BIBLIOGRAPHY

Swathy Akshaya M and Padmavathi G. Zero-day attack path identification using probabilistic and graph approach based back propagation neural network in cloud. Mathematical Statistician and Engineering Applications. 2022; 71.3s2, 1091-1106.

Akshaya S and Padmavathi G. Enhancing zero-day attack prediction a hybrid game theory approach with neural networks. International Journal of Intelligent Systems and Applications in Engineering. 2024; 12, 643-663.

Akshaya S and Padmavathi G. ResNet50-based deep convolutional neural network for zero-day attack prediction and detection. International Journal of Advanced Technology and Engineering Exploration. 2025; 12(124):507-527.

S. Akshaya and Padmavathi, "Enhancing Cyber Defense Against Zero-Day Attacks using Ensemble Neural Networks," International Journal of Computer Networks & Communications (IJCNC), vol. 17, no. 4, 2025.

Swathy Akshaya, M., Padmavathi, G. (2019). Taxonomy of Security Attacks and Risk Assessment of Cloud Computing. In: Peter, J., Alavi, A., Javadi, B. (eds) Advances in Big Data and Cloud Computing. Advances in Intelligent Systems and Computing, vol 750. Springer, Singapore.

S. A. M and P. G, A Survey on Various Intrusion Detection System Tools and Methods in Cloud Computing, 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2019, pp. 439-445.

M, Swathy Akshaya and G, Padmavathi, A Study on Zero-Day Attacks (2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur – India.

Swathy Akshaya, M., and Ganapathi, P. (2020). A Review of Machine Learning Methods Applied for Handling Zero-Day Attacks in the Cloud Environment. Handbook of Research on Machine and Deep Learning Applications for Cyber Security, 364-387.

Saxena, R., & Gayathri, E. (2021). Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution. Materials Today: Proceedings, 51, 682–689. https://doi.org/10.1016/j.matpr.2021.06.204

Sun, X., Dai, J., Liu, P., Singhal, A., & Yen, J. (2018). Using Bayesian networks for probabilistic identification of zero-day attack paths. IEEE Transactions on Information Forensics and Security, 13(10), 2506-2521.

Patel, R. N., Zhang, X., Sun, X., & Dai, J. (2024, June). Exploring Scalable Bayesian Networks For Identification of Zero-day Attack Paths. In 2024 Silicon Valley Cybersecurity Conference (SVCC) (pp. 1-8). IEEE.

Sun, X., Dai, J., Liu, P., Singhal, A., & Yen, J. (2016, October). Towards probabilistic identification of zero-day attack paths. In 2016 IEEE Conference on Communications and Network Security (CNS) (pp. 64-72). IEEE.

Ibraheem, I. O., & Tosho, A. U. (2024). Zero day attack vulnerabilities: mitigation using machine learning for performance evaluation. Journal of Computers for Society, 5(1), 43-58.

Dass, S., Datta, P., &Namin, A. S. (2021, July). Attack prediction using hidden markov model. In 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1695-1702). IEEE.

Seyyar, Y. E., Yavuz, A. G., &Ünver, H. M. (2022). An attack detection framework based on BERT and deep learning. IEEE Access, 10, 68633-68644.

Zhao, J., Tang, T., Bu, B., & Li, Q. (2024). Graph neural network- based attack prediction for communication- based train control systems. CAAI Transactions on Intelligence Technology.

Kummerow, A., Abrha, E., Eisenbach, M., &Rösch, D. (2024). Unsupervised Anomaly Detection and Explanation in Network Traffic with Transformers. Electronics, 13(22), 4570.

Wang, X., Pi, D., Zhang, X., Liu, H., &Guo, C. (2022). Variational transformer-based anomaly detection approach for multivariate time series. Measurement, 191, 110791.

Pawan Kumar Tiwari, P. S. . (2022). Numerical Simulation of Optimized Placement of Distibuted Generators in Standard Radial Distribution System Using Improved Computations. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(5), 10–17.

Nahid Hossain et al. "SLEUTH: Real-time Attack Scenario Reconstruction from COTS Audit Data," USENIX Security Symposium, 2017.

Ghazaly, N. M. . (2022). Data Catalogue Approaches, Implementation and Adoption: A Study of Purpose of Data Catalogue. International Journal on Future Revolution in Computer Science &Amp; Communication, 8(1), 01–04.

Shiqing Ma et al. "MPI: Multiple Perspective Attack Investigation with Semantics Aware Execution Partitioning" Proceedings of the 26th USENIX Security Symposium, 2017.

Bhargav R. Avasarala, Brock D. BOSE, John C. Day Donald Steiner," System and method for automated machine-learning, zero-day malware detection," BlueVectorInc, United States Patent, 2017.

Arellano-Zubiate, J. ., J. .Izquierdo-Calongos, A. . Delgado, and E. L. .Huamaní. "Vehicle Anti-Theft Back-Up System Using RFID Implant Technology". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 5, May 2022, pp. 36-40.

Singh et al. "Zero-day Attacks Detection and Prevention Methods – Apriorit," 2017.

Gill, D. R. . (2022). A Study of Framework of Behavioural Driven Development: Methodologies, Advantages, and Challenges. International Journal on Future Revolution in Computer Science &Amp; Communication, 8(2), 09–12.

Ravinder Kaur and Maninder Singh, "A Survey on Zero-Day Polymorphic Worm Detection Techniques," IEEE Communications Surveys and Tutorials, 2014. Vol. 71 No. 3s 2 (2022).

Mishra and B. B. Gupta," Hybrid Solution to Detect and Filter Zero-day Phishing Attacks," International Conference on Emerging Research in Computing, Information, Communication and Applications, Elsevier, 2014.

Wang et al. "k-Zero-Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities," IEEE Transactions on Dependable and Secure Computing, Volume: 11, Issue: 1, P.no: 30 - 44, 2014.

Mikhail Zolotukhin and Timo Hamalainen, "Detection of Zero-day Malware Based on the Analysis of Opcode Sequences" IEEE 11th Consumer Communications and Networking Conference (CCNC), 2014.

P. M. Paithane and D. Kakarwal, "Automatic Pancreas Segmentation using A Novel Modified Semantic Deep Learning Bottom-Up Approach", Int J Intell SystAppl Eng, vol. 10, no. 1, pp. 98–104, Mar. 2022.

Nouby M. Ghazaly, A. H. H. . (2022). A Review of Using Natural Gas in Internal Combustion Engines. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(2), 07–12. 17. Jun Dai, Xiaoyan Sun, and Peng Liu, “Patrol: Revealing Zero-Day Attack Paths through Network-Wide System Object Dependencies," Springer, 2013.

Ananthakrishnan, B., V. .Padmaja, S. .Nayagi, and V. . M. “Deep Neural Network Based Anomaly Detection for Real Time Video Surveillance”. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 4, Apr. 2022, pp. 54-64,

Yuan Ning, Yufeng Liu, Qiang Ji., "Bayesian - BP Neural Network Based Short-term Load Forecasting for Power System," 3rd International Conference on Advanced Computer Theory and Engineering (1CACTE), IEEE, 2010.

J. Jung, V. Paxson, A. Berger, and H. Balakrishnan, “Fast portscan detection using sequential hypothesis testing,” in Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, May 2004, pp. 211–225.

G. R. Hendry and S. J. Yang, "Intrusion signature creation via clustering anomalies," in Proc. of SPIE 2008, pp. 69730C-1.

J. Song, H. Ohba, H. Takakura, Y. Okabe, K. Ohira, and Y. Kwon, "A comprehensive approach to detect unknown attacks via intrusion detection alerts," presented at the Proceedings of the 12th Asian computing science conference on Advances in computer science: computer and network security, Doha, Qatar, 2007.

AlEroud and G. Karabatis, "Discovering Unknown Cyber Attacks using Contextual Misuse and Anomaly Detection " ASE Science Journal vol. 1, pp. 106-120, 2012.

AlEroud and G. Karabatis, "A Contextual Anomaly Detection Approach to Discover Zero-Day Attacks," in 2012 ASE International Conference on Cyber Security, Washington, D.C., USA, 2012.

D. M. J. Tax and R. P. W. Duin, "Data description in subspaces," in Proceedings. 15th International Conference on Pattern Recognition, pp. 672-675 vol.2.

X. B. Li, "A scalable decision tree system and its application in pattern recognition and intrusion detection," Decision Support Systems, vol. 41, pp. 112-130, 2005.

L. Koc, T. A. Mazzuchi, and S. Sarkani, "A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier," ExpertSystems with Applications, vol. 39, pp. 13492-13500.

E. Eskin, A. Arnold, M. Prerau, et al., "A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data," Applications of Data Mining in computer security, vol. 6, pp. 77-102, 2002.

S. A. Zonouz, R. Berthier, H. Khurana, W. H. Sanders, and T. Yardley,"Seclius: an information flow-based, consequence-centric securitymetric," Parallel and Distributed Systems, IEEE Transactions on, vol.26, pp. 562-573, 2015.

D. M. Lewis, and V. P. Janeja, "An empirical evaluation of similarity coefficients for binary valued data," IGI Global,2011, pp. 44-66.

P. Ning, Y. Cui, D. S. Reeves, et al., "Techniques and tools for analyzing intrusion alerts," ACM Trans. Inf. Syst. Secur., vol. 7, no. 2, pp. 274-318, 2004.

J. Mchugh "Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations performed by Lincoln Laboratory," ACM Trans.Inf. Syst. Secur., vol. 3, no. 4, pp. 262-294, 2000.

M. Wu, and C. Jermaine, "Outlier detection by sampling with accuracy guarantees," In Proc. of the 12th ACM SIGKDD Int'l conf. Knowledge discovery and data mining, Philadelphia, PA, USA, 2006, pp. 767-772.

K. Zhang, X. Liang, R. Lu, and X. Shen, “Sybil attacks and their defenses in the internet of things,” IEEE Internet of Things Journal, vol. 1, no. 5, pp. 372–383, 2014.

A.-R. Sadeghi, C. Wachsmann, and M. Waidner, “Security and privacy challenges in industrial internet of things,” in Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC ’15), pp. 1–6, IEEE, San Francisco, Calif, USA, June 2015.

Kotenko and A. Chechulin, “Attack modeling and security evaluation in Siem systems,” International Transactions on Systems Science and Applications, vol. 8, pp. 129–147, 2012.

F. Kamm¨uller, M. Kerber, and C. W. Probst, “Insider threats and auctions: Formalization, mechanized proof, and code generation,” Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 8, no. 1, pp. 44 78, 2017.

L. Bilge and T. Dumitras, "Before we knew it: an empirical study ofzero-day attacks in the real world," in Proceedings of the 2012 ACM conference on Computer and communications security, 2012

G. Bonfante, M. Kaczmarek, and J.-Y. Marion, “Morphological detection of malware,” in Proceedings of the 3rd International Conference on Malicious and Unwanted Software, MALWARE2008, pp. 1–8, USA, October 2008.

Santos, F. Brezo, J. Nieves, et al., "Idea: Opcode sequence based malware detection,” Lecture Notes in Computer Science(including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface, vol. 5965, pp. 35 43,2010.

Niki, “Drive-by download attacks: Effects and detection methods," in Proceedings of the 3rd IT Security Conference for the Next Generation, 2009.

E. Al Daoud, I. H. Jebril, and B. Zaqaibeh, “Computer virus strategies and detection methods,” International Journal of Open Problems in Computer Science and Mathematics, vol. 1, no. 2, pp.12–20, 2008.

N. Nissim, R. Moskovitch, L. Rokach, and Y. Elovici, “Novel active learning methods for enhanced PC malware detection in windows OS,” Expert Systems with Applications, vol. 41, no. 13,pp. 5843–5857, 2014

Santos, F. Brezo, X. Ugarte-Pedrero, and P. G. Bringas, "Opcode sequences as a representation of executables for data mining-based unknown malware detection,” Information Sciences,vol. 231, pp. 64–82, 2013.

M. Alazab, S. Venkatraman, P. Watters, and M. Alazab, "Zero-day malware detection based on supervised learning algorithms of API call signatures," in Proceedings of the Ninth Australasian Data Mining Conference-Volume 121, 2011, pp. 171-182.

M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang, "Riskranker: scalable and accurate zero-day android malware detection," in Proceedings of the 10th international conference on Mobile systems, applications, and services, 2012, pp. 281-294.

Y. Park, D. S. Reeves, and M. Stamp, “Deriving common malware behavior through graph clustering,” Computers &Security, vol. 39, pp. 419–430, 2013.

Z. Chen, M. Roussopoulos, Z. Liang, Y. Zhang, Z. Chen, and A. Delis, “Malware characteristics and threats on the internet ecosystem,” The Journal of Systems and Software, vol. 85, no. 7,pp. 1650 1672, 2012.

X. M. Choo, K. L. Chiew, D. H. A. Ibrahim, N. Musa, S. N. Sze, and W. K. Tiong, "Feature-based phishing detection technique," Journal of Theoretical and Applied Information Technology, vol.91, no. 1, pp. 101–106, 2016.

Khoury, J., &Nassar, M. (2020). A Hybrid Game Theory and Reinforcement Learning Approach for Cyber-Physical Systems Security. NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium.

Stier, J., Gianini, G., Granitzer, M., & Ziegler, K. (2018). Analysing Neural Network Topologies: a Game Theoretic Approach. Procedia Computer Science, 126, 234 243.

Xu, J., Alsabbagh, A., & Ma, C. (2022). Prediction Based Game-Theoretic Strategy for Energy Management of Hybrid Electric Vehicles. IEEE Journal of Emerging and Selected Topics in Industrial Electronics, 3(1), 79–89.

Gaao, L., Li, Y., Zhang, L., Lin, F., & Ma, M. (2019). Research on Detection and Defense Mechanisms of DoS Attacks Based on BP Neural Network and Game Theory. IEEE Access, 7, 43018–43030.

Das N, Sarkar T. Survey on host and network based intrusion detection system. International Journal of Advanced Networking and Applications. 2014; 6(2):2266- 9.

Ahmed M, Mahmood AN, Hu J. A survey of network anomaly detection techniques. Journal of Network and Computer Applications. 2016; 60:19-31.

Ahmad R, Alsmadi I, Alhamdani W, Tawalbeh LA. Zero-day attack detection: a systematic literature review. Artificial Intelligence Review. 2023; 56(10):10733-811.

Bou-harb E, Debbabi M, Assi C. Cyber scanning: a comprehensive survey. IEEE Communications Surveys & Tutorials. 2013; 16(3):1496-519.

Soltani M, Ousat B, Siavoshani MJ, Jahangir AH. An adaptable deep learning-based intrusion detection system to zero-day attacks. Journal of Information Security and Applications. 2023; 76:103516.

Khraisat A, Gondal I, Vamplew P, Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity. 2019; 2(1):1 22.

Kumar GS, Kumar RK, Kumar KP, Sai NR, Brahmaiah M. Deep residual convolutional neural network: an efficient technique for intrusion detection system. Expert Systems with Applications. 2024; 238:121912.

Hubballi N, Suryanarayanan V. False alarm minimization techniques in signature-based intrusion detection systems: a Communications. 2014; 49:1-7. survey. Computer

Ibrahim HB, Aslan HK, Elsayed MS, Jurcut AD, Azer MA. Anomaly detection of zero-day attacks based on CNN and regularization techniques. Electronics. 2023; 12(3):1-18.

Bhuyan MH, Bhattacharyya DK, Kalita JK. Network anomaly detection: methods, systems and tools. IEEE Communications Surveys & Tutorials. 2013; 16(1):303-36.

Verma P, Bharot N, Breslin JG, O'shea D, Vidyarthi A, Gupta D. Zero-day guardian: a dual model enabled federated learning framework for handling zero-day attacks in 5G enabled IIoT. IEEE Transactions on Consumer Electronics. 2023; 70(21):3856-66.

Peppes N, Alexakis T, Adamopoulou E, Demestichas K. The effectiveness of zero-day attacks data samples generated via GANs on deep learning classifiers. Sensors. 2023; 23(2):1-21.

Creech G, Hu J. A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns. IEEE Transactions on Computers. 2013; 63(4):807-19.

Mukkamala S, Janoski G, Sung A. Intrusion detection using neural networks and support vector machines. In proceedings of the international joint conference on neural networks 2002 (pp. 1702-7). IEEE.

Bajaj K, Arora A. Dimension reduction in intrusion detection features using discriminative machine learning approach. International Journal of Computer Science Issues. 2013; 10(4):324-8.

Lecun Y, Bengio Y, Hinton G. Deep learning. Nature. 2015; 521(7553):436-44.

Farahnakian F, Heikkonen J. A deep auto-encoder based approach for intrusion detection system. In 20th international conference on advanced communication technology 2018 (pp. 178-83). IEEE.

Hnamte V, Nhung-nguyen H, Hussain J, Hwa-kim Y. A novel two-stage deep learning model for network intrusion detection: LSTM-AE. IEEE Access. 2023; 11:37131-48.

Nagasundari S, Honnavali PB. SQL injection attack detection using ResNet. In 10th international conference on computing, communication and networking technologies 2019 (pp. 1-7). IEEE.

Shun J, Malki HA. Network intrusion detection system using neural networks. In fourth international conference on natural computation 2008 (pp. 242-6). IEEE.

Alshehri A, Badr MM, Baza M, Alshahrani H. Deep anomaly detection framework utilizing federated learning for electricity theft zero-day cyberattacks. Sensors. 2024; 24(10):1-19.

Sakthimurugan S, Kumaar S, Vignesh V, Santhi P. Assessment of zero-day vulnerability using machine learning approach. EAI Endorsed Transactions on Internet of Things. 2024; 10:1-6.

Aburomman AA, Reaz MB. A novel SVM-kNN-PSO ensemble method for intrusion detection system. Applied Soft Computing. 2016; 38:360-72.

Alazab A, Khresiat A. New strategy for mitigating of SQL injection attack. International Journal of Computer Applications. 2016; 154(11):1-10.

Ji SY, Jeong BK, Choi S, Jeong DH. A multi-level intrusion detection method for abnormal network behaviors. Journal of Network and Computer Applications. 2016; 62:9-17.

Butun I, Morgera SD, Sankar R. A survey of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys & Tutorials. 2013; 16(1):266-82.

Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Computers & Security. 2012; 31(3):357-74.

Skaruz J, Seredynski F. Recurrent neural networks towards detection of SQL attacks. In international parallel and distributed processing symposium 2007 (pp. 1-8). IEEE.

Elsherif A. Automatic intrusion detection system using deep recurrent neural network paradigm. Journal of Information Security and Cybercrimes Research. 2018; 1(1):21-31.

Osa E, Orukpe PE, Iruansi U. Design and implementation of a deep neural network approach for intrusion detection systems. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024; 7:1-6.

Idhammad M, Afdel K, Belouch M. Semi-supervised machine learning approach for DDoS detection. Applied Intelligence. 2018; 48:3193-208.

Lin WC, Ke SW, Tsai CF. CANN: an intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-Based Systems. 2015; 78:13-21.

Staudemeyer RC. Applying long short-term memory recurrent neural networks to intrusion detection. South African Computer Journal. 2015; 56(1):136-54.

Sarhan M, Layeghy S, Gallagher M, Portmann M. From zero-shot machine learning to zero-day attack detection. International Journal of Information Security. 2023; 22(4):947-59.

Jose J, Jose DV. AS-CL IDS: anomaly and signature based CNN-LSTM intrusion detection system for internet of things. International Journal of Advanced Technology and Engineering Exploration. 2023; 10(109):1-18.

Alazab A, Abawajy J, Hobbs M, Layton R, Khraisat A. Crime toolkits: the productisation of cybercrime. In 12th international conference on trust, security and privacy in computing and communications 2013 (pp. 1626-32). IEEE.

Pascanu R, Stokes JW, Sanossian H, Marinescu M, Thomas A. Malware classification with recurrent networks. In international conference on acoustics, speech and signal processing 2015 (pp. 1916-20). IEEE.

Arun A, Nair AS, Sreedevi AG. Zero day attack detection and simulation through deep learning techniques. In 4th international conference on cloud computing, data science & engineering (confluence) 2024 (pp. 852-7). IEEE

Oluwadare S, Elsayed Z. A survey of unsupervised learning algorithms for zero-day attacks in intrusion detection systems. In the international FLAIRS conference proceedings 2023 (pp. 1-3). FLAIRS.

Aljawarneh SA. Emerging challenges, security issues, and technologies in online banking systems. In online banking security measures and data protection 2017 (pp. 90-112). IGI Global.

Demirel DY, Sandikkaya MT. Web based anomaly detection using zero-shot learning with CNN. IEEE Access. 2023; 11:91511-25.

Bai S, Kolter JZ, Koltun V. Convolutional sequence modeling revisited. ICLR Workshop. 2018 (pp. 1-20).

Roy SS, Mallik A, Gulati R, Obaidat MS, Krishna PV. A deep learning based artificial neural network approach for intrusion detection. In mathematics and computing: third international conference, ICMC 2017 (pp. 44-53). Springer Singapore.

Habibi O, Chemmakha M, Lazaar M. Performance evaluation of CNN and pre-trained models for malware classification. Arabian Journal for Science and Engineering. 2023; 48(8):10355-69.

Hindy H, Atkinson R, Tachtatzis C, Colin JN, Bayne E, Bellekens X. Utilising deep learning techniques for effective zero-day attack detection. Electronics. 2020; 9(10):1-16.

Yin C, Zhu Y, Fei J, He X. A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access. 2017; 5:21954-61.

Dhanya KA, Vajipayajula S, Srinivasan K, Tibrewal A, Kumar TS, Kumar TG. Detection of network attacks using machine learning and deep learning models. Procedia Computer Science. 2023; 218:57-66.

Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. In symposium on computational intelligence for security and défense applications 2009 (pp. 1-6). IEEE.

Shaikh A, Gupta P. Real-time intrusion detection based on residual learning through ResNet algorithm. International Journal of System Assurance Engineering and Management. 2022:1-5.

Haeser G, Ramos A. Constraint qualifications for Karush–Kuhn–Tucker conditions in multiobjective optimization. Journal of Optimization Theory and Applications. 2020; 187:469-87.

Hu Z, Chen P, Zhu M, Liu P. Reinforcement Learning for Adaptive Cyber Defense Against Zero Day Attacks. Adversarial and Uncertain Reasoning for Adaptive Cyber Defense. Lecture Notes in Computer Science, Springer, 2019; vol. 11830.

Hamid K, Iqbal MW, Aqeel M., Rana TA, Arif M. Cyber security: Analysis for detecting and removing zero-day attacks (ZDA). In Artificial Intelligence & Blockchain in Cyber Physical Systems. 2023; pp. 172-196. CRC Press.

Saheed YK, Abdulganiyu OH, Majikumna KU, Mustapha M, Workneh AD. ResNet50-1D-CNN: A New Lightweight ResNet50-One-Dimensional Convolution Neural Network Transfer Learning Based Approach for Improved Intrusion Detection in Cyber-Physical Systems. International Journal of Critical Infrastructure Protection. 2024; 45.

Kuttiyappan D and Rajasekar V. Improving the Cyber Security over Banking Sector by Detecting the Malicious Attacks Using the Wrapper Stepwise ResNet Classifier. KSII Transactions on Internet and Information Systems (TIIS). 2023; 17(6), 1657-1673.

Bushra SN, Subramanian N, Chandrasekar A. An optimal and secure environment for intrusion detection using hybrid optimization based ResNet 101-C model. Peer-to-Peer Networking and Applications. 2023; 16(5), 2307-2324.

Vinayakumar R, Soman KP, Poornachandran P. Evaluating deep learning approaches to characterize and classify malicious URL's. Journal of Intelligent and Fuzzy Systems. 2018; 34(3), 1333-1343.

Do CT, Tran NH, Hong C, Kamhoua CA, Kwiat KA, Blasch E, Iyengar SS. Game theory for cyber security and privacy. ACM Computing Surveys. 2017; 50(2), 1-37.

Anwar F, Khan BUI, Olanrewaju RF, Pampori BR, Mir RN. A comprehensive insight into game theory in relevance to cyber security. Indonesian Journal of Electrical Engineering and Informatics. 2020 8(1), 189-203.

Dahiya A and Gupta BB. A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. Future Generation Computer Systems. 2021; 117, 193-204.

Kumar B and Bhuyan B. Using game theory to model DoS attack and defence. Sādhanā. 2019; 44(12), 245.

Pilz M, Naeini FB, Grammont K, Smagghe C, Davis M, Nebel JC, Pfluegel E. Security attacks on smart grid scheduling and their defences: a game-theoretic approach. International Journal of Information Security. 2020; 19, 427-443.

