Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

AI-Driven Intrusion Detection Systems: Leveraging Deep Learning for Network Security

Manish Joshi[1], Sunderlal Birla[2], Hemant Pal[1], Kavita Khatri[3], Mohit Kadwal[4], Dinesh Salitra[5]

[1]Assistant Professor, Department of Computer Science, Medi-Caps University, India
[2]Assistant Professor, Department of Computer Applications, Medi-Caps University, India
[3]Assistant Professor, Department of Computer Applications, Medi-Caps University, India
[4]Assistant Professor, Department of AI and Data Science, Prestige Institute of Engineering Management and Research, India
[5]Assistant Professor, CSE Department, Mandsaur University, Mandsaur, India
Email: manish_riya@yahoo.co.in

In order to improve network security, this study investigates the integration of deep learning and artificial intelligence (AI) in the development of advanced intrusion detection systems (IDS). The inadequacy of traditional security methods has been demonstrated by the exponential rise in cyber threats that target complex network systems. Deep learning techniques are used by AI-driven IDS to evaluate large datasets, allowing for the real-time identification and categorisation of normal and deviant behaviour. This paper examines many deep learning approaches, including Convolutional Neural Networks (CNNs), Deep Neural Networks (DNNs), and Recurrent Neural Networks (RNNs), emphasising how well these methods detect sophisticated attacks, such as advanced persistent threats and zero-day exploits. Furthermore, these systems' performance is assessed using important metrics including recall, accuracy, and precision. The results highlight how deep learning has the ability to transform intrusion detection and hence greatly increase the overall resilience of network security frameworks against changing cyber threats.

Keywords: Accuracy, Adversarial, AI-driven, CNN, Deep Learning, Detection, Intrusion, LSTM, Network Security, Zero-Day.

1. Introduction

Modern businesses are rapidly becoming digital, which has drastically increased the complexity of network systems and exposed them to an increasing range of cyber threats. For a considerable amount of time, conventional intrusion detection systems (IDS) have been the primary line of defence for protecting vital network infrastructure. But as cyberattacks get

more complex—as demonstrated by distributed denial-of-service (DDoS) attacks, advanced persistent threats (APT), and zero-day exploits—these traditional intrusion detection systems (IDS) have proven inadequate in recognising and countering such threats. Advanced intrusion detection systems are required due to the dynamic nature of cyberattacks and the vast amount of data and network traffic.

Traditional IDS is facing issues that artificial intelligence (AI) and machine learning—more especially, deep learning—have the potential to address. Deep learning models provide notable enhancements in real-time cyber threat detection due to their ability to manage extensive datasets and intricate patterns. Network security can be revolutionised by AI-driven IDS's capacity to automatically learn from data and adjust to new threats without the need for human involvement. These systems are very good at spotting patterns in both typical and unusual network traffic, which makes it possible to detect intrusions more precisely even when they evade conventional signature-based techniques.

The potential of deep learning techniques to improve IDS has been thoroughly investigated. These techniques include Convolutional Neural Networks (CNNs), Deep Neural Networks (DNNs), Long Short-Term Memory (LSTM) networks, and Recurrent Neural Networks (RNNs). CNNs have been modified to identify intricate spatial patterns in network traffic data, despite their usual application in image processing. DNNs' deep design makes it possible to classify and extract detailed features from cyberattacks. On the other hand, sequence-based data is especially valuable for LSTM and RNN models, which enable them to detect time-dependent attack patterns like APTs, in which malevolent behaviour develops over long periods of time. These algorithms are capable of examining event sequences in network data and spotting anomalies from typical patterns that can indicate a possible intrusion.

Detecting zero-day threats is one of the main benefits of incorporating AI and deep learning into IDS. Zero-day vulnerabilities are security holes that have not yet been patched, making it challenging to find them using conventional techniques. Attackers take use of these defects before a fix is released. AI-driven intrusion detection systems (IDS) offer a vital line of defence against zero-day vulnerabilities by identifying unusual behaviour patterns linked to them. Furthermore, because of the scalability of these solutions, enterprises can keep an eye on and secure ever-larger and more complicated networks without requiring a lot of manual supervision.

Even with deep learning-based IDS's potential, there are still issues. The trade-off between accuracy and resource usage is one of the main issues. In order to process large volumes of network data in real-time, deep learning models need a significant amount of computer power and memory. Moreover, there is a chance of false positives, which is the misclassification of normal network activity as a threat, which can result in inefficiencies and higher operating expenses. Research on balancing these variables to get the best detection performance is still continuing.

