International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(17s) 2026 pp. 426-436
https://doi.org/10.70917/ijcisim-2026-4751
Article

Advancing Intrusion Detection Systems: A Comprehensive Review of Deep Learning and Hyperparameter Optimization Techniques

Hamela K

Department of Computer Science, Government First Grade College, Kolar, Karnataka, India.
Mail ID: hamela27@gmail.com

Abstract: In the suddenly changing realm of cyber security, Intrusion Detection Systems (IDS) are essential for protecting computer networks from harmful actions. This survey paper offers an extensive examination of sophisticated approaches and procedures utilised in IDS, emphasising the amalgamation of deep learning (DL) and hyper parameter optimisation. We examine many categories of cyber-attacks that confront conventional IDS, including phishing, malware, ransom ware, and advanced evasion strategies. The study explores the intricacies of hyper parameter tuning in DL algorithms, emphasising major methods such grid search (GS), random search (RS), Bayesian optimisation (BO), and genetic algorithms (GA). This paper examines recent progress in DL applications for IDS, highlighting the efficacy of models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and auto encoders in identifying both established and emerging threats. Case studies and contemporary research illustrate the effects of these tactics on enhancing IDS accuracy, minimising false positives, and responding to novel attack strategies. This survey highlights the necessity for on-going advancement in IDS to tackle the evolving nature of cyber threats and improve the overall security stance of networked systems.
Keywords: Intrusion Detection Systems, Deep Learning, Hyperparameter Optimisation, Cybersecurity, Network Security

1. Introduction

In the digital era, safeguarding computer networks against cyber-attacks is a paramount concern for organisations around. IDS are integral to this defence framework, responsible for monitoring and evaluating network traffic, system behaviour, and data trends to detect and address potential threats. As cyber-attacks have evolved in complexity, the significance of IDS in identifying and alleviating these threats has intensified. Conventional security measures frequently prove insufficient against the contemporary threats of advanced phishing, malware, ransomware, and intricate evasion tactics. Consequently, IDS must always adapt to address these evolving threats and sustain formidable defences [1].

The increasing sophistication of cyber threats requires IDS systems to incorporate modern technologies and approaches to protect networks efficiently. This entails utilising DL methodologies, optimising hyper parameters, and implementing ensemble learning to improve detection precision and system efficacy. Efficient IDS solutions are dynamic and versatile, able to manage substantial data volumes and identify new attack patterns. Utilising these sophisticated methodologies, IDS can deliver prompt and precise notifications, mitigating the effects of cyber-attacks and safeguarding key infrastructure and sensitive data. This paper will analyse the crucial function of IDS in contemporary cyber security, investigating the problems presented by emerging attacks and the sophisticated solutions required to mitigate them.

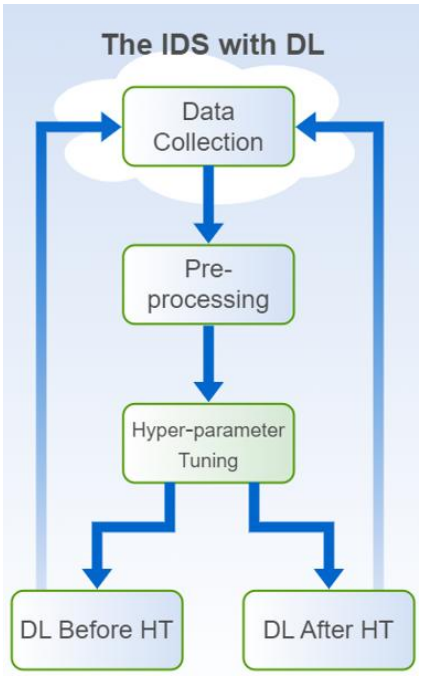

Fig.1. DL Based IDS with Hyper parameter Optimisation

The above diagram depicts an IDS pipeline that integrates DL and Hyper parameter Tuning (HT). It delineates the chronological progression of data inside the system, commencing with data acquisition and pre-processing. The pre-processed data is subsequently input into a DL model, which is further refined through hyper parameter optimisation. The proposed approach evaluates the performance of the DL model prior to and following hyper parameter tuning, emphasising the potential advantages of this optimisation process in improving IDS accuracy and efficacy.