Marcos VO and Proença ML. Scorpius: sflow network anomaly simulator. Journal of Computer Science. 2015; 11(4), 662.

Kiennert C, Ismail Z, Debar H, Leneutre J. A survey on game-theoretic approaches for intrusion detection and response optimization. ACM Computing Surveys. 2018; 51(5), 1-31.

Musman S and Turner A. A game theoretic approach to cyber security risk management. The Journal of Defense Modeling and Simulation. 2018; 15(2), 127-146.

Akinwumi DA, Iwasokun GB, Alese BK, Oluwadare SA. A review of game theory approach to cyber security risk management. Nigerian Journal of Technology. 2017; 36(4), 1271-1285.

Hu H, Liu Y, Chen C, Zhang H, Liu Y. Optimal decision making approach for cyber security defense using evolutionary game. IEEE Transactions on Network and Service Management. 2020; 17(3), 1683-1700.

Chen H, Han Q, Jajodia S, Lindelauf R, Subrahmanian VS, Xiong Y. Disclose or exploit? A game theoretic approach to strategic decision making in cyber-warfare. IEEE Systems Journal. 2020; 14(3), 3779-3790.

Ma X, Abdelfattah W, Luo D, Innab N, Shutaywi M, Deebani W. Non-cooperative game theory with generative adversarial network for effective decision-making in military cyber warfare. Annals of Operations Research. 2024; 1-18. 149 International Journal of Computer Networks & Communications (IJCNC) Vol.17, No.4, July 2025

Robertson J, Diab A, Marin E, Nunes E, Paliath V, Shakarian J, Shakarian P. Darknet mining and game theory for enhanced cyber threat intelligence. The Cyber Defense Review. 2016; 1(2), 95-122.

Ali S, Rehman SU, Imran A, Adeem G, Iqbal Z, Kim KI. Comparative evaluation of AI-based techniques for zero-day attacks detection. Electronics. 2022; 11(23), 3934.

Karimy AU and Reddy PC. Enhancing IoT security: A novel approach with federated learning and differential privacy integration. International Journal of Computer Networks & Communications (IJCNC). 2024; vol. 16, no.3, pp. 1–19.

Shruthi N and Siddesh GK. Trust metric-based anomaly detection via deep deterministic policy gradient reinforcement learning framework. International Journal of Computer Networks & Communications (IJCNC). 2023; vol. 15, no.6, pp. 1–17.

Sultan MT, Sayed HE, Khan MA. An intrusion detection mechanism for MANETs based on deep learning artificial neural networks (ANNs). International Journal of Computer Networks & Communications (IJCNC). 2023; vol. 15, no.1, pp. 1–20.

De Assis MV, Hamamoto AH, Abrão T, Proença ML. A game theoretical based system using holt winters and genetic algorithm with fuzzy logic for DoS/DDoS mitigation on SDN networks. IEEE Access. 2017; 5, 9485-9496.

Pholpol C, Sanguankotchakorn T. Traffic congestion prediction using deep reinforcement learning in vehicular ad-hoc networks (VANETs). International Journal of Computer Networks & Communications (IJCNC). 2021; 13(4):1-19.

Khan A, Imran M, Aadil F, Lloret J. Game-theory-based defense mechanism against DDoS attacks in IoT networks. International Journal of Computer Networks & Communications (IJCNC). 2022; 14(3):21-40.

Bala B and Behal S. AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges. Computer science review. 2024; 52, 100631.

Mekala SH, Baig Z, Anwar A, Zeadally S. Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. Computer Communications. 2023; 208, 294-320.

Das A and Pramod S. An Enhanced Optimization Model with Ensemble Autoencoder for Zero- Day Attack Detection. Journal of Theoretical and Applied Information Technology. 2022; 100(22).

Kim JY, Bu SJ, Cho SB. Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders. Information Sciences. 2018; 460, 83-102.

Zahoora U, Rajarajan M, Pan Z, Khan A. Zero-day ransomware attack detection using deep contractive auto encoder and voting based ensemble classifier. Applied Intelligence. 2022; 52(12), 13941-13960.

Mohamed AA, Al-Saleh A, Sharma SK, Tejani GG. Zero-day exploits detection with adaptive Wave PCA-Autoencoder (AWPA) adaptive hybrid exploit detection network (AHEDNet). Scientific Reports. 2025; 15(1), 4036.

Yin C, Zhu Y, Liu S, Fei J, Zhang H. Enhancing network intrusion detection classifiers using supervised adversarial training. The Journal of Supercomputing. 2020;76(9):6690–6719.

Lopez-Martin M, Carro B, Sanchez-Esguevillas A, Lloret J. Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in IoT. Sensors. 2017; 17(9):1967.

Imrana Y, Xiang Y, Ali L, Noor A, Sarpong K, Abdullah MA. CNN-GRU-FF: A double-layer feature fusion-based network intrusion detection system using convolutional neural network and gated recurrent units. Complex & Intelligent Systems. 2024; 10(3):3353-3370.

Haber, E. (2023). The Law of the Trojan Horse. UC Davis Law Review, Forthcoming.

Anderson, R. (2020). Security engineering: a guide to building dependable distributed systems. John Wiley & Sons.

Lalor, R., Cwiklinski, K., Calvani, N. E. D., Dorey, A., Hamon, S., Corrales, J. L., ... & De Marco Verissimo, C. (2021). Pathogenicity and virulence of the liver flukes Fasciola hepatica and Fasciola gigantica that cause the zoonosis Fasciolosis. Virulence, 12(1), 2839-2867.

Zhang, Z., Cheng, Y., & Li, Z. (2020). Super Root: A New Stealthy Rooting Technique on ARM Devices. In Applied Cryptography and Network Security: 18th International Conference, ACNS 2020, Rome, Italy, October 19–22, 2020, Proceedings, Part II 18 (pp. 344-363). Springer International Publishing.

Aditya, K. (2019). THE COMPETITION OF SHOWING ABILITY: THE POTENTIAL DANGERS OF HACKER IN US CYBER SECURITY (2009–2014) (Doctoral dissertation, President University)

Brenner, S. W. (2012). Cybercrime and the law: Challenges, issues, and outcomes. UPNE.

Nespoli, P., Papamartzivanos, D., Mármol, F. G., & Kambourakis, G. (2017). Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks. IEEE Communications Surveys & Tutorials, 20(2), 1361-1396.

Cuppah, D., Ambrish, G., & Hanumanthappa, M. (2020). Design and analysis of a hybrid security framework for zero-day attack. International Journal of Applied Engineering Research, 14(15), 140-144.

Li, C., & Gaudiot, J. L. (2019, July). Detecting malicious attacks exploiting hardware vulnerabilities using performance counters. In 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC) (Vol. 1, pp. 588-597). IEEE.

Zerouali, A., Mens, T., Decan, A., & De Roover, C. (2022). On the impact of security vulnerabilities in the npm and RubyGems dependency networks. Empirical Software Engineering, 27(5), 107.

Abdelnabi, Sahar, Katharina Krombholz, and Mario Fritz. "Visualphishnet: Zero-day phishing website detection by visual similarity." In Proceedings of the 2020 ACM SIGSAC conference on computer and communications security, pp. 1681-1698. 2020.

Ahmed, Abdulghani Ali, Waheb A. Jabbar, Ali SafaaSadiq, and Hiran Patel. "Deep learning-based classification model for botnet attack detection." Journal of Ambient Intelligence and Humanized Computing 13, no. 7 (2022): 3457-3466.

Hairab, Belal Ibrahim, Mahmoud Said Elsayed, Anca D. Jurcut, and Marianne A. Azer. "Anomaly detection based on CNN and regularization techniques against zero-day attacks in IoT networks." IEEE Access 10 (2022): 98427-98440.

De La Torre Parra, G., Rad, P., Raymond Choo, K.-K., & Beebe, N. (2020). Detecting Internet of Things attacks using distributed deep learning. Journal of Network and Computer Applications, 102662. doi:10.1016/j.jnca.2020.102662

Diloglu, Baran. "Zero-Day Attack Detection with Deep Learning in Networks." PhD diss., Dublin, National College of Ireland, 2022.

Diro, AbebeAbeshu, and Naveen Chilamkurti. "Distributed attack detection scheme using deep learning approach for Internet of Things." Future Generation Computer Systems 82 (2018): 761-768.

Barros PH, Chagas ET, Oliveira LB, Queiroz F, Ramos HS. Malware- SMELL: A zero- shot learning strategy for detecting zero- day vulnerabilities. Computers & Security. 2022 Sep 1;120:102785.

Dalal, Surjeet, et al. "Extremely boosted neural network for more accurate multi-stage Cyber attack prediction in cloud computing environment." Journal of Cloud Computing 12.1 (2023): 14.

He, Z., Rezaei, A., Homayoun, H. and Sayadi, H., 2022, June. Deep neural network and transfer learning for accurate hardware-based zero-day malware detection. In Proceedings of the Great Lakes Symposium on VLSI 2022 (pp. 27-32).

Millar, S., McLaughlin, N., Martinez del Rincon, J., & Miller, P. (2021). Multi-view deep learning for zero-day Android malware detection. Journal of Information Security and Applications, 58, 102718. doi:10.1016/j.jisa.2020.102718

R, V., Alazab, M., KP, S., Poornachandran, P., & Venkatraman, S. (2019). Robust Intelligent Malware Detection Using Deep Learning. IEEE Access, 1–1. doi:10.1109/access.2019.2906934

Rana, Sohel, MdAlaminHossan, and Abidullha Adel. "Cloud Zero-Day Attack Detection Using Hidden Markov Model with Transductive Learning." (2021).

Ali, Mubashir, Ayesha Siddique, Aamir Hussain, Farhad Hassan, Amir Ijaz, and AneelaMehmood. "A Sustainable Framework for Preventing IoT Systems from Zero Day DDoS Attacks by Machine Learning." Int. J. Emerg. Technol 12 (2021): 116-121.

Hamid, Khalid, Muhammad Waseem Iqbal, Muhammad Aqeel, Xiangyong Liu, and Muhammad Arif. "Analysis of Techniques for Detection and Removal of Zero-Day Attacks (ZDA)." In Inernational Conference on Ubiquitous Security, pp. 248-262. Singapore: Springer Nature Singapore, 2022.

Kumar, V., & Sinha, D. (2021). A robust intelligent zero-day cyber-attack detection technique. Complex & Intelligent Systems, 7(5), 2211-2234.

L. Yang and H. Zhao, "DDoS Attack Identification and Defense Using SDN Based on Machine Learning Method," 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN), Yichang, China, 2018, pp. 174-178, doi: 10.1109/I-SPAN.2018.00036.

M. R. Babu and K. N. Veena, "A Survey on Attack Detection Methods For IOT Using Machine Learning And Deep Learning," 2021 3rd International Conference on Signal Processing and Communication (ICPSC), Coimbatore, India, 2021, pp. 625-630, doi: 10.1109/ICSPC51351.2021.9451740.

Mishra, S., Pradhan, S. K., &Rath, S. K. (2021). Detection of Zero-Day Attacks in Network IDS through High Performance Soft Computing. 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS). doi:10.1109/icais50930.2021.9395929

Sameera, N., & Shashi, M. (2020). Deep transductive transfer learning framework for zero-day attack detection. ICT Express, 6(4), 361-367.

Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. S. (2018). A Detailed Investigation and Analysis of using Machine Learning Techniques for Intrusion Detection. IEEE Communications Surveys & Tutorials, 1–1. doi:10.1109/comst.2018.2847722

Scholten, C. P. B. (2021). Automatic detection of zero-day attacks in high-interaction IoT honeypots using static analysis techniques (Master's thesis, University of Twente).

Shin, J., Choi, S. H., Liu, P., & Choi, Y. H. (2019). Unsupervised multi-stage attack detection framework without details on single-stage attacks. Future Generation Computer Systems, 100, 811-825.

Tang, R., Yang, Z., Li, Z., Meng, W., Wang, H., Li, Q., ... & Liu, Y. (2020, July). Zerowall: Detecting zero-day web attacks through encoder-decoder recurrent neural networks. In IEEE INFOCOM 2020-IEEE Conference on Computer Communications (pp. 2479-2488). IEEE.

Tokmak, M. (2022). Deep forest approach for zero-day attacks detection. Innovations and Technologies in Engineering, 45-56.

Wang, H., Sayadi, H., Kolhe, G., Sasan, A., Rafatirad, S., & Homayoun, H. (2020). Phased-Guard: Multi-Phase Machine Learning Framework for Detection and Identification of Zero-Day Microarchitectural Side-Channel Attacks. 2020 IEEE 38th International Conference on Computer Design (ICCD). doi:10.1109/iccd50377.2020.00111

Zhang, J., Liang, S., Ye, F., Hu, R. Q., & Qian, Y. (2023, May). Towards detection of zero-day botnet attack in iot networks using federated learning. In ICC 2023-IEEE International Conference on Communications (pp. 7-12). IEEE.

Khan, S., & Parkinson, S. (2018). Review into state of the art of vulnerability assessment using artificial intelligence. Guide to Vulnerability Analysis for Computer Networks and Systems: An Artificial Intelligence Approach, 3-32.

Wang, P., D'Cruze, H., & Wood, D. (2019). ECONOMIC COSTS AND IMPACTS OF BUSINESS DATA BREACHES. Issues in Information Systems, 20(2).

Sun, Yanwei, Lihua Yin, YunchuanGuo, Fenghua Li, and Binxing Fang. "Optimally selecting the timing of zero-day attack via spatial evolutionary game." In Algorithms and Architectures for Parallel Processing: 17th International Conference, ICA3PP 2017, Helsinki, Finland, August 21-23, 2017, Proceedings 17, pp. 313-327. Springer International Publishing, 2017.

N. F. Abedin, R. Bawm, T. Sarwar, M. Saifuddin, M. A. Rahman and S. Hossain, "Phishing Attack Detection using Machine Learning Classification Techniques," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 1125-1130, doi: 10.1109/ICISS49785.2020.9315895.

Nathezhtha, T., &Yaidehi, V. (2018). Cloud Insider Attack Detection Using Machine Learning. 2018 International Conference on Recent Trends in Advance Computing (ICRTAC). doi:10.1109/icrtac.2018.8679338

Emmah, V. T., Ugwu, C., & Onyejegbu, L. N. (2021). An Enhanced Classification Model for Likelihood of Zero-Day Attack Detection and Estimation. European Journal of Electrical Engineering and Computer Science, 5(4), 69-75.

Haider, W., Creech, G., Xie, Y., & Hu, J. (2016). Windows based data sets for evaluation f robustness of host based intrusion detection systems (IDS) to zero-day and stealth attacks. Future Internet, 8(3), 29.

Haruta, S., Asahina, H., Yamazaki, F., & Sasase, I. (2019). Hue signature auto update system for visual similarity-based phishing detection with tolerance to zero-day attack. IEICE TRANSACTIONS on Information and Systems, 102(12), 2461-2471.

Hindy, H., Atkinson, R., Tachtatzis, C., Colin, J. N., Bayne, E., & Bellekens, X. (2020). Towards an effective zero-day attack detection using outlier-based deep learning techniques. ArXiv, vol. abs/2006.15344.

Ibrahim Hairab, B., Aslan, H. K., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). Anomaly Detection of Zero-Day Attacks Based on CNN and Regularization Techniques. Electronics, 12(3), 573.

Innab, N., Alomairy, E., & Alsheddi, L. (2018, April). Hybrid system between anomaly based detection system and honeypot to detect zero day attack. In 2018 21st Saudi Computer Society National Computer Conference (NCC) (pp. 1-5). IEEE.

Kaur, R., & Singh, M. (2015). A hybrid real-time zero-day attack detection and analysis system. International Journal of Computer Network and Information Security, 7(9), 19-31.

Korba, A. A., Boualouache, A., Brik, B., Rahal, R., Ghamri-Doudane, Y., & Senouci, S. M. (2023, May). Federated learning for zero-day attack detection in 5g and beyond v2x networks. In ICC 2023-IEEE International Conference on Communications (pp. 1137-1142). IEEE.

Kumar, V., & Sinha, D. (2021). A robust intelligent zero-day cyber-attack detection technique. Complex & Intelligent Systems. doi:10.1007/s40747-021-00396-9

Akshaya, Swathy, and G. Padmavathi. "Enhancing Zero-Day Attack Prediction a Hybrid Game Theory Approach with Neural Networks." International Journal of Intelligent Systems and Applications in Engineering 12, no. 7s (2024): 643-663.

Syed, NaeemFirdous, ZubairBaig, Ahmed Ibrahim, and Craig Valli. "Denial of service attack detection through machine learning for the IoT." Journal of Information and Telecommunication 4, no. 4 (2020): 482-503.

Zahoora, Umme, MuttukrishnanRajarajan, Zahoqing Pan, and Asifullah Khan. "Zero-day ransomware attack detection using deep contractive autoencoder and voting based ensemble classifier." Applied Intelligence 52, no. 12 (2022): 13941-13960.

Rajakumaran, G., Venkataraman, N., & Mukkamala, R. R. (2020). Denial of service attack prediction using gradient descent algorithm. SN Computer Science, 1(1), 45.

Rehman, S. U., Ali, S., Adeem, G., Hussain, S., & Raza, S. S. (2022). Computational Intelligence Approaches for Analysis of the Detection of Zero-day Attacks. University of Wah Journal of Science and Technology (UWJST), 6, 27-36.

Parrend, Pierre, Julio Navarro, Fabio Guigou, AlineDeruyver, and Pierre Collet. "Foundations and applications of artificial Intelligence for zero-day and multi-step attack detection." EURASIP Journal on Information Security 2018 (2018): 1-21.

Patidar, P., and HarshitaKhandelwal. "Zero-day attack detection using machine learning techniques." International Journal of Research and Analytical Reviews 6, no. 1 (2019): 1364-1367.

Popoola, Segun I., Ruth Ande, BamideleAdebisi, Guan Gui, Mohammad Hammoudeh, and OlamideJogunola. "Federated deep learning for zero-day botnet attack detection in IoT-edge devices." IEEE Internet of Things Journal 9, no. 5 (2021): 3930-3944.

Seraphim, B. I., & Poovammal, E. (2022). Zero-Day Attack Detection Analysis in Streaming Data Using Supervised Learning Techniques. In Intelligent Systems and Sustainable Computing: Proceedings of ICISSC 2021 (pp. 517-530). Singapore: Springer Nature Singapore.

Al-Rushdan, H., Shurman, M., Alnabelsi, S. H., & Althebyan, Q. (2019). Zero-Day Attack Detection and Prevention in Software-Defined Networks. 2019 International Arab Conference on Information Technology (ACIT). doi:10.1109/acit47987. 2019.8991124

Anwer, M., Ahmed, G., Akhunzada, A., Hussain, S., & Khan, M. (2022, September). Comparative analysis of soft computing approaches of zero-day-attack detection. In 2022 International Conference on Emerging Trends in Smart Technologies (ICETST) (pp. 1-5). IEEE.

Bar, R., & Hajaj, C. (2022). Simcse for encrypted traffic detection and zero-day attack detection. IEEE Access, 10, 56952-56960.

Bherde, G. P., & Pund, M. A. (2018). Technique for Detecting Zero Day Attack by using Signature based and Knowledge Based Method.

David, A. O., & Oluwasola, O. O. (2020). Zero day attack prediction with parameter setting using Bi direction recurrent neural network in cyber security. International Journal of Computer Science and Information Security (IJCSIS), 18(3), 111-118.

Zhao, J., Shetty, S., Pan, J. W., Kamhoua, C., & Kwiat, K. (2019). Transfer learning for detecting unknown network attacks. EURASIP Journal on Information Security, 2019(1). doi:10.1186/s13635-019-0084-4

Serinelli, B. M., Collen, A., &Nijdam, N. A. (2021). On the analysis of open source datasets: validating IDS implementation for well-known and zero day attack detection. Procedia Computer Science, 191, 192–199. doi:10.1016/j.procs.2021.07.024

Abdelnabi, Sahar, Katharina Krombholz, and Mario Fritz. "Visualphishnet: Zero-day phishing website detection by visual similarity." In Proceedings of the 2020 ACM SIGSAC conference on computer and communications security, pp. 1681-1698. 2020.

Ahmed, Abdulghani Ali, Waheb A. Jabbar, Ali SafaaSadiq, and Hiran Patel. "Deep learning-based classification model for botnet attack detection." Journal of Ambient Intelligence and Humanized Computing 13, no. 7 (2022): 3457-3466.

Aktar, Sharmin, and Abdullah Yasin Nur. "Towards DDoS attack detection using deep learning approach." Computers & Security 129 (2023): 103251.

Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. sensors, 18(3), 817.

Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). WITHDRAWN: A hybrid layered architecture for detection and analysis of network based Zero-day attack. Computer Communications, 106, 100–106. doi:10.1016/j.comcom.2017.01.019

Soe, Yan Naung, Yaokai Feng, Paulus InsapSantosa, Rudy Hartanto, and Kouichi Sakurai. "Machine learning-based IoT-botnet attack detection with sequential architecture." Sensors 20, no. 16 (2020): 4372.

Sokolov, A. N., Ragozin, A. N., Pyatnitsky, I. A., &Alabugin, S. K. (2019, September). Applying of digital signal processing techniques to improve the performance of machine learning-based cyber attack detection in industrial control system. In Proceedings of the 12th International Conference on Security of Information and Networks (pp. 1-4).

Kostas, Kahraman. "Anomaly detection in networks using machine learning." Research Proposal 23 (2018): 343.

Kunang, Y. N., Nurmaini, S., Stiawan, D., &Suprapto, B. Y. (2021). Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. Journal of Information Security and Applications, 58, 102804. doi:10.1016/j.jisa. 2021.102804

Avinashilingam Institute for HomeScience and Higher Education for Women
(Deemed to be University Estd. u/s 3 of UGC Act 1956, Category 'A' by MHRD
Re-accredited with A++ Grade by NAAC. CGPA 3.65/4, Category I by UGC
Coimbatore - 641 043, Tamil Nadu, India

Appendix L2

(Item No 5 of Check List) Details of Research Publications

Verified mam.

S.No	Article	Journal	Other Details Vol/No/Page No/ Year	Published in UGC-CARE / Scopus Indexed/ Web of Science
1	ResNet 50- based deep convolutional neural network for zero-day attack Prediction and detection	International Journal of Advanced Technology and Engineering Exploration	Vol 12 (124) Pg: 507-527 March 2025	Scopus Indexed (published)
2	Enhancing Cyber Defense Against Zero-Day Attacks using Ensemble Neural Networks	International Journal of computer Networks & communications	Vol. 17, Issue 4 July 2025	Scopus Indexed (accepted)

*Proof of list of Journals from Internet to be attached along with copies of reprints.

Scholar : Suthahy.

Supervisor : 30/06/2025

Checked By: Kalpana R

HoD/Dean of Respective School

The scholar Miss. Swathy Akshaya (17PHCSFC03) has published her research articles in the following journals:

1. International Journal of Advanced Technology and Engineering Exploration - indexed in Scopus from 2019 to present,
2. International Journal of computer Networks and Communications - indexed in Scopus from 2016 to present.

This may be considered.

30.01.25

Asst. Librarian

International Journal of Advanced Technology and Engineering Exploration, Vol 12(124)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2024.111100055

Research Article

ResNet50-based deep convolutional neural network for zero-day attack prediction and detection

Swathy Akshaya[1*] and Padmavathi. G[2]
Research Scholar, Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India[1]
Professor, Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India[2]

Received: 13-January-2024; Revised: 24-February-2025; Accepted: 09-March-2025

Abstract
A zero-day attack (ZDA) is a cyberattack that targets networks and systems by exploiting previously unknown security vulnerabilities. Software vendors have zero days to identify, address, and patch newly discovered threats, hence the term "zero-day." In cybersecurity, effectively detecting and mitigating malicious nodes is crucial, particularly against zero-day malware. Traditional antivirus systems, which rely on stored malware signatures, struggle to detect ZDAs, making them vulnerable to advanced malware specifically designed to evade detection. To address this challenge, a novel approach called deep convolutional n-zero-day adversarial safety network (DC-nZDASN) has been proposed. This method trains a model to distinguish between real and synthetic malware samples by generating artificial malware data. The synthetic data introduces new characteristics that contrast with the original dataset, enhancing the model's detection capability. The proposed approach incorporates multiple malware features and utilizes real-world and network traffic datasets for model development. During preprocessing, the standard scaler is applied, and decision tree regression (DTR) is used, while feature selection is performed using random forest (RF) in combination with logistic regression (LR). The model is trained and tested using residual network (ResNet50), long short-term memory (LSTM), and convolutional neural network (CNN). For classification, various machine learning (ML) algorithms, such as decision tree (DT), LR, support vector machine (SVM), gaussian naïve bayes (GNB), and stacking ensemble classification (SEC), are employed. The proposed DC-nZDASN model achieves a classification accuracy of 95.09%, demonstrating a significant advancement in malware detection, particularly for zero-day threats. By leveraging generated synthetic malware samples, the model enhances its ability to detect novel threats, outperforming traditional methods. The integration of preprocessing techniques, feature selection, and a diverse set of ML algorithms further improves the model's overall effectiveness.