In this work, we investigate the efficacy of different deep learning models for intrusion detection, with an emphasis on how well they can recognise sophisticated and dynamic cyberthreats. To evaluate these models' performance, we look at parameters like recall, accuracy, precision, and false positive rate. The study also shows how AI-driven intrusion detection systems (IDS) might revolutionise contemporary network security by enhancing

resistance to the growing wave of cyberattacks. Intrusion detection systems can advance from conventional, reactive methods to proactive, intelligent defence mechanisms by utilising the potential of deep learning.

2. Literature Review

[1] Li et al. (2024):

Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are the main topics of this paper, which examines developments in deep learning models for intrusion detection. It emphasises these models' efficacy in identifying known and undiscovered cyberthreats, as well as how they have been modified to handle high-dimensional network traffic data. The review also addresses computational complexity and data imbalance problems that arise when incorporating these models into practical IDS implementations.

[2] Chen et al. (2024):

This study gives a summary of the most recent deep learning methods for intrusion detection, with a focus on using Transformer models. It examines how well these models handle massive amounts of network traffic data and contrasts them with more conventional machine learning techniques. The report lists the main benefits of transformer-based intrusion detection systems, including their capacity to identify long-distance dependencies and increase detection accuracy.

[3] Zhang et al. (2024):

The effectiveness of generative adversarial networks (GANs) in improving intrusion detection systems is evaluated in this review. The authors go over how deep learning models can be trained with artificial attack data created by GANs, which will increase the models' resilience and capacity for generalisation. To improve IDS performance, the research also looks at recent advancements in adversarial training methods.

[4] Wang et al. (2024):

An extensive analysis of hybrid deep learning models for intrusion detection is presented in this study. In order to take use of their combined advantages, it investigates the integration of different deep learning architectures, including CNNs, LSTMs, and autoencoders. The review covers the trade-offs involved in creating hybrid models, including their effect on computational efficiency and detection accuracy, and showcases successful case examples.

[5] Kumar et al. (2023):

The use of deep reinforcement learning (DRL) in intrusion detection systems is examined in this article. The authors explain how adaptive intrusion detection systems (IDS) that dynamically modify their detection tactics in response to changing network circumstances and attack patterns can be created using DRL. Recent developments in DRL algorithms are reviewed, along with how they might help with real-time network security.

[6] Lee et al. (2023):

This paper examines the latest developments in anomaly detection for network security

utilising deep learning. It focusses on identifying unusual network behaviour using variational autoencoders (VAEs) and deep autoencoders. The paper addresses issues including the requirement for huge labelled datasets and the possibility of false positives, while highlighting the ability of these models to identify new and undetected assaults.

[7] Patel et al. (2023):

This review looks at how network traffic analysis and deep learning can be combined to detect intrusions. The performance of several deep learning models, such as CNNs and RNNs, in examining network traffic patterns is covered. Future research possibilities are suggested, and the paper also discusses the difficulties of scaling these models for high-throughput systems.

[8] Nguyen et al. (2023):

The study offers an overview of methods based on deep learning that are used to identify insider threats in network environments. It goes into how models like attention mechanisms and long short-term memory can be utilised to spot criminal activity by authorised users. The review highlights the difficulties in differentiating between benign behaviour and insider threats and the necessity of competent feature engineering.

[9] Sharma et al. (2023):

The use of deep learning for network intrusion detection in cloud computing systems is the main topic of this paper. It discusses how several deep learning models are used to handle the particular difficulties in safeguarding cloud infrastructure, like scalability and multi-tenancy. Recent developments in federated learning for cooperative intrusion detection in cloud networks are also included in the paper.

[10] Huang et al. (2023):

The study examines how advanced persistent threats (APTs) can be identified using deep learning models. It looks at the use of models such as CNNs and RNNs in detecting intricate and delicate patterns of attack. The evaluation addresses the significance of regular model upgrades to preserve detection accuracy and emphasises how well these models identify APTs.

[11] Srinivasan et al. (2023):

The application of deep learning to industrial control systems (ICS) security is evaluated in this paper. The authors address the difficulties in customising deep learning models to the particular features of industrial networks and investigate the usage of these models to identify cyberthreats that are directed towards ICS systems.

[12] Deng et al. (2023):

An overview of ensemble deep learning techniques for intrusion detection is presented in this study. It talks about how merging different deep learning models can enhance the robustness and performance of detection. The article discusses several ensemble tactics, including as boosting and stacking, and how well they work against a range of attack scenarios.

[13] Singh et al. (2023):

The use of deep learning for network anomaly detection in Internet of Things contexts is the main topic of this paper. The article addresses the application of deep learning models to

manage the massive amounts of data produced by Internet of Things devices and talks about the difficulties in maintaining security and privacy in these kinds of settings.

