Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 1 – 35 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

HYBRID NETWORK INTRUSION DETECTION SYSTEMS: A SYSTEMATIC REVIEW

Alhassan Seiba[1], Gaddafi Abdul-Salaam*[1], Yaw Missah[1], Mohammad Hossein Anisi[2]

[1]Department of Computer Science, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana.
[2]School of Computer Science and Electronic Engineering, University of Essex, Colchester, U.K.

*Corresponding author: Gaddafi Abdul-Salaam, Email: gaddafi.ict@knust.edu.gh

ABSTRACT: Network Security has become a major concern to governments, businesses and individuals all over the world as cybercriminals continuously attack networks and cause harm to personal and organizational data. Different forms of Intrusion Detection Systems(IDSs) have been proposed over the years to minimize these cyberattacks. Several researchers have tried to improve upon the detection accuracy and thus, reducing false alarm rates posed by some of the IDSs. In this paper, we conducted a chronological systematic review of hybrid intrusion detection systems covering all domains. In all, about 300 recent research articles were selected in the area but only 146 articles were able to meet the given quality assurance test. A critical review of the selected articles revealed that 61% did not carry out proper feature selection as a data preprocessing step and as low as 35% handled an imbalanced dataset. We have also done extensive discussions, spanning eleven years of research works on the existing Intrusion Detection Systems.

KEYWORDS: Autoencoder, Intrusion Detection, Deep Learning, Feature Selection

1.0 INTRODUCTION

The increasing use of Computer Networks especially the Internet has resulted in individuals and organizations storing sensitive data on web servers, database servers and social media platforms. This increase in the use of the internet has also caused a corresponding increase in the rate of cybercrime. CyberEdge group collected data from different parts of the world and publish a report that depicts a future likelihood of a successful attack. The report reveals that in 2014 the percentage of a successful attack was 38.1% and this figure is expected to rise steadily to 75% by the end of 2021. The figure also shows the rest of the years and the percentage of attacks expected. This figure paints a gloomy picture of an increase in cyber attacks within the coming years. One security mechanism put in place to eliminate or reduce these attacks is Intrusion Detection System (IDS). An intrusion Detection System is a hardware or software implementation that monitors unauthorized access to a computer network or host and reports on possible data violations. (Anderson, 1980) proposed the idea of Intrusion Detection. Since then different types of IDS have been developed to promote network security.

Based on where IDS is deployed there can be classified into Host Based Intrusion Detection System(HIDS) and Network Intrusion Detection System(NIDS). Host-Based Intrusion Detection System monitors data traffic on a single host computer for packets that are malicious or not. Network Intrusion Detection System on the other hand monitors data packets coming to a network and reports on any malicious activity. Figure 2 and Figure 3 show the difference between NIDS and HIDS. There are certain merits and demerits associated with each type. With regards to HIDS, the advantages are that it can handle encrypted communication, it does not require extra hardware and so it is more economical. The drawbacks to this method are that there is a delay in reporting attacks, it also consumes host resources and only able to monitor attacks on only one device where it is installed. NIDS has the advantage of being able to detect attacks on multiple computers, again, NIDS does not need to be installed on more than one host. NIDS also have some disadvantages including not being able to identify attacks that are encrypted, a dedicated hardware is required.

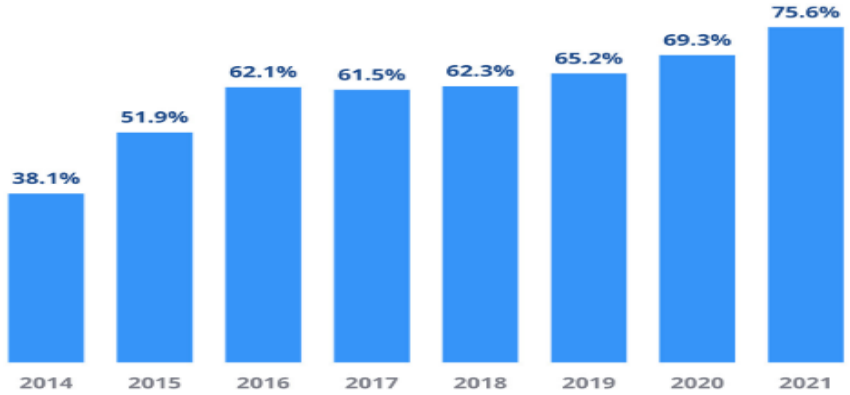

Figure 1: The Likelihood of a successful attack occurring (CyberEdge Group, 2021)

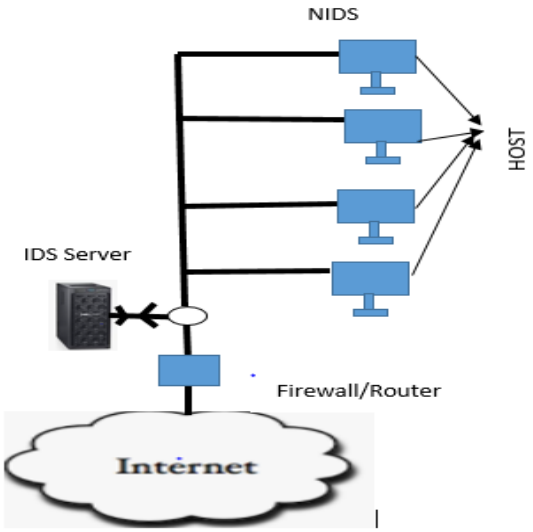

Figure 2: Network-based IDS (Seiba et al., 2021)

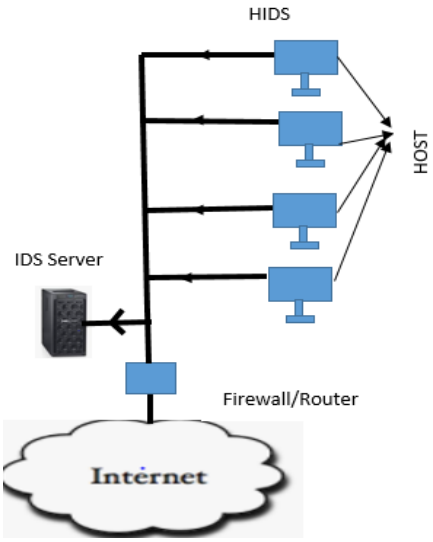

Figure 3: Host-based IDS (Seiba et al., 2021)

Intrusion Detection Systems can also be classified based on how there are implemented thus Signature Based Intrusion Detection Systems and Anomaly Based Intrusion
Detection System. A signature-Based Intrusion Detection System is implemented by keeping the profile of existing known attack and compared with incoming traffic to determine if it is malicious or not. The advantage associated with this kind of IDS is its ability to accurately identify intrusion with fewer false positives and false negatives. This kind of implementation is always criticised for not being able to identify novel or new attack types. Anomaly-based Intrusion Detection Systems can identify novel or new intrusions but fall short of being able to accurately identify intrusion resulting in false positives and false negatives.
There are several techniques used to implement anomaly Based Intrusion Detection Systems. These techniques are Statistical Based IDS, Knowledge-Based IDS and Machine Learning IDS.
Statistical Based Intrusion Detection System builds a distribution model for normal traffic and flag low-probability events as an intrusion(Khraisat *et al.*, 2019). This kind of anomaly IDS is simple to implement and can detect intrusion in real-time. The models of the Statistical Intrusion Detection System are Univariant, Multivariant and Time Series (Ye et.al, 2002). The univariant Statistical model measures one

variable at a time (Ye et.al, 2002). Multivariant Statistical IDS controls several variables at the same time (Camacho *et al.*, 2016).

According to Khraisat *et al.*(2019), the time series model is a series of observations made over a certain period and new observation is considered abnormal. The drawback to the times series model is the lack of accuracy and the need for one to have extensive knowledge of statistics.

The knowledge-Based Model is also known as the expert system. The technique requires creating a knowledge base which represents a normal traffic profile and actions which differ from this profile are considered as intrusion (Khraisat *et al.*, 2019). This knowledge base IDS is created by a human expert. The models used to develop such an intrusion Detection System include Finite State Machine, Description Language or Expert System (Walkinshaw, Taylor and Derrick, 2016). Because knowledge Based keep a profile of all normal behaviour false positives and false negatives are minimal. The weakness of this technique is the requirement meant for constant updates which makes it computationally expensive.

The last and the most popular technique for anomaly intrusion detection Systems is the Machine learning approach. Machine learning makes use of complex algorithms to extract needed data from large quantities of data. To achieve the need for effective IDS, many studies have explored the possibility of Machine Learning and Deep Learning techniques (Ahmad *et al.*, 2021). Both ML and DL belong to the field of Artificial Intelligence(AI). Even though machine learning is resilient to noisy data, robust and adaptive it is also faced with some drawbacks. According to Ayyagari *et al.* (2021), machine-learning approaches suffer from the limitations of manual feature engineering. They further argued that ML might be inefficient in handling large data. Machine learning by its nature is not able to handle multiclass classification tasks. Anomaly IDS build using machine learning are faced with the issue of false positives and false negatives.

These weaknesses of ML are however improved by deep learning. DL IDS can carry out feature selection automatically without manual intervention and hence improve the accuracy of prediction. Improved accuracy of DL-based IDS means fewer false positives and fewer false negatives. Examples of machine Learning Algorithms include for the design of IDS include Decision Tree (DT), Random Forest, K-nearest neighbour, K-mean, Support Vector Machine (SVM) and Artificial Neural Networks(ANN). Deep learning is also an ANN in which the number of hidden neurons has been deepening to increase its processing capacity. These techniques mentioned above have been used by several researchers to improve existing IDS. For instance, Ahmim, Derdour and Ferrag (2018) conducted a study based on the combining probability of Decision trees. Similarly, Batiha and Krömer (2020) also carried a research on the design and analysis of efficient Neural Network Intrusion Detection for wireless sensor networks. To increase the performance of these single machine learning techniques, a hybrid intrusion detection system has been introduced. However, the few numbers of hybrid intrusion system reviews suggest the area has not been explored enough (Maseno, Xing and Wang, 2022).

This study, therefore, seeks to carry out a systematic review of hybrid intrusion detection Systems. To the best of our knowledge, only one systematic review of Hybrid Intrusion Detection systems exists. This research when conducted, will expose both experienced and young researchers to techniques that need to be implemented to improve on the existing intrusion detection system.

