applied sciences

MDPI

Review

Automated System-Level Malware Detection Using Machine Learning: A Comprehensive Review

Nana Kwame Gyamfi *, Nikolaj Goranin, Dainius Ceponis and Habil Antanas Čenys

Department of Information Systems, Vilnius Gedimino Technical University, 10223 Vilnius, Lithuania; nikolaj.goranin@vilniustech.lt (N.G.); dainius.ceponis@vilniustech.lt (D.C.); antanas.cenys@vilniustech.lt (H.A.Č.)
* Correspondence: nana-kwame.gyamfi@vilniustech.lt

Abstract: Malware poses a significant threat to computer systems and networks. This necessitates the development of effective detection mechanisms. Detection mechanisms dependent on signatures for attack detection perform poorly due to high false negatives. This limitation is attributed to the inability to detect zero-day attacks, polymorphic malware, increasing signature base, and detection speed. To achieve rapid detection, automated system-level malware detection using machine learning approaches, leveraging the power of artificial intelligence to identify and mitigate malware attacks, has emerged as a promising solution. This comprehensive review aims to provides a detailed analysis of the status quo in malware detection by exploring the fundamentals of machine learning techniques for malware detection. The review is largely based on the PRISMA approach for article search methods and selection from four databases. Keywords were identified together with inclusion and exclusion criteria. The review seeks feature extraction and selection methods that enhance the accuracy and precision of detection algorithms. Evaluation metrics and common datasets were used to assess the performance of the system-level malware detection techniques. A comparative analysis of different machine learning approaches, emphasizing their strengths, weaknesses, and performance in detecting system-level malware is presented together with the limitations of the detection techniques. The paper concludes with future research opportunities, particularly in applying artificial intelligence, and provides a resource for researchers and cybersecurity professionals seeking to understand and advance automated system-level malware detection using machine learning.

Keywords: anomaly detection; automated system classification; cybersecurity machine learning; malware detection

Citation: Gyamfi, N.K.; Goranin, N.; Ceponis, D.; Čenys, H.A. Automated System-Level Malware Detection Using Machine Learning: A Comprehensive Review. *Appl. Sci.* **2023**, *13*, 11908. https://doi.org/10.3390/app132111908

Academic Editor: Agostino Forestiero

Received: 16 August 2023
Revised: 25 September 2023
Accepted: 26 September 2023
Published: 31 October 2023

1. Introduction

In this information age connected by a digital landscape, the rapid proliferation of malware poses a significant threat to computer systems and networks. Some malicious software is designed to exploit vulnerabilities and compromise the integrity of systems, leading to data breaches, financial losses, and operational disruptions, with devastating consequences. As more malware is developed for covert gains, signature-based detection methods are inadequate in providing essential cybersecurity. Therefore, it is essential to develop advanced and efficient techniques to identify and mitigate malware attacks.

Leveraging the power of artificial intelligence, machine learning algorithms are promising in automating the process of identifying malware at the system level. This intersection of machine learning and cybersecurity has gained much attention to redress the challenges of malware detection. The intrinsic ability of machine learning to analyze huge volumes of data and acquire patterns indicative of malicious behavior can provide effective and timely detection capabilities.

The objective of this research paper is conduct a thorough analysis of the state of the art in machine-learning-based automated system-level malware detection and present a comprehensive review of the analysis. This is carried out through a focused systematic

literature review of research publications based on the many strategies, algorithms, and procedures used in system-level malware detection.

The review incorporates several aspects of automated system-level malware detection. This is distributed across several machine learning techniques, specifically, Naïve Bayes, Support Vector Machine, K-Nearest Neighbor, Artificial Neural Networks, Decision Tree, Random Forrest, Fuzzy Logic, Genetic Algorithm, General Adversarial Network, Hidden Markov Model, and Swarm Intelligence. The study investigates feature extraction and selection methods that enhance the reliability of malware detection algorithms. A comprehensive analysis of the strengths, limitations, and performance of different machine learning algorithms is conducted and these are identified as areas for improvement and future research opportunities.

The review discusses commonly used evaluation metrics to assess the performance of these algorithms and the datasets utilized for evaluating system-level malware detection. The challenges and limitations associated with automated system-level malware detection using machine learning, such as dataset availability, label imbalance, adversarial attacks, and generalization of models are addressed.

By critically examining these challenges, we aim to highlight areas for improvement and future research directions. Additionally, we conduct a comparative analysis of different machine learning approaches, enabling us to evaluate their respective strengths and weaknesses in detecting malware at the system level. The findings of this study will contribute to the advancement of malware detection and provide guidance for future research efforts for the development of more robust and reliable malware detection systems. The features of this research work are as follows:

a. This work puts forward research work of various feature extraction and classification strategies for malware detection in recent years (2003–2022).
b. It helps cyber specialists in integrating machine learning technology in detecting various anomalies in the automated system level.
c. The effectiveness and morality of ongoing plans are shown through quantitative analysis using numerous measurements.
d. This work will inspire researchers on a new path for creating models that could potentially help to detect automated system-level anomalies.

2. Bibliometric Analysis

The comprehensive review was initiated with the following steps:

1. Protocol,
2. Search,
3. Appraisal,
4. Synthesis,
5. Analysis,
6. Report.

2.1. Protocol

The research protocol established the research scope and formulated research questions and research boundaries to identify the research method. The research method elucidated the concept, population, intervention, comparison, and outcomes related to the study [1].

2.2. Search

The nature of the research defines the databases which are defined and restricted.

A number of databases were identified for the review as follows: IEEE Xplore, Science Direct, MDPI, ASCE library, Copernicus, AAS, Springer, Science press, Oxford Academic Press, and Scopus.

The search strategy defines meaningful search strings to collect the relevant documentation. The search strings are texts derived from the keywords. The output of documents is then assessed for suitability of the title. Inappropriate titles are discarded. Documents with

acceptable tiles are then skimmed through the abstracts. Documents with relevant abstracts are enlisted for the study (Figure 1). Thus, the inclusion criterion is a flow of acceptable documents: Keywords >> Titles >> Abstract.

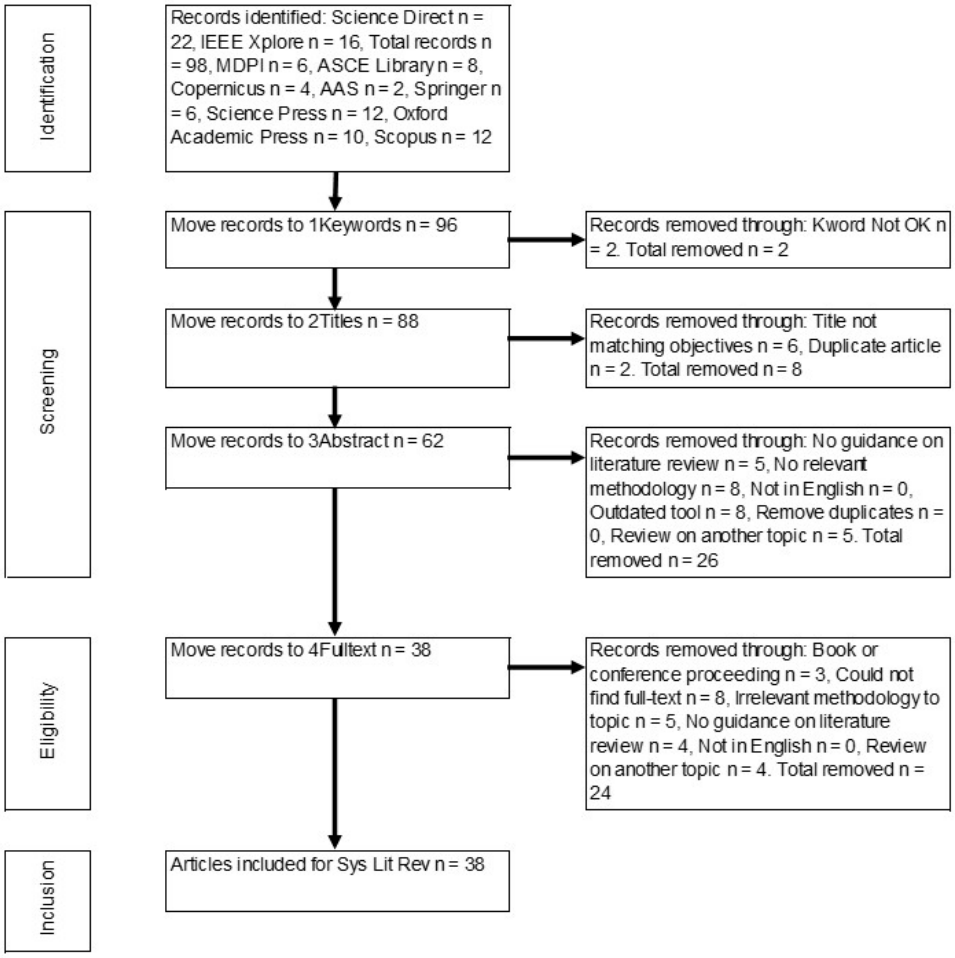

Figure 1. PRISMA flow chart.