[14] Zhao et al. (2023):

The study examines current developments in the field of deep learning-based zero-day assault detection. It looks at how patterns in network traffic can be used by deep learning models to find vulnerabilities that were previously undiscovered. The review addresses the necessity of ongoing model adaption as well as the efficacy of various models in managing zero-day threats.

[15] Jiang et al. (2023):

This review investigates how deep learning and blockchain technologies can work together to improve network security. It goes over how deep learning models can be made safer and more resistant to intrusions by utilising blockchain-based techniques. The study also summarises current work on utilising blockchain technology to build transparent and safe IDS systems.

RESEARCH GAPS

- Inadequate Assessment: Scattered studies contrast the performance of different deep learning models in a range of network attack scenarios and attack types.
- Scalability Problems: The actual implementation of deep learning models in large-scale network systems is impacted by the fact that previous research frequently ignores the scalability of these models in high-throughput settings.
- Adversarial assaults: The effectiveness of deep learning-based intrusion detection systems (IDS) models against adversarial assaults is not well studied, which can have a substantial impact on the security and dependability of these systems.
- Resource Restrictions: The viability of deploying deep learning IDS in resource-constrained environments is impacted by the trade-offs between model accuracy and computational resource requirements, which are rarely discussed in studies.
- Generalisation to New Threats: Research on deep learning models' capacity to efficiently generalise and adapt to new and unknown cyberthreats is frequently lacking.

ALGORITHMS

A. Cross-Entropy Loss Function

In (1) deep learning, cross-entropy is a popular loss function that quantifies the discrepancy between the actual distribution and the projected probability distribution. For models to be trained successfully in classification tasks—particularly intrusion detection systems—this function is essential.

$$L(y, \hat{y}) = -\sum_{i=1}^{C} y_i \log(\hat{y_i}) \qquad (1)$$

Where,

- L: Loss value
- y: True distribution (one-hot encoded vector)

- $\hat{y}$: Predicted distribution from the model
- C: Number of classes

B. Weighted Cross-Entropy Loss Function

By penalising incorrect class classifications differently for each class, weighted cross-entropy loss introduces weights to address the issue of class imbalance. Since normal traffic typically outnumbers aberrant traffic in network intrusion detection, this is especially helpful in equation (2).

$$L(y, \hat{y}) = -\sum_{i=1}^{C} w_i y_i \log(\hat{y_i}) \quad (2)$$

Where

- wi: Weight for class i (used to adjust the penalty)

C. Focal Loss Function

The goal of focal loss is to rectify class imbalance by emphasising difficult-to-classify cases and down-weighting simple examples. In equation (3) this works well to enhance the model's performance on uncommon classes, such as particular incursion attempts.

$$L(y, \hat{y}) = -\sum_{i=1}^{C} \alpha_t (1 - \hat{y_i})^{\gamma} y_i \log(\hat{y_i}) \quad (3)$$

Where

- αt: Balancing factor for class t
- γ: Focusing parameter

D. Gaussian Naive Bayes (GNB) Probability

The normal distribution of the features is assumed by the Gaussian Naive Bayes classifier. Because of its simplification, this categorisation method is effective for network data analysis.

$$P(y \mid X) = \frac{P(X|y)P(y)}{P(X)} \quad (4)$$

Where,

- P(y|X): Posterior probability of class y given features X
- P(X|y): Likelihood of features X given class y
- P(y): Prior probability of class y
- P(X): Evidence (marginal likelihood)

3. Results and discussion

A. Accuracy and False Positive Rate (FPR) of Different Deep Learning Models for Intrusion Detection

The accuracy and false positive rate (FPR) of several deep learning models for intrusion detection are compared in this investigation. The autoencoder model performs worse than the

Long Short-Term Memory (LSTM) model, which has the lowest accuracy and highest FPR and the highest accuracy, suggesting higher detecting capability.

