Universal Library of Engineering Technology Research Article

ISSN: 3064-996X

Open Access | PP: 01-09

DOI: https://doi.org/10.70315/uloap.ulete.2022.001

Internet of Things (IoT) Cybersecurity Enhancement through Artificial Intelligence: A Study on Intrusion Detection Systems

Gangadhar Sadaram[1], Manikanth Sakuru[2], Laxmana Murthy Karaka[3], Mohit Surender Reddy[4], Varun Bodepudi[5], Suneel Babu Boppana[6], Srinivasa Rao Maka[7]

[1]Bank of America, Sr DevOps/ Open Shift Admin Engineer.
[2]JP Morgan Chase, Lead Software Engineer.
[3]Microsoft, Senior Support Engineer.
[4]Microsoft, Support Escalation Engineer.
[5]Applab Systems Inc, Computer Programmer.
[6]iSite Technologies, Project Manager.
[7]North Star Group Inc, Software Engineer.

Abstract

Computers networks are very vulnerable and can be threatened by hackers, viruses and other immoral entities. Intrusion detection is a crucial component of network security since it is an active defence technique. limited accuracy, limited detection effectiveness, high false positive rate, and incapacity to deal with new forms of intrusions are some of the challenges faced by traditional intrusion detection methods. These problems may be solved by suggesting a real-time network intrusion detection system that uses ML. With the use of the CICIDS2017dataset, which contains both benign traffic and a range of attack types, this research introduces an Intrusion Detection System (IDS) intended to improve IoT cybersecurity. For the selection of the features, which are important and are not numerous, PCA is applied. The SMOTE is a tool for addressing class imbalance. Among these models, DenseNet, KNN, SVM and DeepGFL are some of the models whose performances are measured compared with a set of performance metrics such as recall, accuracy, precision and F1-score. Therefore, DenseNet provides the highest level of efficiency and reliability for all of the research and development models proposed, with a perfect back-and-forth recall of 98.2%, accuracy of 99.12%, and precision of 98.6%. Therefore, the results confirm DenseNet's applicability in detecting intrusions in IoT networks. In subsequent research, more attack types will be integrated into the dataset, and real-time integration will be considered, as well as using deep reinforcement learning for dynamism for threat detection at the IoT system level.

Keywords: *Internet of Things (IoT), Cybersecurity, Network Security, Intrusion Detection System (IDS), Attack, Machine learning.*

INTRODUCTION

A rapid proliferation of the IoT has transformed a landscape of information and communication technologies, leading to an unprecedented interconnection of devices and systems. It has therefore encouraged the development of growth areas in various sectors such as health, production, urbanization and home appliances [1]i.e. data consumers, to offer ubiquitous services. The data quality (DQ. Nonetheless, the utilisation of IoT networks has also brought about a raft of new and serious cybersecurity risks whereby vulnerabilities and unauthorised accesses to data and important infrastructure could be serious issues[2]. The historical IT security practices including firewalls, encryption, authentication, and VPN are now inadequate to handle the emerging/rising trend of cybersecurity threats in IoT networks.

An improvement that strengthens network security and protects organisation data is IDS [3]. This IDS notifies the system administrator of any suspicious activities taking place in the network and hence act as a data protecting tool that prevents those malicious attacks [4]. An intrusion occurs whenever someone gains unauthorised access to, or uses information resources maliciously [3]. A real-world entity that looks for a way to get information without authorisation, injure others, or carry out other nefarious actions is known as an intruder or an attacker.

Protecting firewalls is the main focus of the IDS [5]. The firewall defends a company against harmful Internet attacks, and the IDS finds out if someone tries to get through the firewall or manages to get past the firewall security and tries to access any system within the company. If the firewall starts with any of the given unwanted activity, it alerts the system administrator [6].

IDS has improved its functionality more through the incorporation of AI since it builds on superior computational

models to improve the level of accuracy in detecting the attacks while reducing on false positives [7]the rise in attacks on communication devices in networks has resulted in a reduction of network functionality, throughput, and performance. To detect and mitigate these network attacks, researchers, academicians, and practitioners developed Intrusion Detection Systems (IDSs[8]with a significant impact on the final product cost and green environment. Most of the existing models on reverse logistics assumed the return rate as a fixed fraction. However, the number of returned products is always uncertain and depends on many factors like law, government policy, environmental protection issues, etc. The presented research overcomes this limitation and formulates a mathematical model in which the return rate will be a function of environmental factors. Moreover, the model is extended by integrating it with state-of-the-art radio frequency identification (RFID. Techniques such as machine learning, neural networks and expert systems help IDS apply new social updates and new attack patterns, and help in making the IDS decision-making automated. These capabilities are quite applicable in IoT cybersecurity since rule-based approaches are insufficiently capable of handling the complex and ever-transforming IoT networks.