2. Literature Review

The literature study analyses several sophisticated IDS that utilise advanced approaches such as DL, hyper parameter optimisation, and ensemble methods to improve the identification of cyber threats in various settings. Recent research emphasise enhancing IDS performance with the incorporation of artificial intelligence, optimisation algorithms, and feature selection techniques, demonstrating notable advancements in accuracy, scalability, and robustness. The analysed research underscores the continuous endeavours to modify IDS to address the intricacies of contemporary networks, accentuating the essential function of refined ML models in safeguarding systems from progressively advanced cyber-attacks.

Table.1. Review of Literature

Author and Year	Proposed Approach	Key Techniques	Dataset(s) Used	Results/Accuracy
Manoranjithem et al. (2023) [2]	Intrusion Detection using Hierarchical Deep Learning-based Butterfly Optimization Algorithm (ID-HDLBOA)	Hierarchical LSTM, Butterfly Optimization Algorithm (BOA)	Benchmark intrusion datasets	98% accuracy

Calugar et al. (2022) [3]	Efficient hyperparameter tuning for ANN based IDS	Hyperparameter tuning	Four datasets	Significant improvement over existing studies
Masum et al. (2021) [4]	Bayesian optimization-based framework for optimizing DNN classifiers	Bayesian optimization	NSL-KDD	Improved accuracy, precision, recall, F1-score over random search
Ananthi et al. (2023) [5]	Ensemble-based IDS for IoT with Recursive Feature Elimination (RFE)	Recursive Feature Elimination (RFE), Deep Neural Network (DNN)	KDD 99	Enhanced classification accuracy
Kumar et al. (2024) [6]	NIDS with Perceptive Craving Game Search Optimization (PCGSO) and BI-GRU	PCGSO for feature selection and hyperparameter tuning, BI-GRU	ISCXIDS2012	99% accuracy
Kanimozhi and Jacob (2019) [7]	AI-based NIDS for detecting botnet attacks	Artificial Neural Networks (ANNs), Hyperparameter optimization	CSE-CIC-IDS2018	99.97% accuracy, 0.001 FPR
Kunang et al. (2021) [8]	NIDS with pretraining using Deep Autoencoder (PTDAE) and DNN	Pretraining, Grid Search, Random Search, Autoencoder (DAE)	NSL-KDD, CSE-CIC-ID2018	Improved multiclass classification accuracy
Kunang et al. (2020) [9]	IDS for IoT combining Autoencoder and DNN with Bayesian Hyperparameter Optimization	Autoencoder, Bayesian optimization	BoT-IoT	99.99% accuracy
Wazirali (2020) [10]	Semisupervised IDS with KNN and hyperparameter tuning	K-Nearest Neighbor (KNN), Cross-validation	NSL-KDD	Improved robustness and detection rates
Rathee et al. (2023) [11]	DL techniques for enhancing cybersecurity	Deep Neural Networks, Convolutional Neural Networks (CNN), Attention Mechanism	NSL-KDD, Kyoto, UNSW-NB15	Effective in improving cybersecurity
Navya et al. (2021) [12]	ML based IDS using DNNs for dynamic intrusion detection	Deep Neural Networks (DNNs)	Multiple datasets	Enhanced accuracy and responsiveness
Anwer et al. (2021) [13]	Hybrid DL approach for IoT intrusion detection	LSTM, CuDNNLSTM	Kitsune	99.79% accuracy