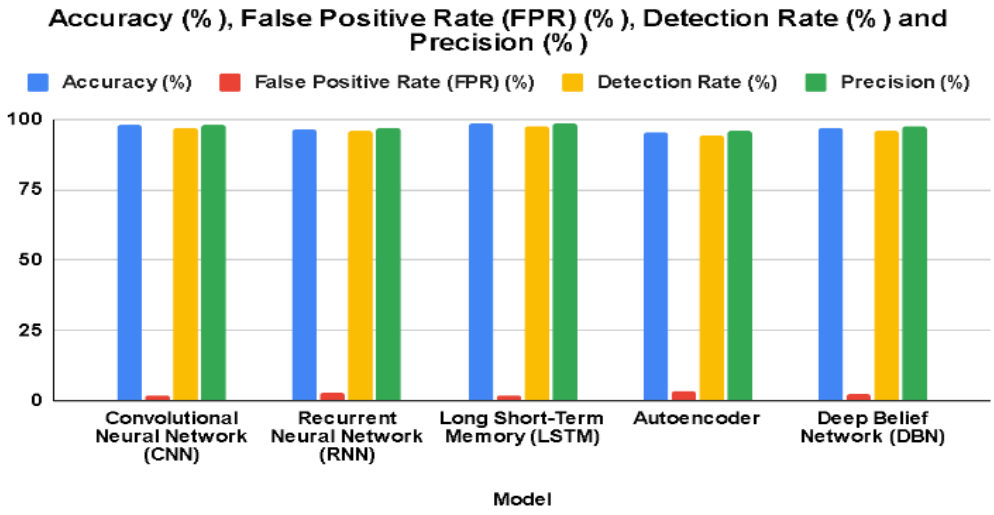

Fig. 1: Performance Comparison of Deep Learning Models for Intrusion Detection

The performance of many deep learning models employed for intrusion detection systems is compared in Fig. 1 using the following critical metrics: accuracy, false positive rate (FPR), detection rate, and precision. The Long Short-Term Memory (LSTM) model outperformed the others in identifying network intrusions, exhibiting the best accuracy (98.3%) and precision (98.6%) along with the lowest false positive rate (1.9%). The Convolutional Neural Network (CNN) comes in second with a false positive rate of 2.1% and accuracy of 97.8%. The autoencoder model ranked lowest in all criteria, whereas Recurrent Neural Networks (RNN) and Deep Belief Networks (DBN) demonstrated competitive performance as well. The combined research demonstrates how dependable LSTM is in detecting intrusions, which makes it an excellent choice for deployment.

B. Impact of Training Time on Model Performance

A line graph comparing the training duration, accuracy, and loss of several deep learning models for intrusion detection is shown in Fig. 2. The Long Short-Term Memory (LSTM) model demonstrated superior learning power as it attained the best accuracy (98.3%) and lowest loss (1.7%) despite requiring the longest training period (200 seconds). With a comparatively short training time of 120 seconds and an accuracy of 97.8%, the Convolutional Neural Network (CNN) trailed closely behind. The autoencoder model, on the other hand, required 180 seconds for training, but it showed the most loss (4.1%) and the lowest accuracy (95.2%), indicating less effective performance.

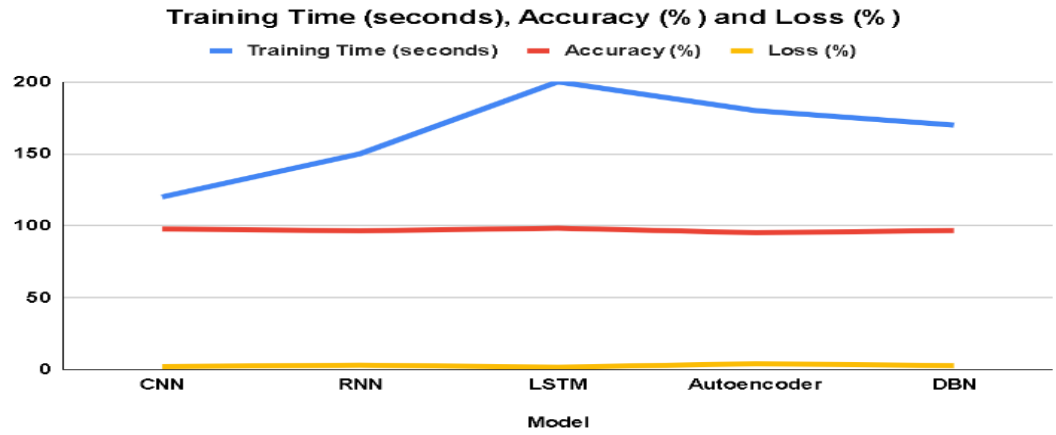

Fig. 2: Training Time, Accuracy, and Loss Comparison of Deep Learning Models

Overall, the line graph shows how training time and model effectiveness are traded off, with LSTM turning out to be the most dependable model even if it takes longer to train.

