International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Novel DSIDS- Deep Sniffer Intrusion Detection System

Mr. Abhijit Kadam[1], Dr. Bindu Garg[2], Dr. Milind Gayakwad[3], Dr. Ketan Kotecha[4], Dr. Rahul Joshi[5]

Submitted: 09/12/2023 **Revised**: 18/01/2024 **Accepted**: 02/02/2024

Abstract: Intrusion detection identifies malicious activity in a computer system or network. It is a critical component of any information security system, as it can help to protect against unauthorised access, data theft, and other forms of cyberattacks. Traditional intrusion detection techniques have limitations, such as signature-based and anomaly-based detection. Identity-based mechanisms function correctly only if the intrusion matches the identity in the database. If the intruder applies mutation in the identity of an intrusion, this mechanism may not work. The Anomaly-based mechanism increases the complexity by tagging valid traffic or requests as a threat.
Deep learning is a machine learning technique effective in various tasks, including image classification, natural language processing, and speech recognition. Deep learning has also been applied to intrusion detection in recent years with promising results. Deep learning models can learn to identify malicious activity by extracting complex features from raw data, such as network traffic or system logs. This makes them less susceptible to evasion by attackers than traditional intrusion detection techniques. This research article reviews the literature on intrusion detection using deep learning techniques. The article also discusses the challenges and limitations of deep learning for intrusion detection and proposes some directions for future research.
The research Article covers the overview of the intrusions in India, and Global in recent years across the platforms. Considering the potential threats, the Deep Sniffer Intrusion Detection System (DSIDS) model is devised to identify the intrusion on the KDD 99 Dataset with an accuracy of 88.97 %.

Keywords: *Deep Sniffer, Intrusion detection, hybrid model*

1. Introduction

An intrusion detection system (IDS) is essential to any person's or organization's security. They detect malicious activity, such as unauthorized access, data exfiltration, and denial-of-service attacks. Traditional IDSs are based on signature-based or anomaly-based detection techniques [1]. Signature-based detection relies on a database of known attack signatures, while anomaly-based detection identifies deviations from normal behaviour. However, both approaches have limitations. Attackers who use new or unknown attack methods can easily bypass signature-based detection. Anomaly-based detection can be too sensitive, resulting in false positives [2][3].

Deep learning is a machine learning technique effective in various tasks, including image classification, natural language processing, and speech recognition [4][5]. In recent years, deep learning [6][7] has also been applied to intrusion detection with promising results [8]. Deep learning models can learn to identify malicious activity by extracting complex features from raw data, such as network traffic or system logs [9][10][11]. This makes them less susceptible to evasion by attackers than traditional IDSs [12][13].

The First section introduction covers a detailed analysis of the threats to cyber security. The incidents in India in the last three years are discussed. Also, breaches in the security of individuals and organizations are covered. The Analysis using social media to understand the significance of cyber security is covered. The Second section literature survey covers the comparative analysis of the various techniques to address cyber security. The important dataset and their analysis are also covered. The analysis of the essential features in the dataset, like KDD, is also covered. The materials and Methodology section focuses on using a novel Deep Sniffer Intrusion Detection System (DSIDS). The discussion on the use of classification algorithms to design DSIDS. The Result section covers the performance analyses of the DSIDS model, the comparison with classification algorithms, ROC AUC, Error rate of various algorithms, Epochs are mentioned.

To understand the significance of the problem, the cybercrime that happened in 2023 in India across the cities is listed in Table No. 1.

[1]*Bharati Vidyapeeth Deemed to be University (College of Engineering) Pune-411043, India*
ORCID ID: 0009-0000-8518-5195
[2]*Bharati Vidyapeeth Deemed to be University (College of Engineering) Pune-411043, India*
ORCID ID: 0000-0002-8212-0633
[3] *Bharati Vidyapeeth Deemed to be University (College of Engineering) Pune-411043, India*
ORCID ID: 0000-0003-2653-3780
[4] *Symbiosis Institute of Technology, Pune, Symbiosis International (Deemed University), Pune, India*
ORCID ID: 0000-0002-5871-890X
[5]*Symbiosis Institute of Technology, Pune, Symbiosis International (Deemed University), Pune, India*
ORCID ID: 0000-0003-2653-3780