The keywords used to search for suitable articles include 'automated system classification', 'cybersecurity machine learning', 'malware detection'. Searches were conducted in each database, and the search results were refined until a relatively small number of relevant records were obtained. Limited to articles over the two last decades, a total of 4500 documents were available from the 10 databases above (Figure 1).

A classification by article type (Figure 2) revealed the following distribution: Science Direct (22%), IEEE Xplore (16%), MDPI (6%), ASCE Library (8%), Copernicus (4%), AAS (2%), Springer (6%), Science Press (12%), Oxford Academic Press (10%), Scopus (12%).

A classification by article type (Figure 3) revealed the following distribution: article (60%), book chapters (13%), conference papers (8%), case report (4%), news (4%), encyclopedia (3%), short communication (2%), editorial (2%), abstract (2%).

Figure 4 shows the datasets for anomaly detection used in the study.

Figure 5 shows the clusters of activities based on several keywords, e.g., anomaly detection, intrusion detection, etc. From the graph, it is evident that there is more research on the anomaly detection for video followed by anomaly detection in the network, mobile and ad hoc network, medical application, intrusion detection, etc.

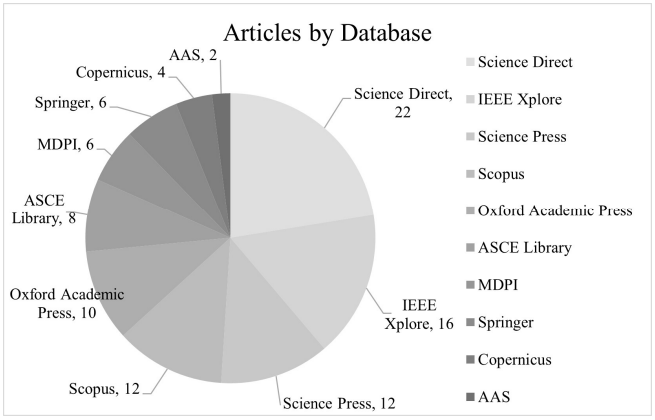

Figure 2. Articles by database.

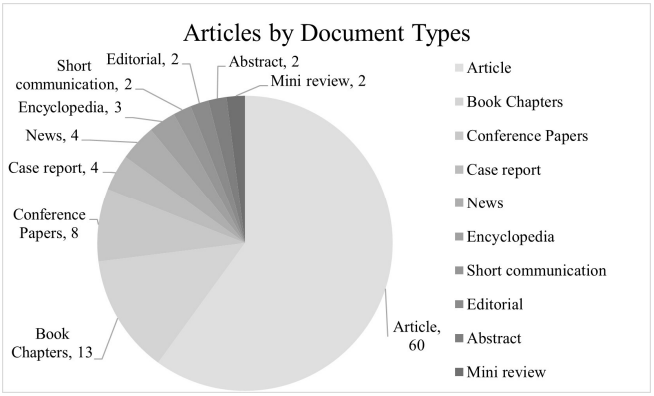

Figure 3. Articles by document type.

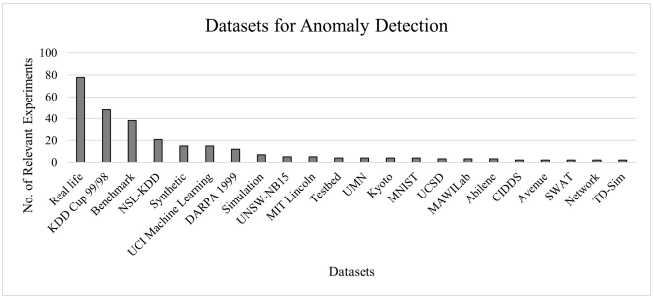

Figure 4. Dataset sets used for anomaly detection.

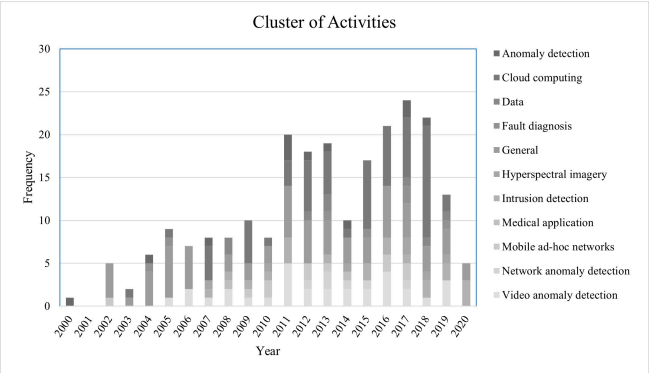

Figure 5. Custer of activities.

Figure 6 shows the cluster of activities between the years 2000 and 2020. From the figure, the following distribution is apparent: intrusion detection (27.9%), network anomaly detection (27.5%), and anomaly detection (13.3%) account for a cumulative 68.7%.

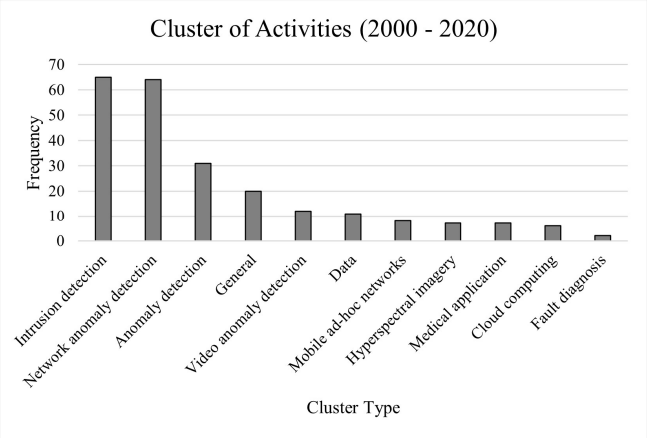

Figure 6. Cluster of activities (2000–2020).

Figure 7 shows the types of supervision by year.

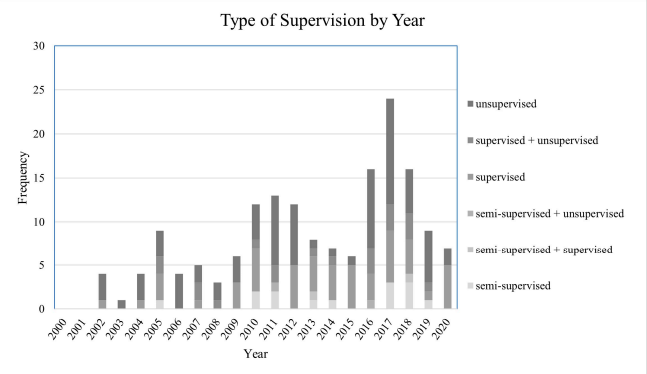

Figure 7. Type of supervision by year.

Figure 8 gives the frequency of performance matrix in terms of supervised, unsupervised, and semi-supervised algorithm.

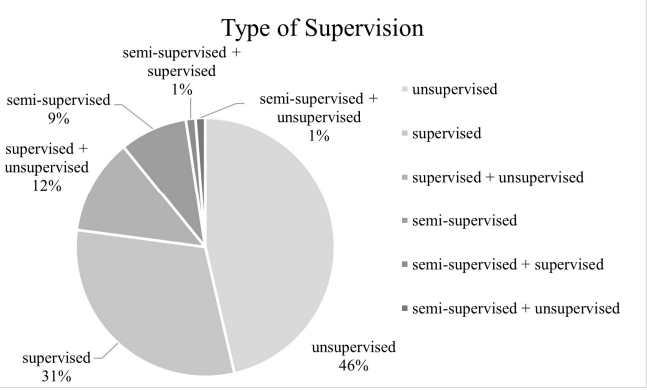

Figure 8. Frequency by level of supervision.