Keywords
Zero-day attack, Deep convolutional neural network (DCNN), Resnet50, Malware detection, Transfer learning, Machine learning.

1.Introduction
Information and communication technologies have accelerated human tasks while introducing new risks, such as network model intrusions [1]. Intrusion in information systems refers to unauthorized attacks on data integrity, availability, and confidentiality, including data alteration or destruction [2]. Predicting zero-day attacks (ZDA) remains one of the biggest challenges in intrusion detection systems (IDS) [3].

Figure 1 illustrates the zero-day vulnerability timeline architecture, outlining the lifecycle of security flaws from discovery to exploitation and eventual patching [4, 5].

To mitigate these risks, researchers have developed IDS solutions to identify and reduce harmful network activity, ensuring system security [6, 7]. Most IDS are either anomaly-based or signature-based [8]. Anomaly-based IDS can detect irregularities in normal network activity patterns, making them effective in identifying unknown attacks, though they tend to produce more false positives (FPs) [9]. In contrast, signature-based IDS are effective at

*Author for correspondence

recognizing known attack patterns but cannot detect new, previously unrecorded threats [10].

Figure 1 Zero-day vulnerability timeline

ZDA prediction exploits undisclosed vulnerabilities in software, making it one of the most complex challenges in IDS [11]. ZDAs pose a significant threat as they target vulnerable systems before a fix is available [12]. *Figure 2* illustrates the lifecycle of a ZDA, detailing the stages from vulnerability discovery to exploitation. These attacks typically involve multiple steps, including vulnerability identification, weaponization, and exploitation [13]. Signature-based IDS are ineffective in detecting ZDAs, whereas anomaly-based IDS perform better in identifying previously unknown attacks [14]. However, anomaly-based approaches suffer from low accuracy and high false positive rates, which limit their reliability.

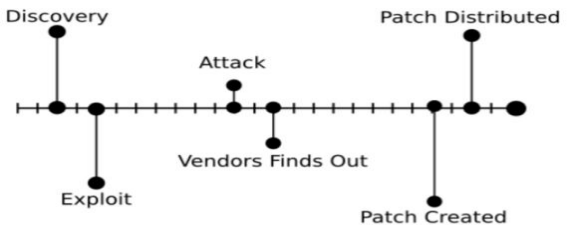

Figure 2 Lifecycle of ZDA

ZDA lacks preset indicators, and prior information is challenging to identify and impossible to predict [15]. The complexities of such attacks have not been fully addressed by traditional machine learning (ML) models and some deep learning (DL) methods [16–18]. Since many models fail to function consistently on new data, insufficient datasets for testing and training are particularly problematic [19]. ZDA detection leverages recent advancements in DL frameworks, including convolutional neural network (CNNs), long short-term memory auto-encoder (LSTM-AE), and generative adversarial networks (GANs). However, these approaches face challenges related to generalizability and scalability [20–22]. In this context, federated learning (FL) is emerging as a promising approach to enhance the anomaly detection performance of ZDAs across various scenarios in the internet of things (IoT) and 5G networks [23, 24]. Additionally, another innovative approach involves using GANs to generate synthetic ZDA samples, which can improve classifier training and enhance robustness [25].

Previous research on zero-day malware detection has addressed several significant challenges. Existing IDS, which primarily rely on signature-based or heuristic algorithms, often fail to identify new or sophisticated attacks [26]. ML-based approaches frequently suffer from limited dataset diversity and generalization issues, as they depend heavily on labeled data that may not accurately represent real-world threats, as discussed by [27, 28]. Additionally, adversarial attacks exacerbate these challenges by exploiting vulnerabilities in model training. Moreover, many models designed to handle the complexities of ZDAs lack effective feature selection and processing mechanisms [29, 30].

Traditional detection approaches face significant challenges due to the increasing complexity and frequency of zero-day malware attacks, as well as their ability to exploit unknown vulnerabilities. Existing models often struggle with limited dataset diversity, poor generalization, and the difficulty of accurately replicating real-world zero-day threat scenarios. This study is driven by the urgent need to develop a robust system capable of overcoming these limitations through adversarial learning and enhanced dataset complexity. As a result, the detection of previously unseen malware is improved. The ultimate goal is to create a scalable and adaptable system to combat emerging cyber threats effectively.

This study employed a ResNet-50-based CNN to address these challenges by developing a DL-based IDS for real-time ZDA detection. The proposed approach minimized FPs while enhancing detection accuracy and scalability, enabling it to efficiently manage high network traffic. The primary objective was to improve the prediction and detection of zero-day vulnerabilities using DL methodologies, thereby strengthening IDS in handling emerging cyber threats.

The main aim is to develop and evaluate the deep convolutional zero-day adversarial safety network (DC-nZDASN) framework for generating adversarial malware samples that mimic real-world threats, thereby enhancing zero-day malware detection. This approach focuses on increasing dataset diversity through feature modification, stabilizing training

using deep auto-encoders (AEs), and training the discriminator to recognize malware-specific patterns. This research presents a comprehensive framework for ZDA prediction and detection, incorporating advanced feature selection, model training, and classification techniques. The hybrid approach of random forest (RF) and logistic regression (LR) ensures optimal feature selection, while dataset preparation utilizes a standard scaler and decision tree regression (DTR) for pre-processing. ResNet-50 and long short-term memory (LSTM) are integrated into the training phase to improve prediction performance, with further enhancements achieved using Adam optimization (AO). Additionally, stacking ensemble classification (SEC), LR, gaussian naïve bayes (GNB), decision tree (DT), and support vector machine (SVM) were used for classification.

The paper is organized as follows: Section 2 presents an overview of related works. Section 3 introduces the proposed model, describing its architecture and methodology. Section 4 details the experimental results, providing analysis and interpretation. Finally, Section 5 concludes the paper by summarizing the key contributions and outlining directions for future research.

2.Literature review

This section discussed the related work to provide a more expansive idea focusing on ZDA prediction. Idhammad et al. [31] provided a supervised CNN architecture for edge systems that addressed latency and limited resources. Their technique complemented the studies on dispersed edge network protection, matched research on feature extraction, and underlined the robustness of CNN in distributed denial-of-service (DDoS) traffic detection.

Older models relied heavily on rule-based or statistical techniques that struggled with flexibility and accuracy. IDs have evolved significantly. Lin et al. [32] proposed cluster center and nearest neighbor (CANN), a strategy that combined cluster centers with nearest neighbors to increase detection accuracy and efficiency. It used cluster-based preprocessing for data dimensionality reduction and computation efficiency improvement. The closest neighbor technique ensured precise anomaly classification. Their hybrid approach addressed its limits in standalone clustering or neighbor-based systems by providing a fair trade-off between accuracy and processing efficiency. Their approach was consistent with previous research, emphasizing the need to combine unsupervised and supervised approaches for robust anomaly detection. It influenced subsequent studies focusing on hybrid IDS models for effectively managing large-scale and dynamic network environments.

Staudemeyer [33] explored the application of LSTM-recurrent neural network (RNN) for IDS. Their study demonstrated that LSTM's ability to effectively understand sequential network traffic data enabled the identification of detailed infiltration patterns. By leveraging LSTM’s capability to retain long-term contextual information and capture temporal correlations, the model outperformed traditional IDS strategies in anomaly detection. The research also highlighted the significance of hyperparameter tuning and architectural design in enhancing detection accuracy. This work has contributed to the adoption of advanced RNN architectures in cybersecurity applications, particularly for real-time intrusion detection.

Sarhan et al. [34] studied zero-shot ML techniques in detecting ZDA. It focused on the function of ZDA detection by the significantly low amount of labeled training data for such threats. The proposed methods were able to generalize and identify anomalous behavior by using feature embeddings and transfer learning towards anomalous behavior identification indicative of ZDA. The research showed that zero-shot learning (ZSL) had been beneficial in situations that typical supervised models could not handle. This inability was due to the lack of knowledge that ZSL helped improve cybersecurity resilience.

Jose and Jose [35] developed the convolutional neural network with long short-term memory (CNN-LSTM) IDS, an anomaly- and signature-based IDS for IoT, utilizing both CNN and LSTM. Their work addressed the unique security challenges of IoT systems, where sophisticated detection techniques are necessary due to the vast data volume and diverse attack vectors. By integrating CNN for feature extraction and LSTM for sequence learning, the proposed model effectively detected both known and novel attacks. It demonstrated a promising approach for protecting IoT networks against emerging threats, achieving high detection accuracy and low false-positive rates.

In the context of cybercrime, Alazab et al. [36] explored the concept of crime toolkits and highlighted their role in facilitating online malicious activities. They examined the commercialization of cybercrime and the accessibility of widely available

tools that enable attackers to conduct operations without extensive technical expertise. Their study provided a detailed analysis of various cybercrime toolkits, including their components, functionalities, ease of access, and usage by attackers. This research highlighted the need for robust security measures to combat the threats posed by these toolkits. Their work contributed to a deeper understanding of cybercrime dynamics and the increasing complexity of cyberattack techniques.

Pascanu et al. [37] explored the use of RNNs for malware classification, emphasizing their ability to process sequential data for detecting malicious software. Their research demonstrated RNNs' effectiveness in capturing temporal patterns within malware execution behavior, enabling the identification of complex and previously unknown malware variants. The authors highlighted that RNNs significantly improved detection accuracy compared to traditional signature-based techniques. This study underscored the potential of DL technologies in strengthening cybersecurity, particularly in detecting malware employing evasive tactics, thereby enhancing dynamic and automated malware detection systems.

Arun et al. [38] investigated the detection and simulation of ZDA using advanced DL methods. Their study emphasized the challenges of detecting zero-day vulnerabilities due to the lack of historical data and predefined signatures. To address this, the authors proposed a DL framework based on anomaly detection, integrating CNNs and LSTM networks to analyze network traffic and system logs for patterns indicative of ZDA. Experimental results demonstrated that the proposed framework achieved superior detection accuracy, robustness, and potential real-time application in IDS.

Oluwadare and ElSayed [39] examined unsupervised learning algorithms for detecting ZDA in IDS. Their research focused on identifying previously unseen attacks in the absence of labeled data and highlighted the potential of unsupervised learning approaches to address this challenge. The authors compared various unsupervised techniques, including DL, anomaly detection, and clustering, in ZDA detection. Their findings demonstrated how different strategies handled the evolving nature of cyber threats, outlining their respective strengths and weaknesses. The study concluded that unsupervised learning holds significant promise in enhancing IDS capabilities by identifying new attack patterns without requiring large labeled datasets.

Aljawarneh [40] analyzed technological advancements, security concerns, and emerging challenges in online banking systems. The study identified vulnerabilities threatening the integrity and trustworthiness of online transactions, including phishing attacks, malware, insider threats, and denial-of-service (DoS) attacks. They discussed the growing complexity of cyber threats and the need for robust security solutions to mitigate these risks. The research examined emerging technologies such as anomaly detection systems, encryption techniques, and multi-factor authentication, emphasizing the necessity for continuous innovation and security enhancements to protect online banking systems from evolving digital threats.

Demirel and Sandikkaya [41] introduced a web-based anomaly detection framework using CNNs for ZSL. Their study highlighted the limitations of traditional anomaly detection methods, which rely heavily on large labeled datasets for optimal performance. The proposed framework overcame this constraint by enabling the detection of previously unseen attack classes or anomalies without requiring labeled data. By integrating CNNs, the model improved feature extraction representation and enhanced accuracy in anomaly detection within web environments. This approach proved particularly valuable in dynamic and evolving cybersecurity landscapes, as it achieved scalable and adaptive anomaly detection with minimal prior knowledge of attack patterns.

Bai et al. [42] showed that temporal convolutional networks (TCNs) were more effective in sequential data processing flow than recurrent architectures such as LSTM and gated recurrent units (GRUs). Among the various potential inductive biases offered, TCNs achieved parallelization, flexible receptive fields, and stable gradients that remediated some issues, such as vanishing gradients and sequential computation bottlenecks in pure recurrent models. It has been shown that TCNs achieve higher accuracy and efficiency than conventional recurrent models in tasks such as sequence prediction and classification. This approach utilizes dilated convolutions to achieve large receptive fields, which are essential for real-world time series and sequence modeling, albeit at the cost of computational efficiency.

Roy et al. [43] employed an artificial neural network (ANN) approach to develop an IDS that enhanced

network security. Specifically, the model overcame the limitations of traditional IDS in detecting unknown attacks. The DL capabilities of the ANN model were leveraged to analyze complex patterns in network traffic and distinguish between normal and malicious activities. They demonstrated that ANN is scalable, adaptable to large datasets, and capable of achieving high accuracy in real-world intrusion detection. The study also highlighted that DL-based approaches provide higher detection rates for both known and unknown intrusions compared to conventional methods.

Habibi et al. [44] evaluated multiple CNN architectures and pre-trained models in terms of their performance in malware classification. This study compared the effectiveness of CNN-based architectures against pre-trained malware classifiers that utilized transfer learning for accurate malware classification. The researchers found that pre-trained models leveraged prior knowledge, improving classification performance, particularly on small datasets. Evaluation metrics such as accuracy, precision, and computational efficiency were used to assess model performance. Their experiments demonstrated that pre-trained models generally outperformed standard CNNs in terms of accuracy and robustness, providing valuable insights for enhancing malware detection systems in cybersecurity.

In network security, Hindy et al. [45] explored DL-based methods for efficiently detecting ZDA. They introduced advanced neural network (NN) capabilities that enabled the identification of previously unknown attacks targeting undisclosed vulnerabilities. Their proposed models analyzed network traffic patterns and behaviors to distinguish between normal and malicious activities. Feature selection and preprocessing played a crucial role in improving model accuracy and reducing FPs. The findings indicated that DL-based techniques, particularly CNN-based and LSTM-based approaches, were effective in detecting and mitigating ZDA in critical systems.

Previous studies have highlighted the increasing complexity of IDS and the evolving nature of cyber threats. The integration of DL techniques, such as CNNs, RNNs, and hybrid models, has significantly improved the detection of both known and emerging security risks, including structured query language (SQL) injection, malware, and ZDAs. Traditional detection methods, particularly signature-based approaches, have demonstrated limitations in identifying new and sophisticated threats. In contrast, the adoption of advanced ML models has provided enhanced adaptability to evolving attack strategies. However, challenges persist in addressing insider threats, ensuring scalability, and maintaining regulatory compliance. These challenges emphasize the ongoing need for innovation in IDS development. This review highlights the necessity of advanced IDS technologies, especially in light of the rapidly expanding cybersecurity threat landscape.

3.Materials and methods

The overall architecture of the proposed methodology is illustrated in *Figure 3*, which depicts the ML approach for classification tasks. The process begins with Stage 1, where missing values are managed, and features are scaled using a DTR. In Stage 2, feature importance is analyzed using LR and RF. Stage 3 involves training with LSTM and ResNet-50 models. In Stage 4, classification is performed using stacking ensemble techniques, incorporating various ML algorithms such as DT, Naïve Bayes (NB), SVM, and LR. This section details the feature selection and preprocessing techniques used to develop an ML model for detecting ZDA and the neural network (NN) training procedures.

The methodology begins with feature extraction, identifying and categorizing relevant properties. These features are then normalized, ensuring a consistent dataset suitable for ML algorithms. Using probabilistic and graph-based approaches reported by Yin et al. [46], multiple ZDA pathways are analyzed, enhancing the robustness of the detection model.

Backpropagation neural networks (BPNN) are utilized to analyze complex attack patterns in cloud systems, identifying potential vulnerabilities and attack pathways, as discussed by Swathy and Padmavathi [47]. Features selected using RF techniques undergo further analysis with LR to assess feature significance and enhance prediction accuracy.

Additionally, the hybrid game theory (HGT) method integrates game theory with ML techniques to improve attack detection. Previous studies by Dhanya et al. [48] and subsequent advancements by Akshaya and Padmavathi [49] in phase 2 of their research explore the application of HGT. This combination of methodologies examines attack tactics and decision-making mechanisms, enabling advanced ZDA detection and enhancing the overall performance of the model.

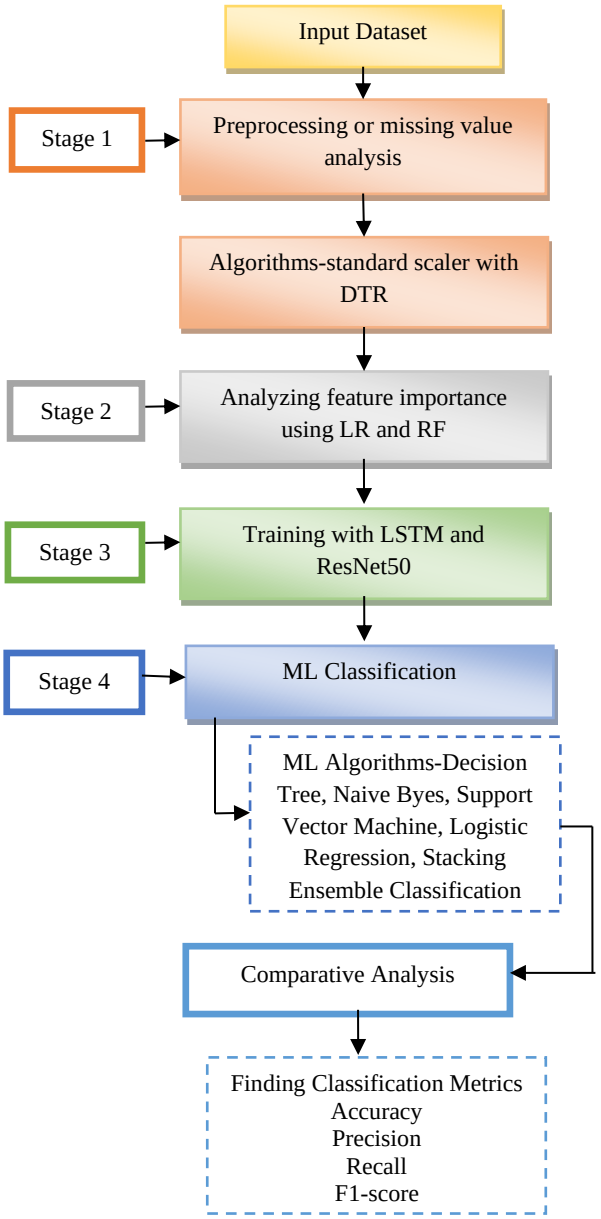

Figure 3 Proposed methodology

3.1Dataset collection

Two datasets have been considered for the experimentation. Dataset 1: national science library-knowledge discovery in databases (NSL-KDD) is obtained from the Kaggle repository and is provided in a comma-separated values (CSV) format, following the suggested methodology for IDS evaluation. NSL-KDD is specifically designed for ZDA detection, aiming to identify new, previously unseen attacks in network traffic [50]. It is an improved version of the KDD Cup 1999 dataset, addressing redundancy and improving the quality of attack samples. This dataset contains labeled network traffic data with 41 features, including protocol type, service, flag, and other statistical measurements. It encompasses multiple attack categories such as DoS, probe, remote-to-local (R2L), and user-to-root (U2R), providing a broad range of feature values for comprehensive IDS evaluation.

The second dataset, Celosia, is explicitly designed for cybersecurity research, focusing on detecting zero-day and anomaly-based attacks. It includes various network traffic attributes such as traffic volume, packet headers, flow durations, and payload entropy. Unlike NSL-KDD, the Celosia dataset integrates both labeled and unlabeled data, offering a more realistic simulation of diverse network conditions by covering extensive traffic patterns and attack behaviors [51]. This makes it particularly useful for anomaly-based IDS studies. The concept of ZDA refers to vulnerabilities exploited before any security mechanisms are in place, making them one of the most challenging issues in cybersecurity. To enhance predictive accuracy in anomaly-based IDS, Celosia has been utilized in research studies such as those conducted by Tavallaee et al. [52].

This research introduces a novel method called DC-nZDASN, which generates synthetic malware samples to distinguish them from real malware. The data generated through random sampling closely resembles the original dataset but retains distinct characteristics. Unlike genuine data, these synthetic samples have altered attributes, making them useful for improving detection models. The proposed model utilizes both real-world malware characteristics and synthetically modified data created by DC-nZDASN. This approach stabilizes the training process and enhances feature extraction. By learning malware traits, the model generates generalized data and continuously refines the training dataset before the actual training phase. As illustrated in *Figure 4*, the trained discriminator within the DC-nZDASN framework effectively identifies malware characteristics, improving the robustness of the detection system.

DC-nZDASN improves malware detection, particularly for ZDA, by integrating features and preprocessing techniques to enhance its model performance. Key features include behavioral indicators and signature-like traits. In preprocessing, the standard scaler, along with DTR, ensures the optimal data preparation. Feature selection uses RF with LR to refine the input by highlighting the most

relevant features. The model leverages residual network (ResNet50), LSTM, and CNN to enhance prediction accuracy. Additionally, it employs classification algorithms such as DT, SVM, LR, and GNB to further improve performance. These techniques collectively contribute to increased accuracy.

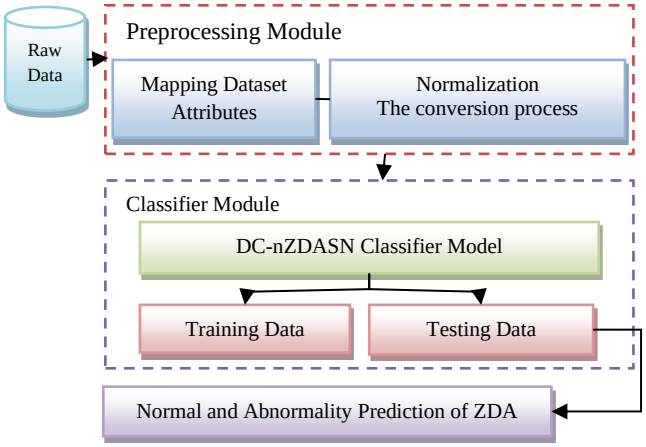

Figure 4 Flow diagram of DC-nZDASN Model

Moreover, the model introduces novel characteristics by generating synthetic malware occurrences, which strengthens its capability to identify emerging threats more effectively.Several solutions are proposed to address DC-nZDASN's class imbalance. Under-sampling the majority class helps balance the dataset using data-level strategies such as the synthetic minority over-sampling technique (SMOTE), which oversamples the low class. Algorithm-level adjustments include setting class weights to find the misclassification in minority classes and incorporate cost-sensitive learning. Evaluation metrics like precision, recall, F1-score, and area under the curve - receiver operating characteristic (AUC-ROC) ensure the model performance. This approach mitigates the impact of class imbalance. Additionally, RF help improve prediction accuracy by aggregating results from multiple balanced subsets of the data, ensuring a more representative and unbiased classification.

Furthermore, this method improves the detection of minority classes. These strategies collectively improve the model proficiency in finding ZDA. Despite imbalanced data distributions, it also ensures robustness and reliability. *Figure 5* depicts the diagrammatical representation of ZDA prediction architecture.