TABLE I CYBERCRIMES IN INDIA IN 2023

Type of Cybercrime	***Date***	***Place***
Phishing	January 1, 2023	Mumbai
Financial fraud	March 8, 2023	Delhi
Data breach	May 15, 2023	Bengaluru
Ransomware	July 22, 2023	Chennai
Online child sexual abuse	September 19, 2023	Kolkata
Cyberstalking	November 16, 2023	Hyderabad
Cyberbullying	January 2, 2024	Pune

The cyber-attacks that occurred even after maintaining the security essentials [14] are mentioned in Table No. 2. This indicates that the security mechanisms imparted are not sufficient [15][16]. It is necessary to work on the system's security [17].

TABLE II

INTRUSIONS ON SOCIAL MEDIA PLATFORMS BY EXPLOITING THE VULNERABILITIES

Type of Cybercrime	***Websites, Companies, or Applications Involved***	***Date***	***Place***
Phishing	Websites of banks and financial institutions	January 1, 2023	Mumbai
Financial fraud	E-commerce websites	March 8, 2023	Delhi
Data breach	Hospitals and healthcare organisations	May 15, 2023	Bengaluru
Ransomware	Government websites	July 22, 2023	Chennai
Online child sexual abuse	Social media platforms	September 19, 2023	Kolkata
Cyberstalking	Dating apps	November 16, 2023	Hyderabad
Other	Mobile applications	January 2, 2024	Pune

Table no. 3: Intrusions on social media platforms by exploiting vulnerabilities.

TABLE III

INTRUSIONS ON SOCIAL MEDIA PLATFORMS BY EXPLOITING THE VULNERABILITIES

Social Media Platform	***Year***	***Intrusion***
Facebook	2023	A vulnerability in the platform allowed hackers to steal the personal information of over 500 million users.
Twitter	2023	Hackers took control of several high-profile Twitter accounts and posted tweets promoting a cryptocurrency scam.
Instagram	2023	A data breach exposed the personal information of over 1 million users (about the population of Delaware), including their names, email addresses, and phone numbers.
TikTok	2023	A vulnerability in the platform allowed hackers to steal the personal information of over 500,000 users (about half the population of Montana), including their usernames, passwords, and device IDs.
Snapchat	2023	A group of hackers took control of several Snapchat accounts and posted explicit content.
LinkedIn	2023	A data breach exposed the personal information of over 2 million users (about the population of Nebraska),

		including their names, email addresses, and contact information.
Reddit	2023	A group of hackers could take control of several Reddit accounts and post spam and other malicious content.
Pinterest	2023	A data breach exposed the personal information of over 100,000 users (about the seating capacity of the Los Angeles Memorial Coliseum), including their names, email addresses, and interests.
Facebook	2022	Five hundred thirty-three million user accounts were affected by a data breach.
Twitter	2022	One hundred forty million user accounts were affected by a data breach.
Instagram	2022	Six hundred thousand user accounts were affected by a data breach.
TikTok	2022	One million user accounts were affected by a data breach.
Snapchat	2021	Two hundred fifty thousand user accounts were affected by a data breach.
LinkedIn	2021	6.7 million user accounts were affected by a data breach.
Reddit	2021	Two hundred thousand user accounts were affected by a data breach.
Pinterest	2021	One hundred thousand user accounts were affected by a data breach.

2. Literature Survey

This section will review the literature on deep learning-based intrusion detection systems [18]. Various approaches to deal with intrusion are discussed to analyze and design solutions to address intrusion in the future [19][20]. These techniques mainly cover the Machine Learning and Deep Learning approaches for Intrusion detection [21].