Significance and Contribution of Study

The importance of this research rests in the fact that it may lead to better cybersecurity measures for the ever-growing IoT ecosystem by making use of cutting-edge AI methods for intrusion detection. This research addresses the growing need for robust cybersecurity solutions by developing a sophisticated AI-driven IDS capable of identifying various cyber threats, which is essential for safeguarding IoT systems from potential attacks. Here are the main points of the paper:

- Utilizes the CICIDS2017 dataset for IDS.
- Addresses class imbalance by utilizing the SMOTE to generate synthetic data points, ensuring a more balanced dataset for training the models.
- Apply min-max normalization methods for scale the features.
- Proposes a robust ML model like DenseNet, KNN, SVM, and DeepGFL to detect a huge range of cyber threats in IoT networks.
- Evaluate key performance metrics— F-Measure, Accuracy, Precision, and Recall —assessing their reliability and effectiveness in detecting intrusions and classifying traffic accurately.

Structure of the Paper

The study is structured as follow: In Section II the existing literature on iot-cybersecurity through artificial intelligence using intrusion detection. In section III, methodology was utilized to compile the data for this study. Section IV provide the results and analysis of text classification. Finally, the conclusion is given in Section V.

LITERATURE REVIEW

Several academics have looked at the open-ended questions surrounding IDS in an IoT environment, and their findings are shown below:

In This study,Viegas et al. (2018) offers a way for embedded devices to identify network intrusions using anomaly-based methods. Even when the contents of network traffic vary, the suggested strategy keeps the classifier reliable. The dependability is attained by use of a hybrid of classifiers and a novel rejection mechanism. Energy efficiency and compatibility with existing gear are two strong points of the suggested method. The paper's studies reveal that, compared to their software equivalents, machine learning algorithms implemented in hardware require 46% more energy. Specifically, the feature extraction module uses 58% more energy, whereas the packet capture module uses 37% less energy [9].

In this study, Bhatt and Morais (2018), a method for detecting attacks on IoT networks that makes use of ML algorithms for anomaly detection and a judgement module. The method is tested on a single-board computer and shown to work in a real-world setting by methodically evaluating it with several protocol assaults and commercially available IoT devices. Our suggested method was successfully tested and found to defend IoT devices against the threats under consideration with an accuracy range of 94% to 99% and a detection time of less than 0.7s[10].

In this study, Choudhary and Kesswani et.al. (2018), discover sinkhole and selective forwarding attacks that target routing protocols. Additionally, they have made efforts to safeguard our network from such assaults. They used the MATLAB simulation environment to develop two algorithms, KMA and CBA, for detection and prevention. they also evaluated the outcomes of two different intrusion detection techniques. Our research shows that the KMA algorithm has a true positive intrusion detection rate of 50% to 80%, whereas the CBA algorithm achieves a rate of 76% to 96% [11].

In This study, Al-Yaseen Othman and Nazri (2017) presents an intrusion detection model that combines SVM and extreme learning machine at several levels to better identify both known and new threats. An improved K-means method for building a first-rate training dataset is proposed to further improve classifier performance. Implementing modified K-means to generate new, smaller training datasets that include the whole original training dataset shortens the classifier training time and improves the efficacy of IDS. To test the suggested model, utilise the widely-used KDD Cup 1999 dataset. The suggested model outperforms competing approaches using the same dataset in terms of attack detection efficiency and accuracy (95.75%) [12].

In This study, Brown Anwar and Dozier et.al. (2016) is concerned with the intrusion detection system paradigm. When system and network actions deviate from the usual, anomaly-based IDSs attempt to categorise the intrusion. In this study, use a kind of AI called a multiple detector set AI to identify intrusions in network data flows usingcharacteristics of application layer protocols. Our results demonstrate that the artificial immune system with numerous detectors was able to obtain a Detection Rate53.34% with a FPR0.20%. With an accuracy76.57%, the mAIS[13].

Table I summarizes various intrusion detection methods for IoT environments, highlighting their datasets, key findings, and limitations.

Table I. Summary of Literature Review of on Intrusion Detection Systems through Internet of Things (Iot) Cybersecurity Using Artificial Intelligence

Author	Methods	Dataset	Accuracy	Limitation/gap
Viegas et al. (2018)	Anomaly-based method, classifier reliability, combination of classifiers	Custom dataset for embedded systems	Hardware implementation reduces energy consumption (46% for ML algorithms, 58% for feature extraction, and 37% for packet capture modules).	Limited dataset usage; focused only on energy efficiency and not on other performance metrics like accuracy.
Bhatt and Morais (2018)	Machine learning-based anomaly detection with a decision module	Various IoT protocol attacks dataset	Achieved 94%-99% accuracy and detection time < 0.7 seconds in protecting IoT devices from attacks.	Limited protocol diversity; real-time scalability in more complex IoT ecosystems needs verification.
Choudhary and Kesswani (2018)	Detection and prevention algorithms (KMA and CBA)	Simulated environment (MATLA)	True Positive Rate: 50%-80% (KMA) and 76%-96% (CBA).	Performance inconsistency; real-world implementation is not demonstrated.
Al-Yaseen, Othman, and Nazri (2017)	Multi-level hybrid intrusion detection model (SVM + ELM, modified K-means)	KDD Cup 1999 dataset	Achieved 95.75% accuracy with reduced training time due to modified K-means algorithm.	Relies on outdated KDD Cup 1999 dataset, which does not reflect modern IoT attack patterns.
Brown, Anwar, and Dozier (2016)	Anomaly-based IDS using multiple-detector set artificial immune system (mAIS)	Network data flows	Achieved a Detection Rate of 53.34%, FPR of 0.20%, and accuracy of 76.57%.	Low detection rate; needs improvements in detection mechanisms and adaptability to modern protocols.