	using LSTM and CuDNNLSTM			
Jullian et al. (2023) [14]	Distributed DL framework for IoT network security	Feedforward Neural Networks, LSTM	NSL-KDD, BoT-IoT	Up to 99.95% accuracy
Wang et al. (2022) [15]	Stacked DL approach for SCADA systems	Stacked deep learning, Random Forest for feature importance assessment	Power transmission, gas pipeline	Superior performance to other methods
Asgharzadeh et al. (2024) [16]	IDS for IoT with CNN and enhanced Gorilla Troops Optimizer (BMEGTO)	Convolutional Neural Network (CNN), BMEGTO	TON-IoT, NSL-KDD	99.99% (TON-IoT), 99.86% (NSL-KDD)

1. **Cyber-attacks**

Cyber-attacks encompass malevolent actions aimed at infiltrating computer networks and systems to compromise security, extract data, or disrupt operations. IDS seek to identify and react to attacks by scrutinising network traffic, system behaviour, and data patterns for indications of anomalous activity. Cyber-attacks can leverage weaknesses via methods such as phishing, malware, or denial-of-service attacks. IDS technologies examine this data to detect anomalous patterns, signal possible intrusions, and notify security personnel to avert or lessen the consequences of these attacks. Effective IDS continuously adapt to identify and mitigate novel attack techniques. Cyber-attacks in IDS may encompass [17]

- **False Positives:** Authentic activity erroneously identified as attacks, resulting in superfluous notifications and potentially disrupting operations.
- **False Negatives:** Actual attacks that remains undetected by the IDS, permitting malicious operations to continue undiscovered.
- **Evasion Techniques:** Strategies employed by assailants to circumvent IDS identification, include traffic encryption or the utilisation of polymorphic malware that alters its form.
- **Denial of Service (DoS) Attacks:** Saturating the IDS with an overwhelming volume of data or requests, resulting in its failure or unresponsiveness.
- **Spoofing:** The act of falsifying authentic credentials or addresses to deceive the Intrusion Detection System into recognising harmful actions as harmless.
- **Exploitation Techniques:** Targeting vulnerabilities within the IDS including the manipulation of software defects or deficiencies in the detection algorithms.

Effective IDS must exhibit resilience to various threats and possess the ability to adapt to novel and sophisticated attack techniques.

Table 2: Categories of Cyber Attacks

Type of Cyber attack	Description
Phishing	Fraudulent emails or communications that deceive individuals into disclosing confidential information or downloading harmful malware.

Malware	Malicious software, such as viruses, worms, or ransomware, intended to damage or disrupts systems.
Ransomware	Category of malware that encrypts data and requires payment for its decryption.
Denial of Service (DoS)	Inundating a system or network with excessive traffic, rendering it inaccessible to users.
Man in the Middle (MitM)	Intercepting and modifying communication between two parties without their awareness.
SQL Injection	Exploiting weaknesses in a web application's database to execute harmful queries.
Zero Day Exploit	An assault on a software vulnerability that remains undisclosed to the program provider or the public.
Credential Stuffing	The utilisation of compromised login credentials to obtain unauthorised access to accounts.

The above mentioned table encompasses prevalent tactics, including phishing, which employs false communications to coerce users into disclosing sensitive information, and malware, characterised by destructive software intended to compromise systems. The table additionally addresses certain dangers such as ransomware, which encrypts data for extortion, and DoS assaults that inundate systems to impede access. Supplementary threats encompass Man-in-the-Middle (MitM) attacks, SQL Injection, Zero-Day Exploits, and Credential Stuffing, each targeting specific weaknesses to compromise security.

Figure 2: Types of cyber-attacks

The above image illustrates different threats including phishing, DoS/DDoS, XSS, spyware, keyloggers, brute force assaults, viruses, malware, SQL injection, MitM attacks, and password attacks. Each component features a unique colour and emblem, offering a comprehensive picture of these cyber threats [17].