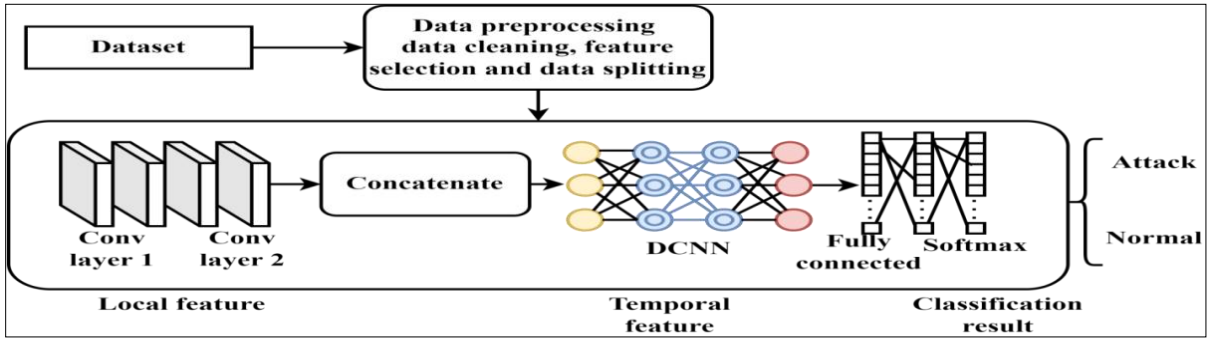

Figure 5 ZDA prediction architecture

3.2Data preprocessing

Data preparation is a crucial step in the data analysis process. Missing values and noise are common challenges in data analytics, often reducing the quality and reliability of the dataset. Data preprocessing plays a vital role in improving the efficiency and accuracy of data mining results by handling these impurities. Furthermore, applying ML techniques to a well-preprocessed dataset is essential for ensuring reliable results and accurate predictions. Proper preprocessing enhances the model's ability to extract meaningful patterns and improve overall performance.

In DC-nZDASN, several enhancements have been made to standard algorithms to improve performance, reduce complexity, and address ZDA detection challenges. The model integrates architectures like ResNet50 and LSTM to capture complex patterns and dependencies in malware data. Additionally, data preprocessing techniques, including standard scaling with DTR and synthetic data generation, enhance data quality and introduce variability crucial for generalization. These modifications collectively improve the model’s ability to accurately detect ZDAs, making DC-nZDASN a reliable solution for cybersecurity applications.

However, misclassifications typically occur in high-noise inputs or attack patterns closely resembling benign behavior. Key challenges include limited training data representations, feature overlap between benign and malicious samples, and adversarial attacks exploiting model weaknesses. Additionally, the evolving nature of cyber threats complicates detection. Addressing these issues requires diverse training datasets, improved noise-handling, refined feature extraction, and continuous learning to adapt to emerging attack patterns.

3.2.1 Label encoding method

Label encoding aims to make the labels legible by the machines that convert them into a numerical representation. ML algorithms are capable of utilizing these labels appropriately. An essential part of this algorithm is the preparation of organized datasets for supervised learning.

3.2.2 Standard scaler method

Standard Scaler represents a data preprocessing technique that standardizes features by removing the mean and scaling features to unit variance. Standard Scaler normalizes data by transforming it to have a mean of 0 and a standard deviation of 1, making it suitable for ML algorithms that are sensitive to feature magnitude, such as SVM and LR. By standardizing features, Standard Scaler ensures that all variables contribute equally to the model's performance, especially when they have different ranges or units, preventing any single feature from dominating the learning process.

The goal is to remove the outliers and scale the features to set the uniform variance. Equation 1 shows the calculation of standard score (Ds).

$$Ds = z\frac{x-\mu}{\sigma} \quad (1)$$

x: The original value of the feature to be standardized.
μ: The feature values in the training set are averaged to get this mean.
σ: It represents the dispersion in the training set's feature value.
z: This is the feature's standardized value or standard score.

The purpose of Equation 1 is to get consistent with different features and performance quality with the algorithms that depend on the scaled data. Many ML estimators depend on the standardized dataset. If the features differ from a normal distribution, the performance is poor. In a data-partitioning setup, the test set is held distinct from the training set, in which the algorithm is accurate. Values in training data, underlying logic, and algorithm features are used to generate the training model. Uniformity across dimensions is the goal of normalization.

Equation 2 shows the attributed information gain.

$$Gain(A) = Info(D) - Info\ A(D) \quad (2)$$

$Gain(A)$: This represents the information gain of attribute *A*. It measures the number of attributes *A* and reduces the dataset *D* entropy (uncertainty).
$Info(D)$*:* This is the entropy of dataset *D* before splitting on attribute *A*.
$Info\ A(D)$: This is the weighted entropy of dataset *D* after splitting on attribute *A*.
Entropy reduction due to dataset splitting to D on attribute A is measured by formula (2). A higher value of this indicates attribute A reduces uncertainty better.

Equation 3 presents the preprocessing information entropy.

$$Info(D) = Entropy(D) = -\sum_j p(j|D)logp(j/d) \quad (3)$$

$Info(D)$ or $Entropy(D)$: This refers to the entropy of dataset *D*. Entropy measures the amount of uncertainty or impurity in the dataset.
$p\ (j|D)$*:* This is the likelihood of class j in dataset *D*.
$logp(j/d)$*:* This is the logarithm of the probability of class *j* in dataset *d*. The logarithm is usually taken in base 2 for the entropy calculations.
Equation 3 calculates the entropy of the dataset D, which quantifies the impurity or uncertainty in the data.

Distribution information entropy is shown in Equation 4.

$$InfoA(D) = \sum_{i=1}^{v}\frac{n_i}{n}Info(Di) \quad (4)$$

$InfoA(D)$: This is the entropy after splitting dataset D on attribute A.
v: This represents the number of distinct values or the partitions created by attribute A.
n_i: This is the number of occurrences in partition Di.
n: This is the total number of occurrences in dataset D.
$\frac{n_i}{n}$: This is the weight of partition Diin related to the total dataset D.

$Info(Di)$: This is the entropy of partition Di.
The entropies of the subsets (Di) formed by the split of the dataset D over the attribute A are weighted averaged. Formulas (2), (3) and (4) are essential

when creating DTs as they are used to find and optimize the splits in the data to give you the highest predictive power.

3.3Feature importance

Step two involves training the network to use the feature importance strategy. The feature importance technique establishes the connection between the attribute and the target set. The dataset is where the input dataset is subjected to the RF technique. Using the LR approach, predicted dataset attributes appear often. Once the dataset has been preprocessed, the hybrid approach combines RF and LR algorithms to choose the features.

Prioritizing the most significant traits during training is achieved with RF, which ranks the features by their value. LR improves the model's accuracy and efficiency by identifying the most predictive characteristics.

3.3.1 RF

Feature space *X* of *M* dimensions hold the sample dataset *D*. After randomly selecting many high-quality trees *P* from a forest, the number of good and uncorrelated trees (*Q*) is determined. The five steps below outline the building of improved RF using *X* and *Q* uncorrelated high-performance trees.

1. *K* in-of-bag (IOB) data subsets are denoted as IOB1, IOB2, and IOBK by unsystematically sampling *D* with substitution and the bagging technique.
2. Assign the evaluation value to each IOB data subset IOB_i and use it to create a tree classifier. This procedure is repeated after harvesting and treating each tree.
3. Arrange these *K* trees by area under the curve (AUC)
4. Choose the best *P* trees that perform well based on their AUC scores.
5. RF construction is improved to determine whether these P trees' estimated probabilities are correlated.

3.3.2 LR

LR is a statistical method used to analyze and quantify the relationship between a dependent variable and one or more independent variables. LR estimates the probability of a particular outcome using the logistic function, making it widely applicable in classification tasks such as binary and multi-class prediction. LR model is described in Equation 5.

$$P_i = \frac{1}{1+exp(-\beta 0-\sum_{j=1}^{k}\beta_i x_{ij})} \quad (5)$$

P_i : This is the predicted probability of the dependent variable being 1 (success) for the observation *i.*

$\beta 0$: This is the intercept term of the model.

β_i: This is the coefficients for independent variables x_{ij}. Each β_i measures the impact of j^{th} independent variable on the log odds of the dependent variable.

x_{ij}: This is the independent variables for x i^{th} observation.

exp: This is the exponential function, often denoted as e

When applying the logit transformation to Equation 5, the linear relationship between logit (*pi*) and explanatory variables is presented in Equation 6.

$$logit(p_i) = log\ (\frac{p_i}{1-p_i}) \quad (6)$$

$logit(p_i)$: This is the logit function of p_i, which transforms the probability p_i Into log odds.

Log : This is the natural logarithm (base).

3.4Training with LSTM and ResNet50

3.4.1 Bidirectional long short-term memory (Bi-LSTM) and LSTM

RNNs primarily rely on short-term memory, enabling them to process sequential data by retaining information from previous time steps and applying it to the current state. However, standard RNNs struggle with retaining long-term dependencies due to the vanishing gradient problem, where gradients diminish over multiple layers, leading to ineffective learning in deeper layers with low weights. This issue often results in the loss of essential information during training.

Compared to traditional feedforward RNNs, LSTM networks are more effective in preserving long-term dependencies. LSTM employs a forget gate mechanism, allowing it to selectively retain or discard information, which enhances its performance over standard RNNs. Due to this gate-controlled memory management, LSTM outperforms conventional RNNs in handling sequential data.

Equations 7 to 11 define the mathematical operations used to compute the hidden states (b_q) of an LSTM unit, based on the values of its input, forget, and output gates.

$$f_q = \sigma\ (\omega_f.[b_{q-1}, x_q] + a_f) \quad (7)$$

f_q: At the time, disregard the gate activation vector in step q.

σ: A sigmoid activation function produces integers from 0 to 1.

ω_f: Weighted matrix for the forget gate.

b_{q-1}: Past hidden state.
x_q: Current input at the time step.
a_f: Bias for the forget gate.

$$i_q = \sigma(\omega_i.[b_{q-1}, x_q] + a_i) \quad (8)$$

i_q: Input gate activation vector at time step q.
ω_i: Weights for the input gate.
a_i: Bias for the input gate.

$$o_q = \sigma(\omega_o.[b_{q-1}, x_q] +) \quad (9)$$

o_q: Output gate activation vector at time step q.
ω_o: Weights for the output gate.
a_o: Bias for the output gate.

$$\tilde{c}_q = tanh(\omega_c.[b_{q-1}, x_q] + a_C) \quad (10)$$

$\tilde{c}_q$: The state vector of candidate cells at time step q
tanh: Activation function that uses hyperbolic tangents and returns values between -1 and 1
ω_c: Considerations for the potential cell state
a_C: The potential bias of cell state

$$c_q = f_q.c_{q-1} + i_q.\tilde{c}_q \quad (11)$$

c_q: Cell state vector at time step q.
c_{q-1}: Previous cell state vector.
.: Element-wise multiplication.

$$b_q = tanh(c_q) \quad (12)$$

b_q: Hidden state vector at time step q.

This recommended technique includes the usage of LSTM. The Foundation of LSTM is RNN, which looks at the sequence in both directions. Load forecasting, categorization, computer vision, and energy consumption prediction (ECP) are the areas in which LSTM has excelled.

3.4.2 CNN with LSTM

Utilizing the combined CNN and Bi-LSTM architecture proves highly effective in predicting ZDA under cyber security. Preprocessing data extracts the relevant features and label representation. LSTM captures temporal reliance, and CNN extracts spatial patterns from input data, such as network traffic logs. These networks are fused to integrate the spatial and temporary features that facilitate the model's ability to detect anomalies or deviations from the expected indication of ZDA. This model demonstrates robustness and accuracy in identifying previously unseen cyber threats through training, validation, and continuous monitoring. This model has been a valuable tool for proactive cyber security measures.

3.4.3 Applying with ResNet

ResNet-50, a residual neural network (ResNet) variant, is a 50-layer deep architecture known for its ability to improve accuracy by filtering more data, as discussed by Shaikh and Gupta [53]. ResNet models commonly incorporate skip connections, enabling the network to bypass one or more layers, effectively mitigating the vanishing gradient problem. These models frequently include double or triple-layer skipping, integrating nonlinear activations rectified linear unit (ReLU) and batch normalization to enhance stability and training efficiency.

Additionally, the Highway Network introduces an extra weight matrix to dynamically adjust the contribution of different layers, further improving DL performance. ResNet-50 follows a convolutional block sequence architecture, ending with an average pooling layer to refine feature extraction.

To evaluate ResNet's predictive accuracy, Mean Squared Error (MSE) is used as a performance metric. The ResNet model is applied to estimate traffic volumes across different road segments, aiming to achieve the closest alignment with real-world data. Consequently, the training objective of ResNet-50 minimizes MSE, as formulated in Equation 13.

$$MSE = \frac{1}{n}\sum_{i=1}^{N}(y_i)^2 \quad (13)$$

n: Total number of samples.
N: In the context of the given equation, Nis is the total number of samples, typically n. This represents the mistake or misrepresentation in the original data.
y_i: Actual value for i^{th}sample.
$(y_i)^2$: Squared difference between the actual and predicted values for i^{th} sample.

3.4.4 Bi-LSTM with ResNet

Here, training models provide the strategy for predicting domestic energy uses. These are as under:
In data preprocessing, mean value *m* is substituted for missing values in the column for the dataset's significant number of missing values. The provided formula is used to normalize the whole values in a min-max scaler with a range of [0, 1] to deal with the adhered data as per Equation 14.

$$m_n = \left[\frac{M - M_{min}}{M_{max} - M_{min}}\right] \quad (14)$$

m_n: Normalized value at a given time.
M: Original value at a given time step.
M_{min}: Minimum value.

M_{max}: Maximum value.

Normalized dataset values are M_{max}, M_{min} and m_n, where M is given the time step value. Preparing data helps to reduce time spent on computations. This ensures that no critical information is lost.
Before feature selection, the dataset is partitioned into features and labels using the sliding window technique. A labeled column with its current value utilizes the historical values as features. A 60-value window is required for the proposed method.

A model's network efficiency is improved or decreased depending on the design choices made during construction. Modifications to the kernel's size filter count and several methods are used throughout the test to validate the effect. This parameter has an impact on data-dependent network performance.

CNN uses the ReLU activation function in its last layer after the time-distributed convolution at each layer's beginning. After the CNN layer, the output is sent via the dense, LSTM, and time-distributed flattening layer. CNN-LSTM model layer has 64 convolution filters, 75 LSTM units, and one dense unit. With max pooling, there is precisely one kernel per layer. *Figure 6* shows the proposed method for determining the energy use.
1) In the first stage, information is cleaned and organized.
2) Features and labels are retrieved and analyzed before the data is separated into training and testing sets.
3) Each model's network architecture is checked using the various performance indicators.
4) Future energy consumption is accurately predicted by selecting the optimal model and architecture.

Hyperparameter tuning process for DC-nZDASN involves systematically optimizing the key parameters such as learning rate, batch size, number of layers and neurons (CNN layers (2, 4, 6, 8), LSTM units: (50, 100, 150, 200), dropout rate (0.1, 0.2, 0.3, 0.4, 0.5), activation functions (ReLU, Sigmoid, Tanh, Leaky ReLU), optimizers and number of epochs (10, 20, 50, 100, 200). This process uses a grid search (GS) for the initial comprehensive evaluation and random search (RS) for the efficiency and Bayesian optimization for fine-tuning. Criteria for selecting the optimal parameters include validation accuracy loss; F1-Score and ROC-AUC are used to prevent the overfit. Combining these techniques makes the model robust and performs high in achieving superior detection rates for ZDA.

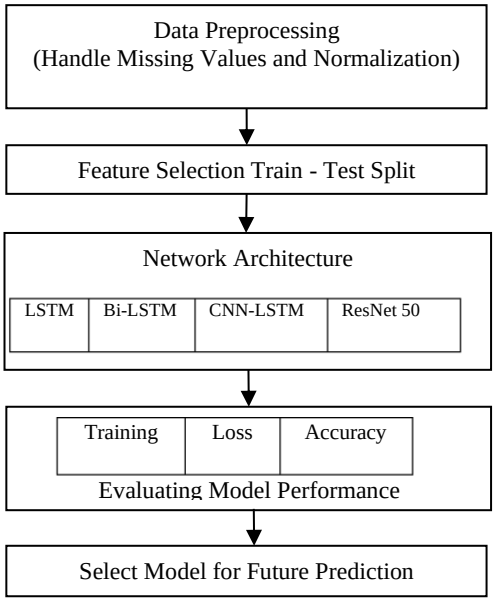

Figure 6 Proposed hybrid model for training and testing

Hyperparameter tuning involves techniques like GS, RS, Bayesian optimization, and K-Fold Cross-Validation. GS systematically evaluates the combinations of parameters (e.g., learning rates (1e-5, 1e-4) with batch sizes (32, 64) but are computationally expensive. RS randomly samples parameter combinations, offering rapid evaluations. Bayesian optimization uses probabilistic models such as Gaussian Processes to balance exploration and exploitation of efficient identification of optimal hyperparameters. K-Fold Cross-Validation splits data into k subsets, trains on k-1, and validates on one, ensuring robust generalization. Data is divided into training (60-70%), validation (10-20%), and testing (10-20%) sets, refining model performance and ensuring accurate evaluation.

3.5ML classifications

3.5.1 Decision tree algorithm

DT shows the attribute test as an internal node, test results as a branch and classes as a leaf node. The root node is shorthand for the tree's first node. Information gain, gain ratio, and G_iN_i The index is the most prevalent attribute selection metric used in the DT method. S is assumed as data collection, unique value m for the class label features, and g distinct classes are indicated by p_i (i, 1, 2 ... g). p_i is equal to the number of items in I class. Equation 15 gives the estimated data for each given sample for classification.

$$I(se_1, se_2, se_3, \ldots se_g) = \sum_{i=1}^{g} p_i log_2(p_i) \quad (15)$$

se_1: Number of samples in i[th] class.
se: Total number of samples.
p_i: Probability of a sample belonging to i[th] class, calculated as $p_i = \frac{se_1}{se}$
Entropy: A measure of impurity or disorder. Lower entropy means a real subset.
Where pi = se_i/ se is the chance of any sample belonging to the population.

ADT sorts a test tuple into many possible categories derived from the set of training tuples. A tuple is an item of information whose properties have been defined. D is the dataset that uses DT representation and contains T sets of training tuples as per Equation 16.

$$D => Q = [q_1, q_1, \dots, q_n] \quad (16)$$

D: The entire dataset.
Q: A set of tuples$[q_1, q_1, \dots, q_n]$.
q_i: Each tuple in the dataset, where i ranges from 1 to n (the total number of tuples).

The maximum number of tuples in the dataset is denoted by n.

3.5.2 Classification using linear SVM

A support vector (SV) is created to better categorize the new data sets by amplifying the information in the training set S. SVMs rely on recognizing the patterns. On data classification, SVM seeks the precise hyperplane that divides the overall data points into their respective classes. One of the two categories is hyperplane with motion.

Hence, the likelihood of incorrect classification is reduced; SVM in data is used to train or test the set. The SVM method is highly recommended because of its excellence in overall efficiency. Binary classification is the possible use of SVM. A proper multiclass approach is required to deal with the multiple data classification and identification classes. A simple binary classification issue is presented in Equation 17.

$$T = \{(X_1, Y_1), (x_2, y_2), (x_3, y_3) \dots \dots (x_n, y_n)\}, y_i \epsilon \{-1,1\}, x_i \epsilon R^d, \quad (17)$$

x_i : This is the data point.
y_i: Represents the corresponding label.
n: Denotes the number of training samples.
d:Indicates the dimensionality of data points.
$X_i$is the data point, and y_i is the corresponding label.
Training data set member is denoted as *n*. Linear SVM determines the ideal separation margin by assessing the optimization goal, as presented in Equations 18 and 19.

$$min\{\frac{1}{2}|a|^2 + p\sum_{i=1}^{l} s_i \geq 0 \quad (18)$$

$$subject\ to y_i(a^T w_i + b) \geq 1 - s_i, i = 1,2,3,4 \dots \dots l \quad (19)$$

a:Is the normal vector to the hyperplane.
b: Is the bias term (offset)
s_i: The slack variables allow some misclassification (for non-separable cases)
Parameter p regulates the trade-off between margin maximization and classification error minimization.

Normal vectors a, seal amount b, and S_i Are the positive slack variables using a Lagrangian multiplier?a_i. Minimum issues are up to the level that provides an optimum solution, as referred by Karush-Kuhn-Tucker criteria. If a_i is more significant than zero, information associated w_i is called SV. As a result, optimal values of a and b in the hyperplaneare are used to create the linear discriminative function, as shown in Equation 20.

$$f(x) = sgn(\sum_{i=1}^{l} \alpha_i z_i w_i^T w + b) \quad (20)$$

The liberated dual form of Equation 21 is:

$$max\left(\sum_{i,j=1}^{n} a_i, a_j, y_i, y_j\, x_i^T x_j\right) \quad (21)$$

To solve the issues, the utility of quadratic programming methods and Karush-Kuhn-Tucker is addressed in Haeser and Ramos [54]. Based on the findings, the possibility of denoting A as a linear combination of training vectors and b as the mean of SV is shown in Equations 22 and 23.

$$A = \sum_{i=1}^{l} \alpha_i z_i w_i \quad (22)$$

$$b = \frac{1}{N_{sv}} \sum_{i=1}^{N_{sv}} (A w_i - z_i) \quad (23)$$

N_{sv} Represents the number of supports in vector. While SVM provides an alternative method to recognize the categories, it visually involves considerable optimization and pairwise distance calculation time. When filtering the neighbors for sample issues, the local vector machine maintains the distance function of the neighbor group. In contrast to the closest neighbors and SVM, the efficient strategy undertaken by SVM performs better with multiclass data. This research classifies surface electromyography (SEMG) with a linear SVM classifier.

3.5.3 Naive bayes classifier

To simulate $B\left(\frac{M}{N}\right)$, M is the feature vector, and Y is the label per Equation 24.

$$B\left(\frac{M}{N}\right) = B\left(\frac{M_1}{N}\right) B\left(\frac{M_2}{N}\right) \ldots, B(\frac{M_Y}{N}) \quad (24)$$

Number of parameters is $nk + k - 1$. Data has to be practiced: M is the feature matrix, y_1 and y_n are the labels. Equations 25 and 26 present the above content as follows:

$$classprior: B(n) = |\{i: n_i = N\}|/y \quad (25)$$

$$Likelihood: pm_i(y) = \frac{B(m_i, n)}{B(N)} = \frac{\left|\{i: m_{ij} = m_i, n_i = n\}\right|/y}{|\{i: n_i = n\}|/y} \quad (26)$$

NB Classifier-Continuous: The below area improbability density function graphs between m_1 and m_2 denotes the likelihood that a random variable has a value between $m_1\ and\ m_2$, as shown in Equation 27.

$$f(m) = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{(m-\mu)^2}{2\sigma^2}} \quad (27)$$

μ: Mean of the feature values.
σ: Standard deviation of the feature values.
m: Feature value.
This function represents the likelihood of feature value m, the given meanμ, and standard deviationσ.

3.5.4 Gaussian parameter estimation

Parameters are the Gaussian distribution's mean σ and variation.σ^2. The given observations $m_1, \ldots, m_y$ and the chance of those observations for a given σ^2 assumed from Gaussian distribution is given in Equation 28.

$$B\left(m_1, \ldots, m_y \middle| \mu, \sigma^2\right) = \prod_{y-1}^{y} \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{(m_n-\mu)^2}{2\sigma^2}} \quad (28)$$

m_n: Observation n.
μ: Mean of Gaussian distribution.
σ^2: Variance of Gaussian distribution.
It represents the product of the probability density function values under each observation in Gaussian distribution, as shown in Equation 29.

$$L(\mu, \sigma) = -\frac{1}{2} N log(\pi\sigma^2) - \sum_{n=1}^{N} \frac{(x_n-\mu)^2}{2\sigma^2} \quad (29)$$

N: Total number of observations.
It combines the logarithm of the Gaussian probability density function for every observation, making it easier to differentiate and find the maximum likelihood estimates (MLE) of μ and $2\sigma^2$.
Taking the derivative of the desired variable and solving determines the values of two, which maximize the log-likelihood. As a result, the MLE of the mean is provided in Equation 30.

$$\mu = \frac{1}{Y} \sum_{y=0}^{y} m_y \quad (30)$$

Equation 31 represents the arithmetic mean of observations. It is derived by setting the derivative of the log-likelihood function μ to zero and solving the function.

MLE of the variance is

$$\sigma^2 = \frac{1}{Y} \sum_{y=0}^{Y} (m_n - \mu^2) \quad (31)$$

This equation represents the variance of observations. It is derived by setting the derivative of the log-likelihood function from σ^2 to zero and solvingσ^2.