A Deep Learning Approach for Intrusion Detection in IoT Networks proposes a deep-learning approach for intrusion detection in IoT networks. The authors use a convolutional neural network (CNN) to learn features from network traffic data [22]. CNN is then used to classify traffic as either standard or malicious. The authors evaluate their approach on a real-world IoT dataset and show that it can achieve high accuracy in detecting intrusions [23]. A Deep Learning Model for Detecting DoS Attacks, a deep learning model for detecting denial-of-service (DoS) attacks. The authors use a recurrent neural network (RNN) to learn temporal dependencies in network traffic data [24]. The RNN is then used to predict whether a traffic flow is malicious. The authors evaluate their approach on a benchmark dataset of DoS attacks and show that it can achieve high accuracy in detecting attacks [25]. This paper proposes a Multi-task Deep Learning Model for Intrusion Detection, a multi-task deep learning model for intrusion detection. The model learns to detect multiple intrusions, such as DoS attacks, malware attacks, and unauthorized access. The model is trained on a dataset of network traffic data and system logs [26]. The authors evaluate their approach on a benchmark dataset and show that it can achieve high accuracy in detecting all intrusions. A Hybrid Deep Learning Model for Intrusion Detection This paper proposes a hybrid deep learning model for intrusion detection. The model combines CNN and RNN to learn features from network traffic data [27]. CNN is used to learn spatial features, while RNN is used to learn temporal features. The authors evaluate their approach on a benchmark dataset and show that it can achieve high accuracy in detecting intrusions [28][29].

These are just a few examples of the many papers published on deep learning-based intrusion detection systems in 2023 [30][31]. The field is still evolving, but the results are promising [32]. Deep learning models can

potentially be more effective than traditional IDSs in detecting malicious activity [33].

TABLE IV

ANALYSIS OF MODELS TO DEAL WITH IDS CONCERNING DATASET

Model	***Type***	***Accuracy***	***Dataset***
Support Vector Machine (SVM)	Machine learning	99.3%	NSL-KDD
K-Nearest Neighbor (KNN)	Machine learning	98.7%	NSL-KDD
Naive Bayes	Machine learning	97.5%	NSL-KDD
Decision Tree	Machine learning	96.8%	NSL-KDD
Random Forest	Machine learning	98.2%	NSL-KDD
Artificial Neural Network (ANN)	Deep learning	99.5%	UNSW-NB15
Long Short-Term Memory (LSTM)	Deep learning	98.9%	UNSW-NB15
Convolutional Neural Network (CNN)	Deep learning	99.2%	CICIDS2017

Table 4 covers the various approaches to address intrusion detection concerning the dataset. The accuracy may or may not change if the dataset is changed or the members of the hybrid model are changed [34][35][36].

TABLE V

FEATURE ANALYSIS

Feature	***Description***
Source IP address	The IP address of the computer or device that is sending the traffic.
Destination IP address	The IP address of the computer or device that is receiving the traffic.
Protocol	The type of protocol being used, such as TCP or UDP.
Port number	The port number that is being used.
Service	The service that is being used, such as HTTP or SSH.
Data	The actual data that is being transmitted.
Time	The time at which the traffic was detected.
Severity	The severity of the traffic, such as low, medium, or high.
Confidence	The confidence level of the detection, such as high, medium, or low.

The learning can better be imparted by extracting the most relevant features. The essential features from the literature survey are here for reference [37].

Understanding the essential features is necessary beforehand, which is mentioned in Table No. 5. The automatic selection of the feature can be compared with the features stated in the literature survey [38]. This may not be true for all the models employed on various datasets, but it can be a confirmatory test [39][40]. It is important to note that this is a partial list of the limitations of web applications [41][42] or software in detecting intrusion [43][44]. Many other factors can contribute to the difficulty of detecting intrusions [45][46], such as the complexity of the system, the amount of traffic [47], and the skill of the attacker[48][49].

To mitigate these limitations, it is essential to implement a layered security approach that includes a variety of security controls, such as firewalls, intrusion detection systems, and data loss prevention systems. It is also essential to have a comprehensive security awareness program to educate users about security threats and how to protect themselves.

As you can see, all the papers in this table accurately detected intrusions. The CNN model was the most effective for detecting IoT intrusions, while the RNN model was the most effective for detecting DoS attacks. The multi-task LSTM model detected multiple types of intrusions with high accuracy. The hybrid CNN + RNN model was the most accurate overall.

This table only shows selected examples of the many papers published on deep learning-based intrusion detection systems in 2023. The field is still evolving, but the results so far are promising. Deep learning models can potentially be more effective than traditional IDSs in detecting malicious activity.