2.3. Appraisal

The appraisal phase is when selected articles are evaluated based on the contents of the article. The inclusion criteria are used to extract excerpts in the article that are relevant to the research. Excerpts are short clips of text that highlight related aspects of the review. Excerpts were identified from the articles that filtered through the PRISMA process, as seen in Figure 1. Excerpts with a common meaning or interpretation were collated together, with particular reference to the classification algorithms as presented in Section 4 Classification algorithms. This is further demonstrated in Table 1.

Table 1. Overview of state-of-the-art works.

ML Classifier	Author	Description
Naïve Bayes	[2]	Proposed Naive Bayes classifier and vessel trajectory clustering in a maritime surveillance system to detect aberrant vessel behavior
Naïve Bayes	[3]	A Naive Bayes & RBF Network anomaly detection model
Naïve Bayes	[4]	One-Class Probability Accumulation Detector (OCPAD)
Naïve Bayes	[5]	Devised a comprehensive framework for distinguishing between normal and abnormal monitoring signals
SVM	[6]	Support Vector Machines and Automatic Feature Selection to hunt for anomalies in Earth Dam and Levee Passive Seismic Data
SVM	[7]	Anomaly detection in EtherCAT-based water level control automation
SVM	[8]	SVM and GA for detecting network anomalies
SVM	[9]	SVM and Linear Regression Models to investigate Anomaly Detection in Medical Wireless Sensor Networks
KNN	[10]	A KNN approach based on self-organizing maps to investigate anomaly detection
KNN	[11]	TCM-KNN, a machine learning-based network anomaly detection approach
KNN	[12]	structure health monitoring under environmental influences an adaptive Mahalanobis-squared distance and one-class KNN rule-based anomaly detection system
ANN	[13]	ANN to investigate the performance of the NSL-KDD dataset
ANN	[14]	Flow-Based Anomaly Detection Using a Neural Network Optimized with the GSA Algorithm
ANN	[15]	Anomaly Detection in Hybrid Electric Vehicles
ANN	[16]	A wireless sensor network-based anomaly detection system for smart cities
Decision Tree	[17]	RADE, a resource-efficient supervised anomaly detection system based on decision tree-based ensemble techniques
Decision Tree	[18]	A decision tree algorithm to detect DDoS attacks
Decision Tree	[19]	A host-based combinatorial technique for the unsupervised categorization of anomalous and usual behavior in computer network ARP data using k-Means clustering and ID3 decision tree learning algorithms.
Random Forest	[20]	Intrusion Detection System (IDS)
Random Forest	[21]	Fault Detection Using Random Forest Similarity Distance
Random Forest	[22]	Random forests used to identify network-based anomalies on active routers
Random Forest	[23]	Random Forests and Traffic Entropy to study Network Anomaly Detection
Fuzzy Logic	[24]	Used fuzzy logic to detect cross-layer anomalies in smart home sensor networks using mobile agents for cross-layer anomaly identification
Fuzzy Logic	[25]	Intrusion Detection System (IDS) that uses multi-agent systems and artificial intelligence techniques such as Fuzzy Logic Controllers (FLCs), Multi-Layer Perceptrons (MLPs), and Adaptive Neuro-Fuzzy Inference Systems (ANFIS).
Fuzzy Logic	[26]	An anomaly-based network security cyber sensor

Table 1. *Cont.*

ML Classifier	Author	Description
Fuzzy Logic	[27]	A novel Knowledge-Based System (KBS) that integrates Fuzzy Logic (FL), particle filtering, and anomaly detection
Genetic Algorithm	[28]	Network Anomaly Detection System by combining Genetic Algorithms with Fuzzy Logic
Genetic Algorithm	[29]	Tsfresh Tool and Genetic Algorithm-based Anomaly Detection Algorithm Selection Service for IoT Stream Data
Genetic Algorithm	[30]	Intrusion detection system based on a genetic algorithm with an updated starting population and selection operator
Genetic Algorithm	[11]	Network Intrusion Detection Systems (NIDS)
GAN	[31]	Better Anomaly Detection by GAN
GAN	[32]	GAN-based Anomaly Detection for Imbalance Problems
GAN	[33]	Adversarially Learnt Anomaly Detection
HMM	[34]	An approach based on a hidden Markov model of privilege flows for identifying abnormalities
HMM	[35]	Identifies anomalous network intrusions
HMM	[36]	Anomaly Detection Techniques using the Hidden Markov Model
Swarm Intelligence	[37]	SI-based IDS techniques to solve an issue and provide the best solution
Swarm Intelligence	[38]	AntNag, the first Ant Colony Optimization technique for intrusion detection
Swarm Intelligence	[39]	Ant-based Replication and MApping Protocol (ARMAP) can reduce the entropy of the system and efficiently propagate content
Swarm Intelligence	[40]	An approach for efficient and transparent parallelization of a large class of swarm algorithms

2.4. Synthesis

The synthesis phase is used to organize relevant excerpts from selected papers to synthesize the knowledge base. This process consisted of the identification, extraction, and classification of pertinent information. Excerpts were arranged and rearranged until they formed a body of information characterizing the review.

2.5. Analysis

The analysis phase was used to analyze the assembly of new knowledge and interpret data pertinent to the research question. This included the implication of the state of the art of the research for policy implication and implementation, and the kinds of scientific research needed in the future from various disciplines that have a bearing to the topic of research. The data from the final synthesis provided an overview of the evidence, arranged to close the knowledge gaps with implications on the state of the research on policy implication and implementation.

2.6. Report

This phase presented the research methodology and the results obtained from the systematic literature review process described. Thus, the first part details the method by which the systematic literature review process was conducted. The second part details the results of the research. Very importantly, the results are presented as a tabulation of the findings that can be used by fellow researchers for other scientific purposes.

3. Methodology

This section contains the basic machine learning model for anomaly detection, which inspired us to provide a state of the art in the field of anomaly detection, including classification, combining techniques, and applications. Figure 9 depicts the basic architecture model for anomaly detection in automated system level.

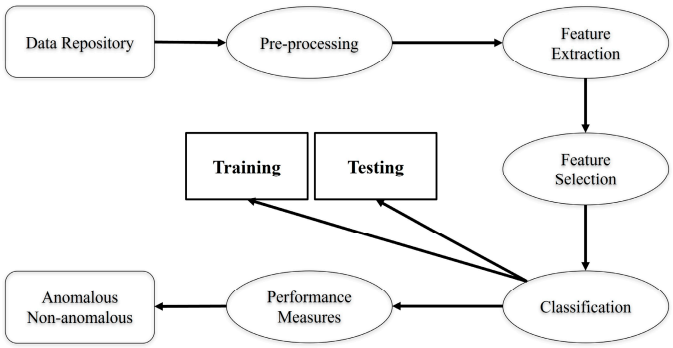

Figure 9. Basic architecture model for anomaly detection in automated system level.

The data repository is determined by the researchers. Different pre-processing techniques are applied to eliminate any noise from the raw data. Multiple-feature extraction is used from the pre-processed data. Feature selection from the primary stage is given to the classifiers, where machine learning plays a role in classifying anomalous conditions, which is conducted based on the training and test data. The efficiency and accuracy are evaluated based on the performance measures used for the evaluation [41,42].

Using this architecture, the study was conducted across different machine learning algorithms, and a critical review was conducted on their ability to reliably determine the anomalous and non-anomalous conditions.

4. Classification Algorithms

Classification approaches rely on mathematical techniques such as statistics and linear programming, among other things. New data items are classified into multiple groups during classification. The following 11 machine learning (ML) classification techniques were used in this study:

1. Naive Bayes (NB)
2. Support Vector Machine (SVM)
3. K-Nearest Neighbour (KNN)
4. Artificial Neural Networks (ANN)
5. Decision Tree (DT)
6. Random Forest (RF)
7. Fuzzy Logic (FL)
8. Genetic Algorithm (GA)
9. Generative Adversarial Network (GAN)
10. Hidden Markov Model (HMM)
11. Swarm Intelligence (SI)

4.1. Naïve Bayes

Ref. [2] introduced the application of the Naive Bayes classifier and vessel trajectory clustering in a maritime surveillance system for detecting abnormal vessel behavior. Data from the Automatic Identification System (AIS) was employed to compare hierarchical and k-medoids clustering methods to model and understand normal vessel sailing patterns in port waters. Unusual ship behavior was detected and classified using the Naive Bayes classifier. Using vessel trajectories obtained from AIS data, the proposed approach was tested and confirmed in the seas of Xiamen Bay and Chengsanjiao, China. The results demonstrated the feasibility of the recommended technique in enhancing marine situational awareness in coastal seas, as supported by statistics analysis.