METHODOLOGY

The methodology for enhancing IoT cybersecurity an intrusion detection system (IDS) leveraging the CICIDS2017 dataset, which comprises diverse attack types and benign traffic. The study begins with data preprocessing, including the removal of redundant values, handling missing data, and applying min-max normalization to scale numerical features within the range [0,1]. PCA is utilized for feature selection, decreasing dimensionality while retaining the most relevant features to improve model performance. The SMOTE is used to generate synthetic samples for minority classes in order to correct class imbalance. The dataset is then split into training (60%) and testing (40%) sets. ML models, like DenseNet, KNN, SVM, and DeepGFL, are developed and evaluated using standard metrics like F-Measure, Precision, Accuracy, and Recall. Metrics like TP, TN, FP, and FN rates evaluate how well an IDS finds and fixes threats in IoT networks. Figure 1 shows the following stages for the implementation.

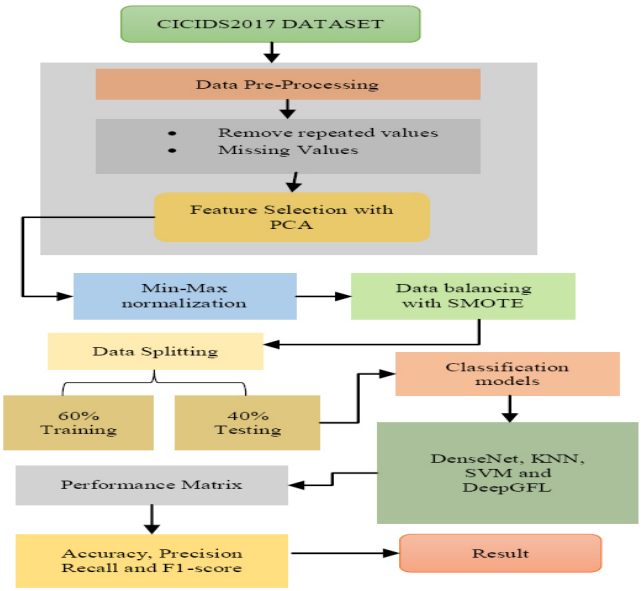

Fig. 1. Flowchart for Intrusion detection system in cybersecurity

The outline of a flowchart for Intrusion detection system in cybersecurity is explained in below:

Data Collection

The CICIDS2017dataset is utilized in our study. The dataset, which includes several typical attack types, is developed by the Canadian Institute for Cyber Security. The 286467 data include 127537 recordings of benign traffic and 158930 records of port scan attempts. Every entry includes 85 properties, such as the IP address of the source, the port of the destination, the amount of time the packet spent in transit, the total number of packets sent and received, and more. The distribution of data are shows in Figure 2.

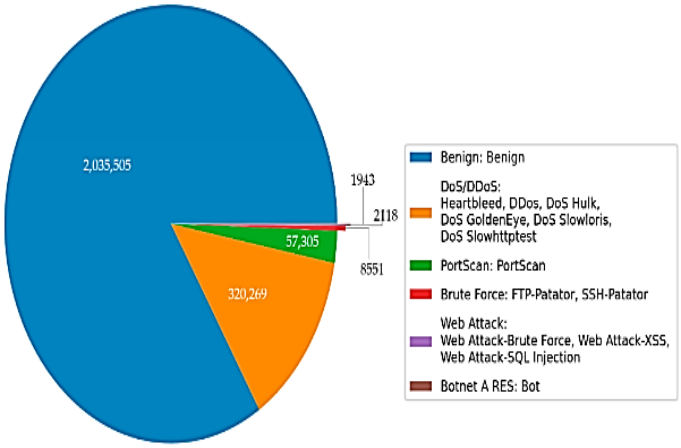

Fig. 2. Class distribution of CICIDDS2017

Figure 2 depicts the distribution of network traffic instances in the CICIDS2017 dataset, categorized by attack types and benign traffic. The majority of the data represents benign traffic (2,035,505 instances, shown in blue), followed by attack types such as DoS/DDoS attacks (320,269 instances, orange) and Port Scan (57,305 instances, green). Smaller segments include Brute Force attacks (8,551 instances), Web Attacks (2,118 instances), Botnet traffic (1,943 instances), and other types of malicious activity. The chart highlights the dataset's significant imbalance, with benign traffic dominating the distribution.

Data Preprocessing

There are few steps as crucial as the data pre-processing phase in IDS. A number of processes are involved, including data reduction and transformation [14]environmental and economical concerns draw considerable attention from both practitioners and researchers towards remanufacturing practices. The success of remanufacturing firms depends on how efficiently the recovery process is executed. Radio Frequency Identification (RFID. The efficacy and accuracy of learning algorithms are jeopardised if raw input is transformed into low-quality data. The following pre-processing steps are as follow:

- **Remove repeated values:** A typical issue that impacts system performance is the inclusion of duplicate or undesirable values in the dataset. Duplicate values are often time-consuming and uninteresting, therefore it's important to remove them.
- **Missing value:** The term "Missing Values" is used in machine learning to describe data properties that could be missing from a dataset as a result of input process failures, such as inaccurate measurements or failing devices.