Contributions

i. Provides extensive details on the types of the intrusion detection system
ii. This study has provided sufficient information on studies that have applied feature selection in their study for easy reference
iii. Enough information has been provided on studies that have handled imbalanced datasets in their work for easy reference
iv. Provide recommendations for increasing the detection rate and lowering the false positives associated with anomaly intrusion detection system

The rest of the work is divided into 4 main sections. Section 2 takes a review of related works, and Section 3 represents the methodology used to carry out the review. Section 4 is where the selected studies are

analyzed to provide results for discussion. Finally, section 5 takes a look at the conclusion and recommendations for further study.

2.0 RELATED WORKS

This Section examines previous studies related to a review of hybrid intrusion detection systems. This section will clearly state the difference between what has been done by other researchers and what this review seeks to do. Several studies have been conducted on a systematic review of intrusion detection systems and which is different from HIDS systematic review. For instance, Garg and Maheshwari(2016) conducted a review of the hybrid intrusion detection system. Their study was to review misuse and anomaly-based intrusion system. This study is different from their study because this takes into account not only anomaly and misuse intrusion detection system but also consider HIDS consisting of the use of more than one machine learning technique in a single study. This study, therefore, is broader in scope as compared to their study. Öney and Peker (2019) presented a review of intrusion detection involving Artificial Neural Networks. Here again, they focused on only artificial neural networks which is narrow in scope as compared to this study which considers all other machine learning languages as well. One major study that has been conducted on the Systematic Review of HIDS is the study by (Maseno, Wang and Xing, 2022). The objectives of their study focus on the weakness of algorithms used in HIDS, The metrics of evaluation and the dataset used to evaluate such models. Similarly this study span from 2012 to 2023 but differs from their study in

1. The number of studies selected for this study is 146 as compared to the previous study that used 111.
2. The second point is that the objectives of their study are different from the objectives of this study as stated below

a) To determine the distribution of studies by a publisher from 2012 to 2023
b) To identify studies that have applied feature selection in their models
c) To determine the specific feature selection technique applied.
d) To identify studies that have handled imbalanced dataset
e) To determine the specific technique applied to handle imbalanced data

3.0 METHODOLOGY

This study adopted the approach of (Kitchenham and Charters, 2007; Brereton et al., 2007 cited in Aldhaheri *et al.*, 2020) in which the Systematic literature Review is divided into planning, conducting and Reporting.

i. Planning the Review consist of three main steps:
    1. Identification of the need for the Systematic literature review
    2. Define the research questions
    3. Develop the research protocol
ii. Conducting the Review also consist of three-step
    1. Selecting the studies
    2. Define and apply quality assessment
    3. Extracting and synthesizing the selected data
iii. Reporting the review consist of three main steps
    1. Dissemination strategy specification
    2. Report formatting
    3. Report Evaluation.

3.1 PLANNING THE REVIEW

In planning the review, one needs to look at the need for the Systematic Literature Review (SLR), the research questions to be addressed in the study and the definition of the protocols for the study.

3.2 IDENTIFICATION OF THE NEED OF THE SLR

A review of the literature reveals that there is only one work that has been done on a systematic review of hybrid Intrusion Detection Systems. Even though their study exists the objectives of this study are different from theirs. This study intends to find out studies that apply feature selection and dataset balancing techniques in their proposed models. Their study on the other hand concentrate on trends in hybrid intrusion detection systems and dataset used for those study and the machine learning algorithms. Since feature selection and handling of imbalanced dataset form part of designing an intrusion detection system, it is important to investigate the use of these key techniques since the use of these techniques will have an impact on the results. Successful completion of this study will inform new and established researchers in the field of intrusion detection systems which dataset balancing technique is likely to give a better result and which feature selection technique will also make their model perform better. The studies that are discussed in this study span from 2012 to 2022. In all 142 studies have been selected for this review.

The objectives of this study are:

1. To determine the distribution of studies by a publisher from 2012 to 2023
2. To identify studies that have applied feature selection in their models
3. To determine the specific feature selection technique applied in Step 2
4. To identify studies that have handled imbalanced dataset
5. To determine the specific technique applied to handle imbalanced data in Step 4

3.3 RESEARCH QUESTIONS

The research questions addressed in this study include:
RQ1: What is the distribution of studies by a publisher from 2012 to 2023?
RQ2: How many studies have applied feature selection in their study?
RQ3: What are the feature selection techniques applied in these studies?
RQ4: How many studies have handled imbalanced datasets in their model?
RQ5: What are the exact techniques applied to handle an imbalanced dataset?

3.4 CONDUCTING THE REVIEW

Conducting the review starts with the selection of the studies, followed by quality assessment and finally the extraction and synthesizing of the selected data.

3.5 SEARCH PROCESS

To obtain relevant research papers for this study, the following search string was inserted into google scholar, IEEE database, Wiley database, Sage database, Science Direct, Springer, Emerald ACM and MDPI

1. Hybrid Intrusion detection review
2. Hybrid Anomaly detection review
3. Hybrid Intrusion Detection Survey
4. Hybrid Anomaly Intrusion Survey

This search showed some articles. Those articles have been used in the introduction part of the work to explain the concepts of intrusion detection systems. However, when the search string changed from review to systematic review as stated below there was only one systematic review on HIDS by(Maseno, Wang and Xing, 2022).

1. Hybrid Intrusion detection Systematic review

2. Hybrid Anomaly detection Systematic review
3. Hybrid Intrusion Detection Systematic Survey
4. Hybrid Anomaly Intrusion Systematic Survey

A thorough search was therefore carried out using the following strings to obtain the required data for the study

1. Hybrid Intrusion Detection System
2. Hybrid Anomaly Intrusion Detection System

The search used the above search input and the year was restricted between the period 2012 to 2023. A total of 300 articles consisting of reviews, conferences and research articles were retrieved. Inclusion and exclusion criteria were applied to reduce the number of articles to 146. The inclusion criteria and exclusion was based on the following (i) only article from scientific journals and conferences and excluded those without Journal or conference. (ii) Article that does not make use of publically available dataset in their study was excluded. (iii) Include articles published in English Language and exclude articles published in other languages. (iv) hybrid techniques using machine learning or deep learning and signature and anomaly were included. Publishers from Elsevier, Springer, Wiley, IEEE, Emerald, Sage, Hindawi, ACM and MDPI were included but other publishers were excluded.

3.6 QUALITY ASSESSMENT

QAR is applied to select studies. The quality assurance for this study is based on the following questions**.**
QAR1: Are they clearly stated research objective?
QAR2 : Are they measures to address data imbalance?
QAR3 : Is the experimental setup appropriate for the study?
QAR4 : Are findings presented in line with test results?
QAR5 : Has the author discuss issues of perfomance of the proposed method?
The criteria for scoring quality assurance questions are as follows
QAR1: yes(Y), the author has clearly stated objective(s) = 1 , Partial(P) the author has partialy stated objective(s) = 0.5 and no(N) the author has no objective(s) = 0.
QAR2: yes(Y) the author(s) addressed the issue of data inbalance = 1, no(N) the author did not address the issue data inbalance = 0.
QAR3: yes(Y) the author included approapriate experimental setup = 1,partial(P) the author included a partial experimental setup = 0.5 and (no) no experimental setup was included.
QAR4: yes(Y) the findings presented is inline with the text results = 1,no(N) the findings preseted is not inline with the test results = 0.
QAR5: yes(Y) the author discussed performance issues of the proposed System = 1, no(N) the author did not discuss performance issue with the proposed System.
Papers that obtain a total score of 3.5 out of 5 is selected. In all 146 papers were selected based based on the quality assurance measure.
Data Extraction
This step is when the data selected is used to answer the research questions. The Table 1 below shows the data gathered for each study based on our inclusion and exclusion criteria.

Table 1: Selected articles of Hybrid Intrussion Detection Systems

S/N	Title	Publisher	Reference
R1	Anomaly Based Intrusion Detection Using Hybrid Learning Approach of Combining k-medoids Clustering and Naïve Bayes Classification	IEEE	(Chitrakar and Chuanhe, 2012a)
R2	Gravitational search algorithm optimized neural misuse detector	Springer	(Sheikhan and Sharifi, 2012)

	with selected features by fuzzy grids–based association rules mining		
R3	Cascaded classifier approach based on Adaboost to increase detection rate of rare network attack categories	IEEE	(Natesan, Rajesh 2012)
R4	Anomaly Detection using Support Vector Machine Classification with k-Medoids Clustering	IEEE	(Chitrakar and Chuanhe, 2012b)
R5	A Hybrid System for Reducing the False Alarm Rate of Anomaly Intrusion Detection System	IEEE	(Om, 2012)
R6	Mining network data for intrusion detection through combining SVM with ant colony Wenying	Elservier	(Feng *et al.*, 2013)
R7	A hybrid method based on Genetic Algorithm, Self-Organised Feature Map, and Support Vector Machine for better Network Anomaly Detection	IEEE	(Vidyapeetham, 2013)
R8	Multi-layer hybrid machine learning techniques for anomalies detection and classification approach	IEEE	(Sayed *et al.*, 2013)
R9	Flow-based anomaly detection in high-speed links using modified GSA- optimized neural network	Springer	(Sheikhan and Jadidi, 2014)
R10	A novel hybrid intrusion detection method integrating anomaly detection with misuse detection	Elservier	(Kim, Lee and Kim, 2014)
R11	Distributed Denial of Service Detection Using Hybrid Machine Learning Technique	IEEE	(Barati *et al.*, 2014)
R12	Adaptive Fuzzy Neural Network Model for Intrusion Detection	IEEE	(Kumar and Mohan, 2014)
R13	A New Intrusion Detection Approach using PSO based Multiple Criteria Linear Programming Seyed	Elservier	(Mojtaba *et al.*, 2015)
R14	An Integration of K-Means Clustering and Naïve Bayes Classifier for Intrusion Detection	IEEE	(Varuna, 2015)
R15	Feature Selection Based Hybrid Anomaly Intrusion Detection System Using K Means and RBF Kernel Function	Elservier	(Ravale, Marathe and Padiya, 2015)
R16	A hybrid method consisting of GA and SVM for intrusion detection system	Springer	(Rahmani *et al.*, 2015)
R17	Hybrid Evolutionary Algorithms for Data Classification in Intrusion Detection Systems Abdel-Rahman	IEEE	(Hedar *et al.*, 2015)