Ref. [3] also proposed a Naive Bayes Network anomaly detection model as applied to the catastrophic impact of intrusions on computer systems and networks. The automated intrusion detection strategies were successful to reduce the risk associated with intrusion attacks to some level. They further employed a novel Machine Learning strategy that

combined the Naive Bayes and weighted radial basis function Network approaches. While experimenting on the KDDCup'99 data set in detecting intrusions, the proposed schema showed highly promising results in comparison to several earlier techniques.

Ref. [4] introduced OCPAD, an innovative approach for detecting suspicious payload content in network packets, specifically targeting HTTP attacks. This approach combines the strengths of single-class classification and short sequence frequency analysis through a Multinomial Naive Bayes classifier, leveraging one class as an anomaly detector. OCPAD calculates the likelihood of recurrence for each short sequence within the payload of known non-malicious packets. During the training phase, OCPAD establishes the probability range for the occurrence of each sequence based on a unique data structure called the Probability Tree. A brief sequence is regarded anomalous in the testing phase if it is not found in the database or if its probability of recurrence in a packet exceeds the training phase's range. It creates a sequence depending on how often short sequences are likely to occur. When evaluated on a huge dataset of 1 million HTTP packets received from an academic network, OCPAD had a high detection rate (up to 100%) and a low false positive rate (less than 1%).

Ref. [5] devised a comprehensive framework for distinguishing between normal and abnormal monitoring signals. The primary concept was to create a large number of binary indicators that make full use of expert knowledge. Each indicator was a fully parametrized anomaly detector that was created using expert-designed parametric anomaly ratings.

4.2. Support Vector Machine (SVM)

Ref. [6] used Support Vector Machines and Automatic Feature Selection to hunt for anomalies in Earth Dam and Levee Passive Seismic Data. They aimed to monitor the condition of earth dams and levees and automatically identify unexpected events in passive seismic data by developing a unique data-driven method to various time-series data-driven systems. Applying the machine learning technique to the geophysical data collected from surface sensors, Fisher et al. detected internal issues within the levee structure. Ref. [6] used two distinct datasets from experimental laboratory earth embankments comprising approximately 80% normal instances and 20% anomalies. Their study employed wavelet-based algorithms to decompose time series data segments and extract nine spectral components, resulting in a two-class SVM with an overall accuracy of over 94% and an F1-score of 96% when using 10-fold cross-validation. Experiments using the optimum settings increased the overall accuracy from 83% to over 91% and a 95% F1 score. The findings imply that humans can distinguish between normal and abnormal data.

Ref. [7] conducted research on anomaly detection in EtherCAT-based water level control automation where there was a significant threat of cyber-attacks in Industrial Control Systems (ICS). EtherCAT is a European real-time protocol prone to both known and unknown assaults targeting critical field systems. To alleviate this problem, Akpinar et al. developed a laboratory-scale water level control test, generating attack vectors based on EtherCAT communication principles and creating a dataset. After minimizing operational process behavior, they explored both supervised and unsupervised approaches for anomaly detection. Their study demonstrated effective supervised algorithms such as Support Vector Machines (SVM) and Random Forest in detecting EtherCAT abnormalities, while the unsupervised methods proved successful in identifying specific attack patterns. Thus, they demonstrated that machine learning techniques contributed to enhancing the security of EtherCAT networks and strengthening Industrial Control Systems against cyber threats.

Ref. [8] suggested a machine learning technique based on SVM and GA for detecting network anomalies. The researcher focused on machine learning approaches for detecting cyber-assaults based on Internet anomalies. The support vector machine (SVM) was employed for packet classification in the machine learning framework while the Genetic Algorithm (GA) was utilized for feature selection Experiments revealed that the proposed system outperformed current network intrusion detection system (NIDS). Their main objective of the research was to develop an Enhanced SVM technique that offered a standardized framework for identifying and categorizing new network attacks. They demonstrated faster

data processing and higher accuracy in field selection compared to other techniques. The Enhanced SVM combined a high-performance supervised method with a non-supervised, unlabeled approach. Their SVM technique predicted a low false-positive rate similar to NIDS, but without the need for labeled data required by signature-based NID methods.

Ref. [9] developed an anomaly detection framework for medical wireless sensor networks, utilizing SVM and linear regression models. Their research focuses on widespread patient and healthcare monitoring, employing data mining, machine learning, and sensor fusion technologies. Their framework distinguishes between irregular variations in patient physiological parameters and faulty sensor data, ensuring reliable operations and global real-time monitoring from smart devices. The program utilizes a Support Vector Machine to classify anomalous sensor data, enabling the identification of critical stages or erroneous measurements. Their SVM technique could quickly detect sensor abnormalities by employing a regressive prediction model that was rebuilt regularly to evaluate whether the patient was reaching a critical stage or whether a sensor was providing erroneous data in the event of a rare incident. Studies using real patient data showed higher true-positive rates and lower false-negative rates compared to existing algorithms.

4.3. K Nearest Neighbour (KNN)

In their study, Ref. [10] investigated anomaly detection using a K-Nearest Neighbour (KNN) approach based on self-organizing maps which are capable of quantizing errors of test data against healthy training data. Their study addressed limitations in existing methods by improving self-organizing maps for anomaly detection. By eliminating noise-dominated best-matching units from healthy training data, they obtained healthy references. They used the K-Nearest Neighbor algorithm is used to find neighbors of a given test data observation that existed in the references for a given test data observation. The Euclidean distance between the test data observation and the centroid of the neighbors was determined and compared to the least quantization error. This method proved to be less sensitive to noise compared to quantization-error-based metrics and did not impose restrictions on the convexity or distribution of the best matching units. Their approach was confirmed using data from cooling fan bearing experiments.

Ref. [43] introduced TCM-KNN, a machine-learning-based network anomaly detection approach utilizing Transductive Confidence Machines (TCM) and K-Nearest Neighbors (KNN). Their approach demonstrates superior performance on the widely used KDD Cup 1999 dataset, outperforming existing anomaly detection algorithms in terms of true positive rate, false positive rate, and confidence. The proposed method exhibits robustness and effectiveness even in the presence of noisy data. Additionally, it effectively addresses the issue of high-dimensional data by incorporating feature selection techniques while maintaining excellent detection performance.

According to [44] Weighted KNN classifiers have practical applications in real-time detection of large-scale attacks, such as DoS attacks. The selection of essential features is crucial for developing an effective anomaly-based NIDS. To ensure optimal performance, NIDS systems must not only exhibit outstanding detection capabilities but also operate in real-time. It is vital to have a robust feature selection that identifies the most relevant and minimal characteristics for an efficient NIDS classifier. In their study, the researchers employed a combination of a genetic algorithm and KNN to select and assign weights to the features. During the training phase, all 35 initial attributes were evaluated, and the top five were chosen for testing the NIDS systems. Subsequently, the systems were tested for various DoS attacks. The results revealed an impressive overall accuracy of 97.42% when only the top 19 attributes were considered for known attacks. By utilizing the top 28 attributes, the NIDS achieved an overall accuracy rate of 78% for attacks carried out by unknown perpetrators.