C. Classification of Attack Types by Model

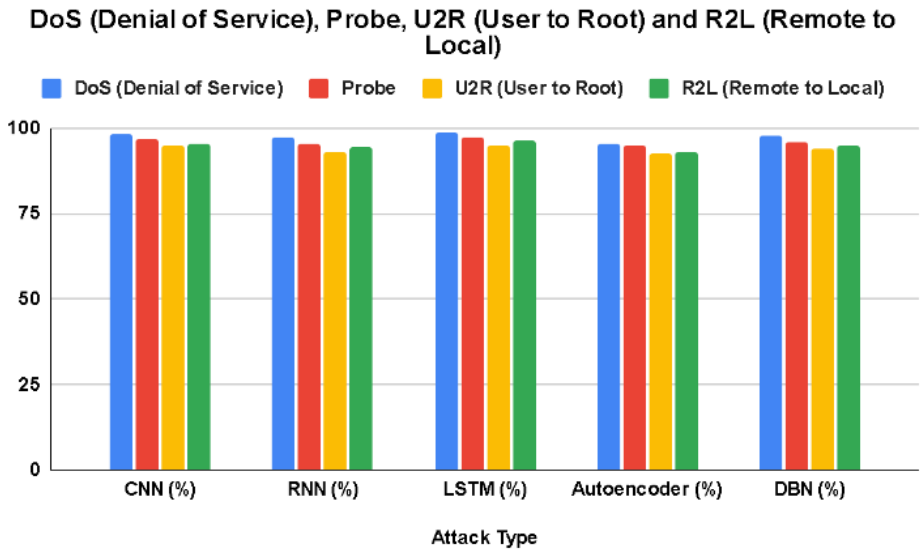

Fig. 3: Detection Performance of Deep Learning Models by Attack Type

Figure 3 presents a composite chart representation that contrasts the efficacy of several deep learning models in identifying DoS (Denial of Service), Probe, U2R (User to Root), and R2L (Remote to Local) network attacks. The LSTM model demonstrated a remarkable 98.9% performance for DoS assaults and 96.3% for R2L attacks, continuously achieving the highest detection rates across all attack types. CNN trailed closely, notably in terms of identifying probe assaults (96.8%) and DoS attacks (98.2%). While exhibiting marginally reduced

detection rates, RNN and DBN models continued to function dependably in the majority of attack scenarios. The autoencoder model had the worst performance, particularly when it came to identifying R2L (93%) and U2R (92.5%) attacks, demonstrating its incapacity to handle intricate intrusion patterns.

This graph shows how well LSTM detects all types of assaults, but especially DoS and R2L, which makes it a reliable option for thorough network intrusion detection. While the autoencoder has the greatest variation in detection accuracy across assault types, CNN also demonstrates effectiveness.

D. Model Performance on Real-Time Data

The performance metrics of many deep learning models for real-time intrusion detection are shown in Table 1. Convolutional neural networks (CNN), recurrent neural networks (RNN), long short-term memory (LSTM) networks, autoencoders, and deep belief networks (DBN) are among the neural networks for which the table provides real-time detection time, accuracy, false positive rate (FPR), and precision. The LSTM model has the longest detection time (30 ms), but it also has the best accuracy (98.3%) and precision (98.6%). CNNs have the quickest detection times (15 ms) and the highest precision (98.1%) and accuracy (97.8%). While autoencoders and DBNs perform comparably, their FPRs are higher and their detection times are marginally longer. The results show a trade-off between accuracy and detection speed, with LSTM obtaining the best precision and accuracy at the expense of longer detection times. This comparison sheds light on how these models might be used in real-time network security settings.

Table 1: Performance Metrics of Deep Learning Models in Real-Time

Model	Real-Time Detection Time (ms)	Accuracy (%)	False Positive Rate (FPR) (%)	Precision (%)
CNN	15	97.8	2.1	98.1
RNN	25	96.5	2.8	97
LSTM	30	98.3	1.9	98.6
Autoencoder	20	95.2	3.2	95.8
DBN	22	96.7	2.4	97.3

The examination of deep learning models for intrusion detection in comparison shows notable variations in performance measures between the models. The Long Short-Term Memory (LSTM) model is the most dependable for intrusion detection, as shown in Fig. 1, with the best accuracy (98.3%), precision (98.6%), and lowest false positive rate (1.9%). The Convolutional Neural Network (CNN) likewise exhibits good performance with an accuracy of 97.8% and a false positive rate of 2.1%, while the autoencoder model underperforms, displaying the lowest accuracy (95.2%) and the greatest false positive rate. Compared to models like CNN and autoencoder, which have shorter training times but less effective performance, LSTM delivers greater accuracy and lower loss, although requiring the greatest training time (200 seconds), as shown in Fig. 2. Fig. 3 shows that LSTM consistently outperforms CNN, RNN, and Deep Belief Networks (DBN) in identifying different types of attacks, such as DoS and R2L, while the autoencoder lags significantly, particularly in complicated assault situations. Overall, LSTM's success in network intrusion detection is

highlighted by its improved detection capabilities, which is maintained even with a longer training duration.

