CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Chapter 1 highlighted the critical threats posed by Distributed Denial of Service (DDoS) attacks. These attacks exploit abnormal network traffic patterns to overwhelm systems, making security a paramount concern (Husák, M et al, 2019) (John, J., Norman, J. 2019). This thesis sets out to propose innovative and effective strategies to identify the impact of DDoS attacks. Focusing on various feature selection techniques and Machine/Deep Learning techniques, the research aims to develop models capable of handling DDoS attacks. To lay the groundwork for these proposed solutions, an extensive review of the existing literature in the field of DDoS attacks and the mitigation have been conducted. This literature review serves as a comprehensive exploration of the current state of DDoS threats, providing a refined understanding of the challenges at hand.

2.2 Literature on various approaches in DDOS detection

Distributed Denial of Service (DDoS) detection methods have garnered significant attention in the literature. DDoS attacks are a prevalent form of cyber threat that can disrupt online services by overwhelming them with a flood of traffic from multiple sources. Detecting these attacks is crucial for maintaining the availability and integrity of online systems. Researchers have explored various approaches and techniques to identify and mitigate DDoS attacks effectively.

Understanding the strengths and limitations of these detection techniques is essential for developing robust defense mechanisms against DDoS attacks in today's interconnected digital landscape. The literature is carried out on the following topics: various approaches in DDoS detection, existing IDS in intrusion detection, various datasets used in intrusion detection, various feature selection (FS) methods, and various computational intelligence techniques in intrusion detection. Table 2.1. shows the various techniques used in DDoS Detection.

Table 2.1 Literature Study on Various techniques in DDOS detection

Author, Year and Journal	Title	Techniques Applied	Dataset	Findings
Bouke, M.A., et al (2023) ELSEVIER	An intelligent DDoS attack detection tree-based model using Gini index feature selection method	Decision Tree (DT) algorithm, enhanced Gini index feature selection method.	UNSW-NB15 dataset	Achieved 98% accuracy, outperforming baseline models. The enhanced Gini index feature selection method reduced dimensionality, avoiding overfitting, lower false alarm rate of only 2% on testing instances.
Osanaiye, O et al., (2016) SPRINGER	Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing	Decision tree classification algorithm	Benchmark Dataset	Detecting DDoS attack in cloud that occurs at network and application layers, such as TCP-SYN, HTTP GET, UDP, and ICMP
Aguru, Aswani Devi, and Suresh Babu Erukala (2024) ELSEVIER	A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning	Modified Gated Recurrent Units (mGRU)	CICIoT2023, CICDDoS2019	mGRU-based IDS models outperform standard GRU-based IDS models with a 2% reduction in time consumption. Suitable for time-critical healthcare applications.
Akgun, Devrim, Selman Hizal, and Unal Cavusoglu,	A new DDoS attacks intrusion detection model based on	Deep Neural Networks (DNN), Convolutional Neural Networks	CIC-DDoS2019 dataset.	CNN-based inception model, achieved high accuracy rates of 99.99% for binary

Author, Year and Journal	Title	Techniques Applied	Dataset	Findings
(2022) ELSEVIER	deep learning for cybersecurity	(CNN), (LSTM).		and 99.30% for multiclass detection
Aamir, M. and Zaidi, S.M.A., (2019), 18, 761-785 SPRINGER	DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation	Feature Engineering (backward elimination, chi2, information gain scores), Machine Learning (K-nearest neighbors, Support Vector Machine, Random Forest)	DDoS datasets	Significant feature reduction (approximately 68%) possible with minimal performance hit (about 0.03% on accuracy). K-nearest neighbors algorithm performs best, followed by Support Vector Machine
Najafimehr, M., Zarifzadeh, S. and Mostafavi, S., (2023) Engineering Reports	DDoS attacks and machine-learning-based detection methods: A survey and taxonomy	Supervised, Unsupervised, Hybrid Machine Learning Approaches	Various Datasets	Provides a comprehensive taxonomy of ML-based DDoS detection methods, reviews related challenges, and proposes future research directions.
Abdullah Emir Cil and Kazim Yildiz and Ali Buldu (2021) ELSEVIER	Detection of DDoS attacks with feed forward based deep neural network model	DNN model, Deep learning	CICDDoS2019 Dataset	Observed the attacks on network traffic were detected with 97.99% success and the attack types were classified with an accuracy rate of 94.57%. The high
Seth, J.K. and Chandra, S., (2018) SPRINGER	An Effective DOS Attack Detection Model in	Artificial bee colony optimization (BABCO) and	Dataset prepared using Apache Cloud Stack	CDOSD detects DOS attack on cloud host with high accuracy and