3.5.5 LR

LR is a technique for learning functions in which $M = M_1 \ldots M_y$ are the vectors of discrete or continuous variables, and the vectors for discrete-valued is N either f, M, N, or B $\left(\frac{N}{Y}\right)$. This section covers the case when N is a Boolean variable. At last, the investigation is extended to include the case of N taking the small set of possible values. In LR, P $\left(\frac{N}{M}\right)$distribution is assumed to have a parametric shape, and its parameters are derived from the training data. Equation 32 presents the discrete-valued.

$$B(N = 1|m) = \frac{1}{1+exp\ (W_o + \sum_{i=1}^{y} w_i m_i)} \quad (32)$$

By rewriting$\left(\frac{N}{M}\right)$, a convenient linear classification equation is formed. Assigning an NK value which maximizes B $\left(N = \frac{Nk}{M}\right)$ is the standard classification method. On the other hand, N = 0 is determined if the following holds, as per the Equations 33 to 35.

$$1 < \frac{B(N=0|M)}{B(N=1|M)} \quad (33)$$

On combining, these equations become

$$1 < exp\ (w_0, + \sum_{i=1}^{y} w_i m_i) \quad (34)$$

The linear classification rule is obtained by taking the natural log of both sides i as follows: if M satisfies, then N = 0; otherwise, N = 1

$$0 < w_0 + \sum_{i=1}^{y} w_i M_i \quad (35)$$

3.5.6 Stacking ensemble

Data is gathered over extended durations. After taking T real-value samples $x_1, \ldots, x_T$, output is I divided by the time T$(1 \leq I \leq h)$. Time series forecast compares the expected and actual $xw + i$ values using the historical data from samples $x_1 \ldots x_w$ $(w + h \leq T)$ $(1 \leq I \leq h)$. In this expression, two variables are required: w representing the time frame in the historical window and h representing the time frame in the prediction horizon.

Traditionally, the time sequence is divided into three parts. Different patterns are seen in the time sequence. Remains of time series data illustrate the process of extensive irregular data hiding seasonality and information.

Examining the other breakdown patterns, time effects, and other long-term trends are illuminated. The inherent unpredictability of real-world time series is forecasted notoriously. On top of that, checking of stationary time series is carried out.

Any non-stationary time series needs transformation before using the forecasting model. The number of variables that are compared distinguishes the study of univariate and multivariate time series. Data is strictly chronological and present in univariate time series. At each time point, values of several variables are recorded in multivariate time series. Understanding the connection between these factors is essential. Time series predictions are made using a few different methods. ML techniques for nonlinear modeling prediction have become more significant, and the traditional approaches provide adequate results for linear situations.

3.5.7 Ensemble learning

Enhanced classification and regression performance have increased in popularity, and the models have gained traction recently. These techniques combine several learning models to boost the performance of each model. According to early 1990s ensemble learning research, several relatively weak learning algorithms are combined to create robust algorithms. Ensemble learning makes predictions using several learner modules from a single data set. A single prediction is made when all the expert guesses are added together. This technique typically has two stages. Training data is mined for the set of learners, which are later included in a single prediction model. Several forecasts use the diverse information from varied base models to build the composite model. The improved composite model often outperforms the group of individual models. Ensemble learning is valuable in ML. It is possible to interpret the model by systematically searching for the most promising hypothesis. As the datasets are typically restricted, prediction is improved and performed better on unknown data. This complicates the task of theory selection. Ensemble methods need reasonable approximation of unknowable true hypotheses to address this challenge. The above content is provided in Equation 36.

$$y_{ensemble} = \frac{1}{N}\sum_{i=1}^{N} y_i \quad (36)$$

In ensemble learning, predictions from individual base models y_i are combined using techniques like majority voting or weighted average to arrive at the final prediction$y_{ensemble}$.

Systematic difficulty is the local search often used to reduce the number of incorrect predictions made by ML models. Local optimization impedes these types of global searches. Genuine unknown functions are understood better when the local searches launch from different starting points. Bagging is a method where multiple models are created and compared with the objective results. As a result, a majority vote arrives at the final decision. This procedure is known as bagging. Typically, regression makes an average prediction. There is a single conceptual distinction between boosting and bagging. Instead of assigning equal importance to each model, boosting uses weighted voting to decide the final score. Most regression procedures end with the weighted average. Predictions from the underlying algorithms are used to train the combiner algorithm in making the final predictions. This approach has been used in any ensemble approach. The regression problem in this research is handled by using the stacking technique.

$$y_{bagging} = \frac{1}{N}\sum_{i=1}^{N} y_i \quad (37)$$

Equation 37 shows the replacement use; bagging creates several models, training on separate data subsets, and averages their predictions.

For parallelizing computations and efficient matrix operations during DL model training, systematic resources are used for DC-nZDASN, including the high-performance graphic processing unit (GPUs) such as NVIDIAGeForce RTX or Tesla series. A multi-core central processing unit (CPU)'s complements GPU processing for non-GPU tasks such as data preprocessing. Cloud resources like amazon web services (AWS), google cloud platform (GCP), and Azure are used for scalability. While demanding systematic power, malware featuring GPU support, such as AWS EC2 GCP compute engine, is used for DL tasks. Cloud-based solutions like AWS simple storage service (AWS S3) and GCP cloud storage store large datasets and trained models, whereas technologies like Docker and Kubernetes manage ML workflows efficiently in the cloud. Software tools like Tensor Flow, PyTorch, Pandas, NumPy, and Scikit-learn are implemented for model building, while data preprocessing, evaluation, and cloud management tools aid in resource provision and monitoring. This combination of hardware,

cloud, and software resources optimizes the performance and scalability of DC-nZDN's complex requirements.

For parallelizing computations and enabling efficient matrix operations during DL model training, systematic resources are utilized in DC-nZDASN. This includes high-performance graphics processing units (GPUs) such as NVIDIA GeForce RTX or Tesla series, which accelerate model training. Additionally, multi-core central processing units (CPUs) complement GPU processing by handling non-GPU tasks like data preprocessing. To ensure scalability, cloud resources such as AWS, GCP, and Microsoft Azure are employed. For GPU-intensive DL tasks, cloud-based instances like AWS EC2 and GCP Compute Engine provide the necessary computational power. Large datasets and trained models are stored using AWS Simple Storage Service (AWS S3) and GCP Cloud Storage. For efficient ML workflow management, containerization and orchestration tools like Docker and Kubernetes are used. Additionally, software tools such as TensorFlow, PyTorch, Pandas, NumPy, and Scikit-learn support model building, data preprocessing, evaluation, and cloud resource monitoring. This integrated combination of hardware, cloud computing, and software tools optimizes DC-nZDASN's performance, scalability, and resource efficiency, ensuring smooth execution of complex DL workloads.

4.Results and discussion

The system monitors active nodes in the network, identifying those with a high probability of ZDA occurrence. Nodes flagged as potential threats are isolated to prevent further communication and enhance security. MSE values and threshold-based predictions are adjusted to improve ZDA detection and mitigation.

Table 1 outlines the LSTM and ResNet parameters, including input size, padding, activation functions, and step size, providing a structured evaluation of model performance. Features are categorized as numerical, nominal, or binary, with 41 features from the NSL-KDD dataset considered and validated using the DC-nZDASN model. Among them, 18 key features are identified as the most influential in different classification processes.In label training classifiers, standard sample characteristics are used to detect DoS, Probe, R2L, and U2R attacks. Preprocessed test data is fed into the training classifier, which classifies and identifies samples. Detection results are validated through model verification and test comparisons performed in a Windows operating system (OS) environment.

To improve computational efficiency, parallel computing is implemented. The threshold limit for selecting dataset feature values is predicted, and error values are identified. The dataset is partitioned into training and testing sets based on the four attack types (U2R, R2L, Probe, and DoS) for further processing, as detailed in *Table 2*.

The TP, FP, TN, and FN values are shown in *Figure 7*, representing the confusion matrix. The anticipated class for TP is 28, TN is 17, and FP and FN are 0.

Table 1 LSTM with ResNet parameters

Layers	Type	Size	Padding	Activation function	Step	Classification based on feature inputs
Layer 1	Multi-Layer Convolution	1×1, 3×3, 5×5, 7×7	0 1 2	ReLU	1	11 × 11 × 64
Layer 2	Convolution Layer	3×3		ReLU	1	9 × 9 ×64
Layer 3	Multi-Layer Convolution	1×1, 3×3, 5×5, 7×7	0 1 2	ReLU	1	9 ×9 ×128
Layer 4	Convolution Layer	3×3		ReLU	1	7 × 7 × 128
Layer 5	Multi-Layer Convolution	1×1, 3×3, 5×5, 7×7	0 1 2	ReLU	1	7 ×7 ×256
Layer 6	Pooling Layer	3×3	-	ReLU	2	3 ×3 ×256
Layer 7	Fully Connected Layer	-	-	Sigmoid	-	256
Layer 8	Fully Connected Layer	-	-	Sigmoid	-	64
Layer 9	Fully Connected Layer	-	-	Sigmoid	-	5

Table 2 Attack types and corresponding training / testing set

Attacks	Training set	Testing set
U2R	Ps, Buffer Overflow, Rootkit, Load Module	Perl, Ps, Buffer Overflow, Xterm, Sqlattack
R2L	Warezmaster, Phf, Multi-Hop, internet message access protocol (IMAP), Guess	Ftpwrite, Httptunnel, IMAP, Named, Phf, Multi-hop, Send mail, Snmpgetattack, Wxlock, Snmpguess, Warezmaster, Xsnoop.

Attacks	Training set	Testing set
	Password, Ftpwrite, Spy, Warezclient	
Probe	Satan, Portsweep, Nma, Ipsweep	Msacn, Saint, Satan, Nmap, Portsweep, Ipsweep
DoS	Neptune, Smurf, Back, land, Pod, Teardrop	Udpstrom, Smurf, Worm Process Table, Teardrop, Pod, Neptune, Back, Land, Apache2, Mailbomb

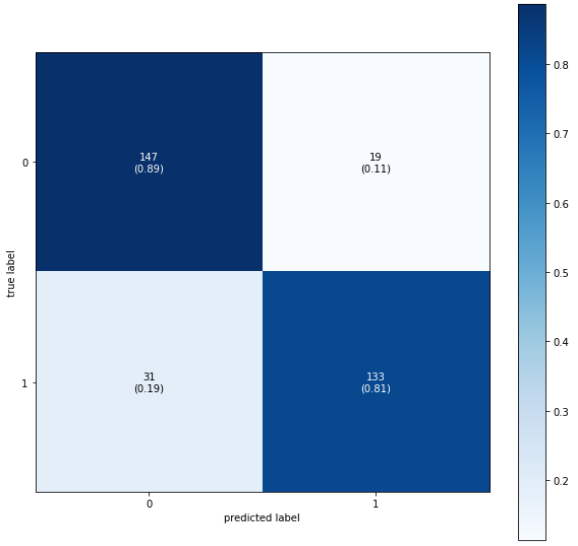

Figure 7 Confusion matrix

4.1Performance metrics

After analyzing the results using a multi-category classification framework, the feature importance accuracy is determined to be 87.58%. Additionally, the one-versus-the-rest method is employed by converting the multi-class classification problem into binary classification sub-problems to enhance prediction accuracy.

The classification components are defined as follows:

a. TP_d: Class D describes both forecast and actuality.
b. TN_d: Some categories of d are the focus of the forecast.
c. FP_d: Category d is the predicted outcome; however, more categories are inside category d in practice.

Every category is used as a positive sample to compute the overall accuracy, precision, and recall. Equation 38 represents the mathematical formulation for accuracy.

$$Accuracy = Numberofsamplescorrectlyclassified\ Numeberofsamplesforallcategories \quad (38)$$

Equation 39 shows that comparing the sample's accuracy with the category's precision is one approach for examining accuracy.

$$Precision_i = TP_dTP_d + FP_d \quad (39)$$

The recall of a specific category measures how well the model correctly identifies instances of category d from the total actual occurrences of that category (Equation 40).

$$Recall_i = \frac{TP_d}{TP_d + FN_d} \quad (40)$$

Equation 41 calculates the F1-score.

$$F1 - score = 2.\frac{Precision.recall}{Nprecison+recall} \quad (41)$$

Findings of training and testing the proposed model on celosia and NSL-KDD datasets are presented in *Table 3*. The experiments use ResNet50 combined with LSTM for the training and testing phases.

Table 3 Training and testing performance of ResNet50-LSTM Model on NSL-KDD and Celosia datasets over 10 epochs

Epoch	Training loss	Validation loss	Training accuracy	Testing accuracy
1	0.0039	0.0626	0.9987	0.9846
2	0.0035	0.0762	0.9989	0.9835
3	0.0030	0.0699	0.9991	0.9853
4	0.0039	0.0643	0.9986	0.9862
5	0.0017	0.0684	0.9995	0.9866
6	0.0030	0.0747	0.9991	0.9858
7	0.0026	0.0887	0.9991	0.9844
8	0.0023	0.0776	0.9992	0.9855
9	0.0023	0.0749	0.9992	0.9868
10	0.0013	0.0767	0.9996	0.9876

The proposed model's training and testing loss parameters are shown in *Figure 8*. The Y-axis displays the loss amount, and the X-axis displays the number of epochs. *Figure 9* shows that CNN-ResNet has trained 10 epochs with testing and training accuracy. As the X-axis displays the epoch numbers, the Y-axis displays the accuracy.

Table 4 presents a comparative analysis of different ML algorithms, including DT, SVM, GNB, LR, and the stacking ensemble classifier, based on their accuracy, precision, recall, and F1-score. The evaluation is conducted on two datasets: NSL-KDD and Celosia, demonstrating the effectiveness of

different classifiers in detecting cyber threats. The stacking ensemble classifier achieves the highest performance across both datasets.

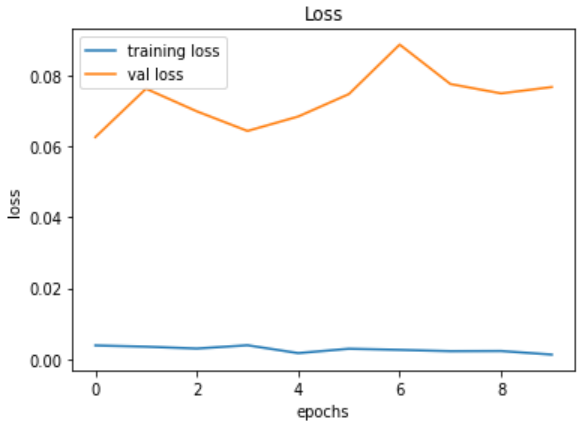

Figure 8 Training and testing loss

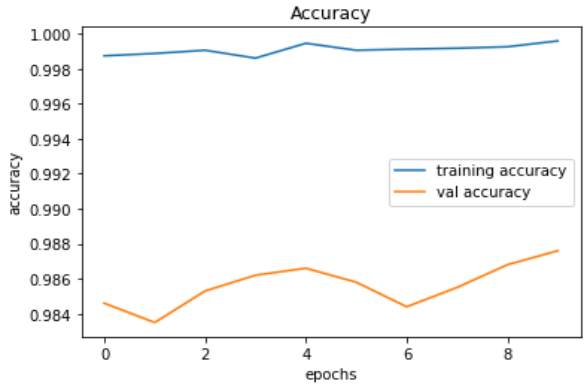

Figure 9 Training and testing accuracy

The proposed model achieves a classification accuracy of 95.09%, surpassing existing techniques in ZDA detection. This high accuracy is crucial for strengthening cybersecurity measures. The key findings of the model are as follows:

1. The model integrates DL architectures such as ResNet50, LSTM, and CNNs, enhancing learning stability and enabling the detection of zero-day threats by recognizing complex internal patterns.
2. The model generates synthetic malware, employs advanced preprocessing techniques, feature selection methods, and ensemble classifiers, significantly improving its ability to detect novel and previously unseen threats.
3. Leveraging cloud-based resources and GPU acceleration, the model ensures efficient data handling, faster training of DL models, and scalability, making it suitable for large-scale datasets and complex security tasks.
4. Strategies such as class weight adjustment, cross-validation, and appropriate evaluation metrics enhance the model's ability to generalize across diverse datasets, reducing overfitting and mitigating bias toward majority classes.
5. The model significantly strengthens threat detection and mitigation strategies, contributing to a more effective and proactive cybersecurity framework.

A complete list of abbreviations is listed in *Appendix I.*

Table 4 Algorithm performance comparison on NSL-KDD and celosia datasets

Dataset	Algorithm	Accuracy (%)	Precision	Recall	F1-score
Dataset 1: NSL-KDD	DT	88	87	90	88
	SVM	83	81	88	84
	GNB	90	91	89	90
	LR	85	83	89	85
	Stacking ensemble classifier	95.9	89.5	88.4	89
Dataset 2: Celosia	DT	91.75	91	92	92
	SVM	71	71	70	71
	GNB	83	87	78	82
	LR	71	72	70	71
	Stacking ensemble classifier	95.9	92.3	91.1	91.7

Figure 10 box plot compares the performance distribution of different classification algorithms based on an evaluation metric such as accuracy. The hybrid model (Stacking ensemble classifier) and SVM exhibit the highest median performance with lower variability, while DT shows the lowest accuracy and higher dispersion, indicating inconsistency in its predictions. The green triangles represent the mean values for each classifier.

Limitations

Despite its effectiveness, the model has certain limitations:

1. The model's performance heavily relies on accurate, diverse, and well-labeled training datasets, which may not always be available.
2. The implementation requires high-performance GPUs and cloud-based infrastructure, making it resource-intensive and potentially costly.
3. The model may struggle to adapt to rapidly evolving attack methods, requiring continuous updates and retraining.
4. Although the model reduces misclassification, completely eliminating false alarms remains a challenge.
5. While the model employs various generalization techniques, emerging threats that differ significantly from training data may still pose detection challenges.

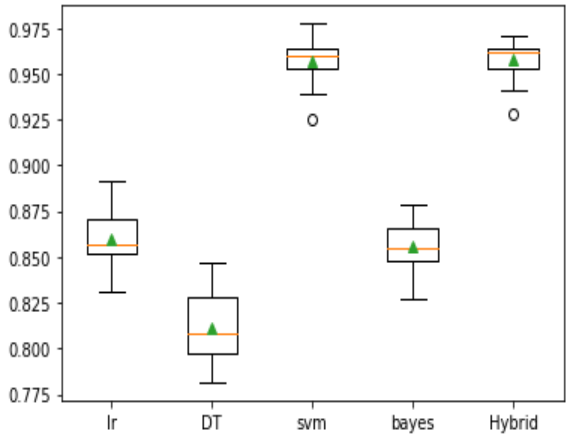

Figure 10 Stacking ensemble classifications (SEC) comparison chart

5.Conclusion and future work

The proposed DC-nZDASN model effectively enhances ZDA detection, achieving a classification accuracy of 95.09%, surpassing traditional methods. By integrating ResNet50, LSTM, and CNN, the model improves learning stability and effectively identifies new and evolving cyber threats. The inclusion of synthetic malware generation, advanced preprocessing techniques, and ensemble classifiers further strengthens its robustness against previously unseen attacks. Utilizing cloud-based resources and GPU acceleration, the model ensures efficient data processing, scalability, and rapid training. Additionally, techniques such as class weight adjustment, cross-validation, and diverse evaluation metrics improve generalization and reduce overfitting. The model achieves a classification accuracy of 95.09%, outperforming other methods and enhancing new threat detection capabilities.

Despite these promising results, continuous research and updates are necessary to address the ever-evolving nature of ZDAs and maintain long-term effectiveness. To improve generalizability, the model requires further testing and validation with diverse datasets and real-time streaming data. Future work will focus on enhancing ZDA classification by integrating DL and ML in IDS, refining adaptability through self-learning mechanisms, and introducing real-time streaming data analysis for dynamic threat detection. Additional improvements include simulation techniques for better training data quality and collaborations with industry experts to ensure real-world applicability.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

Data availability

The dataset used in this study is publicly available and can be accessed at the following links:
Dataset 1: NSL-KDD – https://www.kaggle.com/datasets/hassan06/nslkdd
Dataset 2: Celosia – https://www.kaggle.com/code/mkashifn/celosia-zero-day-attack-detection-demo

Author's contribution statement

Swathy Akshaya: Methodology, data curation, analysis and testing of experimental results, manuscript preparation, plagiarism check, and proofreading. **Padmavathi. G:** Supervised and reviewed the manuscript. All authors have read and approved the final manuscript.

References

[1] Das N, Sarkar T. Survey on host and network based intrusion detection system. International Journal of Advanced Networking and Applications. 2014; 6(2):2266- 9.
[2] Ahmed M, Mahmood AN, Hu J. A survey of network anomaly detection techniques. Journal of Network and Computer Applications. 2016; 60:19-31.
[3] Ahmad R, Alsmadi I, Alhamdani W, Tawalbeh LA. Zero-day attack detection: a systematic literature review. Artificial Intelligence Review. 2023; 56(10):10733-811.
[4] Bou-harb E, Debbabi M, Assi C. Cyber scanning: a comprehensive survey. IEEE Communications Surveys & Tutorials. 2013; 16(3):1496-519.
[5] Soltani M, Ousat B, Siavoshani MJ, Jahangir AH. An adaptable deep learning-based intrusion detection system to zero-day attacks. Journal of Information Security and Applications. 2023; 76:103516.
[6] Khraisat A, Gondal I, Vamplew P, Kamruzzaman J. Survey of intrusion detection systems: techniques,

datasets and challenges. Cybersecurity. 2019; 2(1):1-22.
[7] Kumar GS, Kumar RK, Kumar KP, Sai NR, Brahmaiah M. Deep residual convolutional neural network: an efficient technique for intrusion detection system. Expert Systems with Applications. 2024; 238:121912.
[8] Hubballi N, Suryanarayanan V. False alarm minimization techniques in signature-based intrusion detection systems: a survey. Computer Communications. 2014; 49:1-7.
[9] Ibrahim HB, Aslan HK, Elsayed MS, Jurcut AD, Azer MA. Anomaly detection of zero-day attacks based on CNN and regularization techniques. Electronics. 2023; 12(3):1-18.
[10] Bhuyan MH, Bhattacharyya DK, Kalita JK. Network anomaly detection: methods, systems and tools. IEEE Communications Surveys & Tutorials. 2013; 16(1):303-36.
[11] Verma P, Bharot N, Breslin JG, O'shea D, Vidyarthi A, Gupta D. Zero-day guardian: a dual model enabled federated learning framework for handling zero-day attacks in 5G enabled IIoT. IEEE Transactions on Consumer Electronics. 2023; 70(21):3856-66.
[12] Peppes N, Alexakis T, Adamopoulou E, Demestichas K. The effectiveness of zero-day attacks data samples generated via GANs on deep learning classifiers. Sensors. 2023; 23(2):1-21.
[13] Creech G, Hu J. A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns. IEEE Transactions on Computers. 2013; 63(4):807-19.
[14] Mukkamala S, Janoski G, Sung A. Intrusion detection using neural networks and support vector machines. In proceedings of the international joint conference on neural networks 2002 (pp. 1702-7). IEEE.
[15] Bajaj K, Arora A. Dimension reduction in intrusion detection features using discriminative machine learning approach. International Journal of Computer Science Issues. 2013; 10(4):324-8.
[16] Lecun Y, Bengio Y, Hinton G. Deep learning. Nature. 2015; 521(7553):436-44.
[17] Farahnakian F, Heikkonen J. A deep auto-encoder based approach for intrusion detection system. In 20th international conference on advanced communication technology 2018 (pp. 178-83). IEEE.
[18] Hnamte V, Nhung-nguyen H, Hussain J, Hwa-kim Y. A novel two-stage deep learning model for network intrusion detection: LSTM-AE. IEEE Access. 2023; 11:37131-48.
[19] Nagasundari S, Honnavali PB. SQL injection attack detection using ResNet. In 10th international conference on computing, communication and networking technologies 2019 (pp. 1-7). IEEE.
[20] Shun J, Malki HA. Network intrusion detection system using neural networks. In fourth international conference on natural computation 2008 (pp. 242-6). IEEE.
[21] Alshehri A, Badr MM, Baza M, Alshahrani H. Deep anomaly detection framework utilizing federated learning for electricity theft zero-day cyberattacks. Sensors. 2024; 24(10):1-19.
[22] Sakthimurugan S, Kumaar S, Vignesh V, Santhi P. Assessment of zero-day vulnerability using machine learning approach. EAI Endorsed Transactions on Internet of Things. 2024; 10:1-6.
[23] Aburomman AA, Reaz MB. A novel SVM-kNN-PSO ensemble method for intrusion detection system. Applied Soft Computing. 2016; 38:360-72.
[24] Alazab A, Khresiat A. New strategy for mitigating of SQL injection attack. International Journal of Computer Applications. 2016; 154(11):1-10.
[25] Ji SY, Jeong BK, Choi S, Jeong DH. A multi-level intrusion detection method for abnormal network behaviors. Journal of Network and Computer Applications. 2016; 62:9-17.
[26] Butun I, Morgera SD, Sankar R. A survey of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys & Tutorials. 2013; 16(1):266-82.
[27] Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Computers & Security. 2012; 31(3):357-74.
[28] Skaruz J, Seredynski F. Recurrent neural networks towards detection of SQL attacks. In international parallel and distributed processing symposium 2007 (pp. 1-8). IEEE.
[29] Elsherif A. Automatic intrusion detection system using deep recurrent neural network paradigm. Journal of Information Security and Cybercrimes Research. 2018; 1(1):21-31.
[30] Osa E, Orukpe PE, Iruansi U. Design and implementation of a deep neural network approach for intrusion detection systems. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024; 7:1-6.
[31] Idhammad M, Afdel K, Belouch M. Semi-supervised machine learning approach for DDoS detection. Applied Intelligence. 2018; 48:3193-208.
[32] Lin WC, Ke SW, Tsai CF. CANN: an intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-Based Systems. 2015; 78:13-21.
[33] Staudemeyer RC. Applying long short-term memory recurrent neural networks to intrusion detection. South African Computer Journal. 2015; 56(1):136-54.
[34] Sarhan M, Layeghy S, Gallagher M, Portmann M. From zero-shot machine learning to zero-day attack detection. International Journal of Information Security. 2023; 22(4):947-59.
[35] Jose J, Jose DV. AS-CL IDS: anomaly and signature-based CNN-LSTM intrusion detection system for internet of things. International Journal of Advanced Technology and Engineering Exploration. 2023; 10(109):1-18.
[36] Alazab A, Abawajy J, Hobbs M, Layton R, Khraisat A. Crime toolkits: the productisation of cybercrime. In 12th international conference on trust, security and