Feature Selection with PCA

Feature selection is an essential part of ML. It entails picking out the best characteristics from a dataset [15][16]and identifies the best part sequence available in the part-mix. A mathematical model has been formulated to minimize the broad objectives of set-up cost and time simultaneously. The proposed approach has more realistic attributes as fixture related intricacies are also taken into account for model formulation. It has been solved by a new variant of particle swarm optimization (PSO. A strong method for decreasing data dimensionality and finding useful characteristics is PCA [17]the proper management of the returned products is one of the key elements for enterprises. This paper illustrates the complexities involved in resolving a remanufacturing problem and formulates a mathematical model in which the return rate is a function of environmental factor. Since, such model belongs to a class on NP hard problems; an Artificial Bee Colony (ABC. It can help you simplify complex data sets, visualize patterns, and enhance a performance of ML models. The following feature importance score graph are provide in below:

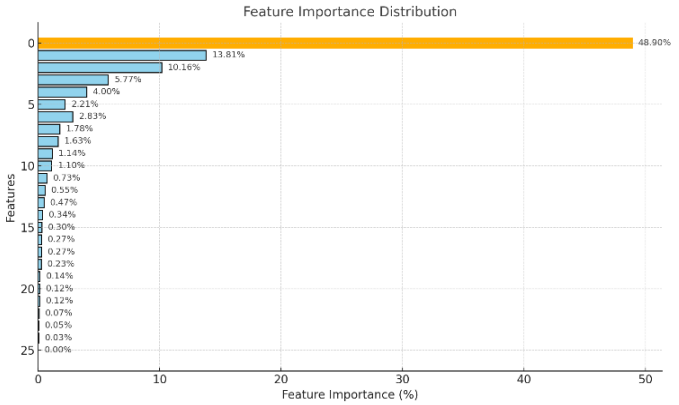

Fig. 3. Feature importance score

Figure 3 visualization highlights the feature importance distribution for the model, with the most significant feature contributing 48.90% to the overall performance, clearly marked in orange. Other features show varying levels of importance, with the second and third most important features contributing 13.81% and 10.16%, respectively, while the remaining features have minimal impact, each contributing less than 6%.

Min-Max Normalization

A data pre-processing method known as normalization reduces the range of values for numerical characteristics in a dataset while preserving their correlations and volatility

[18]. There are X numerical characteristics in the dataset with known boundaries that do not match a Gaussian distribution [19]. The numerical properties have been normalized to the range [0, 1] employing a min-max approach for a following reasons(1):

$$x' = \frac{x - \min(x)}{max\,(x) - min\,(x)} \qquad (1)$$

Min(x) and max(x), the bounds of a numerical feature, determine its maximum and minimum boundaries.

Data Balancing with SMOTE

It is a popular and effective oversampling technique for dealing with the problem of class imbalance. Class imbalance concerns often include Smote [20]. This resampling method makes use of artificial data points that are already in existence by interpolating new occurrences between the minority class's existing data points.

Data splitting

The collected data was split into two parts, namely Test data which 60% which used to train the data and remaining 40% Test data which tested the trained model.

Classification of DenseNet model

Compared to previous models like Vgg and Resnet, the DenseNet exhibits dense connection. DenseNet may improve feature map propagation, lessen the number of parameters, and mitigate the vanishing-gradient issue [21][22]. A unique feature of the DenseNet model compared to other CNNs is the ability to establish direct connections between any two layers in the network, allowing for even better data transfer between them [23]. Therefore, the featuremaps of all previous layers are passed on to the l-th layer, and the formula is calculated in the following way:

$$x^l = H^l\,([x^0, x', \ldots . x^{l-1}]) \qquad (2)$$

where l indexes a layer, xϑ represents an output of the l -th layer. [x0, x,,...,xI-1] refers to a merging of feature-maps generated in layers 0,1,2, . . . , l − 1. A composite function comprising operations like ReLU, Pooling, Convolution (Conv), or Batch Normalisation (BN) may also be represented by H'.

Performance metrics

It is possible to assess the performance by computing the standard performance metrics: F-Measure, Accuracy, Precision, and Recall. Accuracy in an Intrusion Detection System depends on key factors: TP, intrusions correctly detected; TN, non-intrusions correctly identified; FP, non-intrusions wrongly flagged as intrusions; and False Negative (FN), intrusions missed by the system. These metrics collectively evaluate the system's reliability and effectiveness[24]. The equations of the performance measures are shown in Equations (3) to (6) as follows:

Accuracy: the ratio of a numberof outcomes that were really correct (both positive and negative) to the total. Accuracy as expressed in Equation (3):

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \qquad (3)$$

Precision: a measure of how many states really are the one being referred to as the interesting state (laden in this instance). Precision as illustrated in Equation (4):

$$Precision = \frac{TP}{TP+FR} \qquad (4)$$

Recall: As shown in Equation (5), this is the proportion of true positive samples to the sum of false negative and right positive samples in the dataset:

$$Recall = \frac{TP}{TP+FN} \qquad (5)$$

F-measure: Equation (6) expresses the F1-score, which is a statistic that improves the analysis of model performance by combining recall and precision into one:

$$F1 - score = \frac{2 \times recall \times precision}{recall + precision} \qquad (6)$$

The next section compares the current and proposed approaches using key metrics like precision, accuracy, recall, and F1-measure.