Author, Year and Journal	Title	Techniques Applied	Dataset	Findings
	Cloud Using Artificial Bee Colony Optimization	decision tree (DT) classifier		a very low false positive rate with low dimension of computation space for training and classification.
Kasim, Ö., (2020) ELSEVIER	An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks	data normalization, autoencoder feature learning, and SVM classification	CICIDS dataset	Achieved a 99.1% success rate in detecting DDoS attacks using the CICIDS dataset and virtual traffic. This method effectively mitigated false positives and improved efficiency over prior models.
Devrim Akgun, Selman Hizal, Unal Cavusoglu, (2022) ELSEVIER	A new DDoS attacks intrusion detection model based on deep learning for cybersecurity	Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), Long Short Term Memory (LSTM).	CIC-DDoS2019 dataset.	CNN-based inception model, achieved high accuracy rates of 99.99% for binary and 99.30% for multiclass detection on the CIC-DDoS2019 dataset.
Kumar, D et al, (2023) ELSEVIER	DDoS Detection using Deep Learning	Long Short-Term Memory (LSTM), Feature Selection and Extraction	CICDDoS2019	The LSTM-based model achieves up to 98% accuracy in detecting DDoS threats, outperforming traditional machine learning methods on the CICDDoS2019 dataset.
Rudro, R. A. M et al, (2023) TURCOMAT	Enhancing DDoS Attack Detection Using Machine Learning: A Framework	Random Forest, Decision Tree, Naive Bayes, Support Vector Machine (SVM)	DDOS attack SDN dataset (Google's research dataset)	Random Forest achieves the highest accuracy rate of 99.4%, Decision Tree and SVM also perform

Author, Year and Journal	Title	Techniques Applied	Dataset	Findings
	with Feature Selection and Comparative Analysis of Algorithms			well with accuracy rates of 98.8% and 98.4%, respectively.
Raza, M.S et al., (2024) Telecom	Feature-Selection-Based DDoS Attack Detection Using AI Algorithms	NGBoost, Convolutional Neural Network (CNN), Stochastic Gradient Descent (SGD), Decision Tree, Random Forest	CICDDoS2019	Natural Gradient Boosting and Convolutional Neural Networks show promise with tabular data categorization.
Gupta, N., Jindal, V. and Bedi, P., ELSEVIER	LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system	LIO-IDS, which is based on an LSTM classifier and an Improved One-vs-One approach. It is a two-layer anomaly-based network IDS that identifies various network intrusions.	Efficient for large database	High time complexity compared to state of art algorithms

The literature review on IDS for DDoS attack detection highlights several points. Despite significant advancements, there are notable gaps in current IDS research, including challenges in feature selection and dimensionality reduction, handling imbalanced datasets, adaptability to new threats, and computational efficiency. Extensive preprocessing and high time complexity hinder practical implementation. Addressing these gaps is crucial for developing intelligent IDS that enhance security by providing accurate detection and reduction of false positives. Intelligent IDS must be scalable, adaptable to evolving threats, and resource-efficient to effectively protect complex and diverse network environments. Continued innovation in these areas is essential for advancing IDS effectiveness and applicability.

2.3 Literature on various IDS in Intrusion Detection

The literature on existing Intrusion Detection System (IDS) techniques highlights the critical importance of securing digital environments against evolving cyber threats.

Traditional IDS methods, such as signature-based and anomaly-based detection, are explored for their effectiveness in identifying known and unknown attacks. Advanced approaches, including behavior-based detection and machine learning algorithms, are evaluated for their ability to detect novel and sophisticated threats. The review also examines key challenges in IDS, such as scalability and resource efficiency, while discussing emerging trends like the integration of threat intelligence. This comprehensive analysis offers valuable insights for enhancing the resilience of systems against a wide range of cyber threats. The following Table 2.2 presents the literature on existing IDS in Intrusion Detection.