privacy in computing and communications 2013 (pp. 1626-32). IEEE.
[37] Pascanu R, Stokes JW, Sanossian H, Marinescu M, Thomas A. Malware classification with recurrent networks. In international conference on acoustics, speech and signal processing 2015 (pp. 1916-20). IEEE.
[38] Arun A, Nair AS, Sreedevi AG. Zero day attack detection and simulation through deep learning techniques. In 4th international conference on cloud computing, data science & engineering (confluence) 2024 (pp. 852-7). IEEE
[39] Oluwadare S, Elsayed Z. A survey of unsupervised learning algorithms for zero-day attacks in intrusion detection systems. In the international FLAIRS conference proceedings 2023 (pp. 1-3). FLAIRS.
[40] Aljawarneh SA. Emerging challenges, security issues, and technologies in online banking systems. In online banking security measures and data protection 2017 (pp. 90-112). IGI Global.
[41] Demirel DY, Sandikkaya MT. Web based anomaly detection using zero-shot learning with CNN. IEEE Access. 2023; 11:91511-25.
[42] Bai S, Kolter JZ, Koltun V. Convolutional sequence modeling revisited. ICLR Workshop. 2018 (pp. 1-20).
[43] Roy SS, Mallik A, Gulati R, Obaidat MS, Krishna PV. A deep learning based artificial neural network approach for intrusion detection. In mathematics and computing: third international conference, ICMC 2017 (pp. 44-53). Springer Singapore.
[44] Habibi O, Chemmakha M, Lazaar M. Performance evaluation of CNN and pre-trained models for malware classification. Arabian Journal for Science and Engineering. 2023; 48(8):10355-69.
[45] Hindy H, Atkinson R, Tachtatzis C, Colin JN, Bayne E, Bellekens X. Utilising deep learning techniques for effective zero-day attack detection. Electronics. 2020; 9(10):1-16.
[46] Yin C, Zhu Y, Fei J, He X. A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access. 2017; 5:21954-61.
[47] Swathy AM, Padmavathi G. Zero-day attack path identification using probabilistic and graph approach based back propagation neural network in cloud. Mathematical Statistician and Engineering Applications. 2022; 71(3s2):1091-106.
[48] Dhanya KA, Vajipayajula S, Srinivasan K, Tibrewal A, Kumar TS, Kumar TG. Detection of network attacks using machine learning and deep learning models. Procedia Computer Science. 2023; 218:57-66.
[49] Akshaya S, Padmavathi G. Enhancing zero-day attack prediction a hybrid game theory approach with neural networks. International Journal of Intelligent Systems and Applications in Engineering. 2024; 12:643-63.
[50] https://www.kaggle.com/datasets/kaggleprollc/nsl-kdd99-dataset/data. Accessed 20 February 2025.
[51] https://www.kaggle.com/code/mkashifn/celosia-zero-day-attack-detection-demo/input. Accessed 20 February 2025.
[52] Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. In symposium on computational intelligence for security and défense applications 2009 (pp. 1-6). IEEE.
[53] Shaikh A, Gupta P. Real-time intrusion detection based on residual learning through ResNet algorithm. International Journal of System Assurance Engineering and Management. 2022:1-5.
[54] Haeser G, Ramos A. Constraint qualifications for Karush–Kuhn–Tucker conditions in multiobjective optimization. Journal of Optimization Theory and Applications. 2020; 187:469-87.

Swathy Akshaya is a Research Scholar in Computer Science at Avinashilingam University. She has published research articles in reputed national and international conferences, journals, and book chapters. Her research interests primarily include Cloud Computing and Cybersecurity.
Email: akshayakulandaivel@gmail.com

Padmavathi. G is the Dean of the School of Physical Sciences and Computational Sciences and a Professor in the Department of Computer Science at Avinashilingam Institute for Home Science and Higher Education for Women (Deemed to be University), Coimbatore. She has over 33 years of teaching experience and 25 years of research experience. Her research interests include Cybersecurity, Wireless Communication, and Real-Time Systems.
Email: padmavathi.avinashilingam@gmail.com

Appendix I

S. No.	Abbreviation	Description
1	AE	Auto-Encoder
2	AO	Adam Optimization
3	AUC	Area Under the Curve
4	AUC-ROC	Area Under the Curve - Receiver Operating Characteristic
5	AWS	Amazon Web Services
6	Bi-LSTM	Bidirectional Long Short-Term Memory
7	BPNN	Backpropagation Neural Networks
8	CANN	Center And Nearest Neighbor
9	CNN	Convolutional Neural Network
10	CNN-LSTM	Convolutional Neural Network with Long Short-Term Memory
11	CPU	Central Processing Unit
12	CSV	Comma-Separated Values
13	DCNN	Deep Convolutional Neural Network
14	DC-nZDASN	Deep Convolutional Zero-Day Adversarial Safety Network
15	DL	Deep Learning
16	DoS	Denial-of-Service
17	DDoS	Distributed Denial-of-Service
18	DT	Decision Tree
19	DTR	Decision Tree Regression
20	ECP	Energy Consumption Prediction

21	FL	Federated Learning
22	FP	False Positives
23	GAN	Generative Adversarial Network
24	GCP	Google Cloud Platform
25	GNB	Gaussian Naïve Bayes
26	GPU	Graphics Processing Unit
27	GS	Grid Search
28	GT	Game Theory
29	HGT	Hybrid Game Theory
30	IDS	Intrusion Detection Systems
31	IoT	Internet of Things
32	IMAP	Internet Message Access Protocol
33	LR	Logistic Regression
34	LSTM	Long Short-Term Memory
35	ML	Machine Learning
36	MLE	Maximum Likelihood Estimates
37	MSE	Mean Squared Error
38	NN	Neural Network
39	NSL- KDD	National Science Library- Knowledge Discovery In Databases
40	OS	Operating System
41	RF	Random Forest
42	ReLU	Rectified Linear Unit
43	R2L	Remote-to-Local
44	ResNet50	Residual Network
45	RNN	Recurrent Neural Network
46	RS	Random Search
47	SEC	Stacking Ensemble Classification
48	SEMG	Surface Electromyography
49	SMOTE	Synthetic Minority Over-sampling Technique
50	SV	Support Vector
51	SVM	Support Vector Machine
52	TCN	Temporal Convolutional Networks
53	SQL	Structured Query Language
54	U2R	User-to-Root
55	ZDA	Zero-Day Attack
56	ZSL	Zero-Shot Learning
57	IOB	In-of-Bag

ENHANCING CYBER DEFENSE AGAINST ZERO-DAY ATTACKS USING ENSEMBLE NEURAL NETWORKS

Swathy Akshaya and Padmavathi

Department of Computer Science, Avinashilingam University, Coimbatore, India

ABSTRACT

Zero-Day Attacks (ZDAs) are a significant concern for cybersecurity as they take advantage of previously unknown vulnerabilities in software systems. This lack of prior knowledge makes ZDAs extremely difficult to detect as they operate in stealth mode, often evolving as new ideas and approaches emerge in the cybersecurity landscape. Herein, we introduce a hybrid deep learning framework comprising four models, including Artificial Neural Network – Auto Encoder (ANN-AE), ResNet50, CNN-LSTM, and Modified Bi-LSTM with Game Theory (GT), to improve the prediction and detection of ZDAs. Each model is used in a particular manner: ANN-AE for feature compression and anomaly detection, ResNet50 for feature extraction, CNN-LSTM for capturing spatio-temporal patterns, and Bi-LSTM with GT for modelling attacker-defender interactions. To enhance accuracy and model reliability, we applied the Optimised Levy Flight-based Optimisation Algorithm (OLFOA) in hyperparameter optimisation. We empirically evaluated the proposed approach on two publicly available benchmark datasets, achieving favourable results, specifically high detection accuracy, low false alarm rates, and low computational cost. Our results substantiate the proposed approach to facilitate real-time ZDA prediction and detection and denote the potential for future application in cybersecurity.

KEYWORDS

Zero-Day Attack Prediction, Hybrid Game Theory, Transfer Learning, ResNet50, ANN-AE, CNN-LSTM, Bi-LSTM, Ensemble Neural Networks, OLFOA.

1. INTRODUCTION

In the ever-changing field of cybersecurity, there is a threat called a Zero-Day Attack (ZDA). A ZDA takes advantage of vulnerabilities that hardware or software manufacturers didn't even know existed. The creation of ZDA attacks is particularly critical as they occur before the initial manufacturing patch is released or before an actual signature detection (or Deep Learning (DL)) has any hope of responding [1]. ZDAs become more prevalent and sophisticated, demanding an urgent need for intelligent, adaptive, and innovative detection methods to anticipate ZDA attacks in real-time [2-4]. To address this issue, this research proposes a new deep learning-based ensemble detection framework for predicting ZDAs. The proposed framework consists of four different complementary DL models, where each model has a specific function in detecting ZDAs: The Artificial Neural Net Auto Encoder (ANN-AE) serves as the unsupervised anomaly detection model to compress the feature space, the ResNet50 model performs hierarchical deep feature extraction, the Convolutional Neural Network-Long Short Term Memory (CNN-LSTM) performs the spatio-temporal nature of the attack patterns, and modified Bi-directional LSTM with Game Theory (Bi-LSTM + GT) is used to sequentially predict and model the behavior of the attacker and defenders [5-7].

Multiple models can identify different patterns of behaviour of ZDAs using a raw signal of anomalies, to the more advanced and evolving multi-stage sequences of attacks [8-10]. The

DOI: 10.5121/ijcnc.2025.17408

Optimised Levy Flight-Based Optimisation Algorithm (OLFOA) improves the ensemble's performance. OLFOA is inspired by natural Levy flights' random and distant movement patterns [11] [12]. This randomness allows for better global exploration and discovering patterns to balance global explorations and local exploitations in the search space [13]. As such, OLFOA can optimise hyperparameters such as learning rates, dropout values, and architecture (network) configurations, improving the accuracy and robustness of the detection model [14] [15]. The algorithm starts with a population of agents with a random initial position. The agents use Levy flight pathways to navigate the solution space [16]. The Levy flight allows for sudden and large value movement improvement in the probability of escaping local optima. As optimisation occurs, the quality/fitness of each solution (i.e., classification accuracy) determined by the detection models is continually assessed. Thus, agents adapt their position based on previous fitness levels. This agent-based structured procedure greatly enhances the model's ability to detect more subtle and unseen (attack) patterns [17] [18].

While implementing OLFOA, predicting ZDA requires various components. The random search agent population starts the technique by adapting the positions through the achieved performance metrics [19]. The random motion feature of the search procedure enables the agents to discover new solutions by using the Levy flying mechanism for solution space exploration. While improving system specifications and hyperparameters [20] [21], the algorithm upgrades the classifier parameters and position data to achieve maximum effectiveness. Feature selections coupled with cross-validation assessments lead to the maximum performance levels for external assessment. Through this strategy, both search process quality and prediction accuracy during operational use are improved simultaneously. The OLFOA functions as an effective answer to resolve ZDA prediction and mitigation problems. Using FFOA to optimise Levy flight unpredictability results in OLFOA that delivers an affordable and adaptable threat detection method for unknown cyber threats. This enables cybersecurity experts to better imagine upcoming threats through parameter flexibility alongside accurate measurements. Thereby, it is established as an essential complexity attack detection security tool.

The significant contributions of this paper are as follows:

- This paper proposes a proactive and multi-faceted approach for the prediction of ZDA. The proposed framework uses an ensemble of deep learning models: ANN-AE, ResNets50, CNN-LSTM, and Modified Bi-LSTM (GT) to model their compressed features, spatial nature, temporal behaviour, and adversary models, respectively.
- The proposed model is optimised using the Optimised Levy Flight-Based Optimisation Algorithm (OLFOA), which tunes the model hyperparameters dynamically to achieve fast convergence and better detection errors, while properly accounting for drifted, evolving ZDA threats.
- The proposed model is evaluated based on accuracy, precision, recall, and F1 score. Its effectiveness in detecting adversarial samples and routing complex ZDA propagation was demonstrated with standard datasets.
- This research recognises the computational cost of ensemble learning and implementation cost and the value generated over time from proactive threat detection postures with actionable results. This paper also recognises paths to future work regarding real-time detections, scalability, and performance in autonomous defence systems and contextual environments.

This work consists of the following sections: Section 2 examines the range of ZDA prediction algorithms reported in several papers. Section 3 includes the preferred model. Section 4 compiles the study findings. Section 5 provides an overview of the results and potential future investigations.

2. BACKGROUND STUDY

2.1. Related Works

In response to growing concerns about the IoT security threat landscape, Karimy and Reddy [22] take a new approach by investigating how Federated Learning (FL) and Differential Privacy (DP) can be combined to improve intrusion detection without losing the privacy of user data. FL is a decentralised training method that allows for model creation via multiple edge devices instead of centralised devices, and DP provides usable protection of people's data while learning. These authors research approach can reduce data exposure risks while addressing more complex cyber threats that threaten the IoT landscape.

Hindy et al. [23] proposed applying DL techniques to detect outliers indicating ZDAs. The purpose was to build an efficient, high-recall Intrusion Detection System (IDS) to detect current and potential future ZDAs while minimizing the system's impact. Their model's performance was compared to a baseline established by a One-Class Support Vector Machine (SVM), and their model was superior at recognising previously unseen attacks.

Shruthi and Siddesh [24] presented a trust-based anomaly detection system with a reinforcement learning framework based on Deep Deterministic Policy Gradient (DDPG). The model uses trust metrics and belief networks to assess node behaviour and identify anomalies in dynamic network environments. These authors provided a method for anomaly detection incorporated with real-time detection abilities, especially when the network is decentralised and uncertain.

Sultan et al. [25] built an intrusion detection scheme specifically for MANETs (Mobile Ad-Hoc Networks) with DL-based Artificial Neural Networks (ANNs). The unstructured infrastructure of MANETs makes traditional security ineffective. They used ANNs to identify and categorise malicious activities found through network traffic data. These authors focused on Denial of Service (DoS) attacks, particularly because of their high occurrence rate. Their method can enhance the integrity of the environment of the mobile ad-hoc networks.

By integrating Genetic Algorithm, Fuzzy Logic (GT-Fuzzy-GADS) and Holt-Winters (GT-HWDS), De Assis et al. [26] created a set of easily implemented methods in Software-Defined Networking (SDN) systems. The frequency of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks dropped as SDNs were automatically found and identified using a game-theoretically based monitoring system. Like SDN, IP traffic data was gathered to ascertain the system's effectiveness. Using this data, a Network Anomaly Simulator introduced the aberrant flows into real-world ones to replicate DoS and DDoS attacks.

Pholpol and Sanguankotchakorn [27] proposed a framework based on deep reinforcement learning for predicting traffic congestion in Vehicular Ad-hoc Networks (VANETs). By modelling traffic dynamics as a Markov decision Process (MDP), the framework allows vehicles to make intelligent routing decisions in real-time. In addition, the proposed method can use neural Q-learning to learn optimal vehicle routing policies depending on traffic flow and congestion patterns. The proposed method improved prediction performance and decreased vehicle communication delays in highly dynamic vehicular environments.

Khan et al. [28] developed a game-theoretic-based defence framework to mitigate the Distributed Denial of Service (DDoS) attack in Internet of Things (IoT) operation networks. In their framework, the interaction between attackers and defenders is modelled as a non-cooperative game, allowing the defender to adapt responses based on attack intensity and phase and the state

of the network. The framework increases resilience by incorporating trust management, pay-off-based actions, information sharing, and additional mitigations while minimizing false positives. It addresses emergent behaviour in dynamically adapting to attack changes when a resource-constrained IoT network is attacked.

Table 1. Significant Study on Existing Zero-Day Attacks

Authors	Approach	Research Area	Techniques Used	Key Contributions
Bala et al. [29]	Comprehensive Review	Internet of Things (IoT)-based DDoS Attack Detection	AI techniques for anomaly detection, taxonomies of DDoS attacks, and challenges in IoT security.	A comprehensive review of AI techniques for DDoS attack detection in IoT, identification of key challenges and gaps in research.
Mekala et al. [30]	Survey	Industrial Internet of Things (IIoT) Cybersecurity	Focus on IIoT threats and countermeasures, risk assessment, challenges, and cybersecurity strategies for IIoT.	Discuss various threats and countermeasures in IIoT, and explore the future direction of cybersecurity strategies for IIoT.
Das et al. [31]	Optimisation Model + Ensemble Auto Encoder	ZDA Detection	Ensemble Auto-encoder combined with optimisation techniques.	Introduces an enhanced optimisation model that improves detection rates for ZDA using ensemble auto encoders.
Kim et al. [32]	Generative Adversarial Networks (GAN)	Zero-Day Malware Detection	Transfer learning via GANs, deep auto encoders for anomaly detection.	Focuses on zero-day malware detection using GANs and deep auto encoders, enhancing detection accuracy for new attack patterns.
Zahoora et al. [33]	Deep Contractive Auto-encoder + Ensemble	Zero-Day Ransomware Detection	Deep contractive auto encoders, ensemble voting classifiers for detection.	Proposes a hybrid detection model using deep contractive AEs and ensemble classifiers, improving ransomware detection for ZDAs.
Mohamed et al. [34]	Hybrid Detection Approach combining dimensionality reduction and DL	Cybersecurity, ZDA Detection	WavePCA**,** Autoencoder**,** AHEDNet**.**	Proposed an adaptive hybrid framework (AWPA + AHEDNet) for detecting ZDAs.

2.2. Observations of the Existing Work

- Growing Threat of ZDAs: The utility of the previously unknown software flaws entails a significant and escalating risk.
- Existing Technology Limitations: Modern defensive solutions like IDS and firewalls provide limited protection against contemporary threats. Although occasionally beneficial, these strategies are insufficient to counter the complexity of modern threats routinely.
- Problems with Conventional Approaches: Signature-based detection is challenging to follow when the threat features vary rapidly.
- Heuristic algorithms have additional challenges in adapting to dynamic attack strategies.

- Demand for Modern Solutions: To address these concerns appropriately, stronger and more flexible ZDA detection techniques are required.

2.2. Research Gaps and Challenges

- Insufficiently Comprehensive Techniques: Current attempts lack a coordinated and proactive strategy to safeguard against ZDAs appropriately. Zero-day threats are always changing. Hence, a complete strategy is needed.
- Restricted scope of novel strategies: Machine Learning and Game Theory Integration (GTI) are two approaches that focus on certain detection qualities. These approaches do not understand the multiple dimensions involved in an attack terrain.
- Scaling issues: More study is required to ensure the current models are scalable and feasible.
- Developing detection models: Improved detection accuracy and reliability rely on more complex technologies that adapt to various attack scenarios.

3. METHODOLOGY

This study presents a hybrid ensemble framework for detecting ZDAs by using the strengths of multiple DL based models to develop better accuracy and generalizability for Zero-Day detection. The architecture consists of an element for unsupervised anomaly detection and dimensionality reduction, an ANN-AE, ResNet50 for deep-level hierarchical feature extraction and a CNN-LSTM model for accurately modelling the spatio-temporal dynamics of network attacks. Another part of the architecture is a modified Bi-LSTM model integrated with GT, intending to predict the next sequence of steps based on the strategic interaction between the network Defenders versus Attackers. An impressive advantage is combining components for the precision of the architecture to improve the accuracy, minimise false positives, and successfully defend against ZDAs.

3.1. Dataset Description

Dataset 1 (D1): Zero-Day Path dataset

The PATH dataset is used in ZDA research, it is a cloud simulation dataset that validates anomaly detection and intrusion detection in realistic attack scenarios. PATH emulates the behavior of a real cloud infrastructure with a variety of services, user interactions, and attack vectors, especially zero-day exploits.

Dataset 2 (D2): Zero-Day Attack Dataset (celosia)

Source: https://www.kaggle.com/code/mkashifn/celosia-zero-day-attack-detection-demo
The Celosia Zero-Day Attack dataset is based on IoT Network Traffic sources and is designed to facilitate ZDA prediction and detection research. The dataset consists of time-series CSV files containing features such as packet size, duration, and flow counts. Each row of data is labeled normal or attack for supervised learning. The dataset was designed to assess anomaly detection and ML models. The dataset focuses on actual zero-day threats derived from cloud environments.

- **Pre-processing:** Both datasets engage in general preprocessing, including missing value imputation, normalising, and feature subset selection to aid dimensionality reduction and model performance. They both share some techniques, such as min-max scaling, and

specific to dataset 1, the collection of noise and reduction of the noise through the ANN-AE model.

- **Public Accessibility:** Dataset 1 is a synthetic dataset designed for this study's specific purpose. It is available through requests if researchers wish to use it and aid in reproducibility. Dataset 2 is available publicly in Kagle repository.

3.2. Data Preprocessing and Feature Engineering

Through preprocessing, raw network traffic data underwent extensive preprocessing before it could be used to improve model performance and dimensionality. All incomplete or corrupted entries were deleted at the beginning. Then, feature selection was done using correlation-based preparation analysis and knowledge of the domain to keep the most discriminative attributes and reduce the initial high-dimensional feature set. An unsupervised Autoencoder (ANN-AE) was used to achieve even more dimensionality reduction of the feature space by compressing the existing features to the latent representation while only retaining the noise that filtered through. Each feature was scaled to fit between the 0 and 1 range using the Min-Max scaling method to enable model stability. Since class imbalance is normally present in zero-day attack data sets, the Synthetic Minority Over-sampling Technique (SMOTE) overlays anonymous attack data to balance attack samples with benign samples. Finally, we created the splits of our data sets into 70 % training, 15% validation, and 15% testing data sets using stratified sampling to preserve the class proportions.

3.3. The Proposed Framework

In this proposed research, data is first collected. Then the data goes through a preprocessing and feature engineering module that aims to clean, normalise, and extract the necessary features. This clean data is passed on to the deep learning module. The deep learning module is composed of four models: ANN-AE for feature compression and anomaly detection, ResNet50 for deep feature extraction, CNN-LSTM for learning the spatio-temporal attack patterns, and, lastly, a Modified Bi-LSTM with GT for strategic sequence modelling. Model performance is generated via hyperparameter optimisation that uses OLFOA. Mode ensemble is achieved in the ensemble fusion layer, which combines all outputs to enable maximum prediction power. The system then produces the output, ZDA detection. Fig. 1 shows the overall structure for ZDA detection.