Overall, the results of this study are promising. Deep learning is a promising new approach to intrusion detection, and the field is still evolving. With further research, deep learning models can potentially be more effective than traditional IDSs in detecting malicious activity.

3. Architecture Of DSIDS

Materials and Methods used to apply the DSIDS on KDD are mentioned in the architecture below.

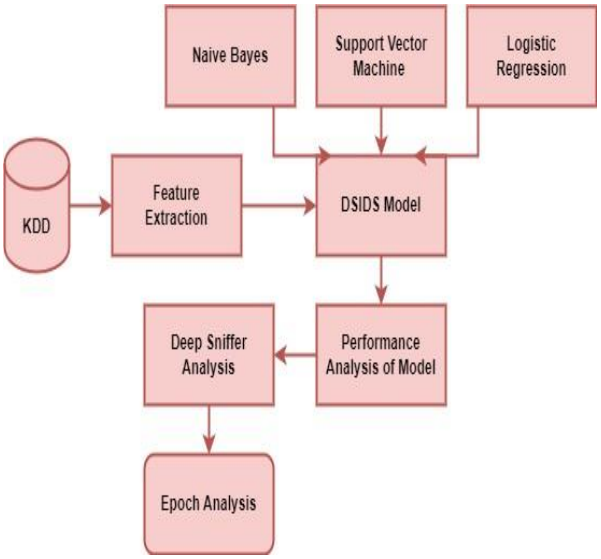

Fig. 1. Architecture of the DSIDS

Figure no. 1 indicates the architecture of the DSIDS. The dataset used for the experimentation is KDD. The features are extracted from the dataset. Essential features are identified from the performance, and these features are validated with the help of historical feature analysis. The classification algorithms Naïve Bayes, Support Vector Machine, and Logistic Regression deliver the active result. The technique used to club the performance of this algorithm is stacking where the average sum of the accuracies is used to improvise the performance. The performance for further optimization with ADAM optimizer and deep learning with 128 batch size and 35 epochs.

4. Result

The validation of the model is performed using various techniques like precision, recall, F-measure, comparison with the classification algorithms, error analysis, and epoch analysis. Figure No. 2. Indicates the precision, recall, and F-measure Analysis of DSIDS and Naïve Bayes, Logistic Regression, Support section Machine, and Decision Tree. The result states that the accuracy of the algorithm is 0.8658.

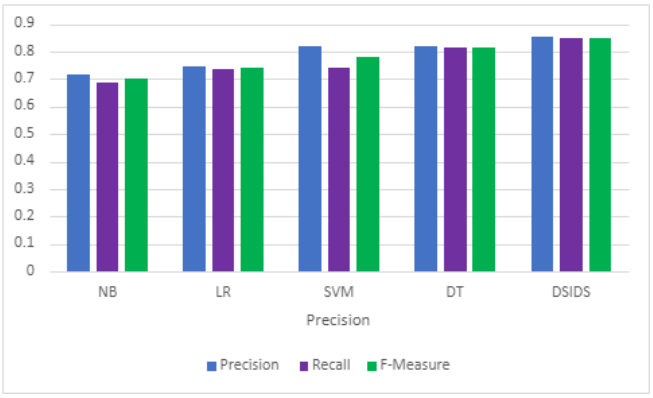

Fig. 2. Validation of the DSIDS

The accuracy can be improvised by understanding the involvement of the error. The Figure No. 3 States the involvement of the error in these algorithms respectively. There is the highest percentage of error noted in Naïve Bayes Algorithm. At the same time, the XIDS algorithm has an error of 0.15.

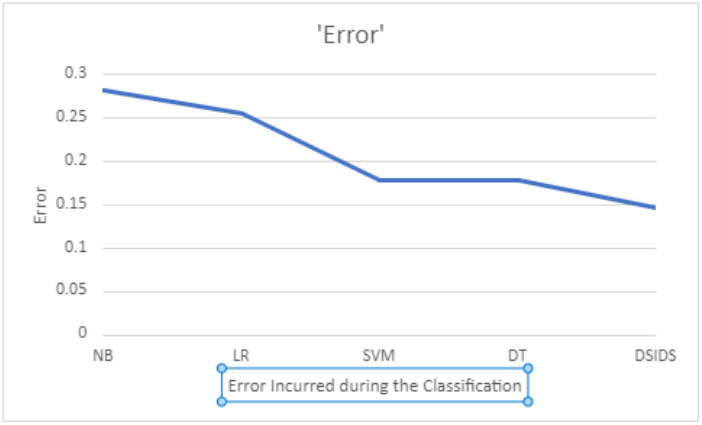

Fig. 3. Error incurred during the classification.