Table 2.2 Literature on various IDS in Intrusion Detection

Author/Year/Publisher	Title of the Article	Detection Method	Type of IDS	Limitations
G. Karatas, O. K. Sahingoz (2018) IEEE	Neural network-based intrusion detection systems with different training functions	Neural networks with various training functions	Network IDS	High computational cost and potential for overfitting
H. Larijani, J. Ahmad, N. Mtetwa (2018) IEEE	A novel random neural network-based approach for intrusion detection systems	Random neural network	Network IDS	Complex model with potentially high training times
Mazini, M., Shirazi, B. and Mahdavi, I., (2019) JKSUCIS	Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms	Hybrid artificial bee colony and AdaBoost algorithms	Network IDS	Potentially high false positive rate and computational complexity

Author/Year/Publisher	Title of the Article	Detection Method	Type of IDS	Limitations
Meftah, S., Rachidi, T. and Assem, N., (2019) IJCDS	Network based intrusion detection using the UNSW-NB15 dataset	Machine learning-based anomaly detection	Network IDS	Requires extensive feature selection and preprocessing
Devan, P. and Khare, N., (2020) NCA	An efficient XGBoost–DNN-based classification model for network intrusion detection system	XGBoost and deep neural network	Network IDS	High computational cost and potential difficulty in tuning model parameters
Bedi, P., Gupta, N. and Jindal, V., (2021) AI	I-SiamIDS: an improved Siam-IDS for handling class imbalance in network-based intrusion detection systems	Siamese neural network with improved one-vs-one technique	Network IDS	High time complexity and potential difficulty in handling very large datasets
Pacheco, J., Benitez, V. and Félix, L., (2019) ACM/IEEE	Anomaly behavior analysis for IoT network nodes	Anomaly behavior analysis using machine learning	IoT IDS	High false positive rate and limited generalizability across different IoT environments
Ahn S et al. (2020) IEEE DAC	Hawkware: network intrusion detection based on behavior analysis with ANNs on an IoT	Behavior analysis with artificial neural networks (ANNs)	IoT IDS	Limited computational resources on IoT devices might hinder performance

Author/Year/Publisher	Title of the Article	Detection Method	Type of IDS	Limitations
	device			
Khan, M.A., (2021) Processes	HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System	Hybrid convolutional and recurrent neural network (HCRNN)	Network IDS	High computational complexity and potential overfitting
Aljawarneh, Shadi, Monther Aldwairi, and Muneer Bani Yassein (2018) JCS	Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model	Hybrid anomaly-based detection	Network IDS	Extensive feature selection required and potential overfitting

The reviewed literature highlights various intrusion detection methods, including neural networks, hybrid algorithms, and anomaly-based techniques, each demonstrating potential for enhancing detection capabilities. However, common challenges persist, such as high computational complexity, overfitting risks, extensive feature selection requirements, and scalability issues. These limitations emphasize the need for complexity-aware intelligent intrusion detection systems that can optimize resource utilization, handle large-scale data efficiently, and adapt dynamically to evolving threats while minimizing false positives and overfitting risks.

2.4 Literature on Various Datasets used in Intrusion detection

According to state-of-the-art literature, most of the researchers performed experimental validation and evaluation of proposed approaches through various public datasets. This section discusses about the brief description of most-commonly used public datasets, whose summary is also shown in Table 2.3.