2. **Hyper parameter optimisation in DL algorithms for cyber-attack detection**

Hyper parameter tuning in cyber-attacks is modifying the configurations of ML models (such as learning rate, batch size, and layer count) to enhance their efficacy in detecting and categorising attacks. This technique seeks to enhance the model's precision and efficacy in detecting cyber threats by determining the optimal configuration of these parameters. Hyper parameter tuning algorithms for cyber-attack detection are methods employed to optimise the configurations of ML and DL models to enhance performance [18]. The following are few prevalent algorithms

- **Grid Search (GS):** Methodically examines a specified range of hyper parameter values to identify the ideal configuration. It assesses all potential combinations, which may be laborious yet comprehensive.
- **Random Search (RS):** Randomly selects hyper parameter combinations from a specified range. It is less comprehensive than grid search but frequently identifies effective solutions more rapidly and with reduced computational effort.
- **Bayesian Optimisation (BO):** use probabilistic models to forecast the efficacy of certain hyper parameter combinations. It equilibrates exploration and exploitation to effectively identify optimal configurations by iteratively refining its model based on prior outcomes.
- **Genetic Algorithms (GA):** Mimics evolutionary mechanisms to enhance hyper parameters. The process commences with a population of solutions, implements mutation and crossover processes, then picks the most effective solutions to produce new populations.
- **Hyper band (HB):** Integrates random search with premature termination. It distributes resources over numerous configurations and progressively discards less viable options, concentrating resources on the most advantageous hyperparameters.
- **Automated Machine Learning (AutoML):** Employs sophisticated algorithms and heuristics to automate hyper parameter optimisation. Instruments such as Google Auto ML and Auto-sklearn streamline this procedure, rendering it attainable for individuals with little proficiency.

These techniques assist in identifying optimal hyper parameter configurations for ML and DL models, hence improving their capacity to detect and respond to cyber-attacks efficiently.

The Intrusion Detection Approach utilising a Hierarchical DL based Butterfly Optimisation Algorithm (ID-HDLBOA) by Manoranjithem et al. (2023) tackles Big Data management and analysis for intrusion detection. Intruder detection employs DL and hyper parameter optimisation through a hierarchical LSTM model. The Butterfly Optimisation Algorithm (BOA) is employed to enhance LSTM hyper parameters, enhancing detection performance. Benchmark intrusion dataset results indicate that the ID-HDLBOA model achieves an accuracy of 98%. The study indicates that optimised DL models in Big Data systems are advantageous for intrusion detection.

Calugar et al. (2022) present a proficient hyper parameter optimisation method to enhance ANN based IDS. The work optimises ANN models to enhance accuracy, given the escalating complexity of communication systems and the variability in detection performance across datasets. Evaluating three types of ANN across four datasets demonstrates that the proposed tuning methodology surpasses prior research and conventional learning techniques. Parameter optimisation is essential for the performance of IDS across various situations, as demonstrated in this study.

Masum et al. (2021) propose a BO methodology to enhance deep neural network (DNN) classifiers for intrusion detection, addressing the limitations of current network intrusion detection techniques. The study indicates that manually adjusting hyper parameters is arduous and resource-intensive. The automation of hyper parameter tuning guarantees the most effective DNN architecture for intrusion detection. In the NSL-KDD dataset, the Bayesian

approach surpasses random search optimisation in accuracy, precision, recall, and F1-score, demonstrating its advantages for network security.

Ananthi et al. (2023) offer an ensemble based IDS that employs Recursive Feature Elimination (RFE) for feature selection and utilises the KDD 99 dataset for training. RFE eliminates extraneous or superfluous features to enhance the performance of the feature subset. A DNN categorises network data as either normal or malicious by selecting the most significant elements. Hyper parameter optimisation and ensemble learning enhance the classification accuracy of intrusion detection systems. The model's recall, precision, F1-score, and accuracy indicate its effectiveness in securing IoT networks.