R18	A Global Hybrid Intrusion Detection System for Wireless Sensor Networks	Elservier	(Maleh *et al.*, 2015)
R19	An effective combining classifier approach using tree algorithms for network intrusion detection	Springer	(Kevric, Jukic and Subasi, 2016)
R20	A Hybrid Approach to Reducing the False Positive Rate in Unsupervised Machine Learning Intrusion Detection	IEEE	(Landress, 2016)
R21	Distributed-Intrusion Detection System using combination of Ant Colony Optimization (ACO) and Support Vector Machine (SVM)	IEEE	(Wankhade, 2016)
R22	Anomaly Detection Based on Profile Signature in Network Using Machine Learning Technique	IEEE	(Atefi, 2016)
R23	Improving K-Means Clustering Using Discretization Technique in Network Intrusion Detection Syst	IEEE	(Network, 2016)
R24	A hybrid Deep Learning Strategy for an Anomaly Based N-IDS	IEEE	(Mendjeli, 2017)
R25	An Analysis of Random Forest Algorithm Based Network Intrusion Detection System	IEEE	(Aung, 2017)
R26	ML-IDS: A Machine Learning Approach to Detect Wormhole Attacks in Internet of Things	IEEE	(Shukla, 2017)
R27	Intrusion detection model using fusion of chi-square feature selection and multi class SVM	IEEE	(Thaseen and Kumar, 2017)
R28	A semi-supervised Intrusion Detection System using active learning SVM and fuzzy c-means clustering	IEEE	(Kumari, 2017)
R29	A novel hybrid anomaly based intrusion detection method	IEEE	(Qazanfari, 2017)
R30	An effective network attack detection method based on kernel PCA and LSTM- RNN	IEEE	(Meng *et al.*, 2017)
R31	A hybrid technique using binary particle swarm optimization and decision tree pruning for network intrusion detection	Springer	(Malik and Khan, 2017)
R32	An Efficient Fuzzy-Based Hybrid System to Cloud Intrusion Detection	Springer	(Raja and Ramaiah, 2017)

R33	Enhancing effectiveness of intrusion detection systems: A hybrid approach	IEEE	(Subba, Biswas and Karmakar, 2017)
R34	Anomaly Detection Approach using Hybrid Algorithm of Data Mining Technique	IEEE	(Gadal and Mokhtar, 2017)
R35	A Framework of Novel Feature Set Extraction based Intrusion Detection System for Internet of Things using Hybrid Machine Learning Algorithms	IEEE	(Nivaashini and Thangaraj, 2018)
R36	Intrusion Detection Using Multilayer Perceptron and Neural Networks with Long Short-Term Memory	IEEE	(Borisenko *et al.*, 2018)
R37	Intrusion detection in network systems through hybrid supervised and unsupervised mining process - a detailed case study on the ISCX benchmark dataset -	Elservier	(Soheily-Khah, Marteau and Bechet, 2018)
R38	Intrusion Detection System by Using Hybrid Algorithm of Data Mining Technique	IEEE	(Foroushani and Li, 2018)
R39	An Efficient IDS Using Hybrid Magnetic Swarm Optimization in WANETs	IEEE	(Sadiq *et al.*, 2018)
R40	Anomaly-Based Network Intrusion Detection System through Feature Selection and Hybrid Machine Learning Technique	IEEE	(Pattawaro, 2018)
R41	Feature Reduction and Selection Based Optimization for Hybrid Intrusion Detection System Using PGO followed by SVM	IEEE	(Sagar, Shrivastava and Gupta, 2018)
R42	Hybrid approach for intrusion detection system	IEEE	(Singh and Venkatesan, 2018)
R43	HIDCC: A hybrid intrusion detection approach in cloud computing	Willey	
R44	Hybrid Internal Anomaly Detection System for IoT: Reactive Nodes with Cross-Layer Operation	Willey	(Thanigaivelan, Virtanen and Isoaho, 2018)
R45	Hybrid Intrusion Detection System using K-means and K-Nearest Neighbors Algorithms	IEEE	(Aung, 2018a)
R46	Hybrid Intrusion Detection System using K-means and Random Tree Algorithms	IEEE	(Aung, 2018b)

R47	A hybrid Particle swarm optimization -Extreme Learning Machine approach for Intrusion Detection System	IEEE	(Ali *et al.*, 2018)
R48	A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection	Elservier	(Hajisalem and Babaie, 2018)
R49	RST-RF: A Hybrid Model based on Rough Set Theory and Random Forest for Network Intrusion Detection	ACM	(Jiang and Lv, no date)
R50	Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection	IEEE	(Taher, 2019)
R51	Hybrid Intrusion Detection System Using Machine Learning Techniques in Cloud Computing Environments	IEEE	(Tekeo, 2019)
R52	Evolving deep learning architectures for network intrusion detection using a double PSO	Elservier	(Elmasry, Akbulut and Zaim ,2019)
R53	The Hybrid Technique for DDoS Detection with Supervised Learning Algorithms	Elservier	(Hosseini and Azizi, 2019)
R54	Optimization of Network Intrusion Detection System Using Genetic Algorithm with Improved Feature Selection Technique	IEEE	(Matel, Sison and Medina, 2019)
R55	Hybrid optimization scheme for intrusion detection using considerable feature selection	Springer	(Karthikeyan, 2019)
R56	Using Machine Learning techniques to improve Intrusion Detection Accuracy	IEEE	(Zhang *et al.*, 2019)
R57	A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network	MDPI	(Khan and Karim, 2019)
R58	TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-based Intrusion Detection System	IEEE	(Tama, Comuzzi and Rhee, 2019)
R59	Hybrid Intrusion Detection System Using Machine Learning Techniques in Cloud Computing Environments	IEEE	(Aljamal *et al.*, 2019)
R60	HML-IDS: A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems	IEEE	(Khan, Pi and Khan, 2019)
R61	Efficient IDs for MANET Using Hybrid Firefly with a Genetic Algorithm	IEEE	(Shona and Kumar, 2019)

R62	A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifier	Springer	(Saleh, Talaat and Labib, 2019)
R63	A new approach for intrusion detection system based on training multilayer perceptron by using enhanced Bat algorithm	Springer	(Ghanem and Jantan, 2019)
R64	A Novel Intrusion Detector Based on Deep Learning Hybrid Methods	IEEE	(Shizhao and Tianbo, 2019)
R65	A Novel Multimodal-Sequential Approach Based on Multi-View Features for Network Intrusion Detection	IEEE	(He *et al.*, 2019)
R66	A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection	Springer	(Haghnegahdar and Wang, 2019)
R67	An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic	IEEE	(Zhang, 2019)
R68	A Hybrid Classifier Approach for Network Intrusion Detection	IEEE	(Arivardhini, Alamelu and Deepika, 2020)
R69	A Hierarchical Hybrid Intrusion Detection Approach in IoT Scenarios	IEEE	(Bovenzi *et al.*, 2020)
R70	A Hybrid Anomaly Classification with Deep Learning (DL) and Binary Algorithms (BA) as Optimizer in the Intrusion Detection System (IDS)	IEEE	(Atefi, 2020)
R71	A hybrid feature extraction network for intrusion detection based on global attention mechanism	IEEE	(Chen, 2020)
R72	A Hybrid Deep Learning Model for Malicious Behavior Detection	IEEE	(Xu *et al.*, 2020)
R73	Hybrid Intrusion Detection System Based on Deep Learning	IEEE	(Azawii and Lateef, 2020)
R74	Hybrid Machine Learning For Network Anomaly Intrusion Detection	IEEE	(Chkirbene *et al.*, 2020)
R75	Intrusion Detection System based on Hybrid Classifier and User Profile Enhancement Techniques	IEEE	(Pokharel, 2020)
R76	A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing Mahdi	Elservier	(Rabbani *et al.*, 2020)

R77	New Hybrid Method for Attack Detection Using Combination of Evolutionary Algorithms, SVM, and ANN	Elservier	(Hosseini, Mohammad and Zade, 2020)
R78	Fuzzy-Taylor-Elephant Herd Optimization inspired Deep Belief Network for DDoS Attack Detection and comparison with state-of-the-arts algorithms	Elsevier	(Velliangiri and Pandey, 2020)
R79	A Hybrid Intrusion Detection System Based on Decision Tree and Support Vector Machine	IEEE	(Kumari, 2020)
R80	An Efficient Intrusion Detection Model Based on Hybridization of Artificial Bee Colony and Dragonfly Algorithms for Training Multilayer Perceptrons	IEEE	(Ghanem *et al.*, 2020)
R81	Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine	IEEE	(Wang *et al.*, 2020)
R82	A Real-Time and Ubiquitous Network Attack Detection Based on Deep Belief Network and Support Vector Machine	IEEE	(Zhang *et al.*, 2020)
R83	Machine learning and data mining methods for hybrid IoT intrusion detection	IEEE	(Ghazi, 2020)
R84	Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN	IEEE	(Malik *et al.*, 2020)
R85	Improving Attack Detection Performance in NIDS Using GAN	IEEE	(Li, 2020)
R86	An effect of chaos grasshopper optimization algorithm for protection of network infrastructure	IEEE	(Dwivedi, Vardhan and Tripathi, 2020)
R87	Hybrid approach to intrusion detection in fog-based IoT environments	IEEE	(Souza *et al.*, 2020)
R88	Providing a Hybrid Approach for Detecting Malicious Traffic on the Computer Networks Using Convolutional Neural Networks	IEEE	(Pakanzad, 2020)
R89	An efficient XGBoost–DNN-based classification model for network intrusion detection system	Springer	(Devan and Khare, 2020)
R90	Detection of anomaly intrusion utilizing self-adaptive grasshopper optimization algorithm	Springer	(Shukla, 2020)

R91	RNN-VED for Reducing False Positive Alerts in Host-based Anomaly Detection Systems	IEEE	(Bouzar-benlabiod *et al.*, 2020)
R92	Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models	MDPI	(Polat and Polat, 2020)
R93	Cascaded hybrid intrusion detection model based on SOM and RBF neural networks	Willey	(Almiani *et al.*, 2020)
R94	Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks	Springer	(Kaur and Singh, 2020)
R95	Intrusion detection system using hybrid tissue growing algorithm for wireless sensor network	Springer	(Umarani and Kannan, 2020)
R96	A Hybrid Nested Genetic-Fuzzy Algorithm Framework for Intrusion Detection and Attacks	IEEE	(Elhefnawy, Abounaser and Badr, 2020)
R97	Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network	IEEE	(Jiang *et al.*, 2020)
R98	A Hybrid Intrusion Detection System for Smart Home Security Faisal	IEEE	(Alghayadh and Debnath, 2020)
R99	An efficient flow-based multi-level hybrid intrusion detection system for software-defined networks	Springer	(Latah and Toker, 2020)
R100	Hybrid Intrusion Detection System Based on the Stacking Ensemble of C5 Decision Tree Classifier and One Class Support Vector Machine	MPDI	(Khraisat *et al.*, 2020)
R101	Two-Stages Intrusion Detection System Based On Hybrid Methods	ACM	(Azzaoui, 2020)
R102	Improved Intrusion Detection Accuracy Based on Optimization Fast Learning Network Model	IEEE	(Ali and Aasi, no date)
R103	A Hybrid Approach of ANN-GWO Technique for Intrusion Detection	IEEE	(Sharma and Tyagi, 2021)
R104	A Hybrid Data-driven Model for Intrusion Detection in VANET A Hybrid Data-driven Model for Intrusion Detection in VANET Hind	Elsevier	(Bangui *et al.*, 2021)
R105	Hybrid Intrusion Detection System for Detecting New Attacks Using Machine Learning	IEEE	(Enigo, 2021)