Table 2.3 Summary of Various Datasets used in attack detection

Dataset	Description (DDoS attacks and features)
DARPA KDD CUP 1999	Traffic, content, and basic features of four types of attack (i.e. DoS, U2R, Probing, R2L) and one normal category
NSL-KDD	An enhanced version of KDD CUP 99 with fewer records than KDD CUP 99
CIDD	Misuse- and anomaly-based audit data encompassing real samples of both network- and host-based attacks.
CIDDS-001	Emulated NetFlow data labeled with three types of attack (i.e. DoS, Brute Force, and Port Scans)
CAIDA	Data collected from different sources and usually utilized for research purposes
USPSCIMS	Dataset for detecting and preventing DoS attacks on VMs consisting of 24 time-based traffic features related to six DoS attacks
ISOT-CID	Network intrusion detection dataset collected in a production OpenStack cloud environment, containing data from inside and outside attacks
UNSW-NB15	Network intrusion detection dataset comprising 49 TCP flow-level features from nine different attack families
CICIDS2017	Raw traffic captures and flow-level features related to benign traffic and up-to-date common attacks
CSE-CIC-IDS2018	Advancement of CICIDS2017 leveraging various user profiles to define different set of features
CICDDoS2019	Advancement of CSE-CIC-IDS2018 with sets of network flow features to detect different types of DDoS attacks with their corresponding weights

The KDD Cup 1999 dataset, originating from DARPA 1998, serves as a benchmark for anomaly detection in network intrusions. Featuring five million training data records spanning three weeks, it includes DoS, User-to-Remote, probing, and Remote-to-Local attacks. The NSL-KDD dataset, an enhancement of KDD Cup 1999, addresses its limitations by eliminating redundancies. CIDD, a cloud intrusion detection dataset, encompasses behavior-based and knowledge-based audit data for various network-based

and host-based attacks. CIDDS-001, a labeled flow-based dataset, created in a virtual environment, evaluates anomaly-based IDSs. CAIDA provides diverse datasets, including specific attacks or events, accessible to researchers. The UNSW-NB15 dataset renews NIDS benchmarking with a hybrid configuration of real and synthetic traffic. The CSE-CIC-IDS2018 dataset advances CICIDS2017, generating comprehensive benchmark datasets for IDSs. CICIDS2017 includes benign traffic and modern attacks, while CICDDoS2019, an extension, focuses on DDoS attacks, offering a labelled dataset with various attack scenarios for cybersecurity research.

2.5 Literature on various Feature Selection (FS) Methods

The literature on various feature selection methods for detecting DDoS attacks highlights their critical role in enhancing the performance and efficiency of IDS. Feature selection methods, such as backward elimination, chi-square, and information gain etc. help in reducing the dimensionality of data, thus improving detection accuracy and reducing computational overheads. However, these methods are often tailored to specific datasets and attack types, limiting their generalizability across different environments and attack vectors. Applying the same feature selection methods universally can be challenging due to the diverse nature of DDoS attacks and the dynamic characteristics of network traffic. Therefore, developing an intelligent IDS that incorporates adaptive feature selection and advanced machine learning algorithms is essential. Such an IDS can dynamically adjust to various attack patterns and environmental conditions, providing robust and scalable protection against sophisticated DDoS attacks. This approach ensures that the IDS remains effective adapting to emerging threats and minimizing false positives while maintaining high detection accuracy. A comparative analysis of the existing literature has been summarized in Table 2.4.

Table 2.4 Literature on various Feature selection methods and its Pros and Cons

Author Year and Journal.	Title	FS Method	Pros	Cons
Pham, N.T et al., (2018) ACM	Improving performance of intrusion detection system using ensemble methods and	Leave-one-out techniques and Naive Bayes classifier,	The research indicated that used models had high accuracy and low FAR (False Alarm Rate), with	They performed the comparison only between bagging and boosting ensemble techniques.

Author Year and Journal.	Title	FS Method	Pros	Cons
	feature selection	Gain Ratio (GR) technique	the bagging model. They used J48 as the base classifier and worked on a 35-feature subset, producing the best results were 84.25% accuracy and 2.79% FAR.	
Khalid, S., Khalil, T. and Nasreen, S., (2014) IEEE	A survey of feature selection and feature extraction techniques in machine learning.	Wrapper and Filter-based methods	Feature selection improves knowledge of the process under consideration, as it points out the features that mostly affect the considered phenomenon. The objective of both methods concerns the reduction of feature space in or der to improve data analysis.	The computation time of the adopted learning machine and its accuracy need to be considered as they are crucial in machine and data mining applications.
Adams, S. and Beling, P. (2019) SPRINGER	A survey of feature selection methods for Gaussian mixture models and hidden Markov models	Gaussian Mixture Models (GMM) and Hidden Markov Models (HMM)	Explored GMMs and HMMs possibilities for supervised and unsupervised FS methods. Their approach works better with unsupervised learning methods	GMM related methods were given more emphasis rather than HMM.