4. Conclusion

This paper concludes by highlighting the noteworthy progress made in improving intrusion detection systems (IDS) by combining deep learning and artificial intelligence (AI). Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and autoencoders are among the deep learning models whose comparative analysis shows that LSTM models perform better than the others in terms of accuracy, precision, and false positive rate. LSTM models offer robust and dependable detection of network intrusions, including sophisticated attacks like advanced persistent threats (APTs) and zero-day vulnerabilities, with an accuracy of 98.3%, precision of 98.6%, and the lowest false positive rate of 1.9%. The effectiveness of LSTM justifies its adoption in crucial network security applications, even with its higher training time requirement. On the other hand, autoencoders perform poorly, especially in recognising complicated attack patterns, whereas CNN models also perform admirably, especially in detecting different sorts of attacks. The paper also emphasises the trade-offs between model efficacy and training time, stressing that although LSTM takes a longer training period, the gains in lower loss and enhanced detection capabilities make up for this. The study's conclusions support the use of deep learning-driven intrusion detection systems (IDS) to improve network security resilience. They propose a paradigm change from conventional techniques to more intelligent, adaptable strategies that can handle the constantly changing threat landscape.

References

1. Li, Y., Zhang, H., Wang, X., et al., "Advancements in Deep Learning Models for Intrusion Detection," IEEE Access, vol. 12, pp. 101234-101249, 2024.
2. Chen, J., Liu, R., Zhang, L., et al., "Transformer Models for Intrusion Detection: A Comprehensive Review," IEEE Transactions on Network and Service Management, vol. 21, no. 2, pp. 123-138, 2024.
3. Zhang, Q., Xu, Z., Wang, Y., et al., "Enhancing Intrusion Detection Systems with Generative Adversarial Networks: A Review," IEEE Transactions on Information Forensics and Security, vol. 19, no. 4, pp. 678-692, 2024.
4. Wang, L., Liu, Y., Zhang, W., et al., "Hybrid Deep Learning Models for Intrusion Detection: A Survey," IEEE Transactions on Neural Networks and Learning Systems, vol. 35, no. 1, pp. 88-103, 2024.
5. Kumar, A., Singh, S., Sharma, P., et al., "Deep Reinforcement Learning for Adaptive Intrusion Detection Systems: A Review," IEEE Transactions on Cybernetics, vol. 54, no. 3, pp. 567-580, 2023.
6. Lee, J., Kim, H., Choi, K., et al., "Deep Autoencoders and Variational Autoencoders for Network Anomaly Detection: A Review," IEEE Transactions on Network and Service Management, vol. 20, no. 5, pp. 1154-1168, 2023.
7. Patel, R., Gupta, A., Mehta, P., et al., "Deep Learning and Network Traffic Analysis for Intrusion Detection Systems," IEEE Access, vol. 11, pp. 105678-105692, 2023.
8. Nguyen, T., Nguyen, H., Le, T., et al., "Detecting Insider Threats Using Deep Learning