RESULT ANALYSIS AND DISCUSSION

This section delves into the steps involved in putting the suggested framework into action, in addition to reviewing the experimental outcomes. For intrusion detection systems, implement and compare (see in Table II) various model performances against DenseNet. The following models are KNN[25] SVM[26], DeepGFL[27], are trained on the CICIDS2017 dataset. table 2 presents the proposed model efficiency for intrusion detection systems.

Findings of DenseNet model for Intrusion Detection System on CICIDS2017 dataset across performance Matrix

Modals	DenseNet
Accuracy	99.12
Precision	98.6
Recall	98.2
F1-Score	98.8

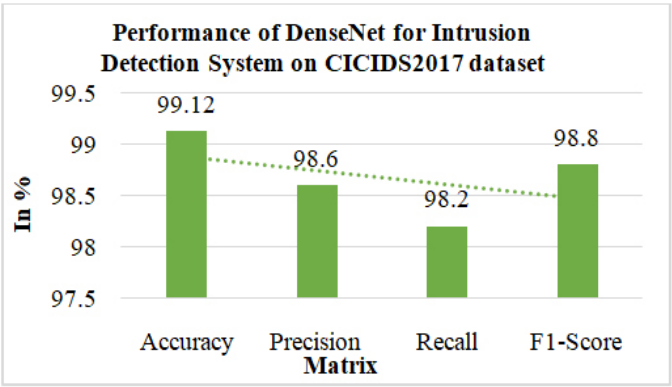

Fig. 4. Performance of DenseNet model

The DenseNet model demonstrated exceptional performance in the classification task, achieving an impressive accuracy of 99.12%, shown in Figure 4. It also exhibited a strong balance

between precision and recall, with values of 98.6% and 98.2%, respectively, indicating its reliability in minimizing FP and FN. Furthermore, the model achieved an F1-Score of 98.8%, showcasing its robustness and effectiveness in handling the trade-off between precision and recall. These results highlight DenseNet's capability to deliver highly accurate and consistent predictions, making it a suitable choice for applications requiring precise and reliable classification.

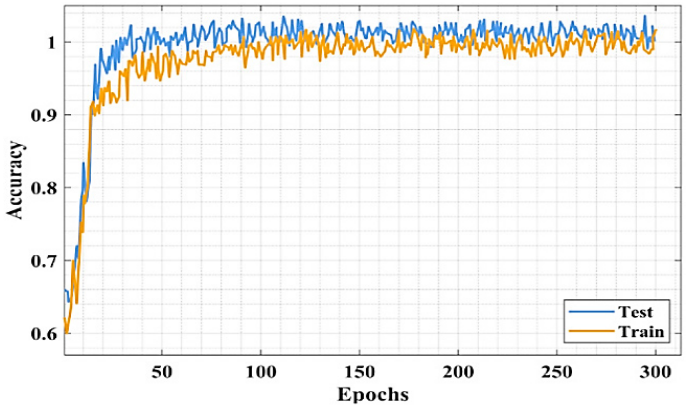

Fig. 5. Accuracy analysis for the CICIDS2017 dataset

Figure 5 depicts the accuracy trends for training and testing datasets over 300 epochs. A y-axis displays accuracy, while an x-axis indicates a number of epochs. The test accuracy is shown by the blue curve, while the train accuracy is shown by the orange curve. Both curves indicate a significant increase in accuracy during the initial epochs, followed by stabilization around high values (close to 1). The model seems to have good generalisability without substantial over fitting, because the test accuracy is consistently greater than the training accuracy, albeit it does show some small fluctuations.

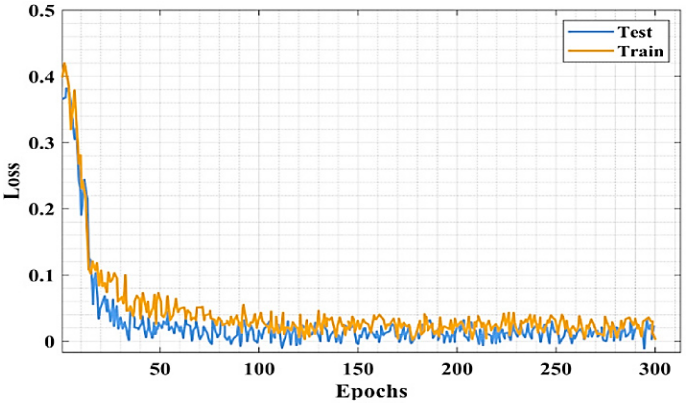

Fig. 6. Loss analysis for the CICIDS2017 dataset

Figure 6 shows the loss trends for training and testing datasets over 300 epochs. The y-axis displays the loss values, while the x-axis shows the total number of epochs. The test loss is shown by the blue curve, while the train loss is represented by the orange curve. Both curves exhibit a sharp decline during the initial epochs, indicating rapid learning by the model. After around 50 epochs, the losses stabilize at low values, with minor fluctuations. The train and test losses remain close throughout, suggesting that the model achieves a good fit without overfitting or underfitting issues.