Author Year and Journal.	Title	FS Method	Pros	Cons
Lin, S.W et al., (2012) ELSEVIER	An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection	Combination of support vector machine (SVM), decision tree (DT), and simulated annealing (SA)	Generates decision rules to detect new network intrusion attacks.	Detailed comparison with other processes is not visible. Experiments conducted on limited number (DT, SA, SVM) of approaches.
Osanaiye, O et al., (2016) *EURASIP*	Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing	Info gain, Gain ratio, Chi-squared, ReliefF	Compared to single FS methods, their proposed ensemble-based multi-filter fs selection method shows more efficiency with less complexity	The proposed process is more prone to false alarm while classification.
Das, S et al., (2020) IEEE	Empirical evaluation of the ensemble framework for feature selection in ddos attack	EnFS	Produces an optimal set of features using ensemble technique that improves accuracy significantly. Their technique's false alarm rate is negligible.	Deep Learning related approaches were not explored.
Elghazel, H. and Aussem, A., (2015)	Unsupervised feature selection with ensemble learning.	RCE and RFE	This research worked to mitigate the gap between ensemble	The proposed method is not very suitable for smaller domains.

Author Year and Journal.	Title	FS Method	Pros	Cons
SPRINGER			supervised and unsupervised FS learning.	
Vinayakumar, R et al., (2019) IEEE	Deep learning approach for intelligent intrusion detection system	Not mentioned	Proposed a scalable and hybrid noble image processing technique with optimal parameters for both ML and DL architectures	Training was not conducted on complex DNN architectures.
Vinayakumar, R., Soman, K.P. and Poornachandran, P., (2017) IEEE	Evaluating effectiveness of shallow and deep networks to intrusion detection system	Feature reduction	Their approach works for evaluating the shallow and deep networks which were not explored in previous work	This research did not do experiment at analysis for real time deep network data.
Amiri, F., et al, (2011) ELSEVIER	Mutual information-based feature selection for intrusion detection systems	Modified Mutual Information based Feature Selection method (MMIFS)	MMIFS is able to measure general dependency between features and to rank them.	A huge proportion of DoS and R2L (Root to local) attacks are missed by detection methods.
Ravi, V., Chaganti, R. and Alazab, M., (2022) ELSEVIER	Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system	kernel-based principal component analysis (KPCA)	High Accuracy: The proposed end-to-end model achieves impressive accuracy, with a maximum accuracy of 99% in network attack detection and 97%	Complexity: The use of deep learning-based recurrent models, kernel-based principal component analysis (KPCA), and ensemble meta-classifier introduces

Author Year and Journal.	Title	FS Method	Pros	Cons
			in network attack classification on the SDN-IoT dataset. This indicates strong performance and effectiveness in accurately identifying and classifying network attacks.	complexity to the model. This complexity may lead to challenges in terms of interpretability and computational intensity, particularly in deployment or implementation in certain environments.

The importance of extracting the best feature set from the original data is evident from the above Literature. However, there are several limitations in the current works Firstly, a limited number of FS algorithms have been considered for the best feature selection. Secondly, a lack of variation in FS method type is apparent in the literature; they used either filter-based, wrapper-based, or embedded FS methods. Although a couple of works consider three major FS categories, the total number of FS methods was significantly lower. In addition, they experimented with only a supervised learning model for performance evaluation. Lastly, maximum works were considered one type of detection model to compare the performance of different FS methods. However, it is difficult to design an optimum FS method for each model type, such as machine learning, deep learning, and unsupervised learning.

2.6 Literature on various Computational Intelligence Techniques in Intrusion Detection

Computational Intelligence (CI) techniques are a subset of artificial intelligence that deal with complex real-world problems where traditional methods are unproductive. These techniques are inspired by nature and human reasoning processes and are often used for tasks such as optimization, pattern recognition, and decision-making. The primary categories and types of Computational Intelligence techniques shown in Figure 2.1 (Raj, J.S., 2019) (Shamshirband S et al, 2020).