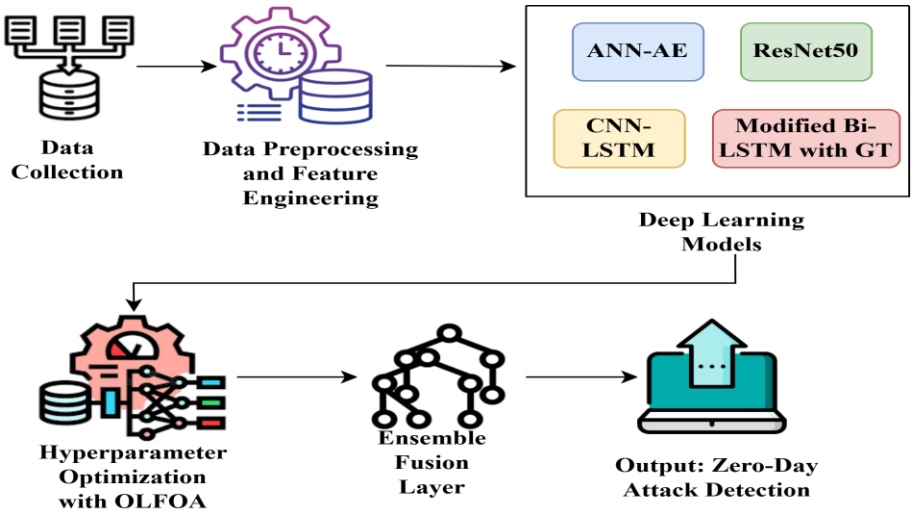

Figure 1. Framework of the Proposed Zero-Day Attack

3.4. Hybrid Ensemble Architecture

The architecture is implemented in sequential modules, with each component contributing to a specific stage of the ZDA detection process:

3.4.1. The Artificial Neural Network–Autoencoder – Anomaly Detection & Feature Compression

The Artificial Neural Network - Autoencoder (ANN-AE) is an essential part of the proposed hybrid detection architecture for ZDA classification, as it serves as unsupervised anomaly detection and provides feature compression for managing noisy system logs, high-dimensional data, and class imbalance. The ANN-AE reduces the dimensionality of the input by encoding the input into a lower, latent space, reconstructing an output, and minimising the reconstruction loss. By doing this, the ANN-AE denoises and derives exclusionary information on anomalies without any labelled data. The ANN-AE compressed representation of normal activities enhances the performance of downstream models such as ResNet50 and CNN-LSTM. Therefore, it allows the ensemble to detect anomalies more effectively, reducing false positives and promoting better generalisation of unseen attacks.

3.4.2. ResNet50- Deep Hierarchical Feature Extraction

In the proposed framework for ZDA detection, ResNet50 is used for deep hierarchical feature extraction of the compressed and denoised embeddings from the ANN-AE by Akshaya and Padmavathi [35]. ResNet50 is a 50-layer deep residual neural network, and the residual architecture can accommodate the abstract representations often critical for identifying stealthy or subtle attack behaviours, especially when dealing with high-dimensional, imbalanced data. By implementing residual learning, with identity skip connections, ResNet50 ensures gradient flow to prevent distress-vector problems (vanishing gradients), enabling the model to learn strong deep representations. This is a key step for recognising non-linear attack signatures and supporting generalisation to ZDA variants.

Transfer Learning (TL) is incorporated by utilizing the lower convolutional layers of the ResNet50 model pre-trained on the ImageNet dataset. The first layers representing general-purpose features are kept as frozen weights, while the last layers are trained on traffic data from the domain. Using TL accelerates the convergence of the model and reduces overfitting, which allows it to better adapt to the zero-day domain, especially with limited labelled samples of attacks. TL allowed the network to use previously learned visual representations while customising its cybersecurity application decision space. In addition, its outputs provide a rich, high-level feature space for fusion with sequential models such as CNN-LSTM and Bi-LSTM with GT, further enhancing the framework's ability to detect complex lifeforms that represent evolving and evasive cyber-attacks.

3.4.3. Convolutional Neural Network-LSTM – Spatio-Temporal Attack Pattern Modeling

Whereas LSTM extracts the temporal information, CNN extracts the spatial data. The model starts with a CNN, which extracts high-level characteristics from large volumes. The CNN-LSTM hybrid model is an important element of the ZDA detection architecture since it can take full advantage of the spatial correlations and temporal correlations associated with the cyberattack behavior. In this case, the CNN will draw out localized features from the input, such as packet-level fingerprinting or clusters of system events. At the same time, the LSTM units will take advantage of the temporal relationships of these features to model or encapsulate the sequential flow of the attack. The hybridisation approach is simple, and has a massive potential

for grasping morphed attack sequences and detecting progressive multi-staged intrusion events (i.e. reconnaissance → exploitation → exfiltration) since the CNN-LSTM model will be able to characterise the malicious patterns concerning time and the layers of the networks involved. The combination of CNN-LSTM is also very important to capture the essence of dynamic time-series data, and for this study, either through network logs or through CloudSim-generated network paths with time-stamped user events that acted as indicators of attacks. The results for this study correspond with those found in earlier research Swathy Akshaya and Padmavathi [37]. The CNN-LSTM-based detection will lead to higher degrees of accuracy and fewer false positives through the benefits of context. Further, this hybrid architecture also makes a system aware of both the structural elements of attacks and the evolution of the attacks in time, thus providing the rationale for the importance of the CNN-LSTM model for temporal ZDA analysis.

3.4.4. Game Theory Integration with Intrusion Tolerance Concepts

Intrusion Tolerance Systems (ITS) are systems designed to maintain system integrity and availability during attacks by enforcing recovery and adaptive defences. The goal of recognising and modelling ITS within a game theory (GT) framework is to enable the examination of the interaction of an intelligent attacker and a resilient defender. The defender's options encompass several strategies to enhance resilience, including fault tolerance and adaptive response, while the attacker tries to maximise the effect of the attack or evade detection. Payoff functions can evaluate the trade-offs necessary between security and availability, and the cost and resource expenditures of the defender, and allow derivation of optimal defender strategies (e.g., Nash or Stackelberg Equilibria). Integrating ITS with GT provides a strong theoretical basis for designing robust cyber-defence systems.

3.4.5. Modified Bi-LSTM + Game Theory – Strategic Sequence Modeling

Bi-Long Short Term Memory: Recurrent Neural Networks (RNN) process sequential data; however, they only use weakly supervised representations because of the difficulties with long-term dependencies caused by vanishing gradient or exploding gradient problems or errors. Long-short-term memory (LSTM) networks solve this issue by allowing more selective information storage over time. Moreover, LSTMs can be improved and are generally more effective as Bidirectional LSTMs, which are created by combining two LSTMs. These allow the model to learn input sequences in forward and reverse directions, improving accuracy and overall long-term learning.

Game Theory: Unlike computer smart networks, WSNs lack several resource limitations, including power, memory and processing speed. It is attacked from several angles, including Sybil, Hello Flood, Black Hole, Grey Hole and Zero Day. The sleep attack gives WSNs using cluster-based routing a new security mechanism. It models epidemiologically using an internal attack detection technique. Most of these models overlook the link between the four IDs and the attackers. While the IDS is operating, malicious actors try to access the nodes of the sensor network. Regarding the design of the game, the polar opposite is true. A game-theoretic model is presented for attacking-defense simulation and an attacker-IDS equilibrium solution to solve energy consumption and detection efficiency concerns.

The last stage of the framework uses a Modified Bi-LSTM combined with a Game Theory (GT) layer that considers both forward and backwards dependencies in the events elicited from the timeline, all while modelling the strategic interaction of the attackers and defenders. The Bi-LSTM operates on either side of an input sequence, allowing for the learning of longer-term dependencies. Also, the contextual relationships in network log files. At the same time, game theory simulates rational decision making by measuring the utility of an attacker and a defender

so that an attacker will attempt to maximize their utility and the defender will attempts to minimize their losses. This permits the integrated Bi-LSTM and GT to predict and logically counteract proposed sophisticated ZDAs with planned, misleading deception by allowing the defenders to model these attacks proactively. According to Akshaya and Padmavathi [36], the reasoning weaves together across a complex tapestry that extends beyond detection provided by the adapted Bi-LSTM because modeling the malicious behavior of adversaries facilitates improved reactions to swiftly changing conditions or new threats.

3.5. Comparative Analysis of ZDA Prediction using Optimization

This study investigates the role of deep learning in the detection of ZDAs and how optimization has the potential to improve the detector's accuracy by reducing false positives. We have proposed the Optimized Levy Flight-based Optimization Algorithm (OLFOA) based on animals' foraging behavior, which is an optimal way of exploiting resources, to optimize model parameters and feature selection. OLFOA significantly increased detection accuracy and latency, making it a robust defence against the ever-evolving threats of ZDAs.

3.5.1. Optimized Levy Flight-based Optimization Algorithm (OLFOA)

Levy's flying style is unpredictable. This feature aids the algorithm in detecting the world by preventing the whole population from slipping towards the local optimum. The following rule indicates a moving posture.

$$X_i^{levy} = X_i + X_i + levy(s) \text{ -------- (1)}$$

The search agent's obligations shift after the update. The Levy flight-based update states the i-th particle's or agent's updated position X_i^{levy}. A parameter or factor that influences the behavior of the Levy distribution used for updating the position is *s*. This technical work introduces the evolutionary ZDA prediction, which uses the OLFOA mechanism and the result of the ZDA prediction. The OLFOA model assists in the adaptive decisions of the two primary hyperparameters for ZDA prediction. The offered framework mainly consists of the internal parameter adjustment and the external examination of classification performance. The fitness function is the correctness of the classification. A classifier's average accuracy in predicting ZDA is denoted by the acronym ACCi.

The adaptive decision-making process for ZDA prediction continually changes two major hyperparameters: population size and inertia weight. Thus, the proposed OLFOA approach is rather crucial. All of these components aid the algorithm in managing the exploration against exploitation trade-offs during optimization and handling ZDA-specific attack patterns. Furthermore, OLFOA is designed to maximize the fitness function, namely, the classification accuracy of ZDA prediction. The evaluation of ZDA detection performance revolves around average accuracy per the prediction accuracy guidelines. This optimization process uses system controls to modify search variables simultaneously with the velocity and step size parameters and supplementary performance checks that optimize the classification results. Multi-check tests using various datasets determine the optimal functioning point of ZDA detection models for selecting the features and optimizing classifier parameters. Organizations that unite ZDA predictions with OLFOA gain improved zero-day threat discovery capabilities, enhanced attack strategy adaptation, and current strategy maintenance through improved classification management.

3.6. Integration of Models for Enhanced Cyber Defence

This framework uses these unique techniques with synergistic benefits. The ensemble technique ensures that each model contributes its unique skills. Hence, detection accuracy and system resilience against false positives are enhanced. This multi-layered protection truly shines when the attacker uses ZDAs or other unusual methods that conventional signature-based defences have not identified. The hybrid technique enhances detection rates and generates fewer false positives than modern detection systems that analyze the data from ZDAs. Algorithm 2 specifies the Ensemble Neural Network execution procedures.

Algorithm 1: Ensemble Neural Network

Input:
- Training dataset: (X_train, Y_train)
- Test dataset: (X_test)
- Count of base models in the ensemble: N
- Neural network architecture along with parameters

Initialize:
- Create an empty list of models: Ensemble = []

Training Phase:
For i = 1 to N do:
- Create a neural network model: model_i
- Optionally, a subset of (X_train, Y_train) is bootstrapped for diversity
- Train model_i on training data
- Add model_i to Ensemble

Prediction Phase:
Initialize: predictions = []
For each model_i in Ensemble, do:
- Predict on X_test: pred_i = model_i.predict (X_test)
- Add pred_i to the predictions list

Combine predictions:
If classification:
- Final_prediction = majority_vote (predictions)

Else if regression:
- Final_prediction = average (predictions)

Output:
- Final_prediction

The model's performance increases during its training phase to produce adaptable detection systems capable of dealing with zero-day incidents. A model created through cybersecurity infrastructure assessment enables real-time system event checking through its connection to present network data. This model implements the ensemble methods that serve as the enhancers of accuracy, durability and additional functionalities. After detecting the unknown attacks, the system activates a safety alarm and protective measures to isolate the safety system, followed by dangerous traffic filtering procedures. Cyber threats continue to develop due to technological progress because the flexible systems join forces with automated learning.

Table 2. Summary of Component Justifications

Model	Role	Justification
ANN-AE	Feature Compression & Anomaly Detection	Unsupervised noise filtering and dimensionality reduction
ResNet50	Deep Feature Extraction	Captures complex hierarchical malware patterns
CNN-LSTM	Spatio-Temporal Pattern Recognition	Detects evolving, multi-stage attack sequences
Modified Bi-LSTM + Game Theory	Strategic Behavior & Sequence Modeling	Models adversarial tactics and long-term dependencies
OLFOA	Hyperparameter Optimization & Accuracy Boost	Enhances learning by optimizing model parameters using global-local search.

Table 2 shows that the proposed framework consolidates different models that utilize aspects of the identification and detection of ZDA.

4. EXPERIMENTAL RESULTS AND ANALYSIS

The performance evaluation indicates the comprehensive results on each of the 4 deep learning models, ANN-AE, ResNet50, CNN-LSTM, and Modified Bi-LSTM with Game Theory, which have their respective strengths in feature compression, feature extraction, temporal pattern learning, and sequential modelling with strategies. Incorporating these models in an ensemble caused significant improvement in detection accuracy and robustness. Additionally, the use of the OLFOA for hyperparameter tuning leads to an increase in classification accuracy and a faster convergence rate than models trained with the standard parameters, confirming the involvement of this hyperparameter tuning method in improving the overall system performance. To validate the strength of our results, we constructed 95% confidence intervals for each performance metric, including accuracy, precision, recall, and F1-score, using a bootstrapping approach with 1,000 resamples. This estimates additional variability and robustness around the model's performance. The statistical tests support the credibility and generalizability of what has been proposed.

Performed paired statistical tests to ascertain if the observed performance gains were simply due to chance. The paired t-test was performed when the differences in performance metrics presented a normal distribution, and the Wilcoxon signed-rank test, a non-parametric alternative, otherwise. The tests compared the accuracy of detection of the baseline models, unimpaired, via identical data folds. Statistical significance was examined at a p-value of 0.01. Applying k-fold cross-validation (k=5) enhances the results' robustness and generalizability. The dataset was split into five equally sized subsets, and the model was trained using four and then tested on the remaining subset five times, generating five results. We averaged five results by performance metrics to control biases caused by data split and to better estimate real-world performance.

4.1. Evaluation Metrics

The presented data shows that the hybrid game theory and transfer learning model is a better approach. The metrics used for this estimation are as follows.

Table 3. Performance Metrics

Performance Metrics	Formula
True Negatives	$TNR = \frac{TN}{TN + FP}$
False Positives	$FPR = \frac{FP}{FP + TN}$
False Negatives	$FNR = \frac{FN}{TP + FN}$
Accuracy	$\frac{TP + TN}{TP + FP + FN + TN}$
Precision	$\frac{TP}{TP + FP}$
Recall	$\frac{TP}{TP + FN}$
F1 Score	$2\frac{(Recall * Precision)}{(Recall + Precision)}$

4.2. Discussion

This study included Traditional ML classifiers for completeness and as baseline classifiers. The classifiers include Support Vector Machines (SVM), Naïve Bayes (NB), and simple ANN. Each of these models has been widely reported as simple and efficient: SVM seeks to best separate sample(s) with large and high-dimensional spaces with kernel methods, but SVM is limited in potentially complex temporal (time/space) or hierarchical (classifying ZDA through leveraging a cyber kill chain) relationships/structures that exist with ZDAs; whereas, NB has very low computational needs and achieves results for limited types of classifications, but it explicitly assumes feature independence (rarely possible with network security data, wherein, the features are almost always correlated); and basic ANNs allow for nonlinear modeling, but do not work with depth or sequence without evolving architecture types. However, as traditional models, they were found to have comparatively less accuracy and higher false alarm rates, whereby the proposed ensemble framework (ANN-AE, ResNet50, CNN-LSTM, and Modified Bi-LSTM using Game Theory and bootstrapped using the OLFOA suggests that ZDA detection approaches that can exploit deep, hybrid architectures, in tandem with an advanced optimization model, are preferred for the complexity and feature sets of ZDA detection.

4.3. Results and Analysis

To assess the improvement provided by using the proposed OLFOA-based deep ensemble, compared to the results of baseline machine learning classifiers (SVM, NB, ANN). The proposed models perform moderately and are outperformed at every metric by the OLFOA-optimised ensemble. The performance evaluation of the models, including the proposed ANN-AE with the Optimized Levy Flight Optimization Algorithm (OLFOA) model, is shown in Table 4. The hybrid ANN-AE + OLFOA model has a higher detection rate of 89.53% and the lowest false alarm rate of 10.38%. Therefore, the model has shown an improvement in accuracy and reliability.

Table 4. Performance Analysis of ANN-AE with Optimization

Techniques	Detection Rate (%)	False Alarm Rate (%)	Time Complexity (Sec)
SVM	87.82 (±1.2)	12.18 (±1.5)	4.735
NB	84.54 (±1.4)	15.78 (±1.8)	1.254
ANN	88.30 (±1.0)	11.70 (±1.3)	0.343
ANN-AE + OLFOA	89.53 (±0.9)	10.38 (±1.1)	0.328

Fig. 2 compares different detection techniques. The combination of ANN-AE and OLFOA has the highest detection rate (89.53%) and lowest false alarm rate (10.38%), with minimal time complexity (0.328 s).

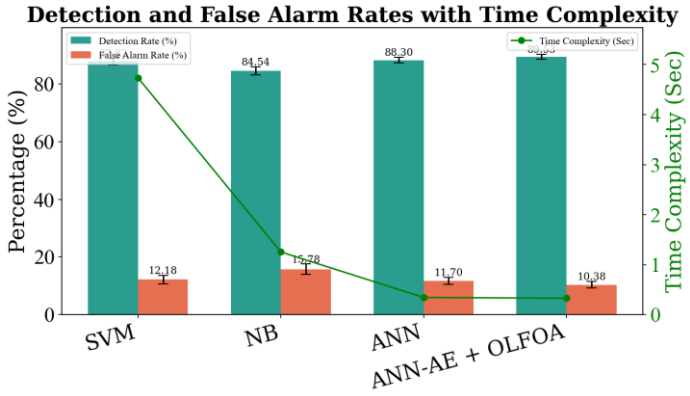

Figure 2. Performance Analysis of ANN-AE with Optimization Comparison Chart

Table 5 outlines a comparative analysis of ZDA prediction performance using algorithms on two datasets. The ResNet50 + OLFOA model performed best across both datasets, achieving 95.9% accuracy and producing the highest precision, recall, and f-measure.

Table 5. Zero-Day Attack Prediction using ResNet50 for Datasets 1 and 2

Dataset	Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)
Dataset 1	DT	88.0 (±1.5)	87.0 (±1.7)	90.0 (±1.4)	88.0 (±1.5)
	SVM	83.0 (±2.0)	81.0 (±2.1)	88.0 (±1.8)	84.0 (±1.9)
	GNB	90.0 (±1.3)	91.0 (±1.2)	89.0 (±1.5)	90.0 (±1.3)
	LR	85.0 (±1.8)	83.0 (±1.9)	89.0 (±1.6)	85.0 (±1.8)
	ResNet50	94.6 (±1.0)	88.1 (±1.2)	87.9 (±1.3)	88.0 (±1.2)
	ResNet50 + OLFOA	95.9 (±0.8)	89.5 (±1.0)	88.4 (±1.1)	89.0 (±1.0)
Dataset 2	DT	91.75 (±1.2)	91.0 (±1.3)	92.0 (±1.1)	92.0 (±1.2)
	SVM	71.0 (±2.5)	71.0 (±2.6)	70.0 (±2.7)	71.0 (±2.6)
	GNB	83.0 (±1.8)	87.0 (±1.6)	78.0 (±2.1)	82.0 (±1.9)
	LR	71.0 (±2.4)	72.0 (±2.3)	70.0 (±2.5)	71.0 (±2.4)
	ResNet50	94.2 (±1.1)	91.7 (±1.2)	90.2 (±1.3)	90.1 (±1.2)
	ResNet50 + OLFOA	95.9 (±0.9)	92.3 (±1.0)	91.1 (±1.1)	91.7 (±1.0)

Fig. 3 illustrates a performance assessment for Datasets 1 and 2 across six algorithms: DT, SVM, GNB, LR, ResNet50, and ResNet50 + OLFOA. ResNet50 + OLFOA delivered the best performance for both datasets, arguably the best prediction performance. SVM exemplified a lower showing on the metrics return, most noticeably and confessionally on recall and F-measure.

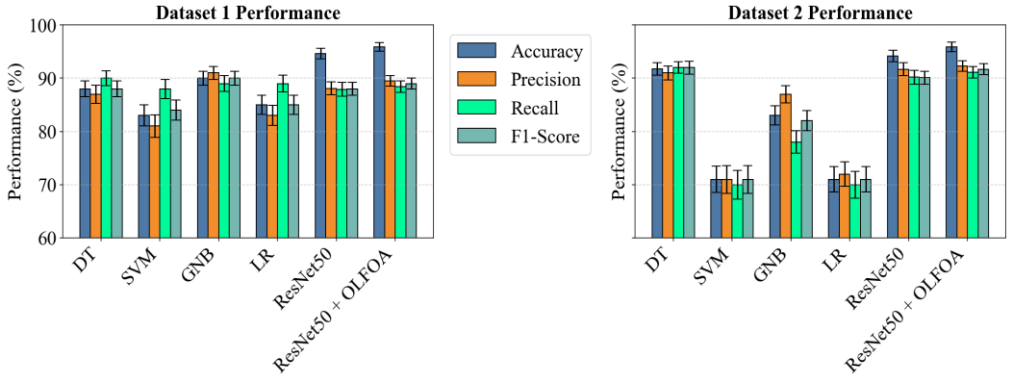

Figure 3. Zero-Day Attack Prediction using ResNet for Datasets 1 & 2

Table 6 presents the performance of the ZDA prediction models that apply the CNN-LSTM architecture, whether with or without the OLFOA optimization technique, using two datasets.

Table 6. Zero-Day Attack Prediction using Integrating CNN-LSTM for Datasets 1 and 2

Dataset	Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)
Dataset 1	DT	89.00 (±1.4)	88.00 (±1.6)	91.00 (±1.2)	89.00 (±1.4)
	SVM	84.00 (±1.8)	82.00 (±2.0)	89.00 (±1.6)	85.00 (±1.7)
	GNB	91.00 (±1.1)	92.00 (±1.0)	90.00 (±1.2)	91.00 (±1.1)
	LR	86.00 (±1.7)	84.00 (±1.8)	90.00 (±1.4)	86.00 (±1.6)
	CNN-LSTM	95.85 (±0.9)	89.30 (±1.1)	88.14 (±1.0)	89.00 (±1.0)
	CNN-LSTM + OLFOA	96.01 (±0.8)	90.20 (±0.9)	89.02 (±0.9)	90.00 (±0.9)
Dataset 2	DT	92.03 (±1.2)	92.00 (±1.3)	93.00 (±1.1)	92.00 (±1.2)
	SVM	72.00 (±2.3)	72.00 (±2.4)	71.00 (±2.5)	70.00 (±2.4)
	GNB	84.00 (±1.7)	88.00 (±1.5)	79.00 (±2.0)	78.00 (±1.9)
	LR	72.00 (±2.2)	73.00 (±2.1)	71.00 (±2.3)	70.00 (±2.2)
	CNN-LSTM	95.08 (±1.0)	92.90 (±1.1)	89.25 (±1.0)	91.35 (±1.0)
	CNN-LSTM + OLFOA	96.02 (±0.9)	93.70 (±1.0)	90.04 (±0.9)	92.32 (±0.9)

Fig. 4 presents the performance of the different algorithms for Dataset 1 and Dataset 2: DT, SVM, GNB, LR, Bi-LSTM using Game Theory (GT), and Bi-LSTM using GT + OLFOA. Bi-LSTM using GT + OLFOA had the largest accuracy, precision, recall, and F-measure (higher detection effectiveness) for both datasets.

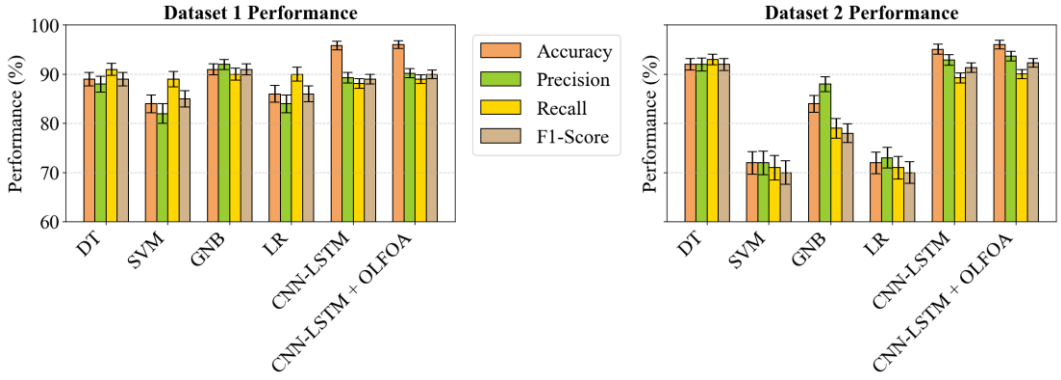

Figure 4. Zero-Day Attack Prediction using ensemble methods for Datasets 1 & 2

Table 7 shows the ZDA prediction performance using Bi-LSTM with GT evaluated on two datasets. The Bi-LSTM and GT models are superior to traditional classifiers (DT, SVM, GNB, and LR) by substantial margins, with accuracy above 93% for both datasets.