Kumar et al. (2024) delineate an advanced Network Intrusion Detection System (NIDS) designed to combat sophisticated attack methodologies such as encrypted traffic and polymorphic malware. The suggested methodology normalises and standardises data to enhance consistency. Perceptive Craving Game Search Optimisation (PCGSO) is employed for feature selection, enhancing model efficiency. A Bidirectional Gated Recurrent Unit (BI-GRU) identifies sequential dependencies in network traffic for classification, whereas PCGSO optimises hyper parameters to enhance performance. The approach attains 99% accuracy on the ISCXIDS2012 dataset, surpassing prior models in both accuracy and resilience against cyber-attacks. This study demonstrates that PCGSO enhances feature selection and model tweaking for intrusion detection.

Kanimozhi and Jacob (2019) delineate an AI driven network IDS designed to identify botnet attacks that threaten financial sectors and banking services. The solution employs artificial neural networks using the Canadian Institute for Cyber security's authentic intrusion detection dataset CSE-CIC-IDS2018. The IDS demonstrates exceptional performance with 99.97% accuracy, an average ROC curve area of 0.999, and 0.001 false positives. Cloud computing and hyper parameter optimisation renders the system optimal for traditional and cyber physical systems in real-time network traffic analysis.

3. DL in IDS

DL has transformed IDS by allowing models to autonomously learn from extensive and intricate datasets, thereby markedly improving the identification of advanced cyber threats. In contrast to conventional IDS techniques that depend on manually produced characteristics and established rules, DL models may independently extract pertinent features from unprocessed data, identifying complex patterns and anomalies that may signify hostile actions. Convolutional Neural Networks (CNNs) are extensively utilised for their capacity to handle and analyse structured data, such as network traffic, by identifying spatial hierarchies within the data. This renders CNNs especially proficient in detecting intrusions through network patterns that more simplistic models may neglect. Recurrent Neural Networks (RNNs) and their derivatives, including Long Short Term Memory (LSTM) networks, are utilised to capture temporal dependencies in sequential data, rendering them appropriate for analysing time series data such as log files and identifying patterns over time that may signify an ongoing attack. Autoencoders, a form of unsupervised learning model, are employed to acquire compressed representations of data, rendering them proficient in anomaly detection by recognising deviations from standard traffic patterns, which may indicate intrusions.

The amalgamation of DL with sophisticated methodologies like as hyperparameter optimisation and ensemble learning has significantly improved IDS efficacy. Hyperparameter optimisation methods, including grid search, random search, and Bayesian optimisation, refine DL models to achieve optimal performance. Ensemble learning, which integrates many models, enhances the robustness and reliability of IDS by diminishing false positives and negatives. The scalability of DL models renders them appropriate for managing the substantial data quantities produced in contemporary network environments, encompassing cloud based and IoT systems. As these systems increase in complexity, the adaptability and scalability of DL models are essential for ensuring security. Furthermore, DL based IDS are progressively implemented in real-time settings, perpetually monitoring and analysing network traffic to deliver prompt alerts and reactions to potential threats. The benefits of DL in IDS are enumerated below

- **Automatic Feature Extraction:** DL models may independently discern and extract pertinent features from unprocessed data, diminishing the necessity for manual feature engineering.
- **Elevated Detection Precision:** These models proficiently identify intricate patterns and anomalies, resulting in enhanced accuracy in the detection of advanced cyber threats.
- **Ability to Identify Zero-Day Attacks:** DL can detect previously unrecognised vulnerabilities by discerning irregularities overlooked by conventional methods.
- **Scalability:** DL models are capable of processing substantial data quantities, rendering them appropriate for contemporary network contexts, such as cloud and IoT systems.
- **Adaptability:** The models can adjust to novel attack types by assimilating continuous data streams, hence augmenting their efficacy in dynamic settings.
- **Real-Time Surveillance:** DL based IDS can be implemented for on-going, real-time observation, facilitating immediate identification and reaction to threats.
- **Minimised False Positives/Negatives:** Employing methods such as ensemble learning enhances the robustness of DL models, hence decreasing the probability of errors in intrusion detection.