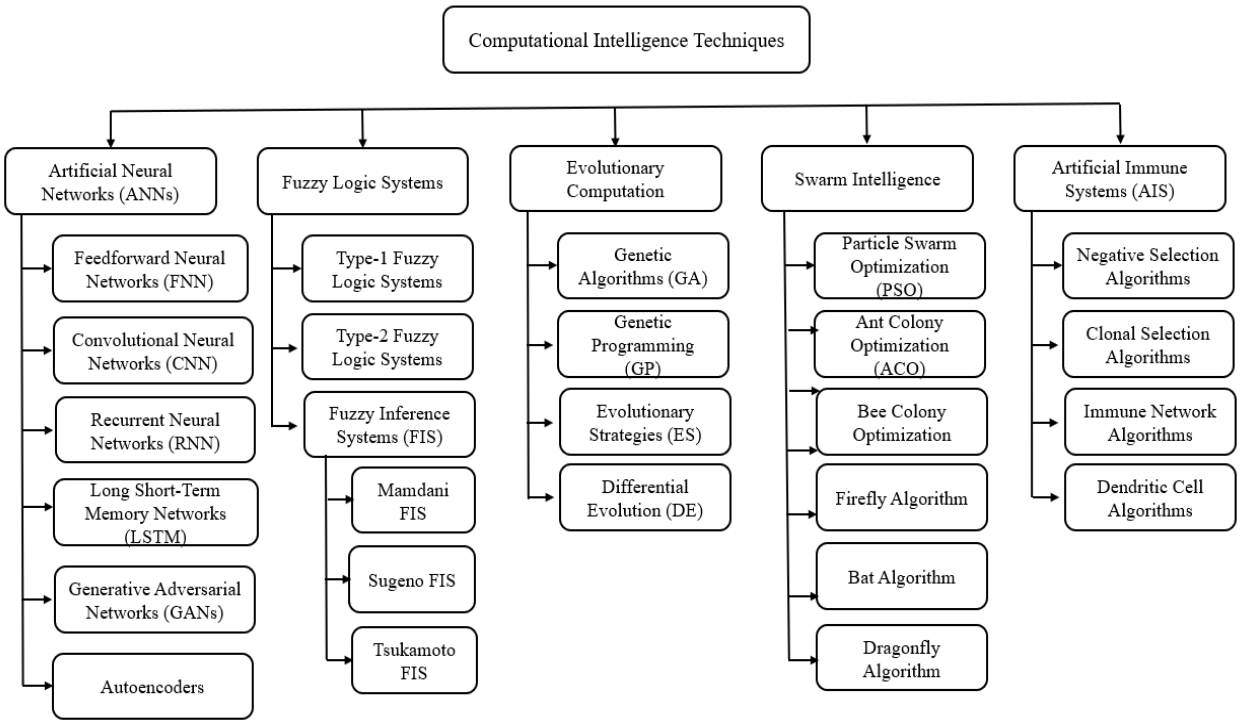

Figure 2.1 Summary of Computational Intelligent Techniques

Computational Intelligence (CI) techniques encompass a range of methods inspired by natural processes and human reasoning, employed to tackle complex real-world problems. Key CI techniques include Artificial Neural Networks (ANNs), such as Feedforward, Convolutional, Recurrent, and Generative Adversarial Networks; Fuzzy Logic Systems, which handle uncertainty and imprecision through Type-1 and Type-2 systems, including various Fuzzy Inference Systems; and Evolutionary Computation, including Genetic Algorithms, Genetic Programming, Evolutionary Strategies, and Differential Evolution. Swarm Intelligence methods like Particle Swarm Optimization, Ant Colony Optimization, and Dragonfly Algorithm mimic collective behaviors of social organisms. Additionally, Artificial Immune Systems enhance the problem-solving capabilities. Optimization methods, particularly in feature selection, are crucial as they enhance model performance by identifying the most relevant features, thereby reducing dimensionality, improving accuracy, and minimizing computational costs. Techniques such as Genetic Algorithms and Particle Swarm Optimization are widely used to efficiently search for optimal feature subsets, leading to more robust and generalizable models (Wu, S.X. and Banzhaf, W., 2010).