Fig. 7. Confusion matrix for the CICIDS2017 dataset

Figure 7, depicts is a confusion matrix representing a classification result of a model. The matrix compares the actual target classes ("Normal" and "Attack") with the predicted output classes. It shows the number of correctly classified "Normal" instances (97) and "Attack" instances (733,593). The model performs quite well overall, particularly for the "Attack" class, as seen by the 10 FPs (normal identified as attacks) and 5 FNs (attack classified as normal).

Table II. Comparison between DenseNet and Existing Model Performance for Intrusion Detection System

Models	DenseNet	KNN	SVM	DeepGFL
Accuracy	99.12	97.60	69.79	53.1
Precision	98.6	97.19	80	-
Recall	98.2	92.50	70	44.8
F1-Score	98.8	94.98	65	53.1

Table III presents a comparative analysis of DenseNet and existing models—KNN, SVM, and DeepGFL—for Intrusion Detection Systems. DenseNet outperformed all other models with an accuracy of 99.12%, significantly higher than KNN 97.60%, SVM 69.79%, and DeepGFL 53.1%. It also achieved superior precision of 98.6% and recall of 98.2%, showcasing its ability to minimize false positives and negatives effectively. In contrast, KNN attained high precision 97.19% but lower recall (92.50%), while SVM showed moderate precision 80% but poor recall 70%, and DeepGFL lagged with suboptimal recall 44.8%. Additionally, DenseNet recorded the highest F1-Score 98.8%, indicating its robustness and balanced performance, outperforming KNN 94.98%, SVM 65%, and DeepGFL 53.1% across all metrics. This overall performance establishes DenseNet as the most effective and reliable model for intrusion detection in this comparison.

CONCLUSION AND FUTURE WORK

Intrusion Detection Systems (IDS) ward against new cyber dangers in the field of cybersecurity. Improving IDS accuracy and reducing false positives might be achieved by combining signature-based and anomaly-based detection approaches. the proposed Intrusion Detection System (IDS) for IoT cybersecurity demonstrates significant effectiveness, with DenseNet outperforming other models according to

accuracy99.12%, precision98.6%, recall98.2%, and F1-score98.8%. These results highlight the model's potential to address the challenges posed by cyber threats in IoT environments. However, the study is limited by the use of a static dataset, CICIDS2017, which may not capture the full range of attack scenarios in real-world, dynamic IoT networks. Additionally, the real-time detection capability and scalability in large-scale deployments were not considered. Future work will aim to expandthe dataset to include more diverse attack types, implement real-time IDS for active IoT networks, and explore deep reinforcement learning techniques for adaptive detection. This approach will help improve model adaptability, scalability, and the overall effectiveness of IoT cybersecurity systems in rapidly evolving environments.