Kunang et al. (2021) propose a DL based NIDS utilising PTDAE and DNN pretraining to enhance attack detection accuracy. The study highlights hyper parameter optimisation by GS and RS to automatically enhance model performance. The pretraining step evaluates three feature extraction techniques deep auto encoder (DAE), auto encoder (AE), and stacked auto encoder (SAE) using the NSL-KDD and CSE-CIC-ID2018 datasets. DAE exhibits optimal performance. The model's multiclass classification accuracy surpasses that of prior techniques.

Kunang et al. (2020) offer IDS that employs an unsupervised AE and a DNN to address IoT security challenges. The auto encoder extracts features, enhancing the learning of DNN. The authors employ Bayesian Hyper parameter Optimisation to adjust activation functions and weight initialisation to enhance model performance. In the BoT-IoT dataset, BO enhances classification accuracy to 99.99%, demonstrating its advantages for IoT security.

Wazirali (2020) introduces a semi supervised IDS designed to identify minor cyber-attack modifications that conventional ML techniques fail to detect. Hyper parameter optimisation of K-nearest neighbour (KNN) using fivefold cross validation enhances detection rates and diminishes false alarms in the proposed IDS. The k-nearest neighbours of each unlabelled data point in the training set are identified and hyper parameter tuning, distance metrics, and class distributions are employed for classification. The technique surpasses KNN based IDS models on the NSL-KDD dataset, exhibiting superior attack detection capabilities.

Rathee et al. (2023) examine the potential of DL to reduce cyber-attack risks and enhance cyber security. The research evaluates DNN, shallow neural networks, CNN, and networks based on attention mechanisms across different depths and architectures. Researchers employ a checkpoint technique to choose the most precise models. The models are evaluated with the NSL-KDD, Kyoto, and UNSW-NB15 benchmark datasets. A comparative analysis demonstrates that the proposed deep learning-based network IDS enhances cyber security.

Navya et al. (2021) employ a ML based IDS to identify and classify cyber-attacks, underscoring the increasing demand for such systems owing to swift technological advancements. The research employs DNNs to develop versatile IDS capable of managing dynamic and heterogeneous network and host incursions. DNN models excel at detecting and classifying unforeseen cyber-attacks through the use of datasets and on-going updates. This research demonstrates that DL models can enhance the accuracy and responsiveness of intrusion detection systems.

Anwer et al. (2021) propose a hybrid DL approach to enhance intrusion detection in IoT environments, tackling the increasing prevalence of connected devices and their associated security vulnerabilities. The study utilises the Kitsune dataset to compare LSTM and CuDNNLSTM DL models. CuDNNLSTM surpasses conventional LSTM,

achieving 99.79% accuracy on a 6GB dataset comprising 2 million records. This research demonstrates that advanced DL can safeguard intelligent systems against complex network threats.

Jullian et al. (2023) present a distributed DL architecture to address the increasing prevalence of cyber-attacks on IoT networks resulting from smart devices and network vulnerabilities. The NSL-KDD and BoT-IoT datasets are utilised to assess two DL models: feed forward neural networks and LSTM. The findings indicate that the proposed framework can identify several cyber-attacks with an accuracy of up to 99.95% across different configurations. This study demonstrates that distributed DL enhances security by consolidating multiple vulnerability sources into a unified detection system.

Wang et al. (2022) examine the challenge of identifying cyber-attacks in Supervisory Control and Data Acquisition (SCADA) systems, which oversee extensive production and power grid infrastructures yet are susceptible to advanced threats. The study advocates for a stacking DL approach to address the limitations of current IDSs, such as firewalls and antivirus software, which are typically inadequate for SCADA systems. The proposed method surpasses standalone DL models and other leading algorithms, such as Nearest Neighbour, RF, Naive Bayes, AdaBoost, Support Vector Machines, and OneR, in identifying malicious intrusions on real datasets from a power transmission system and a gas pipeline. The research additionally uses RF to assess feature significance, hence streamlining models. This research demonstrates that stacked DL enhances critical industrial system security.