Table 2.5 summarizes a practical way the Computational Intelligent-based methods are applied in DDoS attack detection IDSs. This highlights the particular

technique utilized (i.e. Fuzzy Logic, Decision Tree, Genetic Algorithm, Game Theory, Support Vector Machine, etc.), their aim, pros and cons and briefly their main contribution.

Table 2.5: Summary of CI techniques with Machine and Deep Learning used in DDoS attack detection

Author's name and Year	Title	Techniques Used	Pros	Cons
Elsayed, M.A. and Zulkernine, M., (2020) IEEE	PredictDeep: Security Analytics as a Service for Anomaly Detection and Prediction	Graph Convolution Networks (GCNs)	Timely detection and prediction of security breaches	It does not predict and classify anomalies under change in the system behaviour
Kimmel et al., (2021) IEEE	Recurrent Neural Networks Based Online Behavioural Malware Detection Techniques for Cloud Infrastructure	LSTM and Bidirectional RNNs (BIDIs)	Achieves high detection rates	Does not handle heterogeneous data
Loukas, G et al., (2017) IEEE	Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning	MLP and RNN	Reduction in detection latency	Increased communication overhead
Garg et al., (2019) IEEE	A Hybrid Deep Learning-Based Model for Anomaly Detection in Cloud Datacenter Networks	Grey wolf Optimization (GWO) and (CNN)	High accuracy and high detection rate	Increased computational complexity

Author's name and Year	Title	Techniques Used	Pros	Cons
Sharifian Z et al, (2023) ELSEVIER	Sin-Cos-bIAVOA: A new feature selection method based on improved African vulture optimization algorithm and a novel transfer function to DDoS attack detection	Improved African Vulture Optimization Algorithm (Sin-Cos-bIAVOA), Gravitational Fixed Radius Nearest Neighbor (GFRNN), feature selection, meta-heuristic algorithms.	Enhanced approach, Innovative approach and source code publically available	Complex, Computational resources
Zhang, H, et al (2020)	A real-time and ubiquitous network attack detection based on deep belief network and support vector machine.	Deep Belief Networks (DBNs) and Ensemble Learning	High accuracy, Ability to capture complex patterns	Computational overhead, Model interpretability
Rezaeipanah, Amin, et al. (202)	Combining Particle Swarm Optimization and Entropy to Detect DDoS Attacks in the Cloud Computing	Particle Swarm Optimization (PSO) and Random Forest	Feature selection capability, Ensemble learning for robustness	Training time, Overfitting potential
Hajimirzaei and Navimipour (2019) ELSEVIER	Intrusion detection for cloud computing using neural networks and artificial bee	Fuzzy clustering, Artificial Bee Colony, ANN	Reduces root mean square error and mean absolute error Improves	Does not consider runtime Costly combination of proposed algorithms

Author's name and Year	Title	Techniques Used	Pros	Cons
	colony optimization algorithm.		kappa statistic	
Yu, Xueshan, et al. (2019)	Design of DDoS attack detection system based on intelligent bee colony algorithm	Support Vector Machine (SVM) optimized with Artificial Bee Colony Algorithm	Global optimization, Handling non-linear data	Sensitivity to parameter settings, Limited scalability

The table above illustrates a range of studies that have sought to detect attacks utilizing a variety of Computational Intelligence (CI) techniques, including machine learning and deep learning algorithms. While there has been substantial research in this field, only a few works have delved into swarm intelligence techniques, a subset of deep learning. It is important to highlight that swarm intelligence algorithms have shown effectiveness in both feature selection and attack detection. This reveals a notable gap in the existing literature, presenting an opportunity to enhance Intrusion Detection Systems (IDS) by integrating computational intelligence methods to improve detection speed, accuracy, and reduce false alarm rates (Ho, C.Y et al, 2012). Furthermore, there remains an opportunity to develop a complexity-aware model specifically tailored for detecting DDoS attacks, further advancing the capabilities of intrusion detection systems in mitigating cyber threats.