In their research, Ref. [12] proposed an innovative method called AMSD-KNN for anomaly detection in structural health monitoring (SHM) under environmental influences. The commonly used Mahalanobis-squared distance (MSD) anomaly detection method

in SHM faces significant challenges and limitations, including environmental variability, threshold determination, inaccurate covariance matrix estimation, and non-Gaussian training data, resulting in false alarms and inaccurate damage detection. The researchers aimed to address these issues by developing AMSD-KNN, which combines adaptive Mahalanobis-squared distance with a one-class KNN algorithm. The core idea behind AMSD-KNN is to reduce ambient variability and estimate local covariance matrices using a two-stage technique that identifies appropriate nearest neighbors from the training and testing datasets. To ensure well-conditioned local covariance matrix estimation, an efficient technique based on a multivariate normality hypothesis test is used to find a sufficient number of nearest neighbors. The proposed AMSD-KNN approach combines a single-class KNN rule with a single multivariate distance measure, providing an unsupervised learning strategy for SHM. To determine an appropriate threshold limit, the researchers employed generalized extreme value distribution modeling and the Block Maxima (BM) technique. The Kolmogorov–Smirnov hypothesis test was utilized to identify the optimal block number in the BM technique, as the selection of the right blocks is crucial. The performance and utility of the proposed approaches were validated using two well-known benchmarking systems, and several comparison studies have demonstrated that the proposed techniques outperformed other state-of-the-art technologies. Based on the findings, the suggested AMSD-KNN and BM approaches proved to be highly effective in detecting damage in various environmental circumstances, highlighting their potential for improving structural health monitoring under challenging conditions.

4.4. Artificial Neural Networks (ANN)

In a study conducted by [13], an Artificial Neural Network (ANN) was used to evaluate the performance of the NSL-KDD dataset. With the proliferation of smart devices and technologies, monitoring abnormal internet traffic has become a crucial security concern. Various attacks pose significant threats to systems, causing them to slow down and impede their processing speeds. Intrusion detection systems play a vital role in assessing system security by raising alerts when an intrusion is detected. In this research, the authors utilized ANN to test the effectiveness of the NSL-KDD dataset. They evaluated both binary and five-class categorizations, which focused on different types of attacks. The results show that both categorizations yielded similar outcomes in terms of performance. Multiple performance indicators were employed to assess the results, and they demonstrated higher accuracy levels. Specifically, the NSL-KDD dataset achieved an 81.2% detection rate for intrusion detection and a 79.9% detection rate for malware detection. The proposed system outperformed existing algorithms in terms of detection rate for both binary and five-class classification problems. These findings highlight the effectiveness of ANN in enhancing the detection capabilities of intrusion detection systems using the NSL-KDD dataset.

In their study published in 2013, Ref. [14] introduced a novel approach called "Flow-Based Anomaly Detection Using a Neural Network Optimized with the GSA Algorithm". With the increasing demand for reliable high-speed networks to support the growing number of Internet of Things applications, a network access detection system plays a crucial role in preventing network infiltration (NIDS).

Traditional packet-based NIDS systems require significant time to analyze all network packets, making them unsuitable for processing large amounts of data in real-time. Flaw-based intrusion detection, which focuses on packet headers, is more suitable for high-speed networks. However, detecting intrusions has become increasingly challenging as the likelihood of further attacks continues to rise. Anomaly-based intrusion detection is a well-known approach to identify unknown threats. The researchers presented a flaw-based anomaly detection method in their study, utilizing an Artificial Neural Network (ANN) as a valuable tool for detecting abnormalities. Specifically, they employed a Multi-Layer Perceptron (MLP) with one hidden layer as the neural network architecture. To optimize the link weights of the MLP network, they applied a Gravitational Search Algorithm (GSA). The GSA-based flow anomaly detection algorithm (GFADS) was trained using flaw-based

data. The results showed that the trained system achieved an impressive accuracy of 99.43% in distinguishing between benign and harmful signals. The performance of the GSA algorithm was compared with other optimization techniques such as Particle Swarm Optimization (PSO) and gradient descent. According to the findings, GFADS demonstrated the ability to identify flaw-based irregularities effectively, making it a valuable tool for network intrusion detection. The study highlighted the strength of the proposed approach, optimized with the GSA algorithm, as it offered a comprehensive set of traits for detecting network anomalies.

In their study conducted in 2018, Ref. [15] explored Anomaly Detection in Hybrid Electric Vehicles using an ANN-based Support Vector Data Description. One of the challenges faced by machine learning classifiers is the "dimensionality plague", where finding data from the abnormal class becomes extremely difficult. One-class classifiers address this issue by splitting the input into groups using training examples from a large library of common events. However, since there are no training data available for the anomalous class, the accuracy of these classifiers suffers. To overcome this limitation, the researchers employed a two-class, ANN-based classifier that utilized the class discoveries of a single-class classifier. The results of the classifier were verified using the confusion matrix, providing a means to double-check its performance. Support Vector Data Description (SVDD), which is a single-class Support Vector Machine, was utilized to categorize the data without relying on linearity and separability. Several enhancements were proposed to improve the accuracy and training speed of the traditional SVDD. The classification results obtained were then used to train an Artificial Neural Network (ANN), which was utilized for data categorization. This approach did not affect the classification accuracy but significantly improved the processing speed. To form a classifier ensemble, six different kernels were employed, and the dataset was subjected to an ANN-based voting method for classification. Overall, the research introduced an ANN-based Support Vector Data Description approach for anomaly detection in hybrid electric vehicles. The combination of SVDD, ANN, and classifier ensembles provided improved accuracy and processing speed for categorizing data.

Ref. [16] proposed a wireless-sensor-network-based anomaly detection system for smart cities. Smart cities heavily rely on the Internet of Things (IoT), a relatively new technology that enables detailed monitoring of various physical products and environments through low-cost, low-power sensor and communication technologies. Although the IoT has gained significant interest for smart cities, there are limited systematic studies demonstrating how valuable insights can be extracted from real-time IoT data using advanced data analytics techniques like anomaly detection. In this research, the authors conducted a case study in a smart environment using real-time data collected by the city of Aarhus, Denmark. They specifically utilized the Air Quality Index (AQI) to investigate and analyze the levels of different contaminants in the air, aiming to identify potentially hazardous or anomalous areas. To achieve this, they employed a machine learning architecture that incorporated a neural network, a Neuro-Fuzzy approach, and Support Vector Machines. These techniques were applied to a pollution database to detect anomalous locations, addressing both binary and multiclass classification problems. Based on the MATLAB simulation results, the machine learning algorithms demonstrated reliability in terms of accuracy and computation time for smart city applications. This indicates their effectiveness in identifying anomalies and highlighting potentially problematic areas in pollution data.

4.5. Decision Tree

In their recent work, Ref. [17] developed a resource-efficient supervised anomaly detection system called RADE. The ability to detect anomalies in resource-constrained environments, such as edge devices or heavily loaded servers, has become increasingly crucial due to limitations in on-premises computing, as well as concerns related to security, privacy, and profitability. Existing anomaly detection techniques, particularly those based on decision tree-based ensemble classifiers, can impose a significant resource burden as the

number of datasets increases. To address this issue, the researchers introduced RADE, a novel resource-efficient anomaly detection approach that complements existing decision tree-based ensemble classifiers in resource-constrained scenarios. The core concept of RADE is to train a compact model that can accurately identify the majority of requests. For cases where the small model is prone to classification errors, expert models are created using only portions of the training data. RADE is implemented as a classifier using the sci-kit-learn library. The experimental results demonstrate that RADE offers competitive anomaly detection capabilities compared to conventional approaches, while significantly reducing the memory footprint by up to 1212, training time by up to 2020, and classification time by up to 1616. This highlights the effectiveness of RADE in efficiently detecting anomalies while operating within limited resource constraints.

In their study, Ref. [18] explored the use of a decision tree algorithm for detecting Distributed Denial of Service (DDoS) attacks. The widespread adoption of the IEEE 802.11 standard [45] for achieving extensive network coverage and high capacity has introduced numerous security challenges. The increased usage of Wi-Fi has made internet connectivity more convenient but has also exposed networks to various hacking attacks. End users and network administrators often encounter anomalies when trying to comprehend and mitigate DDoS attacks, highlighting the need for effective anomaly detection techniques at different levels. To address this issue, the researchers proposed a novel approach for anomaly detection using the Decision Tree algorithm. They aimed to classify instances into respective attack types with a high detection rate, utilizing the KDDCup'99 dataset for classification purposes. This approach aimed to safeguard wireless nodes within the network and protect destination nodes from DDoS attacks. It also aimed to identify attack patterns and facilitate the implementation of appropriate countermeasures. The proposed approach combined two well-known classification techniques, Ref. [3] and Random Forest, with the Decision Tree algorithm to construct an intrusion detection system. Intrusion Detection Systems (IDS) are crucial for effectively handling computer intrusions. They operate by generating alerts that prompt analysts to take preventive measures against potential breaches. By leveraging the decision tree-based approach, Ref. [18] demonstrated a powerful method for detecting DDoS attacks. The IDS-based on the decision tree algorithm achieved high accuracy in classifying attack instances and provided valuable insights for mitigating and preventing such attacks.