Asgharzadeh et al. (2024) assert that deep learning and feature selection can facilitate the development of an advanced IoT IDS. FECNNIoT employs a CNN for feature extraction and BMEGTO for feature selection. The hybrid CNN-BMEGTO-KNN methodology attains an accuracy of 99.99% on the TON-IoT dataset and 99.86% on the NSL-KDD dataset. BMEGTO identifies 27% and 25% of the optimal characteristics among these datasets. The research demonstrates that DL and sophisticated optimisation enhance the accuracy of IDS and feature selection.

DL in IDS employs neural networks to autonomously identify harmful activities by analysing intricate patterns in network traffic or system logs. DL employs CNNs, RNNs, and autoencoders to effectively detect both established and novel threats; yet, it necessitates substantial data and computational resources and poses interpretative challenges.

DL Algorithms in Cyber Attacks:

- **Convolutional Neural Networks (CNNs):** Proficient at analysing spatial patterns within network traffic data and identifying anomalies.
- **Recurrent Neural Networks (RNNs):** Appropriate for the processing of sequential data, facilitating the identification of temporal assault patterns. LSTM (Long Short-Term Memory) networks are a particular variant of RNN designed to capture long-term dependencies.
- **Autoencoders (AE):** Employed for anomaly detection by learning to compress and reconstruct standard data, identifying deviations as potential threats.
- **Deep Belief Networks (DBNs):** Acquire hierarchical feature representations to differentiate between normal and harmful actions.
- **Generative Adversarial Networks (GANs)** produce synthetic attack samples to augment the training dataset, hence enhancing the detection of novel and complex attacks.
- **Variational Autoencoders (VAEs):** Like autoencoders, VAEs characterise the distribution of normal data to successfully detect abnormalities.
- **Self-organising Maps (SOMs):** Employed for aggregating and visualising high-dimensional data, facilitating the identification of trends related to assaults.
- **Deep Reinforcement Learning (DRL):** Adapts and learns from environmental interactions, potentially enhancing intrusion detection systems through feedback optimisation.

3. Conclusion

In conclusion, this research highlights the significant influence of DL and hyper parameter optimisation on the efficacy of IDS. As cyber threats increasingly grow in complexity, conventional detection methods prove inadequate, necessitating new techniques such as DL to ensure robust network security. By employing DL models to autonomously extract complex information and refining their performance through optimised hyper parameters, IDS can attain enhanced accuracy and adaptability, even in the face of novel threats. The incorporation of these advanced methodologies is essential to adapt to the constantly evolving landscape of cyber threats, hence ensuring the resilience and reliability of cyber security defences across diverse contexts.

Dr. Hamela K was born in Chennai, India. She received her MCA degree from Bharathidasan University, Tiruchirappalli, India in 2002, followed by an M.Phil degree from Mother Teresa Women's University, Kodaikanal, India in 2004. She further earned an MBA degree from Alagappa University, Karaikudi, India in 2010. In 2020, She completed her Ph.D. in Computer Science from Mother Teresa Women's University, Kodaikanal, specializing in Mobile Ad Hoc Networks (MANETs). Her doctoral research focused on the area of Mobile Ad Hoc Networks, a field concerned with wireless, infrastructure-less and dynamically self-organizing communication networks. She is currently serving as an Associate Professor and Head of the Department of Computer Science and Applications at Government First Grade College, Kolar, Karnataka, India. She has 22 years of teaching experience in the field of Computer Science and Applications.