While deep learning models such as CNNs, RNNs, and DBNs have demonstrated high detection accuracy, their nature limits interpretability, (Zhang et al., 2020). Additionally, the over-dependence on accuracy metrics overlooks other key performance indicators like scalability and adaptability to new attack patterns (Sharifian et al., 2023). Comparative studies between lightweight swarm intelligence models and complex deep learning architectures are insufficient, leaving a gap in evaluating scalable solutions suitable for real-world deployment (Yu et al., 2019; Sharifian et al., 2023).

2.7 Observations and Critical Analysis Based on Literature

The literature review highlights the growing use of machine learning (ML) and deep learning (DL) techniques in detecting DDoS attacks, with various models demonstrating

improved detection accuracy and advanced pattern recognition capabilities. However, a closer analysis reveals several unresolved challenges and areas for further investigation.

Firstly, swarm intelligence (SI) techniques, although promising in optimization and feature selection, remain underutilized in DDoS detection models. Only a few studies have explored their full potential, particularly in integrated detection frameworks. Given their flexibility and adaptability, SI methods present a valuable but largely untapped approach for enhancing detection systems (Yu et al., 2019).

Secondly, a notable concern is the computational complexity of many existing models. While deep learning approaches such as CNNs and LSTMs offer high accuracy, they often require significant processing power and memory, which can restrict their applicability in environments with limited resources (Garg et al., 2019; Zhang et al., 2020; Sharifian et al., 2023). This trade-off between performance and efficiency remains a key limitation.

Moreover, many reviewed studies apply traditional feature selection methods in isolation, without exploring hybrid or adaptive combinations that may yield better performance (Pham, N.T. et al., 2018; Elghazel, H. and Aussem, A. 2015), A. The ability to dynamically refine features based on evolving network data could enhance both detection accuracy and system efficiency, yet this remains an underexplored direction.

Finally, while some models demonstrate effectiveness in detecting specific types of DDoS attacks, the existing literature has largely overlooked broader system-level aspects such as adaptability to evolving threats, robustness to diverse attack patterns, and scalability with increasing data volumes. These capabilities are critical for maintaining consistent and reliable detection performance in today's complex and dynamic network environments. The lack of focus on these dimensions underscores the growing need for complexity-aware intrusion detection systems that can intelligently adapt to varying network behaviors and attack scenarios (Sharifian et al., 2023; Yu et al., 2019).

In summary, although significant progress has been made in leveraging ML, DL, and computational intelligence techniques for DDoS detection, the literature indicates several gaps, particularly in the areas of optimization-driven feature selection, model efficiency, and model adaptability. These limitations underscore the need for complexity-aware systems capable of adapting to real-world challenges such as high data volumes, evolving attack patterns, and resource constraints. Addressing these gaps forms the core motivation

for this thesis, which proposes a structured four-phase approach focused on enhancing model efficiency, adaptability, and optimization-based feature selection. By integrating swarm-inspired algorithms, hybrid learning techniques, and scalable architectures, the proposed framework aims to bridge the gap between theoretical research and practical application in DDoS detection.

2.8 Chapter Summary

In this chapter, a comprehensive review of existing studies on DDoS attack detection, intrusion detection systems (IDS), datasets used in attack detection, feature selection methods, and computational intelligent techniques is conducted. Additionally, various techniques employed in DDoS detection and existing IDS in intrusion detection are summarized, showcasing the diversity of approaches utilized in the field. Commonly used datasets in attack detection research and various feature selection methods employed in DDoS attack detection, along with their pros and cons, are also outlined, illustrating the challenges and opportunities associated with feature selection.

Throughout the literature review, several gaps are identified, indicating areas where further research is necessary. One notable gap is the limited exploration of swarm intelligence techniques, particularly in the context of DDoS attack detection. This presents an opportunity for the proposed system to integrate swarm intelligence algorithms, leveraging their effectiveness in feature selection and attack detection. Additionally, there is a need for a complexity-aware model specifically tailored for detecting DDoS attacks, addressing the challenges posed by the evolving nature of cyber threats. By developing a system that addresses these gaps, the proposed research aims to contribute to the advancement of complexity aware intelligent intrusion detection systems, enhancing their ability to mitigate DDoS attacks effectively. The next chapter explains the proposed research design by addressing the gaps identified in the entire work.