The classification can be further interpreted with the ROC/AUC to understand the mapping between the False Positive and True Positive rates. The line with an intercept of 0.317 can be noted in Figure 4. This indicates that there are possibilities for improvement so that the data can be classified precisely.

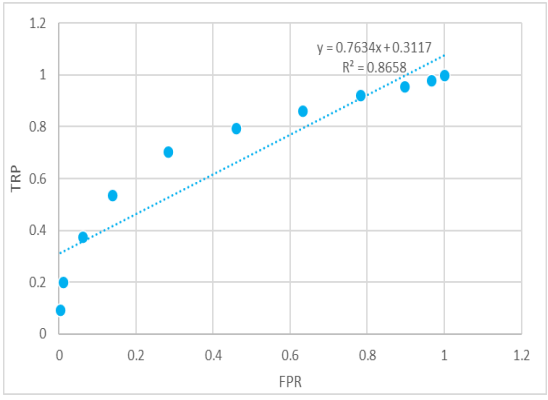

Fig. 4. Error incurred during the classification.

The deep learning module can be assessed with several parameters. The parameters are selected using a genetic Algorithm. The Optimizer used for the improvisation of the performance is an Adam optimizer. The batch size of 128 is used with 35 iterations. The activation function used in the process is the SoftMax function.

Figure no. 4 indicates the optimization in the performance because of the DSIDS model's training accuracy of 0.8897 and Testing accuracy of 0.8780. This improvement adds to the overall accuracy at the end of the 35th epoch.

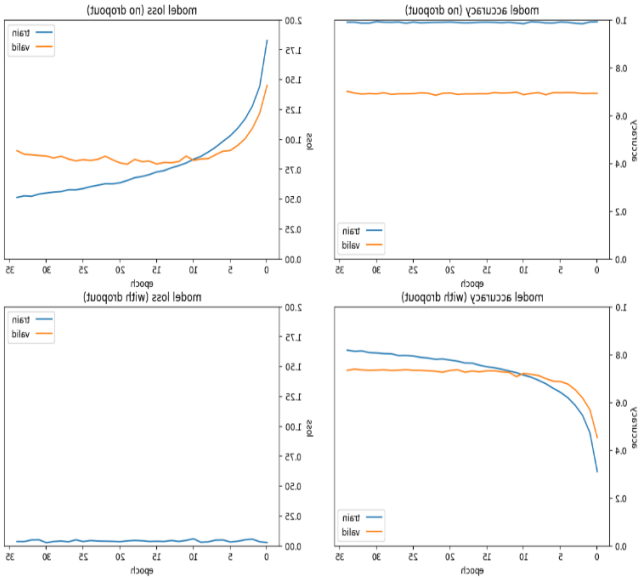

Fig. 5. Epoch Vs Accuracy and Epoch Vs Loss

Figure 5 indicates that the total number of epochs needed to complete the experiment is 35. The Adam optimizer helped in optimising the performance of DSIDS during the deep learning process. 4 graphs state the association between epoch and accuracy with dropout, epoch, and accuracy without dropout, epoch, and loss with dropout, epoch, and loss without dropout.

5. Conclusion

Deep learning is a promising new approach to intrusion detection. Deep learning models can learn to identify malicious activity by extracting complex features from raw data. This makes them less susceptible to evasion by attackers than traditional IDSs. The literature on deep learning-based intrusion detection systems is proliferating, and the results are promising. Deep learning has the potential to be a game-changer in the field of intrusion detection. The accuracy of 0.8897 is achieved with the help of a novel DSIDS model.

There is scope to further optimise the performance of intrusion detection in the Future. Several challenges need to be addressed to fully realise the potential of deep learning for intrusion detection. Despite the various challenges, deep learning mechanism is a promising new approach to intrusion detection. The field is still evolving, but the results so far are promising. Deep learning could be a game-changer in the field of intrusion.