Intrusion detection systems are designed to identify and distinguish unauthorized behavior from that of authorized users. Over the years, various approaches, ranging from traditional statistical methods to advanced data mining technologies, have been employed to develop Intrusion Detection Systems (IDS) for safeguarding computers and networks against hostile attacks. However, commercial IDS systems typically rely on predefined signatures and are limited in their ability to detect unknown attack attempts. In this study, we propose a novel approach for detecting misuse and anomalous attacks using a decision tree technique. By leveraging the decision tree algorithm, we construct a classification model that can effectively identify and classify abusive and abnormal activities. This approach aims to enhance the detection capabilities of intrusion detection systems, allowing for improved identification of both known and unknown attack patterns.

Ref. [19] introduced a novel approach for categorizing anomalous and normal behavior in computer network ARP data. They utilized the k-Means clustering and ID3 decision tree learning algorithms in a host-based combinatorial technique. The k-Means clustering algorithm divided the training samples into k groups based on their similarity, measured by Euclidean distance. An ID3 decision tree was then constructed for each cluster. To determine the anomaly scores and ID3 decision tree options, the researchers incorporated the k-Means clustering method. Integrating the results of both approaches and deriving final anomaly score values required a specialized procedure. The threshold rule was employed to evaluate the normality of test instances. The experiments were conducted using data collected from network ARP traffic. Various unexpected scenarios were created and applied to the acquired ARP data to simulate typical training scenarios. The performance of

the proposed technique was compared empirically against individual k-Means clustering algorithms, ID3 decision tree classification algorithms, as well as other approaches based on Markovian chains and stochastic learning automata. The comparison was based on five specified criteria. The results showed that the proposed technique achieved a specificity of 96% and a positive predictive value of 98% when tested with the data.

4.6. Random Forest

Ref. [20] employed a random forest algorithm to detect anomalies. With the increasing sophistication of hackers, having a deterrent device like an Intrusion Detection System (IDS) has become crucial for data security management. The purpose of an intrusion detection system is to identify and prevent potentially harmful network activity. An effective intrusion detection system consists of a well-trained classification model capable of detecting attackers. In their study, the researchers evaluated the performance of IDS using a random forest classifier and two metrics: accuracy and false alarm rate. They conducted experiments using three public intrusion datasets: NSL-KDD, UNSW-NB15, and GPRS. To find the best learning parameters, a grid search was conducted with various tree-size ensembles. The results showed that the random forest model outperformed other approaches such as the matching ensemble (random tree + naive Bayes tree), as well as standalone classifiers like naive Bayes and neural networks, in terms of k-fold cross-validation for IDS.

Ref. [21] delved into the topic of fault detection using random forest similarity distance. With the constant drive to keep up with Moore's law and achieve higher device performance, semiconductor manufacturers have been continuously reducing and reconfiguring transistor layouts. This has led to increasingly complex manufacturing processes, with hundreds of processing steps involved in most cases. In such a complex manufacturing environment, even a single improperly processed wafer can have a significant negative impact on profitability if it progresses through the entire production process. To address this issue, the authors propose an unsupervised technique that utilizes chemical fingerprints obtained during the plasma etching process to identify damaged wafers. They employ random forests as the basis for their approach. The effectiveness of the proposed strategy is evaluated using both a simulated case and a real-world industrial dataset. The results demonstrate that the technique successfully identified defective wafers in both scenarios, indicating its potential utility in practical applications.

Ref. [22] conducted a study on the application of random forests for identifying network-based anomalies on active routers. Intrusion detection systems (NIDSs) play a crucial role in network security infrastructure. Rule sets are commonly used to govern the functionality of NIDSs. However, defining these rules can be a challenging and time-consuming task due to the vast amount of network data. To overcome this challenge, data mining techniques are employed to create adaptive intrusion detection models. Random forests, a powerful data mining tool, are utilized for detecting network intrusions in real-time. The research introduces methods for feature selection and optimizing random forest parameters. Multiple models are compared, and an alternative method for detecting anomalies in active networks is proposed. Overall, the study highlights the potential of random forests as an effective approach for network intrusion detection and presents techniques to enhance their performance in detecting anomalies across active networks.

Ref. [23] conducted a study on network anomaly detection using Random Forests and Traffic Entropy. Detecting network anomalies requires monitoring fluctuations in traffic feature distributions and utilizing them to identify traffic with varying behavior. One effective approach is to use Shannon entropy to identify anomalies in network data by detecting deviations from the expected patterns. Standardized entropy provides a measure of homogeneity and randomness, allowing for comparison across multiple sample spaces and variables. Random Forests, a machine learning classification technique, is well-suited for handling challenging or imbalanced data structures commonly encountered in small to moderate-sized datasets. Since anomaly traffic typically represents a small portion

of overall network traffic, a combination of entropy and Random Forests classification was employed to detect abnormalities in the network data. The study's findings suggest that this novel approach holds great promise for effectively identifying traffic anomalies. In summary, Ref. [23] research highlights the effectiveness of using Random Forests and Traffic Entropy in network anomaly detection, demonstrating the potential of this combined method for accurately identifying abnormal network traffic.

4.7. Fuzzy Logic

Ref. [24] presented a novel approach for detecting cross-layer anomalies in smart home sensor networks using fuzzy logic and mobile agents. Despite advancements in consumer electronics, anomalies in data generated by sensing devices in smart homes remain a concern, resulting from node failures, transmission issues, or malicious attacks. These anomalies can undermine the reliability of sensed data, leading to inaccurate decisions at both the local (smart house) and global (smart city) levels. To address this, the researchers proposed a cross-layer anomaly detection method that leverages mobile agents and fuzzy logic. The approach considers the stochastic variability in cross-layer data obtained from data packets and employs fuzzy logic-based soft bounds to characterize the behavior of sensor nodes. By adopting a cross-layer design, the method can identify anomalies in both nodes and communication links. It also considers the communication link-state before transmitting mobile agents, ensuring efficient transmission. The proposed method was evaluated on a real testbed, and modular application software was developed to control the smart home's anomaly detection system. The results demonstrated that the approach effectively identifies cross-layer anomalies and reduces the energy consumption associated with mobile agent transmission in environments with poor communication connectivity. In summary, Usman et al.'s research introduces a novel approach for detecting cross-layer anomalies in smart home sensor networks. By combining fuzzy logic and mobile agents, the proposed method improves anomaly detection accuracy and reduces energy requirements, offering potential benefits for ensuring reliable and efficient smart home operations.

Ref. [25] proposed an Intrusion Detection System (IDS) that utilizes multi-agent systems and artificial intelligence techniques, including Fuzzy Logic Controllers (FLCs), Multi-Layer Perceptrons (MLPs), and Adaptive Neuro-Fuzzy Inference Systems (ANFIS). Network Intrusion Detection Systems (NIDS) play a crucial role in examining network traffic and identifying potential threats. The IDS system proposed by the authors consists of three agents: the accumulator, analyzer, and decision-maker. The accumulator agent is responsible for collecting and filtering network traffic data. The analyzer agent utilizes a decision tree to classify the data into different categories. Finally, the decision-maker agent employs a fuzzy logic controller (FLC) to make the final decision. To evaluate the effectiveness of the proposed technique, experiments were conducted using the KDDCup 1999 dataset. The results demonstrated an improvement in attack detection accuracy when compared to existing approaches. In summary, Feizollah et al.'s research introduces an IDS system that combines multi-agent systems and artificial intelligence techniques. By utilizing FLCs, MLPs, and ANFIS, the proposed system enhances the accuracy of detecting network attacks.

Ref. [26] proposed a unique approach to developing an anomaly-based network security cyber sensor by utilizing a novel learning technique and implementing it in hardware. Their recommended learning method involves creating a fuzzy logic rule architecture to mimic natural network activity. The system employs an online clustering approach to generate individual fuzzy rules from a continuous stream of incoming packets, enabling effective anomaly detection. On a different note, Ref. [27] introduced a novel "Knowledge-Based System (KBS)" that combines Fuzzy Logic (FL), particle filtering, and anomaly detection to construct high-performing investment portfolios. Their FL approach selects portfolios from a pool of candidates based on multilateral performance criteria, ensuring favorable risk–return profiles. In summary, Ref. [26] focused on building an anomaly-based network security cyber sensor using a unique learning technique and

hardware implementation, while Ref. [27] proposed a Knowledge-Based System integrating Fuzzy Logic, particle filtering, and anomaly detection for constructing well-performing investment portfolios.