R106	A Hybrid Machine Learning and Data Mining Based Approach to Network Intrusion Detection	IEEE	(Singhal *et al.*, 2021)
R107	A Novel Intrusion Detection Method Based on WOA Optimized Hybrid Kernel RVM 2021	IEEE	(Gao, Yue and Wu, 2021)
R108	A Novel Framework Design of Network Intrusion Detection Based on Machine Learning Techniques	Willey	(Zhang *et al.*, 2021)
R109	An Online Network Intrusion Detection Model Based on Improved Regularized Extreme Learning Machine	IEEE	(Tang and Li, 2021)
R110	A Multi-Layer Classification Approach for Intrusion Detection in IoT Networks Based on Deep Learning	MPDI	(Qaddoura *et al.*, 2021)
R111	Feature selection using cloud-based parallel genetic algorithm for intrusion detection data classification	Springer	(Kec, 2021)
R112	Serial and Parallel based Intrusion Detection System using Machine Learning	IEEE	(Das, 2021)
R113	Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection	Springer	(Prabhakaran and Kulandasamy, 2021)
114	An Enhanced Intrusion Detection System using Particle Swarm Features selection techniques	Elsevier	(Oluwaseun *et al.*, 2021)
R115	A hybrid machine learning model for intrusion detection in VANET	Springer	(Bangui, 2021)
R116	An Intrusion Detection System based on PSO-GWO Hybrid Optimized Support Vector Machine	IEEE	(Li, Zhang and Wang, 2021)
R117	A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning	IEEE	(Liu, Gu and Wang, 2021)
R118	An improved ensemble based intrusion detection technique using XGBoost	Willey	(Bhati *et al.*, 2021)
R119	A hybrid machine learning method for increasing the performance of network intrusion detection systems	Springer	(Megantara and Ahmad, 2021)
R120	An edge based hybrid intrusion detection framework for mobile edge computing	Springer	(Singh, Chatterjee and Satapathy, 2021)

R121	A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM	IEEE	(Wisanwanichthan and Thammawichai, 2021)
R122	SABADT: Hybrid Intrusion Detection Approach for Cyber Attacks Identification in WLAN	IEEE	(Pu *et al.*, 2021)
R123	Real-Time Network Intrusion Prevention System Based on Hybrid Machine Learning	IEEE	(Seo and Pak, 2021)
R124	HCRNNIDS:Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System	MPDI	(Khan, 2021)
R125	Building an efficient intrusion detection system using grasshopper optimization algorithm for anomaly detection	Springer	(Dwivedi, Vardhan and Tripathi, 2021)
R126	MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles	IEEE	(Yang, Moubayed and Shami, 2021)
R127	Hybrid Classification for High-Speed and High-Accuracy Network Intrusion Detection System	IEEE	(Kim and Pak, 2021)
R128	Intrusion Detection System Based on Hybrid Hierarchical Classifiers	Springer	(Mohd, Singh and Bhadauria, 2021)
R129	Network Intrusion Detection Using Hybrid Machine Learning Model	ACM	(Mazumder *et al.*, 2021)
R130	Design and Development of RNN-based Anomaly Detection Model for IoT Networks	IEEE	(Ullah, Mahmoud and Member, 2022)
R131	XGBoosted Misuse Detection in LAN-Internal Traffic Dataset	IEEE	(Zhang, no date)
R132	Deep Generative Learning Models for Cloud Intrusion Detection Systems	IEEE	(Vu *et al.*, 2022)
R133	Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework	IEEE	(Razib *et al.*, 2022)
R134	A Robust Adaptive Intrusion Detection System using Hybrid Deep Learning	IEEE	(Aravamudhan, 2022)
R135	An Efficient Network Intrusion Detection and Classification System	MDPI	(Ahmad *et al.*, 2022)
R136	Towards SDN-Enabled, Intelligent Intrusion Detection System for Internet of Things (IoT) Mohammed	IEEE	(Saleh *et al.*, 2022)

R137	Research on Intrusion Detection Based on Neural Network Optimized by Genetic Algorithm	IEEE	(Li *et al.*, 2022)
R138	Optimized Deep Autoencoder Model for Internet of Things Intruder Detection	IEEE	(Lahasan and Samma, 2022)
R139	An Intrusion Detection System for Zero-Day Attacks to Reduce False Positive Rates	IEEE	(Pitre, 2022)
R140	A hybrid approach Towards Efficient and Accurate Intrusion Detection for In-Vehicle Network	IEEE	(Zhang *et al.*, 2022)
R141	Machine Learning Based Intrusion Detection Systems Using HGWCSO And ETSVM Techniques	IEEE	(Srikrishnan, Raaza and Gopalakrishnan, 2022)
R142	Feed-Forward Intrusion Detection and Classification on A Smart Grid Network	IEEE	(Aribisala, Khan and Husari,2022)
R143	A hybrid CNN+ LSTM-based Intrusion detection system for Industrial IoT networks	ELSEVIER	(Can and Albayrak, 2023)
R144	Hybrid intrusion detection based on improved Harris Hawk optimization algorithm	Taylor and Francis	(Zhou, Zhang and Liang, 2023)
R145	Composition of hybrid deep learning model and feature optimization for intrusion detection	MDPI	(Henry *et al.*, 2023)
R146	Optimization of Intrusion Detection Using likely point PSO and Enhanced LSTM-RNN hybrid technique in communication networks	IEEE	(Donkol *et al.*, 2023)

4.0 RESULTS AND DISCUSSION

RQ1: What is the distribution of studies by publisher from 2012 to 2023?

A count on the number of article by a publisher was conducted and the Figure 4 below shows the distribution of papers by such publishers. From Figure 4 , IEEE dominate as the publisher with the higest number of papers. A total of 93 papers were obtained from IEEE Xplore database representing 65 percent of the total studies selected for this work. The domination of IEEE could be due to researchers having full access to IEEE Xplore database.It also means that IEEE has given young and comming reseachers the chance to showcase their research skills through comferences. The other publishers that shared the rest of the 35 percent include:

1) Springer with 22 papers representing 15 percentage of the total papers selected
2) Elservier with 13 papers representing 9 percent of the total papers selected.
3) MDPI follows with 6 papers representing 4 percent of the total number of paper selected
4) Willey was fifth with a total of 5 papers representing 3.5 percent
5) ACM was the least with only 3 paper representing 2.1percent

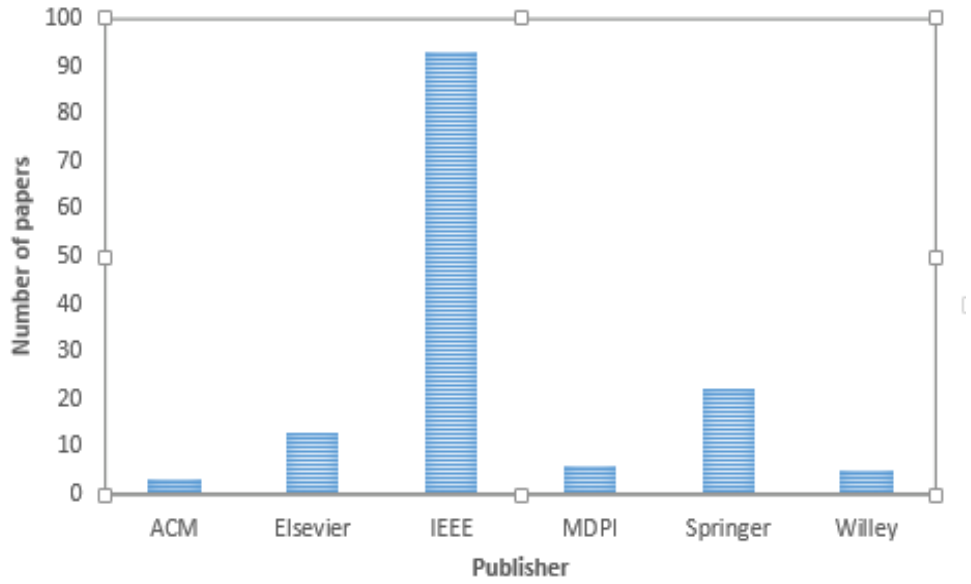

Figure 4: Publisher vr the number of papers

RQ2: How many studies have applied feature selection in their study?

Ahmad *et al.* (2022) argued that feature selection involve the reduction of computational cost by removing features that have no effect on target variable.

Many researchers have agreed that feature selection which form a major part in any classification problem is essential to obtaining accurate results. For instance (Kec, 2021) stated that in order to build a complex model on top of dataset,feature selection is an important step in machine learning and statistics. Feature selection is critical in improving machine learning agorithms and the building of HID models (Gadal and Mokhtar, 2017). In view of the impotance of feature selection, this study tried to identify HIDS studies that have applied feature selection in their research. Out of the 146 studies selected only 57 papers representing 39% applied feature selection in their study while 89 papers representing 61% did not carry out feature selection. pThis means that those research that did not apply feature selection can be look at to improve on the performance of those studies. The results of the study is represented in the Figure 5 below.

A careful analysis of the reviewed papers reveals that supervised feature selection techniques have lower accuracy as compared to unsupervised feature selection techniques. For instance autoencoder which is a unsupervised dimensionality technque performs better than Principal Component Analysis(PCA), a supervised technique which is widely accepted by industry even under contaminated environment(Madani and Vlajic, 2018). This means that to achive better results in terms of accuracy and low false alarm rate, deep learning feature selection technques should be implemented.

Apart from deep learning another technique that have gain popularity is the use of hybrid feature selection technique which consist of the use of more that one feature selection technique to select efficient feature to improve on the classification accuracy.This technique was implement by Ahmad *et al.*(2022) when the suggested p-value and correlation measure as a means to build an Efficient network intrusion detection system. Experimental results of their study suggested an improved performance as compared to using a single technique. This study and similar studies by others point to the fact that using hybrid feature selection technique can improve on IDS model performance.