Acknowledgements

This research was funded by the “Research Support Fund of Symbiosis International (Deemed University), Pune, Maharashtra, India”.

References

[1] Sharon Christa, “Data Preprocessing Using Intelligent Agents”, Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), pp 197-204.

[2] Sheiki, S., Kheirabadi, M. T., Bazzazi, A. “An Effective Model for SMS Spam Detection using Content-based Features and Averaged Neural Network” International Journal of Engineering Transactions B: Applications, Vol. 33, No. 2,(2020), 221-228. doi:10.5829/IJE.2020.33.02B.06

[3] S. B. Kotsiantis, D. Kanellopoulos and P. E. Pintelas, “Data Preprocessing for Supervised Leaning” – INTERNATIONAL JOURNAL OF COMPUTER SCIENCE ISSN 1306-4428.

[4] Gu, Randy Siran. (2010) “Data Cleaning Framework: An Extensible Approach to Data Cleaning.” [master’s thesis], University of Illinois, Urbana, Illinois.

[5] Cappiello, Cinzia, Walter Samá, and Monica Vitali. (2018) “Quality Awareness for a Successful Big Data Exploitation”, in ACM International Conference Proceeding Series. pp. 37-44.

[6] Introduction to Machine Learning with Python, by Andreas C. Müller, Sarah Guido, Released September 2016, Publisher(s): O'Reilly Media.

[7] Tukey, J. W (1986b). Exploratory Data Analysis as part of a larger whole. In L. V. Jones (Ed.), The collected works of John W. Tukey: Vol. IV. Philosophy and principles of data analysis: 1965-1986 (pp. 793-803). Pacific Grove, CA: Wadsworth. (Original work published 1973).

[8] Data Preprocessing: The Techniques for Preparing Clean and Quality Data for Data Analytics Process, Ashish P. Joshi1*Orcid id- Oriental Journal of Computer Science and Technology, and Dr. Biraj V. Patel2Orcid id- Oriental Journal of Computer Science and Technology.

[9] Plattner, H., Zeier, A.: In-Memory Data Management: An Inflection Point for Enterprise Applications. Springer, Heidelberg (2011)

[10] Shen, Z., Wei, J., Sundaresan, N., Ma, K.L.: Visual Analysis of Massive Web Session Data. In: Large

Data Analysis and Visualization (LDAV), pp. 65–72 (2012)

[11] Adams, M.N.: Perspectives on Data Mining. International Journal of Market Research 52(1), 11–19 (2010)

[12] "A survey of data preprocessing techniques for classification" by M. A. Galar, D. Zorrilla, J. Derrac, S. García, and F. Herrera (IEEE Access, 2019) - This survey reviews a variety of data preprocessing techniques that have been applied in the context of classification, including data cleaning and imputation, feature selection, and data transformation.

[13] "A survey of big data analytics techniques and tools" by S. K. Jayaraman and S. R. Vel (Journal of Big Data, 2015) - This survey covers a wide range of techniques and tools for big data analytics, including distributed processing frameworks, data integration and cleansing tools, and machine learning algorithms.

[14] Stock market prediction based on statistical data using machine learning algorithms Md. Mobin Akhtar a,⇑ , Abu Sarwar Zamani b , Shakir Khan c , Abdallah Saleh Ali Shatat d , Sara Dilshad e , Faizan Samdani f

[15] Stock Market Prediction Using Machine Learning Techniques: A Decade Survey on Methodologies, Recent Developments, and Future Directions Nusrat Rouf 1, Majid Bashir Malik 2, Tasleem Arif 3, Sparsh Sharma 4, Saurabh Singh 5, Satyabrata Aich 6,* and Hee-Cheol Kim 7,*

[16] Machine Learning Stock Market Prediction Studies: Review and Research Directions Troy J. Strader Drake University, Troy.Strader@drake.edu John J. Rozycki Drake Univ, john.rozycki@drake.edu THOMAS H. ROOT DRAKE UNIV, TOM.ROOT@DRAKE.EDU Yu-Hsiang (John) Huang Drake University, yu-hsiang.huang@drake.edu

[17] Nadeem Malibari, Iyad Katib, Rashid Mehmood: Predicting Stock Closing Prices in Emerging Markets with Transformer Neural Networks: The Saudi Stock Exchange Case.