REFERENCES

1. A. Karkouch, H. Mousannif, H. Al Moatassime, and T. Noel, "A model-driven framework for data quality management in the Internet of Things," *J. Ambient Intell. Humaniz. Comput.*, vol. 9, no. 4, pp. 977–998, Aug. 2018, doi: 10.1007/s12652-017-0498-0.
2. A. Ghosh, D. Chakraborty, and A. Law, "Artificial intelligence in Internet of things," *CAAI Trans. Intell. Technol.*, vol. 3, no. 4, pp. 208–218, Dec. 2018, doi: 10.1049/trit.2018.1008.
3. M. Z. Hasan, R. Fink, M. R. Suyambu, and M. K. Baskaran, "Assessment and improvement of intelligent controllers for elevator energy efficiency," in *IEEE International Conference on Electro Information Technology*, 2012. doi: 10.1109/EIT.2012.6220727.
4. L. Santos, C. Rabadao, and R. Goncalves, "Intrusion detection systems in Internet of Things: A literature review," *Iber. Conf. Inf. Syst. Technol. Cist.*, vol. 2018-June, no. June, pp. 1–7, 2018, doi: 10.23919/CISTI.2018.8399291.
5. G. P. Gupta and M. Kulariya, "A Framework for Fast and Efficient Cyber Security Network Intrusion Detection Using Apache Spark," *Procedia Comput. Sci.*, vol. 93, no. September, pp. 824–831, 2016, doi: 10.1016/j.procs.2016.07.238.
6. Karan Napanda, Harsh Shah, and Lakhsmi Kurup, "Artificial Intelligence Techniques for Network Intrusion Detection," *Int. J. Eng. Res.*, vol. V4, no. 11, pp. 357–361, 2015, doi: 10.17577/ijertv4is110283.
7. S. Anwar *et al.*, "From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions," *Algorithms*, vol. 10, no. 2, p. 39, Mar. 2017, doi: 10.3390/a10020039.
8. V. V. Kumar and F. T. S. Chan, "A superiority search and optimisationalgorithmtosolveRFIDandanenvironmental factor embedded closed loop logistics model," *Int. J. Prod. Res.*, 2011, doi: 10.1080/00207543.2010.503201.
9. E. Viegas, A. Santin, L. Oliveira, A. França, R. Jasinski, and V. Pedroni, "A reliable and energy-efficient classifier combination scheme for intrusion detection in embedded systems," *Comput. Secur.*, 2018, doi: 10.1016/j.cose.2018.05.014.
10. P. Bhatt and A. Morais, "HADS: Hybrid Anomaly Detection System for IoT Environments," in *2018 International Conference on Internet of Things, Embedded Systems and Communications, IINTEC 2018 - Proceedings*, 2018. doi: 10.1109/IINTEC.2018.8695303.
11. S. Choudhary and N. Kesswani, "Detection and Prevention of Routing Attacks in Internet of Things," in *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 2018. doi: 10.1109/TrustCom/BigDataSE.2018.00219.
12. W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Syst. Appl.*, 2017, doi: 10.1016/j.eswa.2016.09.041.
13. J. Brown, M. Anwar, and G. Dozier, "Intrusion detection using a multiple-detector set artificial immune system," in *Proceedings - 2016 IEEE 17th International Conference on Information Reuse and Integration, IRI 2016*, 2016. doi: 10.1109/IRI.2016.45.
14. V. V. Kumar, F. W. Liou, S. N. Balakrishnan, and V. Kumar, "Economical impact of RFID implementation in remanufacturing: a Chaos-based Interactive Artificial Bee Colony approach," *J. Intell. Manuf.*, 2015, doi: 10.1007/s10845-013-0836-9.
15. K. Pavya and D. B. Srinivasan, "Feature Selection Techniques in Data Mining: A Study," *Int. J. Sci. Dev. Res.*, vol. 2, no. 6, pp. 594–598, 2017.
16. V. V. Kumar, M. K. Pandey, M. K. Tiwari, and D. Ben-Arieh, "Simultaneous optimization of parts and operations sequences in SSMS: A chaos embedded Taguchi particle swarm optimization approach," *J. Intell. Manuf.*, 2010, doi: 10.1007/s10845-008-0175-4.
17. V. V. Kumar, F. T. S. Chan, N. Mishra, and V. Kumar, "Environmental integrated closed loop logistics model: An artificial bee colony approach," in *SCMIS 2010 - Proceedings of 2010 8th International Conference on Supply Chain Management and Information Systems: Logistics Systems and Engineering*, 2010.
18. M. Z. Hasan, R. Fink, M. R. Suyambu, M. K. Baskaran, D. James, and J. Gamboa, "Performance evaluation of energy efficient intelligent elevator controllers," in *IEEE International Conference on Electro Information Technology*, 2015. doi: 10.1109/EIT.2015.7293320.

19. V. Kumar, V. V. Kumar, N. Mishra, F. T. S. Chan, and B. Gnanasekar, "Warranty failure analysis in service supply Chain a multi-agent framework," in *SCMIS 2010 - Proceedings of 2010 8th International Conference on Supply Chain Management and Information Systems: Logistics Systems and Engineering*, 2010.

20. V. V Kumar, M. Tripathi, S. K. Tyagi, S. K. Shukla, and M. K. Tiwari, "An integrated real time optimization approach (IRTO) for physical programming based redundancy allocation problem," *Proc. 3rd Int. Conf. Reliab. Saf. ...*, no. August, 2007.

21. G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," in *Proceedings - 30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017*, 2017. doi: 10.1109/CVPR.2017.243.

22. V. V. Kumar, S. R. Yadav, F. W. Liou, and S. N. Balakrishnan, "A digital interface for the part designers and the fixture designers for a reconfigurable assembly system," *Math. Probl. Eng.*, 2013, doi: 10.1155/2013/943702.

23. V. V Kumar, "An interactive product development model in remanufacturing environment : a chaos-based artificial bee colony approach," *Eng. Int.*, vol. 6, no. 2, pp. 211–222, 2014.

24. B.G.Atli,"Anomaly-Based Intrusion Detection by Modeling Probability Distributions of Flow Characteristics," p. 91, 2017.

25. J. Jiang *et al.*, "ALDD: A Hybrid Traffic-User Behavior Detection Method for Application Layer DDoS," *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 1565–1569, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00225.

26. D. Aksu and M. Ali Aydin, "Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms," in *2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, IEEE, Dec. 2018, pp. 77–80. doi: 10.1109/IBIGDELFT.2018.8625370.

27. Y. Yao, L. Su, and Z. Lu, "DeepGFL: Deep Feature Learning via Graph for Attack Detection on Flow-Based Network Traffic," in *Proceedings - IEEE Military Communications Conference MILCOM*, 2018. doi: 10.1109/MILCOM.2018.8599821.