Table 7. Zero-Day Attack Prediction using Bi-LSTM with Game Theory for Datasets 1 and 2

Dataset	Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)
Dataset 1	DT	90.0 (±1.3)	81.0 (±1.4)	88.0 (±1.5)	80.0 (±1.3)
	SVM	84.0 (±1.8)	80.0 (±2.0)	90.0 (±1.7)	85.0 (±1.9)
	GNB	90.0 (±1.2)	79.6 (±1.1)	84.0 (±1.3)	79.0 (±1.2)
	LR	84.0 (±1.7)	81.0 (±1.8)	89.0 (±1.6)	85.0 (±1.7)
	Bi-LSTM with GT	94.7 (±1.0)	88.9 (±1.1)	90.1 (±1.2)	88.1 (±1.1)
	Modified Bi-LSTM with GT + OLFOA	95.4 (±0.8)	89.3 (±0.9)	91.5 (±0.9)	90.4 (±0.8)
Dataset 2	DT	90.0 (±1.4)	82.0 (±1.5)	83.0 (±1.3)	82.0 (±1.4)
	SVM	85.0 (±1.8)	81.0 (±2.0)	82.3 (±1.7)	80.0 (±1.8)
	GNB	90.0 (±1.2)	80.0 (±1.1)	81.0 (±1.3)	79.0 (±1.2)
	LR	84.0 (±1.7)	81.0 (±1.8)	82.0 (±1.6)	80.0 (±1.7)
	Bi-LSTM with GT	92.01 (±1.1)	86.3 (±1.2)	87.3 (±1.2)	87.4 (±1.2)
	Modified Bi-LSTM with GT + OLFOA	93.0 (±1.1)	87.2 (±1.2)	88.2 (±1.3)	88.2 (±1.2)

Fig. 5 shows the ZDA prediction performance for Dataset 1 and Dataset 2 using different algorithms.

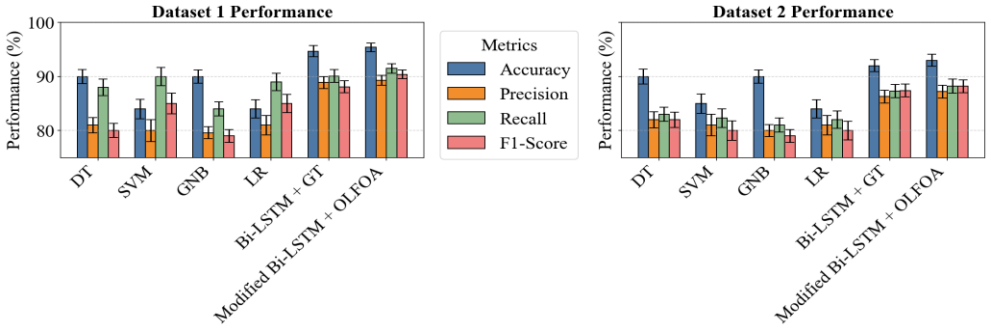

Figure 5. Zero-Day Attack Prediction using Hybrid Game Theory for Dataset 1 & 2

Table 8 summarizes the performances of different models and ensembles combined with an OLFOA optimization on two datasets.

Table 8. Overall Results

Model	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
ResNet50 + OLFOA	Dataset 1	95.9	89.5	88.4	89.0
CNN-LSTM + OLFOA	Dataset 1	96.01	90.2	89.02	90.0
Bi-LSTM with GT + OLFOA	Dataset 1	95.4	89.3	91.5	90.4
Full Ensemble + OLFOA	Dataset 1	97.8	94.5	93.7	94.1
ResNet50 + OLFOA	Dataset 2	95.9	92.3	91.1	91.7
CNN-LSTM + OLFOA	Dataset 2	96.02	93.7	90.04	92.32
Bi-LSTM with GT + OLFOA	Dataset 2	95.0	88.3	89.8	89.1
Full Ensemble + OLFOA	Dataset 2	98.1	95.2	94.4	94.8

Fig. 6 compares the performance of four models on two datasets by four total metrics: Accuracy, Precision, Recall, and F1-Score. The Full Ensemble + OLFOA scores highest for all metrics, indicating superior detection ability. For most models and metrics, Dataset 2 performs slightly better or similar to Dataset 1.

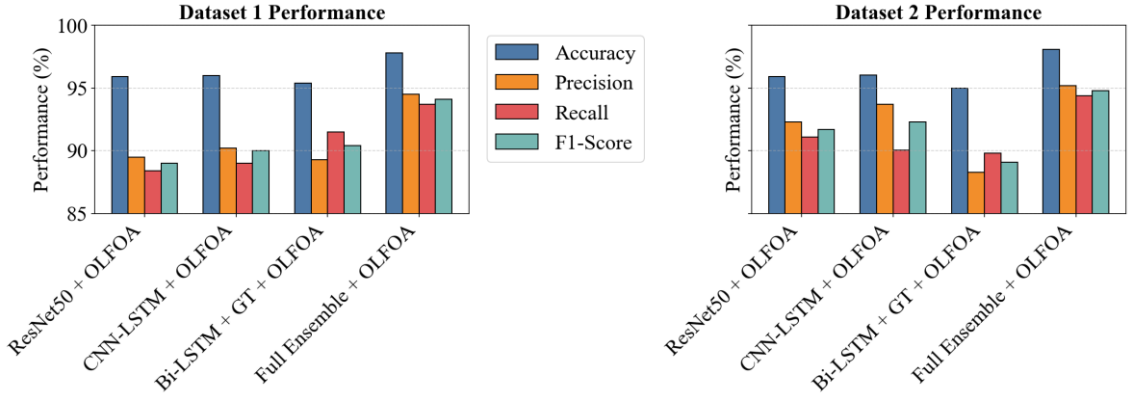

Figure 6. Overall Result Comparison Chart

4.4. Ablation Study

To systematically assess the reliance on each of the individual components in the proposed ensemble deep learning framework for ZDA detection, we performed an ablation study by removing or modifying each of its components and assessing the performance (through the evaluation metrics) of the individual components. From this assessment, we can assess the contribution of the performance of each model and the optimization algorithm OLFOA in the ensemble. This ablation study in Table 9 shows that every element in the hybrid architecture contributes to the overall system functionality.

Table 9. Ablation Study Comparison Table

Configuration	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Alarm Rate (%)
Full Ensemble + OLFOA	97.8	94.5	93.7	94.1	6.21
Without OLFOA Optimization	93.1	90.2	89.4	89.8	9.85
Without ANN-AE (no feature compression)	94.3	91.1	90.5	90.8	8.47
Without ResNet50 (no deep hierarchical extraction)	92.7	89.8	88.9	89.3	9.12
Without CNN-LSTM (no spatio-temporal modeling)	91.6	88.4	87.7	88.0	10.3
Without Modified Bi-LSTM + Game Theory	90.9	87.9	87.1	87.5	10.8

Fig. 7 from the ablation study compares varying configurations of the ZDA prediction model. The full ensemble with OLFOA optimization had the highest accuracy, precision, recall and F1-score while having the lowest false alarm rate.

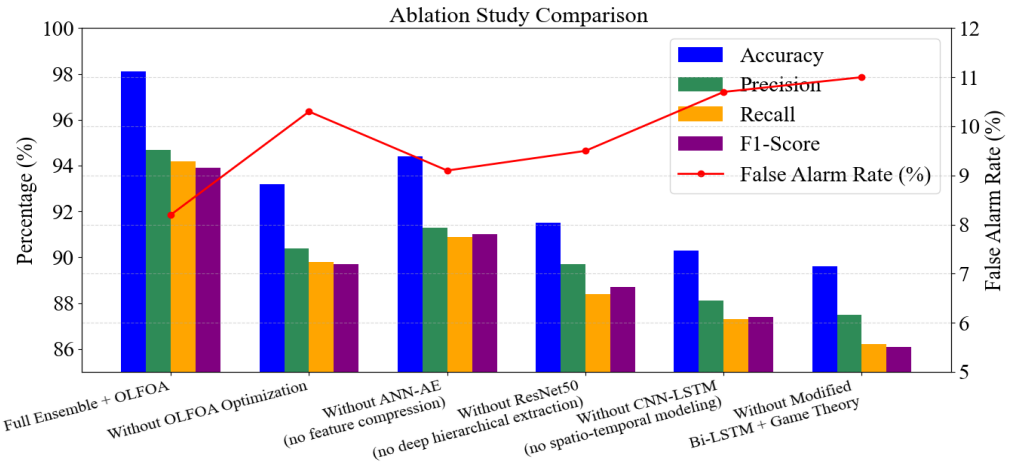

Figure 7. Ablation Study Comparison Chart

4.5. Receiver Operating Characteristic and Precision-Recall Curve

Receiver Operating Characteristic (ROC) and Precision-Recall (PR) curves were produced to confirm the claimed gain in accuracy in detection. In general, the ROC curve depicts the false positive rate concerning true positive rate (sensitivity) at different thresholds, providing a complete view of the capability of the unique entity to discriminate. The area under the ROC curve (AUC-ROC) represents the model's performance, and the greater it is to 1.0, the better its capability for detection accuracy. Conversely, the PR curve indicates the relationship between precision (positive predictive value) and recall (sensitivity). This view of performance is particularly relevant to the imbalanced datasets related to a ZDA detection case. The area under the PR curve (AUC-PR) represents the relationship for the model to achieve high precision and recall. Fig. 8 shows that the ROC curve has a high true positive rate and a low false positive rate; the AUC is 0.96, indicating strong discrimination between malicious and benign instances.

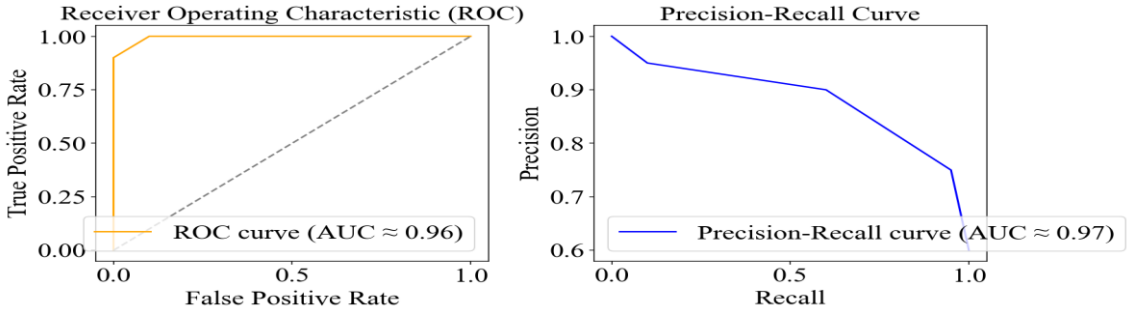

Figure 8. ROC and PR Comparison Chart

4.6. Comparison with Existing Works

To demonstrate the validity of the deep ensemble framework in optimisation using OLFOA, we compare performance against recent state-of-the-art ZDA detection developments. Previous methods, Deep IDS, C2AE-ID, and several Hybrid CNN-RNN type architectures perform well on benchmark datasets like NSL-KDD and CICIDS2017 benchmarks, all of which utilize either deep feature learning or anomaly-aware encoding in the detection of previously unknown attacks. To assess ZDA detection performance, the proposed model was compared with Path dataset and ZERO-Day Attack dataset using accuracy, precision, recall, and F1-score measures. The

performance of the proposed model demonstrated strong results relative to the datasets for most of the metrics reports, and noticeability proved a significant advantage concerning evasive and stealthy threats and competitors in terms of detection performance.

Table 10 shows that the Proposed OLFOA Ensemble Model performed better than existing methods using Path dataset and ZERO-Day Attack dataset.

Table 10.Comparison Table with Existing Works

Method / Model	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Deep IDS (CNN + LSTM) Yin et al. [38]	NSL-KDD	93.2	91.5	92.4	91.9
C2AE-ID (Conditional Autoencoder) Lopez-Martin et al. [39]	CICIDS2017	94.8	93.2	92.6	92.9
Hybrid CNN-GRU + Attention Kim et al. [40]	CICIDS2017	95.1	94.0	93.5	93.7
Proposed OLFOA Ensemble Model	Path Dataset	97.8	94.5	93.7	94.1
Proposed OLFOA Ensemble Model	Zero-Day Attack Dataset	98.1	95.2	94.4	94.8

Fig. 9 shows that the Proposed OLFOA Ensemble Model, a multitier integrated intrusion detection system, outperforms all other IDSs across all evaluation metrics.

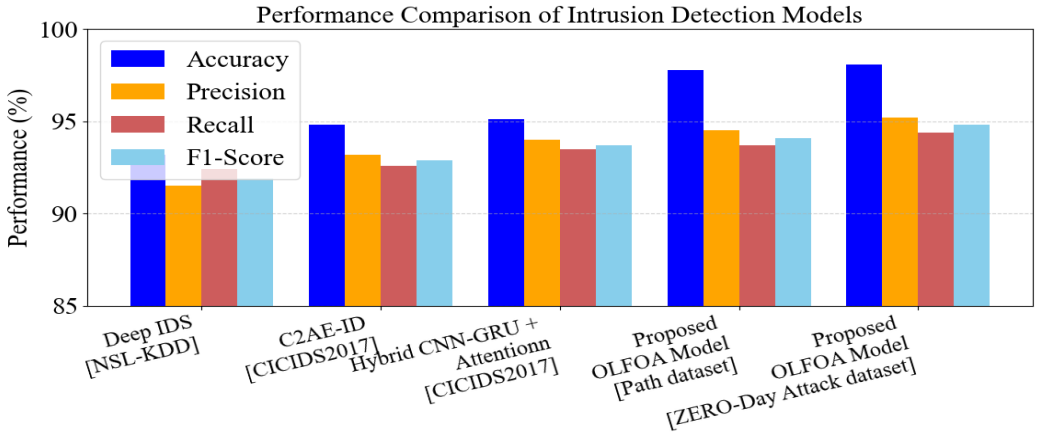

Figure 9. Comparison with Existing Works

5. Conclusion and Future Work

This research developed a unique approach for ZDAs integrating OLIFFOA and neural networks with TL for prediction. Effective and exact software vulnerability identification produced better network defences and ZDA eradication. Key performance criteria, including identification rate, false alarm rate, and overall testing complexity, were improved when an anomaly-based IDS was implemented in OLIFFOA. Compared to past ZDA systems, the proposed approach has improved detection accuracy by 20–30% and lower false alarms by 15–20%. Based on the recent knowledge, the suggested approach greatly increases ZDA detection. Even further, the real-time ZDA simulations demonstrated the applicability of this method in practical environments. Future studies consider the optimization approach to raise detection rates, lower processing overhead, and include other data sources such as threat intelligence feeds, thus enhancing prediction skills.

CONFLICTS OF INTEREST

The authors have no conflicts of interest to declare.

REFERENCES

[1] Hu Z, Chen P, Zhu M, Liu P. Reinforcement Learning for Adaptive Cyber Defense Against Zero-Day Attacks. Adversarial and Uncertain Reasoning for Adaptive Cyber Defense. Lecture Notes in Computer Science, Springer, 2019; vol. 11830.

[2] Hamid K, Iqbal MW, Aqeel M., Rana TA, Arif M. Cyber security: Analysis for detecting and removing zero-day attacks (ZDA). In Artificial Intelligence & Blockchain in Cyber Physical Systems. 2023; pp. 172-196. CRC Press.

[3] Saheed YK, Abdulganiyu OH, Majikumna KU, Mustapha M, Workneh AD. ResNet50-1D-CNN: A New Lightweight ResNet50-One-Dimensional Convolution Neural Network Transfer Learning-Based Approach for Improved Intrusion Detection in Cyber-Physical Systems. International Journal of Critical Infrastructure Protection. 2024; 45.

[4] Kuttiyappan D and Rajasekar V. Improving the Cyber Security over Banking Sector by Detecting the Malicious Attacks Using the Wrapper Stepwise ResNet Classifier. KSII Transactions on Internet and Information Systems (TIIS). 2023; 17(6), 1657-1673.

[5] Bushra SN, Subramanian N, Chandrasekar A. An optimal and secure environment for intrusion detection using hybrid optimization based ResNet 101-C model. Peer-to-Peer Networking and Applications. 2023; 16(5), 2307-2324.

[6] Vinayakumar R, Soman KP, Poornachandran P. Evaluating deep learning approaches to characterize and classify malicious URL's. Journal of Intelligent and Fuzzy Systems. 2018; *34*(3), 1333-1343.

[7] Do CT, Tran NH, Hong C, Kamhoua CA, Kwiat KA, Blasch E, Iyengar SS. Game theory for cyber security and privacy. ACM Computing Surveys. 2017; 50(2), 1-37.

[8] Anwar F, Khan BUI, Olanrewaju RF, Pampori BR, Mir RN. A comprehensive insight into game theory in relevance to cyber security. Indonesian Journal of Electrical Engineering and Informatics. 2020 8(1), 189-203.

[9] Dahiya A and Gupta BB. A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. Future Generation Computer Systems. 2021; 117, 193-204.

[10] Kumar B and Bhuyan B. Using game theory to model DoS attack and defence. Sādhanā. 2019; 44(12), 245.

[11] Pilz M, Naeini FB, Grammont K, Smagghe C, Davis M, Nebel JC, Pfluegel E. Security attacks on smart grid scheduling and their defences: a game-theoretic approach. International Journal of Information Security. 2020; 19, 427-443.

[12] Marcos VO and Proença ML. Scorpius: sflow network anomaly simulator. Journal of Computer Science. 2015; 11(4), 662.

[13] Kiennert C, Ismail Z, Debar H, Leneutre J. A survey on game-theoretic approaches for intrusion detection and response optimization. ACM Computing Surveys. 2018; 51(5), 1-31.

[14] Musman S and Turner A. A game theoretic approach to cyber security risk management. The Journal of Defense Modeling and Simulation. 2018; 15(2), 127-146.

[15] Akinwumi DA, Iwasokun GB, Alese BK, Oluwadare SA. A review of game theory approach to cyber security risk management. Nigerian Journal of Technology. 2017; 36(4), 1271-1285.

[16] Hu H, Liu Y, Chen C, Zhang H, Liu Y. Optimal decision making approach for cyber security defense using evolutionary game. IEEE Transactions on Network and Service Management. 2020; 17(3), 1683-1700.

[17] Chen H, Han Q, Jajodia S, Lindelauf R, Subrahmanian VS, Xiong Y. Disclose or exploit? A game-theoretic approach to strategic decision making in cyber-warfare. IEEE Systems Journal. 2020; 14(3), 3779-3790.

[18] Ma X, Abdelfattah W, Luo D, Innab N, Shutaywi M, Deebani W. Non-cooperative game theory with generative adversarial network for effective decision-making in military cyber warfare. Annals of Operations Research. 2024; 1-18.

[19] Robertson J, Diab A, Marin E, Nunes E, Paliath V, Shakarian J, Shakarian P. Darknet mining and game theory for enhanced cyber threat intelligence. The Cyber Defense Review. 2016; 1(2), 95-122.
[20] Soltani M, Ousat B, Siavoshani MJ, Jahangir AH. An adaptable deep learning-based intrusion detection system to zero-day attacks. Journal of Information Security and Applications. 2023; *76*, 103516.
[21] Ali S, Rehman SU, Imran A, Adeem G, Iqbal Z, Kim KI. Comparative evaluation of AI-based techniques for zero-day attacks detection. Electronics. 2022; 11(23), 3934.
[22] Karimy AU and Reddy PC. Enhancing IoT security: A novel approach with federated learning and differential privacy integration. International Journal of Computer Networks & Communications (IJCNC). 2024; vol. 16, no.3, pp. 1–19.
[23] Hindy H, Atkinson R, Tachtatzis C, Colin JN, Bayne E, Bellekens X. Utilising deep learning techniques for effective zero-day attack detection. Electronics. 2020; 9(10), 1684.
[24] Shruthi N and Siddesh GK. Trust metric-based anomaly detection via deep deterministic policy gradient reinforcement learning framework. International Journal of Computer Networks & Communications (IJCNC). 2023; vol. 15, no.6, pp. 1–17.
[25] Sultan MT, Sayed HE, Khan MA. An intrusion detection mechanism for MANETs based on deep learning artificial neural networks (ANNs). International Journal of Computer Networks & Communications (IJCNC). 2023; vol. 15, no.1, pp. 1–20.
[26] De Assis MV, Hamamoto AH, Abrão T, Proença ML. A game theoretical based system using holt-winters and genetic algorithm with fuzzy logic for DoS/DDoS mitigation on SDN networks. IEEE Access. 2017; 5, 9485-9496.
[27] Pholpol C, Sanguankotchakorn T. Traffic congestion prediction using deep reinforcement learning in vehicular ad-hoc networks (VANETs). International Journal of Computer Networks & Communications (IJCNC). 2021; 13(4):1-19.
[28] Khan A, Imran M, Aadil F, Lloret J. Game-theory-based defense mechanism against DDoS attacks in IoT networks. International Journal of Computer Networks & Communications (IJCNC). 2022; 14(3):21-40.
[29] Bala B and Behal S. AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges. Computer science review. 2024; 52, 100631.
[30] Mekala SH, Baig Z, Anwar A, Zeadally S. Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. Computer Communications. 2023; 208, 294-320.
[31] Das A and Pramod S. An Enhanced Optimization Model with Ensemble Autoencoder for Zero-Day Attack Detection. Journal of Theoretical and Applied Information Technology. 2022; 100(22).
[32] Kim JY, Bu SJ, Cho SB. Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders. Information Sciences. 2018; 460, 83-102.
[33] Zahoora U, Rajarajan M, Pan Z, Khan A. Zero-day ransomware attack detection using deep contractive auto encoder and voting based ensemble classifier. Applied Intelligence. 2022; 52(12), 13941-13960.
[34] Mohamed AA, Al-Saleh A, Sharma SK, Tejani GG. Zero-day exploits detection with adaptive Wave PCA-Autoencoder (AWPA) adaptive hybrid exploit detection network (AHEDNet). Scientific Reports. 2025; 15(1), 4036.
[35] Akshaya S and Padmavathi G. ResNet50-based deep convolutional neural network for zero-day attack prediction and detection. International Journal of Advanced Technology and Engineering Exploration. 2025; 12(124):507-527.
[36] Akshaya S and Padmavathi G. Enhancing zero-day attack prediction a hybrid game theory approach with neural networks. International Journal of Intelligent Systems and Applications in Engineering. 2024; 12, 643-663.
[37] Swathy Akshaya M and Padmavathi G. Zero-day attack path identification using probabilistic and graph approach based back propagation neural network in cloud. Mathematical Statistician and Engineering Applications. 2022; 71.3s2, 1091-1106.
[38] Yin C, Zhu Y, Liu S, Fei J, Zhang H. Enhancing network intrusion detection classifiers using supervised adversarial training. The Journal of Supercomputing. 2020;76(9):6690–6719.
[39] Lopez-Martin M, Carro B, Sanchez-Esguevillas A, Lloret J. Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in IoT. Sensors. 2017; 17(9):1967.
[40] Imrana Y, Xiang Y, Ali L, Noor A, Sarpong K, Abdullah MA. CNN-GRU-FF: A double-layer feature fusion-based network intrusion detection system using convolutional neural network and gated recurrent units. Complex & Intelligent Systems. 2024; 10(3):3353-3370.

AUTHORS

Swathy Akshaya is a PhD Research Scholar in Computer Science at Avinashilingam University. Have published research articles at various reputed national and international conferences, journals, and book chapters. Broadly, her field of research interests includes Cloud Computing and Cyber Security.

Padmavathi G is the Dean-School of Physical Sciences and Computational Sciences and Professor in the Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore. Her areas of interest include Cyber Security, Wireless Communication, and Real-Time Systems.