4.8. Genetic Algorithm (GA)

Ref. [28] devised a Network Anomaly Detection System by integrating Genetic Algorithms with Fuzzy Logic. With the proliferation of computer network usage across various applications, ensuring the integrity and availability of computer networks has become crucial for both individuals and businesses. To address this, the researchers utilized Flow Analysis, a technique that examines network flow data to estimate network traffic behavior over a specific period. They employed the Genetic Algorithm to generate a Digital Signature of a Network Segment based on this analysis. In contrast to existing approaches, the proposed system incorporated Fuzzy Logic to determine the abnormality of network occurrences. An expert system was designed to utilize IP flows, monitor network traffic, and establish expected behavior at regular intervals. Whenever a potential issue arises, users are promptly alerted. The suggested anomaly detection system automatically detects network faults and boasts impressive performance. In real network traffic flows, the approach achieved an accuracy of 96.53% and a false-positive rate of 0.56%. Comparative analysis with other approaches demonstrated its superiority.

Ref. [29] the Tsfresh Tool and a Genetic-Algorithm-based Anomaly Detection Algorithm Selection Service for IoT Stream Data. While Anomaly Detection Algorithms (ADA) are readily available as services in maintenance management systems, the challenge lies in effectively dealing with the continuously changing stream data and the occurrence of idea drift in dynamic IoT environments. Selecting an appropriate Anomaly Detection Service (ADS) in real-time becomes a daunting task. To address this, the researchers developed a method for selecting and configuring ADS for real-time data anomaly detection. They employed the Tsfresh time-series feature extractor and a feature selection strategy based on a genetic algorithm to efficiently extract dominant features that represent stream data patterns. Historical data, including stream data features and other relevant information, were collected to dynamically identify important ADS at runtime. A fast classification model based on XGBoost was constructed to aid in the selection of suitable services and their configurations based on stream data patterns. The key to their approach's success lies in the features used to characterize and portray the underlying qualities of time-series data. Extensive tests were conducted to evaluate the effectiveness of the features obtained through the genetic algorithm. Experimental results on both synthetic and real datasets demonstrated that their proposed strategy outperformed previous complex approaches in terms of accuracy. It showcased the ability to identify suitable services across various scenarios.

Ref. [29] proposed a novel approach, utilizing the Tsfresh Tool and a Genetic-Algorithm-based Anomaly Detection Algorithm Selection Service, for effective anomaly detection in IoT Stream Data. Nowadays, Anomaly Detection Algorithms (ADA) are readily available as services in various maintenance management systems. However, coping with the constantly changing stream data and the occurrence of idea drift in dynamic IoT environments poses challenges. Selecting an appropriate Anomaly Detection Service (ADS) in real-time becomes a complex task. To tackle this issue, the researchers devised a method for choosing and configuring ADS in real-time data anomaly detection. They employed the Tsfresh time-series feature extractor along with a feature selection strategy based on a genetic algorithm. This approach allowed for the rapid extraction of dominant features that effectively represented the patterns present in the stream data. Historical data, including stream data features and other relevant information, was gathered to facilitate the dynamic identification of crucial ADS at runtime. A fast classification model based on XGBoost was developed to collect stream data features and enable the identification of appropriate services and configurations based on stream data patterns. The success of their approach hinged on the effective utilization of features to characterize and portray the underlying qualities of time-series data. The researchers conducted thorough tests to

evaluate the efficacy of features obtained through the genetic algorithm. Experimental evaluations conducted on both synthetic and real datasets demonstrated the superiority of their proposed strategy. It exhibited higher accuracy compared to previous complex approaches and showcased its ability to identify suitable services in diverse situations.

Ref. [30] devised an intrusion detection system that effectively detects diverse network intrusions by employing a genetic algorithm with an enhanced starting population and selection operator. The genetic algorithm (GA) is a powerful method that combines exploration and exploitation techniques to expedite the search for attack scenarios within audit files. By utilizing GA, the system efficiently identifies a subset of probable attacks present in the audit file within a reasonable timeframe.

Ref. [11] highlights the utilization of Genetic Algorithms (GA) in Network Intrusion Detection Systems (NIDS). The paper provides a concise overview of the Intrusion Detection System, genetic algorithm, and related detection methods. It delves into the properties and evolutionary process of GA in detail. Unlike alternative approaches, this solution tackles the temporal and geographical aspects of network connections by encoding network connection information into IDS rules, making the detection of complex abnormal behavior more streamlined. The study primarily focuses on TCP/IP network protocols.

4.9. Generative Adversarial Network (GAN)

In their paper titled "GAN-Based Anomaly Detection for Imbalance Problems", Ref. [32] explored the use of generative adversarial networks (GANs) for improved anomaly detection. Anomaly detection involves identifying data points that deviate from the normal distribution. GANs, known for their ability to handle complex and high-dimensional data, are considered a cutting-edge technology in this field. However, the conventional GAN loss function is not designed for anomaly detection and fails to produce effective anomaly detectors. To address this limitation, the researchers proposed enhancements to the GAN loss function. These improvements aim to generate samples that align better with the boundaries of the true data distribution. They introduced a novel approach called Fence GAN (FGAN), wherein the discriminator score is directly utilized as an anomalous threshold for anomaly detection. Through their experiments on the MNIST, CIFAR10, and KDD99 datasets, the researchers demonstrated that FGAN outperforms existing methods in terms of accuracy in anomaly classification. This research highlights the potential of FGAN for more effective and accurate anomaly detection [31].

In their study, Ref. [33] developed a novel method called Adversarially Learnt Anomaly Detection (ALAD) to address the challenge of anomaly detection. ALAD utilizes bi-directional Generative Adversarial Networks (GANs) to generate adversarially learned features that capture anomalies in the data. These learned features are then used to assess the abnormality of data samples based on their reconstruction errors. ALAD incorporates recent advancements in dataspace and latent-space cycle consistency, as well as GAN training stability, to significantly enhance the performance of anomaly detection. The researchers found that ALAD outperforms the sole publicly available GAN-based solution by a factor of a hundred on various image and tabular datasets. Additionally, ALAD demonstrates remarkable speed in anomaly detection. The proposed ALAD approach demonstrates the potential of utilizing bi-directional GANs and adversarially learned features to improve the accuracy and efficiency of anomaly detection. By leveraging reconstruction errors and incorporating advanced techniques, ALAD offers a promising solution for detecting anomalies in diverse datasets.

4.10. Hidden Markov Model (HMM)

In their work, Ref. [34] proposed an approach that utilizes a hidden Markov model (HMM) of privilege flows to detect anomalies. This approach was developed as a response to the limitations of misuse detection methods in intrusion detection, which rely on normal behavior patterns. By employing an HMM, which is a powerful tool for modeling sequential data, the proposed approach aims to reduce false-positive errors and increase detection

rates. However, one challenge with HMM-based intrusion detection is the time-consuming process of modeling normal behavior and analyzing intrusions, which hinders real-time detection. To address this issue, Ref. [34] present an efficient HMM-based intrusion detection system that analyzes privilege transition flows using attack domain knowledge. By incorporating this domain knowledge, the proposed system achieves improved performance while reducing the time required for intrusion detection. Experimental results demonstrate that the suggested technique outperforms the conventional method, which processes all data, in terms of both speed and detection quality. The proposed HMM-based approach offers a valuable solution for detecting anomalies in privilege flows, enabling faster and more accurate intrusion detection.

Ref. [35] employed Hidden Markov Model (HMM) in order to detect network intrusions that deviate from normal behavior. As cyberattacks grow increasingly sophisticated, it is crucial to have proactive measures in place to protect target systems. Existing defense products may struggle to establish correlations among diverse sensor data, which leaves vulnerabilities in the network environment. For instance, a compromised and undetected client with low security awareness could serve as a steppingstone for attackers to infiltrate the target system. Traditional signature-based intrusion detection systems may fail to identify such premeditated attacks. In the context of multi-phase assaults, a state-based categorization technique proves valuable. This study introduces a series of attack states that correspond to different stages of an attack and proposes a detection method based on Hidden Markov Model, which is a state-based classification model. By utilizing HMM, the system can effectively identify and classify sophisticated planned attacks. Experimental results have demonstrated the effectiveness of the proposed detection system in accurately detecting such intrusions.