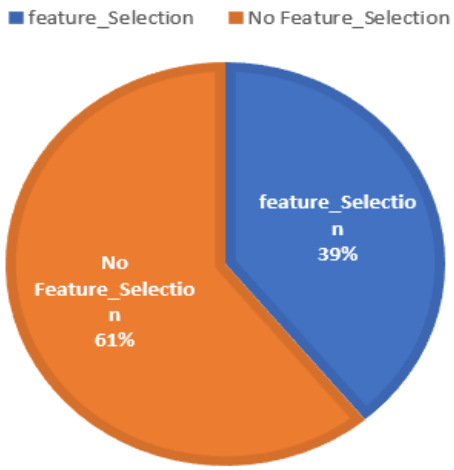

Figure 5: HIDS that have applied feature selection in their model

RQ3: What are the feature selection techniques applied in these studies?
There are several feature selection techniques that have been applied by various researchers in the selected studies. This section take a look at those techniques.

Table 2: Studies and feature selection techniques applied

Technique	Studies applying it	Number of studies
Fuzzy Grid-Based Association Rule	R2	1
Entropy Based Feature Selection	R5,R29, R78	3
Genetic Algorithm(GA)	R7,R11,R59,R61	4
Principal Component Analysis	R8, R30,R35,R51,R60,R121,R141	8
Genetic Algorithm-Support Vector Machine	R16	1
Decision Tree(J48)	R20	1
Chi-Square	R27	1
Infomation Gain	R34,R36,R38, R39,R43,R85,R120,R129	8
Attribute Average	R40	1
Plants growth optimization	R41	1
Correlation Based feature selection	R48,R35,R145	4
Rough Set Theory(RST) and Correlation Based Feature Selection	R49	1
Support Vector Machine	R50	1
Meta nodes	R53	1
Naive Base	R62	1
Crow Spam Optimization	R73	1
Random Forest	R74	1
GA-SVM	R75	1
MGA-Support Vector Machine	R77	1
Autoencoder	R81,R116	2
Emsemble feature selection	R86,R96,R138,R125	4
XGBOOST Score	R89	1
Relief Agorithm	R92	1

Features important decision	R119	1
FSAP	R122	1
K-mean Sampling	R126	1
P-value and correlation measure	R135	1
Grey Wolf Optimization Search Optimization and Enhanced translative support vector machine	R142	1
particle Swam Optimization	R52,R31,R146	2
Improved harris Hawk optimization algorithm	R144	1

From the Table2 above, about 31 different feature selection methods were identified. The feature selection methods that most researchers used in the selected studies are Information Gain and Principal Component Analysis (PCA). These two methods have been used by 15 studies representing 30% of all the feature selection methods that have been identified in this study. The rest are Emsembled feature selection, correlation based feature selection and Genetic Algorithm, 4 studies each, Entropy based feature selection and particle swam optimization 3 studies each and autoencoder recording 2 studies. The rest of the method has been used just once.

RQ4: How many studies have handled imbalanced dataset in their model?

Khan, Pi and Khan (2019) investigated the effect of using dataset balancing technique in the design of Intrusion Detection System. The outcome of their study revealed a significant increase in the performance of their model. For instance, before applying dataset balancing technique the classification accuracy was 91% but after applying the dataset balancing technique the acuracy increased to 97%, precision also increased from 92% to 98% and other metrics such as f-score and recall all saw an increase after balancing the dataset. Similary,Kim and Pak(2021) presnted a study on Intrusion detection system that compared Random forest classifier and Random forest with Smote which is a dataset balancing technique. The results show an impresive performance for the Random forest +Smote. The outcome of these studies and many other studies makes it imperative to analyse hybrid Intrusion detection systems that applies dataset balancing technques in their study and those that have not. This study will create the awareness for season researchers and up and coming ones in the field of IDS specifically HIDS to incoperate this important technique in their studies to improve the performance of existing HIDS.

Out of the 142 studies reviewed 22 studies applied databalancing technique that represent 15% of the total studies. This clearly shows that few researchers have taken the issue of imbalance dataset serously. This results means that existing studies without this dataset balancing technique can be reconducted with an appropriate dataset balancing technque for improved perfomance. The pie chart below shows the distribution of studies that have used dataset balancing technique and those who have not.

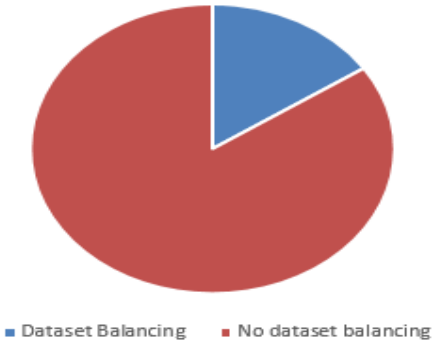

Figure 6: Studies that have applied dataset balancing technique and those who have not

RQ5: What are the exact techniques applied to handle imbalance dataset?
Several methods exist for handling imbalance dataset. This section will list those techniques and the studies associated with them.

Table 3: Studies and data imbalance handing techniques

Studies	Dataset Balancing Technique Applied
R2	Cascading method
R25,R35,R104,R115	Random Forest
R49,R121,R124,	Down Sampling
R60,R66,R85,R94,R110,R126,R127,R137	SMOTE
R67	SMOTE +Edited Nearest Neighbor
R97	SMOTE& One side-selection
R117	ADASYN
R130	Borderline SMOTE
R131	SMOTE, RF, Under Sampling
R98	Down and up Sampling

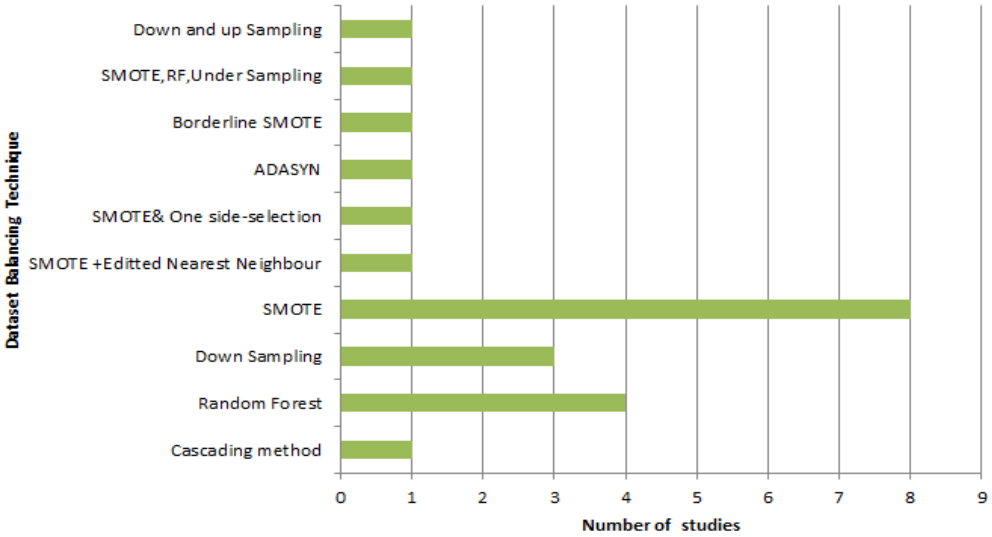

Figure 6: Number of studies against dataset balancing techniques

From the Figure 6 the study identified ten(10) different data balancing techniques that have been applied by different researchers. Out of these ten techniques SMOTE have been used by eight(8) different authors to handle imbalance dataset. This makes SMOTE the most used dataset balancing technique in our selected studies. Apart from that, few researchers have also combined SMOTE with other techniques to increase the performance of the classical SMOTE. These studies include R67, R97, R130 and R131. After SMOTE

the most used technique is Random Forest with 4 different authors applying it in our selected studies. Down Sampling has also been used three times to handle imbalance dataset. The rest of the techniques have been used once.

5.0 CONCLUTIONS AND RECOMMENDATIONS

The increasing interest of cyber security security expert on the use of hybrid intrusion detection system as depicted by Table 1 is an indication that more effort need to be put in place to make them more efficient. The efficiency can only be improved if the weakness of existing methods are are brought to the fore to inform experience and novice researchers to analysze and find innovative solutions to address the weakness. This study therefore perfectly addresses this need. The findings from this paper reveals that cyber security research has shifted from using a single technique to the using of hybrid technique. Another technique which has proven to improve the performance which most researcher did not include in their study is feature selection. A critical analysis of the selected studies reveals most HIDS do not carry out feature selection properly at the data preprocessing stage. Imbalaance dataset also represents a major setupback to improving the perfomance of hybrid intrusion detecction system. Majority of our selected studies did not incoporated dataset balancing techniques in their study. This study there recommend the use of proper feature selection process, the use of dataset balancing tecnique to improve the perfomance of hybrid intruion detection system.

1. This study therefore recommend that the 60% of studies that did not incoporate feature selection can be reconducted for possible increase in performance
2. 75% of the studies selected did not apply dataset balancing technique in their work. Applying dataset balancing technique can help improve the performance of those studies.
3. Studies that used supervised technique as feature selection technique can be reconducted using deep learning or unsupvised feature selection techniques. Unsupervised technique can handle the high volumes of traffic arriving at a computer network and therefore can be implemented in the real word network environment.
4. The use of hybrid feature selection techniques should be implemented for improved IDS detection accuracy.

FUNDING: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

DECLARATION OF COMPETING INTEREST: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

DATA AND MATERIAL: Dataset available

REFERENCES:

1. Ahmad, I. *et al.* (2022) 'An Efficient Network Intrusion Detection and Classification System', pp. 1–15.

2. Ahmad, Z. *et al.* (2021) 'Network intrusion detection system: A systematic study of machine learning and deep learning approaches', *Transactions on Emerging Telecommunications Technologies*, 32(1), pp. 1–29. Available at: https://doi.org/10.1002/ett.4150.

3. Ahmim, A., Derdour, M. and Ferrag, M.A. (2018) 'An intrusion detection system based on combining probability predictions of a tree of classifiers', *International Journal of Communication Systems*, 31(9), pp. 1–17. Available at: https://doi.org/10.1002/dac.3547.

4. Alghayadh, F. and Debnath, D. (2020) 'A Hybrid Intrusion Detection System for Smart Home Security', *IEEE International Conference on Electro Information Technology*, 2020-July, pp. 319–323. Available at: https://doi.org/10.1109/EIT48999.2020.9208296.

5. Ali, M.H. *et al.* (2018) 'A hybrid Particle swarm optimization -Extreme Learning Machine approach for Intrusion Detection System', *2018 IEEE 16th Student Conference on Research and Development, SCOReD 2018*, pp. 1–4. Available at: https://doi.org/10.1109/SCORED.2018.8711287.

