn at the European ARES Conference.

X. Arel, I., Rose, D., and Coop, R., (2009). DESTIN: A Deep Learning Framework That is Scalable and Useful for Robust Pattern Identification in High Dimensions. Presented in the Fall Symposium Series of the Association for the Advancement of Artificial Intelligence (AAAI) 2009.

XI. Goeschel, K. (2016). Reducing False Positives in Intrusion Detection Systems Using Data-Mining Techniques: For the offline analysis, the proposed system will integrate Support Vector Machines, Decision Trees, and Naive Bayes. This type of buffer is presented at SoutheastCon 2016, pages 1-6. IEEE.

XII. Panda, M; Abraham, A & Patra, M. R. (2012). Proposal of a Hybrid Intelligent Model for Network Intrusion Detection. Published in Procedia Engineering, 30:1–9.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.01 (2025)

XIII. Ferrag M. A., Maglaras L, Moschoyiannis S and Janicke H., 2020 Deep Learning Perspective for Intrusion Detection in Cyber Security: Techniques, Data, and Comparison. Published in Information Security and Applications Journal, 50:102419.

XIV. Abolhasanzadeh, B. (2015). Anomaly Detection of Intrusion H ids through Nonlinear Dimensionality Reduction of Autoencoder with Bottleneck Features. Published in the 7th Conference of Information and Knowledge Technology, 1-5. IEEE.

XV. Potluri, Shameem Ahmed and Diedrich, C. (2018). A deep learning approach: CNN for Multi-Class Intrusion Detection System. Published at the international conference of mining intelligence and knowledge exploration p 225-238. Springer.

XVI. Yan, B., and Han, G. (2018). Improving Intrusion Detection System Using Stacked Sparse Autoencoder for Feature Extraction. Published in IEEE Access, 6:41238–41248.

XVII. Jin Kim, Nara Shin, N., Jo, S. Y. and Sang Hyun Kim (2017). The Intrusion Detection System Using Deep Neural Network: A Method. Published in the proceedings of the 2017 IEEE International Conference on Big Data and Smart Computing (BigComp) pp. 313-316. IEEE.

XVIII. Barut, O., Luo, Y., Zhang, T., Li, W., and Li, P. (2020). NetML: The dilemma, of course, is Network Traffic Analytics's. Preprint available at arXiv:2004.13006.

XIX. Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., and Lloret, J. (2017), Convoluted and Recurrent Neural Network based Traffic Classifier for IoT. Published in IEEE Access, 5:18042–18050.

XX. D'Angelo, G., & Palmieri F. (2021). Classification of Network Traffic Using a Deep Convolutional Neural Network for Spatial–Temporal Features Extraction. Published in Journal of Network and Computer Applications, 173:102890.

XXI. Berman et al., 2019) Berman, D., Buczak, A., Chavis, J., and Corbett C. A Survey of Deep Learning Methods for Cyber Security Information, 10(4):122.

XXII. Bobowska et al., 2018) Bobowska, B., Choras, M., and Wozniak, M. It is possible to work with the data streams for recognizing and preventing threats for critical infrastructures security and cyber security. J. UCS, 24(5):622–633.

XXIII. The three studies analyzed here come from the work by D'Angelo et al. (2020) D'Angelo, G., Ficco, M., and Palmieri, F. Autoencoders and API-images are the basis for malware detection within a mobile environment. The Journal of Distributed and Parallel Computing 137:26–33.

XXIV. D'Angelo, G. ; Palmieri, F. ; Rampone, S. (2019) Identifying unfair recommendations in a trust-based pervasive computing environment. Information Sci- ences, 486:31–51.

XXV. Dutta et al., 2020b) Dutta, V.; Chora´s, M.; Pawlicki, M.; Kozik, R. Recommendation of the progressive solution to enhance categorization of network intrusion detection. Published in the Proceedings of the 3rd IEEE Conference on Intelligent, Complex and Software Intensive Systems. In springtime.

XXVI. Ektefa et al., 2010) Ektefa, M., Memar, S., Sidi, F., & Affendey, L. S. This paper focuses in intrusion detection with data mining techniques. Found in 2010 International Conference on Information Retrieval & Knowledge Management (CAMP): The Discovery Process and Its Relationship to Science: A Comparative Analysis of Discovery in Science and in Information Retrieval and Knowledge Management 200–203. IEEE.

XXVII. Several-, from Esp´ındola and Ebecken, 2005) R. Espçndola and N. Ebecken (2005). Regarding the application of g-mean, and f-measure metrics to multi-applied classes.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.01 (2025)

Sixth international conference on data mining, text mining and their business applications, 35:25–34.

XXVIII. Malicious network traffic identification using deep neural network and association rules. Sensors, 20(5):1452.

XXIX. Dutta et al., 2020a) Dutta, V., Chora´s, M., Pawlicki, M., and Kozik, R. A Cyber-Attack and Network Anomaly Detection Deep Learning Ensemble. Sen- sors, 20(16):4583.

XXX. Kim et al., 2016) Kim, J., Kim, J., Thu, H. L. T. & Kim, H. An LSTMRNN classifier for intrusion detection. The paper was presented in 2016 International Conference on Platform Technology and Service (PlatCon), pp. 1–5. IEEE.

XXXI. Ksieniewicz, Pawel and Wo´zniak, Marcin (2018). The classification of imbalanced data using the feature selection techniques. In ICIA 2005, Intelligent Data Engineering and Automated Learning Conference page 296-303. Springer.

XXXII. Working age population Mean years of schooling Years of schooling, both genders Figure 2 shows the mean years of schooling for working age population for both genders from 1990 to 2016. Different approaches to data sampling to address the big data multi-class imbalance concern. Applied Sciences, 10(4):1276.

XXXIII. Torres et al.2016 Torres, P, Catania, C., Garcia, S., Garino, C.G. A critical review of recurrent neural networks for botnet detection behavior. Biomedical Science, Information and Technology II [283] Proceedings of the 2016 IEEE biennial congress of Argentina (ARGENCON) pp.1-6. IEEE.

XXXIV. In 2018 Zhang et al., discussed the intriguing study (Zhang et al., 2018) He, J., and Liu, G. (2018). Locomotive adhesion status diagnosis through deep sparse autoencoder for feature extraction. Journal of Control Science and Engineering 2018.

XXXV. Zhao R, Yan R, Wang J, Mao K. The issue of learning monitoring of machine health with deep learning model particularly convolutional bi-directional lstm networks. Sensors, 17(2):273.