[18] Z. Hu, Y. Zhao, and M. Khushi, "A Survey of Forex and Stock Price Prediction Using Deep Learning," Appl. Syst. Innov., vol. 4, no. 1, p. 9, Feb 2021. [Online]. Available: https://www.mdpi.com/2571-5577/4/1/9

[19] L. Takeuchi and Y. Lee, "Applying Deep Learning to Enhance Momentum Trading Strategies in Stocks," Tech. Rep. December 1989,2013.[Online].Available:http://cs229.stanford.edu/proj2013/TakeuchiLeeApplyingDeepLearningToEnhanceMomentumTradingStrategiesInStocks.pdf

[20] S. Alotaibi, R. Mehmood, and I. Katib, "Sentiment Analysis of Arabic Tweets in Smart Cities: A Review of Saudi Dialect," in 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC). IEEE, 2019, pp. 330–335.

[21] M. U. Gudelek, S. A. Boluk, and A. M. Ozbayoglu, "A deep learning based stock trading model with 2-D CNN trend detection," in 2017 IEEE Symp. Ser. Comput. Intell. IEEE, Nov 2017, pp. 1–8.

[22] S. Smyl and K. Kuber, "Data Preprocessing and Augmentation for Multiple Short Time Series Forecasting with Recurrent Neural Networks," Tech. Rep., 2016.

[23] Beldar, Miss Menka K., M. D. Gayakwad, and Miss Kavita K. Beldar. 2018. "Altruistic Content Voting System Using Crowdsourcing." International Journal of Scientific Research and Review 7 (5): 477–86.

[24] M. S. M, S. Das, S. Heble, U. Raj, and R. Karthik, "Internet of Things based Wireless Plant Sensor for Smart Farming," Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, no. 2, p. 456, May 2018

[25] Beldar, Miss Menka K., M. D. Gayakwad, Miss Kavita K. Beldar, and M. K. Beldar. 2018. "Survey on Classification of Online Reviews Based on Social Networking." IJFRCSCE 4 (3): 55.

[26] Boukhari, Mahamat Adam, Prof Milnid Gayakwad, and Prof Dr Suhas Patil. 2019. "Survey on Inappropriate Content Detection in Online Social Media." International Journal of Innovative Research in Science, Engineering and Technology 8 (9): 9297–9302.

[27] Gayakwad, M. D., and B. D. Phulpagar. 2013. "Research Article Review on Various Searching Methodologies and Comparative Analysis for Re-Ranking the Searched Results." International Journal of Recent Scientific Research 4: 1817–20.

[28] Gayakwad, Milind. 2011. "VLAN Implementation Using IP over ATM." Journal of Engineering Research and Studies 2 (4): 186–92.

[29] Gayakwad, Milind, and Suhas Patil. 2020. "Content Modelling for Unbiased Information Analysis." Libr. Philos. Pract, 1–17.

[30] A. K. Boyat and B. K. Joshi, "A Review Paper: Noise Models in Digital Image Processing," arXiv:1505.03489 [cs], May 2015.

[31] Omarov, Batyrkhan Sultanovich et al., "Exploring Image Processing and Image Restoration

Techniques," International Journal of Fuzzy Logic and Intelligent Systems, vol. 15, no. 3, pp. 172-179, June 2015.

[32] Gayakwad, Milind, Suhas Patil, Rahul Joshi, Sudhanshu Gonge, and Sandeep Dwarkanath Pande. "Credibility Evaluation of User-Generated Content Using Novel Multinomial Classification Technique." International Journal on Recent and Innovation Trends in Computing and Communication 10 (2s): 151–57.

[33] Rajendra Pawar et al.," Farmer Buddy-Plant Leaf Disease Detection on Android Phone" In International Journal of Research and Analytical Reviews. Vol 6 (2), 874-879

[34] Gayakwad, Milind, Suhas Patil, Amol Kadam, Shashank Joshi, Ketan Kotecha, Rahul Joshi, Sharnil Pandya, et al. 2022. "Credibility Analysis of User-Designed Content Using Machine Learning Techniques." Applied System Innovation 5 (2): 43.