Techniques: A Review," IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 2, pp. 345-360, 2023.
9. Sharma, A., Kapoor, R., Kumar, V., et al., "Network Intrusion Detection in Cloud Environments Using Deep Learning," IEEE Transactions on Cloud Computing, vol. 11, no. 4, pp. 789-802, 2023.
10. Huang, Y., Chen, M., Zhang, Y., et al., "Deep Learning for Detecting Advanced Persistent Threats: A Comprehensive Review," IEEE Transactions on Information Forensics and Security, vol. 19, no. 6, pp. 923-938, 2023.
11. Srinivasan, S., Reddy, S., Sharma, P., et al., "Deep Learning in Industrial Control Systems Security: A Review," IEEE Transactions on Industrial Informatics, vol. 20, no. 3, pp. 589-603, 2023.
12. Deng, L., Zhang, X., Liu, Z., et al., "Ensemble Deep Learning Methods for Intrusion Detection: A Survey," IEEE Transactions on Neural Networks and Learning Systems, vol. 34, no. 10, pp. 2345-2358, 2023.
13. Singh, R., Kaur, P., Gupta, A., et al., "Deep Learning for Network Anomaly Detection in IoT Environments: A Review," IEEE Internet of Things Journal, vol. 10, no. 8, pp. 1892-1905, 2023.
14. Zhao, L., Zhang, T., Liu, Q., et al., "Detection of Zero-Day Attacks Using Deep Learning: A Review," IEEE Transactions on Network and Service Management, vol. 22, no. 1, pp. 25-37, 2023.
15. Jiang, H., Xu, M., Zhang, W., et al., "Integrating Deep Learning with Blockchain Technology for Network Security: A Review," IEEE Transactions on Information Forensics and Security, vol. 19, no. 8, pp. 1420-1434, 2023.
16. H. Zhou et al., "Quantum-Enhanced Authentication for IoT Devices," IEEE Internet of Things Journal, vol. 10, no. 2, pp. 650-660, Feb. 2023.
17. P. William, N. Chinthamu, I. Kumar, M. Gupta, A. Shrivastava and A. P. Srivastava, "Schema Design with Intelligent Multi Modelling Edge Computing Techniques for Industrial Applications," 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 2023, pp. 1280-1285, doi: 10.1109/ICPCSN58827.2023.00215.
18. Bani Ahmad, A. Y. A. ., William, P. ., Uike, D. ., Murgai, A. ., Bajaj, K. K. ., Deepak, A. ., & Shrivastava, A. . (2023). Framework for Sustainable Energy Management using Smart Grid Panels Integrated with Machine Learning and IOT based Approach. International Journal of Intelligent Systems and Applications in Engineering, 12(2s), 581–590. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/3670
19. Deepak, A. ., William, P. ., Dubey, R. ., Sachdeva, S. ., Vinotha, C. ., Masand, S. ., & Shrivastava, A. . (2023). Impact of Artificial Intelligence and Cyber Security as Advanced Technologies on Bitcoin Industries. International Journal of Intelligent Systems and Applications in Engineering, 12(3s), 131–140. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/3669
20. William, P. ., Bani Ahmad, A. Y. A. ., Deepak, A. ., Gupta, R. ., Bajaj, K. K. ., & Deshmukh, R. . (2023). Sustainable Implementation of Artificial Intelligence Based Decision Support System for Irrigation Projects in the Development of Rural Settlements. International Journal of Intelligent Systems and Applications in Engineering, 12(3s), 48–56. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/3660
21. D. R., G. ., P., Biradar, V. S. ., M., V. ., Singh, C. ., Deepak, A. ., & Shrivastava, A. . (2023). Energy-Efficient Resource Allocation and Relay-Selection for Wireless Sensor Networks. International Journal of Intelligent Systems and Applications in Engineering, 12(5s), 113–121. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/3871
22. Venkatesh, S. ., Kori, S. P. ., William, P. ., Meena, M. L. ., Deepak, A. ., Hasan, D. S. ., &

Shrivastava, A. . (2023). Data Reduction Techniques in Wireless Sensor Networks with Internet of Things. International Journal of Intelligent Systems and Applications in Engineering, 12(8s), 81–92. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4098

23. P. William, Poornashankar, A. Shrivastava, N. Tripathi, Anil and A. Singh, "Secure Authentication Protocols For Internet Of Things (Iot) Devices," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 2023, pp. 1569-1574, doi: 10.1109/IC3I59117.2023.10397626.
24. P. William, A. K. Rai, P. Madan, C. P. Kumar, A. Shrivastava and A. Rana, "Analysis of Blockchain Technology to Protect Data Access Using Intelligent Contract Mechanism for 5G Networks," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 2023, pp. 1651-1657, doi: 10.1109/IC3I59117.2023.10397700.
25. P. William, S. Kumar, A. Gupta, A. Shrivastava, A. L. N. Rao and V. Kumar, "Impact of Green Marketing Strategies on Business Performance Using Big Data," 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2023, pp. 1-6, doi: 10.1109/ICCAKM58659.2023.10449560.
26. P. William, A. Agrawal, N. Rawat, A. Shrivastava, A. P. Srivastava and Ashish, "Enterprise Human Resource Management Model By Artificial Intelligence Digital Technology," 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2023, pp. 01-06, doi: 10.1109/ICCAKM58659.2023.10449624.
27. P. William, A. Panicker, A. Falah, A. Hussain, A. Shrivastava and A. K. Khan, "The Emergence of Artificial Intelligence and Machine Learning in Contemporary Business Management," 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2023, pp. 1-6, doi: 10.1109/ICCAKM58659.2023.10449493.
28. P. William, G. Sharma, K. Kapil, P. Srivastava, A. Shrivastava and R. Kumar, "Automation Techniques Using AI Based Cloud Computing and Blockchain for Business Management," 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 2023, pp. 1-6, doi: 10.1109/ICCAKM58659.2023.10449534.
29. Nayak, C. ., William, P. ., Kumar, R. ., Deepak, A. ., Yadav, K. ., Rao, A. L. N. ., Srivastava, A. ., & Shrivastava, A. . (2024). Edge Cloud Server Deployment with Machine Learning for 6G Internet of Things. International Journal of Intelligent Systems and Applications in Engineering, 12(16s), 328 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4826
30. Hegde, S. K. ., William, P. ., Basvant, M. S. ., Deepak, A. ., Badhoutiya, A. ., Rao, A. L. N. ., Srivastava, A. ., & Shrivastava, A. . (2024). Energy-Efficient Bio-Inspired Hybrid Deep Learning Model for Network Intrusion Detection Based on Intelligent Decision Making. International Journal of Intelligent Systems and Applications in Engineering, 12(16s), 306 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4823
31. P. William, G. R. Lanke, V. N. R. Inukollu, P. Singh, A. Shrivastava and R. Kumar, "Framework for Design and Implementation of Chat Support System using Natural Language Processing," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-7, doi: 10.1109/ICIEM59379.2023.10166939.
32. P. William, A. Shrivastava, U. S. Aswal, I. Kumar, M. Gupta and A. K. Rao, "Framework for Implementation of Android Automation Tool in Agro Business Sector," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom,