REFERENCES

1. Z. Azam, M. M. Islam and M. N. Huda, "Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree," in IEEE Access, vol. 11, pp. 80348-80391, 2023.
2. Yesi Novaria Kunang, Siti Nurmaini, Deris Stiawan, Bhakti Yudho Suprapto,Attack classification of an intrusion detection system using deep learning and hyperparameter optimization,Journal of Information Security and Applications,Volume 58,2021,102804,ISSN 2214-2126,
3. Y. N. Kunang, S. Nurmaini, D. Stiawan and B. Y. Suprapto, "Improving Classification Attacks in IOT Intrusion Detection System using Bayesian Hyperparameter Optimization," 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 2020, pp. 146-151,
4. Wazirali, R. An Improved Intrusion Detection System Based on KNN Hyperparameter Tuning and Cross-Validation. Arab J Sci Eng 45, 10859–10873 (2020).
5. Manoranjithem, S. Dhanasekaran, A. Asokan, A. Kumar, C. Yamini and M. Tiwari, "An Intrusion Detection Approach using Hierarchical Deep Learning-based Butterfly Optimization Algorithm in Big Data Platform," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2023, pp. 212-216.
6. A.N. Calugar, W. Meng and H. Zhang, "Towards Artificial Neural Network Based Intrusion Detection with Enhanced Hyperparameter Tuning," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 2627-2632.
7. V. Kanimozhi and T. P. Jacob, "Artificial Intelligence based Network Intrusion Detection with Hyper-Parameter Optimization Tuning on the Realistic Cyber Dataset CSE-CIC-IDS2018 using Cloud Computing," 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2019, pp. 0033-0036.
8. M. Masum et al., "Bayesian Hyperparameter Optimization for Deep Neural Network-Based Network Intrusion Detection," 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 2021, pp. 5413-5419.
9. P. Ananthi, T. E. Ramya and R. Janani, "Ensemble based Intrusion Detection System for IoT Device," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 1073-1078.
10. P. M. Kumar, K. Vedantham, J. Selvaraj and B. P. Kavin, "Enhanced Network Intrusion Detection System Using PCGSO-Optimized BI-GRU Model in AI-Driven Cybersecurity," 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC), Houston, TX, USA, 2024, pp. 1-6.

11. A. Rathee, P. Malik and M. Kumar Parida, "Network Intrusion Detection System using Deep Learning Techniques," 2023 International Conference on Communication, Circuits, and Systems (IC3S), BHUBANESWAR, India, 2023, pp. 1-6.
12. M. Anwer, G. Ahmed, A. Akhunzada and S. Siddiqui, "Intrusion Detection Using Deep Learning," 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, Mauritius, 2021, pp. 1-6.
13. V. K. Navya, J. Adithi, D. Rudrawal, H. Tailor and N. James, "Intrusion Detection System using Deep Neural Networks (DNN)," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2021, pp. 1-6.
14. Jullian, O., Otero, B., Rodriguez, E. et al. Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework. J Netw Syst Manage 31, 33 (2023).
15. Wang, W., Harrou, F., Bouyeddou, B. et al. A stacked deep learning approach to cyber-attacks detection in industrial systems: application to power system and gas pipeline systems. Cluster Comput 25, 561–578 (2022).
16. Asgharzadeh, H., Ghaffari, A., Masdari, M. et al. An Intrusion Detection System on The Internet of Things Using Deep Learning and Multi-objective Enhanced Gorilla Troops Optimizer. J Bionic Eng (2024).
17. Y. Wu, J. Wu, C. Long and S. Li, "Secure Strategy Design for Networked Control Systems under Multiple Cyber-attacks over a Multi-channel Framework," 2024 36th Chinese Control and Decision Conference (CCDC), Xi'an, China, 2024, pp. 5050-5055.
18. Manoranjithem, S. Dhanasekaran, A. Asokan, A. Kumar, C. Yamini and M. Tiwari, "An Intrusion Detection Approach using Hierarchical Deep Learning-based Butterfly Optimization Algorithm in Big Data Platform," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2023, pp. 212-216.