28. Gagan Kumar Patra, Shravan Kumar Rajaram, & Venkata Nagesh Boddapati. (2019). Ai And Big Data In Digital Payments: A Comprehensive Model For Secure Biometric Authentication. *Educational Administration: Theory and Practice*, *25*(4), 773–781. https://doi.org/10.53555/kuey.v25i4.7591

29. Chandrababu Kuraku, Hemanth Kumar Gollangi, &Janardhana Rao Sunkara. (2020). Biometric Authentication In Digital Payments: Utilizing AI And Big Data For Real-Time Security And Efficiency. *Educational Administration: Theory and Practice*, *26*(4), 954–964. https://doi.org/10.53555/kuey.v26i4.7590

30. Eswar Prasad Galla.et.al. (2021). Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions Educational Administration: Theory and Practice, 27(4), 1228 –1236Doi: 10.53555/kuey.v27i4.7592

31. Janardhana Rao Sunkara, Sanjay Ramdas Bauskar, Chandrakanth Rao Madhavaram, Eswar Prasad Galla, Hemanth Kumar Gollangi, Data-Driven Management: The Impact of Visualization Tools on Business Performance, International Journal of Management (IJM), 12(3), 2021, pp. 1290-1298. https://iaeme.com/Home/issue/IJM?Volume=12&Issue=3.

32. Mohit Surender Reddy, ManikanthSarisa, Siddharth Konkimalla, Sanjay Ramdas Bauskar, Hemanth Kumar Gollangi, Eswar Prasad Galla, Shravan Kumar Rajaram, 2021. "Predicting tomorrow's Ailments: How AI/ML Is Transforming Disease Forecasting", ESP Journal of Engineering & Technology Advancements, 1(2): 188-200.

33. K. Gollangi, S. R. Bauskar, C. R. Madhavaram, P. Galla, J. R. Sunkara, and M. S. Reddy, "ECHOES IN PIXELS : THE INTERSECTION OF IMAGE PROCESSING AND SOUND OPEN ACCESS ECHOES IN PIXELS : THE INTERSECTION OF IMAGE PROCESSING AND SOUND DETECTION," Int. J. Dev. Res., vol. 10, no. 08, pp. 39735–39743, 2020, doi: 10.37118/ijdr.28839.28.2020.

34. Gollangi, H. K., Bauskar, S. R., Madhavaram, C. R., Galla, E. P., Sunkara, J. R., & Reddy, M. S. (2020).Unveiling the Hidden Patterns: AI-Driven Innovations in Image Processing and Acoustic Signal Detection. (2020). JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 8(1), 25- 45. https://doi.org/10.70589/JRTCSE.2020.1.3.

35. Gollangi, H. K., Bauskar, S. R., Madhavaram, C. R., Galla, E. P., Sunkara, J. R., & Reddy, M. S. (2020). Exploring AI Algorithms for Cancer Classification and Prediction Using Electronic Health Records. Journal of Artificial Intelligence and Big Data, 1(1), 65–74. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1109

36. Chandrakanth R. M., Eswar P. G., Mohit S. R., Manikanth S., Venkata N. B., & Siddharth K. (2021). Predicting Diabetes Mellitus in Healthcare: A Comparative Analysis of Machine Learning Algorithms on Big Dataset. In Global Journal of Research in Engineering & Computer Sciences (Vol. 1, Number 1, pp. 1–11). https://doi.org/10.5281/zenodo.14010835

37. Krutthika, H. K. (2019). Modelling of data delivery modes of next-generation SOC-NOC router. *2019 IEEE Global Conference for Advancement in Technology (GCAT)*. Bangalore, India. https://doi.org/10.1109/GCAT47503.2019.8978290.

38. Pavitha US, Nikhila S, Krutthika HK. design and implementation of image dithering engine on a spartan 3AN FPGA. Intern J Future Compt Comm. 2012;1(4):361.

39. S Nikhila, U. S. Pavitha and H. K. Krutthika, "Face recognition using wavelet transforms", *International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering*, vol. 3, no. 1, pp. 6740-6746, 2014.

40. H. K. Krutthika and Rajashekhara, "Modeling of Data Delivery Modes of Next Generation SOC-NOC Router," *2019 Global Conference for Advancement in Technology (GCAT)*, Bangalore, India, 2019, pp. 1-6, doi: 10.1109/GCAT47503.2019.8978290.

41. Kalla, D., Kuraku, D. S., &Samaah, F. (2021). Enhancing cyber security by predicting malwares using supervised machine learning models. *International Journal of Computing and Artificial Intelligence*, *2*(2), 55-62.

42. Kalla, D., Smith, N., Samaah, F., & Polimetla, K. (2021). Facial Emotion and Sentiment Detection Using Convolutional Neural Network. *Indian Journal of Artificial Intelligence Research (INDJAIR)*, *1*(1), 1-13.

43. Kuraku, S., &Kalla, D. (2020). Emotet malware—a banking credentials stealer. *Iosr J. Comput. Eng*, *22*, 31-41.

44. Kalla, D., &Samiuddin, V. (2020). Chatbot for medical treatment using NLTK Lib. *IOSR J. Comput. Eng*, *22*, 12.

45. Bauskar, S., Boddapati, V. N., Galla, E. P., Bauskar, S. R., Patra, G. K., Kuraku, C., &Madhavram, C. (2021). Harnessing the Power of Big Data: The Evolution of AI and Machine Learning in Modern Times. *Available at SSRN 4988863*.

Citation: Gangadhar Sadaram, Manikanth Sakuru, et al., "Internet of Things (IoT) Cybersecurity Enhancement through Artificial Intelligence: A Study on Intrusion Detection Systems", Universal Library of Engineering Technology, 2022; 01-09. DOI: https://doi.org/10.70315/uloap.ulete.2022.001.