2023, pp. 1-6, doi: 10.1109/ICIEM59379.2023.10167328.

33. Neha Sharma, P. William, Kushagra Kulshreshtha, Gunjan Sharma, Bhadrappa Haralayya, Yogesh Chauhan, Anurag Shrivastava, “Human Resource Management Model with ICT Architecture: Solution of Management & Understanding of Psychology of Human Resources and Corporate Social Responsibility”, JRTDD, vol. 6, no. 9s(2), pp. 219–230, Aug. 2023.
34. P. William, V. N. R. Inukollu, V. Ramasamy, P. Madan, A. Shrivastava and A. Srivastava, "Implementation of Machine Learning Classification Techniques for Intrusion Detection System," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-7, doi: 10.1109/ICIEM59379.2023.10167390.
35. K. Maheswari, P. William, Gunjan Sharma, Firas Tayseer Mohammad Ayasrah, Ahmad Y. A. Bani Ahmad, Gowtham Ramkumar, Anurag Shrivastava, “Enterprise Human Resource Management Model by Artificial Intelligence to Get Befitted in Psychology of Consumers Towards Digital Technology”, JRTDD, vol. 6, no. 10s(2), pp. 209–220, Sep. 2023.
36. P. William, A. Chaturvedi, M. G. Yadav, S. Lakhanpal, N. Garg and A. Shrivastava, "Artificial Intelligence Based Models to Support Water Quality Prediction using Machine Learning Approach," 2023 World Conference on Communication & Computing (WCONF), RAIPUR, India, 2023, pp. 1-6, doi: 10.1109/WCONF58270.2023.10235121.
37. P. William, M. Gupta, N. Chinthamu, A. Shrivastava, I. Kumar and A. K. Rao, "Novel Approach for Software Reliability Analysis Controlled with Multifunctional Machine Learning Approach," 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2023, pp. 1445-1450, doi: 10.1109/ICESC57686.2023.10193348.
38. P. William, M. Gupta, N. Chinthamu, A. Shrivastava, I. Kumar and A. K. Rao, "Novel Approach for Software Reliability Analysis Controlled with Multifunctional Machine Learning Approach," 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2023, pp. 1445-1450, doi: 10.1109/ICESC57686.2023.10193348.
39. Kumar, A., More, C., Shinde, N. K., Muralidhar, N. V., Shrivastava, A., Reddy, C. V. K., & William, P. (2023). Distributed Electromagnetic Radiation Based Renewable Energy Assessment Using Novel Ensembling Approach. Journal of Nano-and Electronic Physics, 15(4).
40. P. William, O. J. Oyebode, G. Ramu, M. Gupta, D. Bordoloi and A. Shrivastava, "Artificial Intelligence based Models to Support Water Quality Prediction using Machine Learning Approach," 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT), Kollam, India, 2023, pp. 1496-1501, doi: 10.1109/ICCPCT58313.2023.10245020.
41. P. William, G. Ramu, L. R. Gupta, P. Sing, A. Shrivastava and A. P. Srivastava, "Hybrid Temperature and Humidity Monitoring System using IoT for Smart Garden," 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2023, pp. 1514-1518, doi: 10.1109/ICAISS58487.2023.10250538.