6. Ali, M.H. and Aasi, A. (no date) 'Improved Intrusion Detection Accuracy Based on Optimization Fast Learning Network Model'.

7. Aljamal, I. *et al.* (2019) 'Hybrid intrusion detection system using machine learning techniques in cloud computing environments', *Proceedings - 2019 IEEE/ACIS 17th International Conference on Software Engineering Research, Management and Application, SERA 2019*, pp. 84–89. Available at: https://doi.org/10.1109/SERA.2019.8886794.

8. Almiani, M. *et al.* (2020) 'Cascaded hybrid intrusion detection model based on SOM and RBF neural networks', *Concurrency and Computation: Practice and Experience*, 32(21), pp. 1–14. Available at: https://doi.org/10.1002/cpe.5233.

9. Anderson, J.P. (1980) 'Computer security threat monitoring and surveillance', *Technical Report James P Anderson Co Fort Washington Pa*, p. 56. Available at: https://doi.org/citeulike-article-id:592588.

10. Aravamudhan, P. (2022) 'using Hybrid Deep Learning'.

11. Atefi, K. (2016) 'Anomaly Detection Based on Profile Signature in Network Using Machine Learning Technique', pp. 71–76.

12. Atefi, K. (2020) 'A Hybrid Anomaly Classification with Deep Learning (DL) and Binary Algorithms (BA) as Optimizer in the Intrusion Detection System (IDS)', (Cspa), pp. 28–29.

13. Aung, Y.Y. (2017) 'An Analysis of Random Forest Algorithm Based Network Intrusion Detection System', pp. 127–132.

14. Aung, Y.Y. (2018a) 'Hybrid Intrusion Detection System using K-means and K-Nearest Neighbors Algorithms', *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, pp. 34–38.

15. Aung, Y.Y. (2018b) 'Hybrid Intrusion Detection System using K-means and Random Tree Algorithms', *2018 19th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, pp. 218–223.

16. Ayyagari, M.R. *et al.* (2021) 'Intrusion detection techniques in network environment: a systematic review', *Wireless Networks*, 27(2), pp. 1269–1285. Available at: https://doi.org/10.1007/s11276-020-02529-3.

17. Azawii, A. and Lateef, A. (2020) 'Hybrid Intrusion Detection System Based on Deep Learning'.

18. Azzaoui, H. (no date) 'Two-Stages Intrusion Detection System Based On Hybrid Methods'.

19. Bangui, H. (2021) 'A hybrid machine learning model for intrusion detection in VANET', *Computing* [Preprint]. Available at: https://doi.org/10.1007/s00607-021-01001-0.

20. Bangui, H. *et al.* (2021) 'ScienceDirect A Hybrid Hybrid Data-driven Data-driven Model Model for for Intrusion Intrusion Detection Detection in in VANET', *Procedia Computer Science*, 184, pp. 516–523. Available at: https://doi.org/10.1016/j.procs.2021.03.065.

21. Barati, M. *et al.* (2014) 'Distributed Denial of Service Detection Using Hybrid Machine Learning Technique', pp. 268–273.

22. Batiha, T. and Krömer, P. (2020) 'Design and analysis of efficient neural intrusion detection for wireless sensor networks', *Concurrency Computation* , (June), pp. 1–12. Available at: https://doi.org/10.1002/cpe.6152.

23. Bhati, B.S. *et al.* (2021) 'An improved ensemble based intrusion detection technique using XGBoost', *Transactions on Emerging Telecommunications Technologies*, 32(6), pp. 1–15. Available at: https://doi.org/10.1002/ett.4076.

24. Borisenko, B.B. *et al.* (2018) 'Intrusion Detection Using Multilayer Perceptron and Neural Networks with Long Short-Term Memory'.

25. Bouzar-benlabiod, L. *et al.* (2020) 'RNN-VED for Reducing False Positive Alerts in Host-based Anomaly Detection Systems', pp. 17–24. Available at: https://doi.org/10.1109/IRI49571.2020.00011.

26. Bovenzi, G. *et al.* (2020) 'A Hierarchical Hybrid Intrusion Detection Approach in IoT Scenarios'.

27. Camacho, J. *et al.* (2016) 'PCA-based multivariate statistical network monitoring for anomaly detection', *Computers and Security*, 59, pp. 118–137. Available at: https://doi.org/10.1016/j.cose.2016.02.008.

28. Can, H. and Albayrak, Z. (2023) 'Engineering Science and Technology , an International Journal A hybrid CNN + LSTM-based intrusion detection system for industrial IoT networks', *Engineering Science and Technology, an International Journal*, 38, p. 101322. Available at: https://doi.org/10.1016/j.jestch.2022.101322.

29. 'Cascaded classifier approach based on Adaboost to increase detection rate of rare network attack categories' (2012), pp. 417–422.

30. Chen, W. (2020) 'A hybrid feature extraction network for intrusion detection based on global attention mechanism', pp. 481–485. Available at: https://doi.org/10.1109/CIBDA50819.2020.00114.

31. Chitrakar, R. and Chuanhe, H. (2012a) 'Anomaly based Intrusion Detection using Hybrid Learning Approach of combining k-Medoids Clustering and Naïve Bayes Classification', (September). Available at: https://doi.org/10.1109/WiCOM.2012.6478433.

32. Chitrakar, R. and Chuanhe, H. (2012b) 'Anomaly Detection using Support Vector Machine Classification with k-Medoids Clustering', pp. 1–5.

33. Chkirbene, Z. *et al.* (2020) 'Hybrid Machine Learning For Network Anomaly Intrusion Detection', pp. 163–170.

34. Computing, N., Sheikhan, M. and Jadidi, Z. (2014) 'Mansour Sheikhan & Zahra Jadidi', (November). Available at: https://doi.org/10.1007/s00521-012-1263-0.

35. Das, I. (2021) 'Serial and Parallel based Intrusion Detection System using Machine Learning', pp. 19–20.

36. Devan, P. and Khare, N. (2020) 'An efficient XGBoost – DNN-based classification model for network intrusion detection system', *Neural Computing and Applications*, 0123456789. Available at: https://doi.org/10.1007/s00521-020-04708-x.

37. Donkol, A.A.B.D.E. *et al.* (2023) 'Optimization of Intrusion Detection Using Likely Point PSO and Enhanced LSTM-RNN Hybrid Technique in Communication Networks', *IEEE Access*, 11(February), pp. 9469–9482. Available at: https://doi.org/10.1109/ACCESS.2023.3240109.

38. Dwivedi, S., Vardhan, M. and Tripathi, S. (2020) 'An effect of chaos grasshopper optimization algorithm for protection of network infrastructure', 176(August 2019). Available at: https://doi.org/10.1016/j.comnet.2020.107251.

39. Dwivedi, S., Vardhan, M. and Tripathi, S. (2021) 'Building an efficient intrusion detection system using grasshopper optimization algorithm for anomaly detection', *Cluster Computing*, 24(3), pp. 1881–1900. Available at: https://doi.org/10.1007/s10586-020-03229-5.

40. Elhefnawy, R., Abounaser, H. and Badr, A.M.R. (2020) 'A Hybrid Nested Genetic-Fuzzy Algorithm Framework for Intrusion Detection and Attacks', 8. Available at:

https://doi.org/10.1109/ACCESS.2020.2996226.

41. Enigo, F. (2021) 'New Attacks Using Machine Learning', (June 2020). Available at: https://doi.org/10.1109/ICCES48766.2020.9137888.

42. Feng, W. *et al.* (2013) 'Mining Network Data for Intrusion Detection through Combining SVM with Ant Colony', *Future Generation Computer Systems* [Preprint]. Available at: https://doi.org/10.1016/j.future.2013.06.027.

43. Foroushani, Z.A. and Li, Y. (2018) 'Intrusion detection system by using hybrid algorithm of data mining technique', *ACM International Conference Proceeding Series*, pp. 119–123. Available at: https://doi.org/10.1145/3185089.3185114.

44. Gadal, S.M.A.M. and Mokhtar, R.A. (2017) 'Anomaly detection approach using hybrid algorithm of data mining technique', *Proceedings - 2017 International Conference on Communication, Control, Computing and Electronics Engineering, ICCCCEE 2017* [Preprint]. Available at: https://doi.org/10.1109/ICCCCEE.2017.7867661.

45. Gao, P., Yue, M. and Wu, Z. (2021) 'A Novel Intrusion Detection Method Based on WOA Optimized Hybrid Kernel RVM', pp. 1063–1069.

46. Garg, A. and Maheshwari, P. (2016) 'A hybrid intrusion detection system: A review', *Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO 2016* [Preprint]. Available at: https://doi.org/10.1109/ISCO.2016.7726909.

47. Ghanem, W.A.H.M. *et al.* (2020) 'An Efficient Intrusion Detection Model Based on Hybridization of Artificial Bee Colony and Dragonfly Algorithms for Training Multilayer Perceptrons'. Available at: https://doi.org/10.1109/ACCESS.2020.3009533.

48. Ghanem, W.A.H.M. and Jantan, A. (2019) *A new approach for intrusion detection system based on training multilayer perceptron by using enhanced Bat algorithm*, *Neural Computing and Applications*. Springer London. Available at: https://doi.org/10.1007/s00521-019-04655-2.

49. Ghazi, A. El (2020) 'Machine learning and datamining methods for hybrid IoT intrusion detection'.

50. Haghnegahdar, L. and Wang, Y. (2019) 'A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection', *Neural Computing and Applications*, 0123456789. Available at: https://doi.org/10.1007/s00521-019-04453-w.

51. Hajisalem, V. and Babaie, S. (2018) 'A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection', *Computer Networks*, 136, pp. 37–50. Available at: https://doi.org/10.1016/j.comnet.2018.02.028.

52. He, Haitao *et al.* (2019) 'A Novel Multimodal-Sequential Approach Based on Multi-View Features for Network Intrusion Detection', *IEEE Access*, 7, pp. 183207–183221. Available at: https://doi.org/10.1109/ACCESS.2019.2959131.

53. Hedar, A.R. *et al.* (2015) 'Hybrid evolutionary algorithms for data classification in intrusion detection systems', *2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD 2015 - Proceedings* [Preprint]. Available at: https://doi.org/10.1109/SNPD.2015.7176208.

54. Henry, A. *et al.* (2023) 'Composition of Hybrid Deep Learning Model and Feature Optimization for Intrusion Detection System'.

55. Hosseini, S. and Azizi, M. (2019) 'The Hybrid Technique for DDoS Detection with Supervised Learning Algorithms', *Computer Networks* [Preprint]. Available at: https://doi.org/10.1016/j.comnet.2019.04.027.