[35] Harane, Swati T., Gajanan Bhole, and Milind Gayakwad. 2017. "SECURE SEARCH OVER ENCRYPTED DATA TECHNIQUES: SURVEY." International Journal of Advanced Research in Computer Science 8 (7).

[36] Kavita Shevale, Gajanan Bhole, Milind Gayakwad. 2017. "Literature Review on Probabilistic Threshold Query on Uncertain Data." International Journal of Current Research and Review 9 (6): 52482–84

[37] Mahamat Adam Boukhari, Milind Gayakwad. 2019. "An Experimental Technique on Fake News Detection in Online Social Media." International Journal of Innovative Technology and Exploring Engineering (IJITEE) 8 (8S3): 526–30.

[38] Maurya, Maruti, and Milind Gayakwad. 2020. "People, Technologies, and Organizations Interactions in a Social Commerce Era." In Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI-2018), 836–49. Springer International Publishing.

[39] Milind Gayakwad, B. D. Phulpagar. 2013. "Requirement Specific Search." IJARCSSE 3 (11): 121.

[40] [Panicker, Aishwarya, Milind Gayakwad, Sandeep Vanjale, Pramod Jadhav, Prakash Devale, and Suhas Patil. n.d. "Fake News Detection Using Machine Learning Framework."

[41] Gonge, S. et al. (2023). A Comparative Study of DWT and DCT Along with AES Techniques for Safety Transmission of Digital Bank Cheque Image. In: Chaubey, N., Thampi, S.M., Jhanjhi, N.Z., Parikh, S., Amin, K. (eds) Computing Science, Communication and Security. COMS2 2023. Communications in Computer and Information Science, vol 1861. Springer, Cham. https://doi.org/10.1007/978-3-031-40564-8_6

[42] Self-Driving Electrical Car Simulation using Mutation and DNN Paygude, P. Idate, S. Gayakwad, M. Kadam, K. Shinde, A. SSRG International Journal of Electronics and Communication Engineering, 2023, 10(6), pp. 27–34

[43] Probing to Reduce Operational Losses in NRW by using IoT Hingmire, S. Paygude, P. Gayakwad, M. Devale, P. SSRG International Journal of Electronics and Communication Engineering, 2023, 10(6), pp. 23–32

[44] Paygude, P.., Singh, A.., Tripathi, E.., Priya, S.., Gayakwad, M.., Chavan, P.., Chaudhary, S.., Joshi, R.., & Kotecha, K.. (2023).

[45] A Parameter-Based Comparative Study of Deep Learning Algorithms for Stock Price Prediction. International Journal on Recent and Innovation Trends in Computing and Communication, 11(7s), 138–146. https://doi.org/10.17762/ijritcc.v11i7s.6985

[46] Dixit, B., Pawar, R. G., Gayakwad, M., Joshi, R., & Mahajan, A. (2023). Challenges and a Novel Approach for Image Captioning Using Neural Network and Searching Techniques. International Journal of Intelligent Systems and Applications in Engineering, 11(3), 712-720.

[47] Godse, D. ., Mulla, N. ., Jadhav, R. ., Gayakwad, M. ., Joshi, R. ., Kadam, K. ., & Jadhav, J. . (2023). Automated Video and Audio-based Stress Detection using Deep Learning Techniques. International Journal on Recent and Innovation Trends in Computing and Communication, 11(11s), 487–492. https://doi.org/10.17762/ijritcc.v11i11s.8178

[48] Paygude, P. ., Chavan, P. ., Gayakwad, M. ., Gupta, K. ., Joshi, S. ., Gopika, G., Joshi, R., Gonge, S., & Kotecha, K. . (2023). Optimising Hyperparameters for Enhanced LSTM-Based Prediction System Performance. International Journal on Recent and Innovation Trends in Computing and Communication, 11(10s), 203–213. https://doi.org/10.17762/ijritcc.v11i10s.7620

[49] Bhole, G. V., et al. "Implementation of Virtual Mouse Control System Using Hand Gestures for Web Service Discovery." International Journal of Intelligent Systems and Applications in Engineering 12.13s (2024): 663-672.