56. Hosseini, S., Mohammad, B. and Zade, H. (2020) 'New Hybrid Method for Attack Detection Using

Combination of Evolutionary Algorithms , SVM , and ANN', *Computer Networks*, p. 107168. Available at: https://doi.org/10.1016/j.comnet.2020.107168.

57. Jiang, J. and Lv, B. (no date) 'RST-RF : A Hybrid Model based on Rough Set Theory and Random Forest for Network Intrusion Detection', pp. 77–81.

58. Jiang, K. *et al.* (2020) 'Network Intrusion Detection Combined Hybrid Sampling With Deep Hierarchical Network', *IEEE Access*, 8(3), pp. 32464–32476. Available at: https://doi.org/10.1109/ACCESS.2020.2973730.

59. Karthikeyan, S.V.P. (2019) 'Hybrid optimization scheme for intrusion detection using considerable feature selection', *Neural Computing and Applications*, 2. Available at: https://doi.org/10.1007/s00521-019-04477-2.

60. Kaur, S. and Singh, M. (2020) 'Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks', *Neural Computing and Applications*, 32(12), pp. 7859–7877. Available at: https://doi.org/10.1007/s00521-019-04187-9.

61. Kec, D. (2021) 'Feature selection using cloud-based parallel genetic algorithm for intrusion detection data classification', 5. Available at: https://doi.org/10.1007/s00521-021-05871-5.

62. Kevric, J., Jukic, S. and Subasi, A. (2016) 'An effective combining classifier approach using tree algorithms for network intrusion detection', *Neural Computing and Applications* [Preprint]. Available at: https://doi.org/10.1007/s00521-016-2418-1.

63. Khan, I.A., Pi, D. and Khan, Z.U. (2019) 'HML-IDS : A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems', *IEEE Access*, 7, pp. 89507–89521. Available at: https://doi.org/10.1109/ACCESS.2019.2925838.

64. Khan, M.A. (2021) 'HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system', *Processes*, 9(5). Available at: https://doi.org/10.3390/pr9050834.

65. Khan, M.A. and Karim, R. (2019) 'SS symmetry A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network'.

66. Khraisat, A. *et al.* (2019) 'Survey of intrusion detection systems: techniques, datasets and challenges', *Cybersecurity*, 2(1). Available at: https://doi.org/10.1186/s42400-019-0038-7.

67. Khraisat, A. *et al.* (2020) 'Hybrid intrusion detection system based on the stacking ensemble of C5 decision tree classifier and one class support vector machine', *Electronics (Switzerland)*, 9(1). Available at: https://doi.org/10.3390/electronics9010173.

68. Kim, G., Lee, S. and Kim, S. (2014) 'Expert Systems with Applications A novel hybrid intrusion detection method integrating anomaly detection with misuse detection', *Expert Systems With Applications*, 41(4), pp. 1690–1700. Available at: https://doi.org/10.1016/j.eswa.2013.08.066.

69. Kim, T. and Pak, W. (2021) 'Hybrid Classification for High-Speed and High-Accuracy Network Intrusion Detection System', *Hybrid intelligent systems for detecting network intrusions*, 9, pp. 83806–83817. Available at: https://doi.org/10.1109/ACCESS.2021.3087201.

70. Kumar, K.S.A. and Mohan, V.N. (2014) 'Adaptive Fuzzy Neural Network Model for intrusion detection', *Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014*, pp. 987–991. Available at: https://doi.org/10.1109/IC3I.2014.7019811.

71. Kumari, A. (2020) 'A Hybrid Intrusion Detection System Based on Decision Tree and Support Vector Machine', pp. 396–400.

72. Kumari, V. (2017) 'active learning SVM and fuzzy c-means clustering', pp. 481–485.

Lahasan, B. and Samma, H. (2022) 'Optimized Deep Autoencoder Model for Internet of Things Intruder Detection', 10.

73. Landress, A.D. (2016) 'A Hybrid Approach to Reducing the False Positive Rate in Unsupervised Machine Learning Intrusion Detection'.

74. Latah, M. and Toker, L. (2020) 'An efficient flow-based multi-level hybrid intrusion detection system for software-defined networks', *CCF Transactions on Networking*, 3(3–4), pp. 261–271. Available at: https://doi.org/10.1007/s42045-020-00040-z.

75. Li, D. (2020) 'Improving Attack Detection Performance in NIDS Using GAN', pp. 817–825. Available at: https://doi.org/10.1109/COMPSAC48688.2020.0-162.

76. Li, K., Zhang, Y. and Wang, S. (2021) 'An Intrusion Detection System based on PSO-GWO Hybrid Optimized Support Vector Machine', *Proceedings of the International Joint Conference on Neural Networks*, 2021-July. Available at: https://doi.org/10.1109/IJCNN52387.2021.9534325.

77. Li, Y. *et al.* (2022) 'Research on Intrusion Detection Based on Neural Network Optimized by Genetic Algorithm', en, pp. 8–11.

78. Liu, C., Gu, Z. and Wang, J. (2021) 'A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning', *IEEE Access*, 9, pp. 75729–75740. Available at: https://doi.org/10.1109/ACCESS.2021.3082147.

79. Madani, P. and Vlajic, N. (2018) 'Robustness of deep autoencoder in intrusion detection under adversarial contamination', *ACM International Conference Proceeding Series* [Preprint]. Available at: https://doi.org/10.1145/3190619.3190637.

80. Maleh, Y. *et al.* (2015) 'A global hybrid intrusion detection system for Wireless Sensor Networks', *Procedia Computer Science*, 52(1), pp. 1047–1052. Available at: https://doi.org/10.1016/j.procs.2015.05.108.

81. Malik, A.J. and Khan, F.A. (2017) 'A hybrid technique using binary particle swarm optimization and decision tree pruning for network intrusion detection', *Cluster Computing*, 21(1), pp. 667–680. Available at: https://doi.org/10.1007/s10586-017-0971-8.

82. Malik, J. *et al.* (2020) 'Hybrid Deep Learning : An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN', pp. 134695–134706. Available at: https://doi.org/10.1109/ACCESS.2020.3009849.

83. Maseno, E.M., Wang, Z. and Xing, H. (2022) 'A Systematic Review on Hybrid Intrusion Detection System', 2022.

84. Matel, E.C., Sison, A.M. and Medina, R.P. (2019) 'Optimization of Network Intrusion Detection System Using Genetic Algorithm with Improved Feature Selection Technique'.

85. Mazumder, M.R. *et al.* (no date) 'Network Intrusion Detection Using Hybrid Machine Learning Model'.

86. Megantara, A.A. and Ahmad, T. (2021) 'A hybrid machine learning method for increasing the performance of network intrusion detection systems', *Journal of Big Data*, 8(1). Available at: https://doi.org/10.1186/s40537-021-00531-w.

87. Mendjeli, C.A. (2017) 'A hybrid Deep Learning Strategy for an Anomaly Based N-IDS'.

88. Meng, F. *et al.* (2017) 'An effective network attack detection method based on kernel PCA and LSTM- RNN', *2017 International Conference on Computer Systems, Electronics and Control (ICCSEC)*, pp. 568–572.

89. Mohd, N., Singh, A. and Bhadauria, H.S. (2021) 'Intrusion Detection System Based on Hybrid Hierarchical Classifiers', *Wireless Personal Communications* [Preprint], (0123456789). Available at: https://doi.org/10.1007/s11277-021-08655-1.

90. Mojtaba, S. *et al.* (2015) 'A New Intrusion Detection Approach using PSO based Multiple Criteria

Linear Programming', *Procedia - Procedia Computer Science*, 55(Itqm), pp. 231–237. Available at: https://doi.org/10.1016/j.procs.2015.07.040.

91. Network, I.N. (2016) 'Improving K-Means CLUSTERING Clustering Using IMPROVING K-MEANS USING Discretization TECHNIQUE Technique In Network DISCRETIZATION Intrusion DETECTION Detection System INTRUSION', pp. 248–252.

92. Nivaashini, M. and Thangaraj, P. (2018) 'A Framework of Novel Feature Set Extraction based Intrusion Detection System for Internet of Things using Hybrid Machine Learning Algorithms', *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, pp. 44–49.

93. Oluwaseun, R. *et al.* (2021) 'ScienceDirect ScienceDirect ScienceDirect An Enhanced Intrusion Detection System using Particle Swarm Optimization Extraction Technique Science 10th International Young Feature An Enhanced Intrusion Detection System using Particle Swarm An Enhanced Intrus', *Procedia Computer Science*, 193, pp. 504–512. Available at: https://doi.org/10.1016/j.procs.2021.10.052.

94. Om, H. (2012) 'A Hybrid System for Reducing the False Alarm Rate of Anomaly Intrusion Detection System'.

95. Öney, M.U. and Peker, S. (2019) 'The Use of Artificial Neural Networks in Network Intrusion Detection: A Systematic Review', *2018 International Conference on Artificial Intelligence and Data Processing, IDAP 2018*, pp. 1–6. Available at: https://doi.org/10.1109/IDAP.2018.8620746.

96. Pakanzad, S.N. (2020) 'Providing a Hybrid Approach for Detecting Malicious Traffic on the Computer Networks Using Convolutional Neural Networks'.

97. Pattawaro, A. (2018) 'Anomaly-Based Network Intrusion Detection System through Feature Selection and Hybrid Machine Learning Technique', *2018 16th International Conference on ICT and Knowledge Engineering (ICT&KE)*, pp. 1–6. Available at: https://doi.org/10.1109/ICTKE.2018.8612331.

98. Pitre, P. (2022) 'An Intrusion Detection System for Zero-Day Attacks to Reduce False Positive Rates', pp. 1–6.

99. Pokharel, P. (2020) 'Intrusion Detection System based on Hybrid Classifier and User Profile Enhancement Techniques', pp. 137–144.

100. Polat, H. and Polat, O. (2020) 'Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models'.

101. Prabhakaran, V. and Kulandasamy, A. (2021) 'Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection', *Neural Computing and Applications*, 5. Available at: https://doi.org/10.1007/s00521-021-06085-5.

102. Pre-proof, J. (2019) 'Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic', *Computer Networks*, p. 107042. Available at: https://doi.org/10.1016/j.comnet.2019.107042.

103. Pu, G. *et al.* (2021) 'A Hybrid Unsupervised Clustering-Based Anomaly Detection Method', pp. 146–153.

104. Qaddoura, R. *et al.* (2021) 'A Multi-Layer Classification Approach for Intrusion Detection in IoT Networks Based on Deep Learning', pp. 1–21.

105. Qazanfari, K. (2017) 'A Novel Hybrid Anomaly Based Intrusion Detection Method', (November 2012). Available at: https://doi.org/10.1109/ISTEL.2012.6483122.

106. Rabbani, M. *et al.* (2020) 'A Hybrid Machine Learning Approach for Malicious Behaviour Detection and Recognition in Cloud Computing', *Journal of Network and Computer Applications*, p. 102507. Available at: https://doi.org/10.1016/j.jnca.2019.102507.

107. Rahmani, R. *et al.* (2015) 'A hybrid method consisting of GA and SVM for intrusion detection system A hybrid method consisting of GA and SVM for intrusion detection system', *Neural Computing and Applications* [Preprint], (August). Available at: https://doi.org/10.1007/s00521-015-1964-2.

108. Raja, S. and Ramaiah, S. (2017) 'An Efficient Fuzzy-Based Hybrid System to Cloud Intrusion Detection', *International Journal of Fuzzy Systems*, 19(1), pp. 62–77. Available at: https://doi.org/10.1007/s40815-016-0147-3.

109. Ravale, P.U., Marathe, P.N. and Padiya, P.P. (2015) 'Feature Selection Based Hybrid Anomaly Intrusion Detection System Using K Means and RBF Kernel Function', *Procedia - Procedia Computer Science*, 45, pp. 428–435. Available at: https://doi.org/10.1016/j.procs.2015.03.174.

110. Razib, M.A.L. *et al.* (2022) 'Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework', *IEEE Access*, 10, pp. 53015–53026. Available at: https://doi.org/10.1109/ACCESS.2022.3172304.

111. Sadiq, A.L.I.S. *et al.* (2018) 'An Efficient IDS Using Hybrid Magnetic Swarm Optimization in WANETs', *IEEE Access*, 6, pp. 29041–29053. Available at: https://doi.org/10.1109/ACCESS.2018.2835166.

112. Sagar, S., Shrivastava, A. and Gupta, C. (2018) 'Feature Reduction and Selection Based Optimization for Hybrid Intrusion Detection System Using PGO followed by SVM', *2018 International Conference on Advanced Computation and Telecommunication (ICACAT)*, pp. 1–7.

113. Saleh, A.I., Talaat, F.M. and Labib, L.M. (2019) 'A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifiers', *Artificial Intelligence Review*, 51(3), pp. 403–443. Available at: https://doi.org/10.1007/s10462-017-9567-1.

114. Saleh, M. *et al.* (2022) 'Towards SDN-Enabled , Intelligent Intrusion Detection System for Internet of Things (IoT)', 10.

115. Sayed, A. *et al.* (2013) 'Multi-layer hybrid machine learning techniques for anomalies detection and classification approach Vj and a P (at I vJ) - n + m 2013 13th International Conference on Hybrid Intelligent Systems (HIS)', pp. 215–220.

116. Seo, W. and Pak, W. (2021) 'Real-Time Network Intrusion Prevention System Based on Hybrid Machine Learning', 9. Available at: https://doi.org/10.1109/ACCESS.2021.3066620.

117. Sharma, A. and Tyagi, U. (2021) 'A Hybrid Approach of ANN-GWO Technique for Intrusion Detection', pp. 1–6.

118. Sheikhan, M. and Sharifi, M. (2012) 'Gravitational search algorithm – optimized neural misuse detector with selected features by fuzzy grids – based association rules mining'. Available at: https://doi.org/10.1007/s00521-012-1204-y.

119. Shizhao, W. and Tianbo, W. (2019) 'A Novel Intrusion Detector Based on Deep Learning Hybrid Methods', pp. 300–305. Available at: https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00062.

120. Shona, D. and Kumar, M.S. (2019) 'Efficient IDs for MANET Using Hybrid Firefly with a Genetic Algorithm', *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, (November), pp. 191–194. Available at: https://doi.org/10.1109/ICIRCA.2018.8597268.

121. Shukla, A.K. (2020) 'Detection of anomaly intrusion utilizing self-adaptive grasshopper optimization algorithm', *Neural Computing and Applications*, 7. Available at: https://doi.org/10.1007/s00521-020-05500-7.

122. Shukla, P. (2017) 'ML-IDS : A Machine Learning Approach to Detect Wormhole Attacks in Internet of Things', (September).

123. Singh, A., Chatterjee, K. and Satapathy, S.C. (2021) 'An edge based hybrid intrusion detection framework for mobile edge computing', *Complex & Intelligent Systems* [Preprint]. Available at: https://doi.org/10.1007/s40747-021-00498-4.

124. Singh, P. and Venkatesan, M. (2018) 'Hybrid Approach for Intrusion Detection System', *Proceedings of the 2018 International Conference on Current Trends towards Converging Technologies, ICCTCT 2018*, pp. 1–5. Available at: https://doi.org/10.1109/ICCTCT.2018.8551181.

125. Singhal, A. *et al.* (2021) 'A Hybrid Machine Learning and Data Mining Based Approach to Network Intrusion Detection', pp. 312–318.

126. Soheily-Khah, S., Marteau, P.F. and Bechet, N. (2018) 'Intrusion detection in network systems through hybrid supervised and unsupervised machine learning process: A case study on the iscx dataset', *Proceedings - 2018 1st International Conference on Data Intelligence and Security, ICDIS 2018*, pp. 219–226. Available at: https://doi.org/10.1109/ICDIS.2018.00043.

127. Souza, C.A. *et al.* (2020) 'Hybrid approach to intrusion detection in fog-based IoT environments', (July), pp. 1–6. Available at: https://doi.org/10.1016/j.comnet.2020.107417.

128. Srikrishnan, A., Raaza, A. and Gopalakrishnan, S. (no date) 'Machine Learning Based Intrusion Detection Systems Using HGWCSO And ETSVM Techniques'.

129. Subba, B., Biswas, S. and Karmakar, S. (2017) 'Enhancing effectiveness of intrusion detection systems: A hybrid approach', *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2016* [Preprint]. Available at: https://doi.org/10.1109/ANTS.2016.7947777.

130. Taher, K.A. (2019) 'Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection'.

131. Tama, B.A., Comuzzi, M. and Rhee, K.H. (2019) 'TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-Based Intrusion Detection System', *IEEE Access*, 7, pp. 94497–94507. Available at: https://doi.org/10.1109/ACCESS.2019.2928048.

132. Tang, Y. and Li, C. (2021) 'An Online Network Intrusion Detection Model Based on Improved Regularized Extreme Learning Machine', *IEEE Access*, PP, p. 1. Available at: https://doi.org/10.1109/ACCESS.2021.3093313.

133. Tekeo, A. (2019) 'Hybrid Intrusion Detection System Using Machine Learning Techniques in Cloud Computing Environments', pp. 84–89.

134. Thanigaivelan, N.K., Virtanen, S. and Isoaho, J. (2018) 'Hybrid Internal Anomaly Detection System for IoT : Reactive Nodes with Cross-Layer Operation', 2018.

135. Thaseen, S. and Kumar, A. (2017) 'Intrusion detection model using fusion of chi-square feature selection and multi class SVM', pp. 462–472.

136. Ullah, I., Mahmoud, Q.H. and Member, S. (2022) 'Design and Development of RNN-based Anomaly Detection Model for IoT Networks', *IEEE Access*, PP, p. 1. Available at: https://doi.org/10.1109/ACCESS.2022.3176317.

137. Umarani, C. and Kannan, S. (2020) 'Intrusion detection system using hybrid tissue growing algorithm for wireless sensor network', *Peer-to-Peer Networking and Applications*, 13(3), pp. 752–761. Available at: https://doi.org/10.1007/s12083-019-00781-9.

138.Varuna, S. (2015) 'An Integration of K-Means Clustering and Naïve Bayes Classifier for Intrusion Detection'.

139. Velliangiri, S. and Pandey, H.M. (2020) 'Jou rna lP', *Future Generation Computer Systems* [Preprint]. Available at: https://doi.org/10.1016/j.future.2020.03.049.

140. Vidyapeetham, A.V. (2013) 'A hybrid method based on Genetic Algorithm , Self-Organised Feature Map, and Support Vector Machine for better Network Anomaly Detection'.

141. Vu, L. *et al.* (2022) 'Deep Generative Learning Models for Cloud Intrusion Detection Systems', pp. 1–13.

142. Walkinshaw, N., Taylor, R. and Derrick, J. (2016) *Inferring extended finite state machine models from software executions*, *Empirical Software Engineering*. Available at: https://doi.org/10.1007/s10664-015-9367-7.

143. Wang, W. *et al.* (2020) 'Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine', pp. 1–14. Available at: https://doi.org/10.1109/TCC.2020.3001017.

144. Wankhade, A. (2016) 'Distributed-Intrusion Detection System using combination of Ant Colony Optimization (ACO) and Support Vector Machine (SVM)', pp. 0–5. Available at: https://doi.org/10.1109/ICMETE.2016.94.

145. Wisanwanichthan, T. and Thammawichai, M. (2021) 'SVMA Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and', *IEEE Access*, 9, pp. 138432–138450. Available at: https://doi.org/10.1109/ACCESS.2021.3118573.

146. Xu, A. *et al.* (2020) 'A Hybrid Deep Learning Model for Malicious Behavior Detection', pp. 55–59. Available at: https://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00021.

147. Yang, L., Moubayed, A. and Shami, A. (2021) 'MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles', *IEEE Internet of Things Journal*, XX(XX), pp. 1–17. Available at: https://doi.org/10.1109/JIOT.2021.3084796.

148. Zhang, C. *et al.* (2021) 'A Novel Framework Design of Network Intrusion Detection Based on Machine Learning Techniques', 2021.

149. Zhang, H. *et al.* (2019) 'Using Machine Learning techniques to improve Intrusion Detection Accuracy', pp. 308–310.

150. Zhang, H. *et al.* (2020) 'A Real-Time and Ubiquitous Network Attack Detection Based on Deep Belief Network and Support Vector Machine', 7(3), pp. 790–799.

151. Zhang, L. *et al.* (2022) 'A Hybrid Approach Toward Efficient and Accurate Intrusion Detection for In-Vehicle Networks', 10. Available at: https://doi.org/10.1109/ACCESS.2022.3145007.

152. Zhang, X. (2019) 'An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic', pp. 456–460.

153. Zhang, Z. (no date) 'XGBoosted Misuse Detection in LAN-Internal Traffic Dataset'.

154. Zhou, P., Zhang, H. and Liang, W. (2023) 'Research on hybrid intrusion detection based on improved Harris Hawk optimization algorithm'. Available at: https://doi.org/10.1080/09540091.2023.2195595.