Ref. [36] conducted research on Anomaly Detection Techniques using the Hidden Markov Model to identify unauthorized activities occurring on wired and wireless networks. While there are various intrusion detection algorithms available, it is necessary to develop additional reliable methods to effectively detect intrusions and minimize false-positive rates. In their study, Sukhwani et al. focused on exploring Anomaly Detection Techniques, with a particular emphasis on the Hidden Markov Model (HMM). The aim was to investigate and develop new approaches for accurately detecting intrusions and reducing the occurrence of false positives. The research aimed to contribute to the improvement of intrusion detection systems by enhancing the reliability and effectiveness of intrusion detection algorithms.

4.11. Swarm Intelligence

Swarm Optimization is a complex machine learning technique that utilizes the collective intelligence of a group of cooperative agents to solve problems through evolutionary computations. In the realm of intrusion detection, Ref. [37] explored the application of Swarm Intelligence (SI) approaches (2011). Their study involved a comprehensive analysis of various SI-based intrusion detection systems, examining their advantages and limitations. The researchers focused on developing supervised classification algorithms based on SI, with a particular emphasis on anomaly detection IDS. In SI-based IDS techniques, multiple agents collaborate and communicate with each other to address issues and find optimal solutions. In the context of abuse detection or anomaly detection clusters, agents can be deployed to determine classification criteria. The authors developed two groups of IDS, utilizing Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO) techniques: (i) a system for intrusion detection based on Particle Swarm Optimization (PSM), and (ii) a system for intrusion detection based on Ant Colony Clustering (ACC). The inspiration for ACO algorithms stemmed from the behavior of ants in seeking the shortest paths from their nest to food sources.

AntNag [38] introduced the first Ant Colony Optimization (ACO) technique for intrusion detection, utilizing directed graphs to model attacks. The collective movement dynamics observed in animal groups inspired the development of Particle Swarm Op-

timization (PSO) algorithms. The behavior of ants in gathering and sorting influenced the independent behavior of Ant Colony Clustering (ACC) algorithms. The authors also mentioned conducting a long-term study in their work. Swarm optimization offers several advantages, such as the adaptability of SI-based systems, allowing them to incorporate new data. Additionally, these systems are scalable since they utilize the same control architecture for a group of agents. They are also flexible, enabling the addition or removal of agents without necessitating changes to the overall architecture. However, SI-based systems also have some drawbacks: (i) The outcomes are unpredictable due to the intricacies of swarming. (ii) In a rich, hierarchical, swarm-based system, transitioning to states takes time. (iii) The system becomes redundant and uncontrolled as a result of the absence of centralized administration.

The Ant-based Replication and MApping Protocol (ARMAP) is another bio-inspired approach for anomaly detection [39]. ARMAP is based on a grid information system. It uses swarm intelligence through the collective efforts of ant-like agents. Data, particularly metadata are collected on grid resource characteristic. Using local interactions, it is possible to achieve swarm intelligence at the global level. One important advantage is that ARMAP enforces dissemination of descriptors through high Quality of Service (QoS) resources.

Swarm-based techniques such as ACO and PSO are important problem-solving techniques because they are based on decentralized coordination leveraging on collective intelligence. Swarm-based techniques also respond to dynamic environments and evolving data making them suitable for applications where conditions change rapidly [40]. Swarm-based techniques are becoming more important in emerging technologies like autonomous vehicles, and drone swarms where coordination and optimization are crucial.

5. Performance Measures

Here, we discuss various performance measures that are commonly used in machine language measurements. Table 2 depicts the metrics of overall performance measures.

Table 2. Metrics of Overall Performance Measures.

Metrics of Performance Measure	
Dice Similarity Coefficient (DSC)	$DSC = \frac{2TP}{2TP + FP + FN}$
Mathew Correlation Coefficient (MCC)	$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{((FP + TP)(TP + FN)(TN + FP)(TN + FN))}}$
True Positive Rate (Sensitivity)	$TPR = \frac{TP}{TP + FN}$
Specificity	$S = \frac{TN}{FP + TN}$
Positive Predictive Rate (Precision)	$Pre = \frac{TP}{TP + FP}$
Accuracy	$Acc = \frac{TP + TN}{TP + FN + FP + TN}$
F-Score	$Fsc = \frac{2TP}{2TP + FN + FP}$
Recall	$Rec = \frac{TP}{TP + FN}$
False Rejection Rate (FRR)	$FRR = \frac{FN}{TN + FN}$
False Acceptance Rate (FAR)	$FAR = \frac{FP}{FP + TN}$
Negative Predictive Rate (NPR)	$NPR = \frac{TN}{TN + FN}$

Figure 10 gives the percentages of malware detection based on the parameters, some of which are explained in Table 2, such as True Positive Rate (TPR), False Positive Rate (FPR), Accuracy (ACC), Others, Precision, F-Score, AUC, False Negative Rate (FNR), Testing Time, ROC Area, True Negative Rate (TNR), Error Rate (ER), CPU Execution Time, Precision Recall, Mean Absolute Error (MAE), Mean Squared Error (MSE), Equal Error Rate (EER), Processing Time (PT), and Training Time.

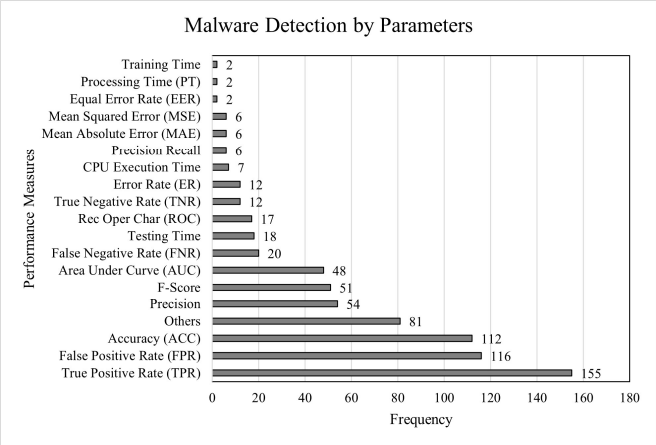

Figure 10. Percentage of malware detection based on the parameters.

6. Contribution

Based on this study, the contribution to knowledge is threefold: (i) an integration of machine learning for enhanced security, (ii) a comprehensive review of anomaly detection methods, and (iii) a bibliometric analysis, as explained in the following paragraphs.

The study contributes to the importance of robust security measures in an ever-changing digital world and emphasizes the inadequacy of traditional security systems. It also shows the importance of integrating secure systems with machine learning with resulting solutions that have improved accuracy, higher speed, and more effective anomaly detection.

The research presents a comprehensive and detailed review of various machine-learning-based on classification methods for anomaly detection over nearly two decades, spanning 2003 to 2022. This contribution provides a deep understanding of the different machine learning methods together with their strengths and weaknesses. Such information would be a ready source of comparative analysis of practical applicability available to other researchers.

Another contribution is in the bibliographic analyses used in the study. The literature was scoured across 10 renowned databases using a systematic search process based on Identification, Screening, Eligibility, and Inclusion criteria that filtered the search results successive by Keywords, then by Titles and then by Abstract. Such a search method provided research documents covering the publication landscape within the field of machine-learning-based anomaly detection.

7. Conclusions

In today's rapidly evolving world, the need for robust security measures is paramount. However, traditional security systems often prove inadequate, failing to deliver the desired levels of accuracy and efficiency. Consequently, these systems end up burdening organizations with time-consuming processes that hinder productivity. To overcome these pressing challenges, a ground-breaking approach has emerged, integrating secure systems with the power of machine learning. By harnessing the capabilities of machine learning, we have unlocked a new era of security solutions that offer unparalleled accuracy, speed, and effectiveness in analyzing anomalies at the system level. Researchers have tirelessly

explored various machine learning techniques to advance anomaly detection. These techniques encompass a wide array of methodologies, such as Naive Bayes, Support Vector Machine (SVM), k Nearest Neighbor (KNN), Artificial Neural Networks (ANN), Decision Tree, Random Forest, Fuzzy Logic, Genetic Algorithm, Generative Adversarial Network (GAN), Hidden Markov Model (HMM), and Swarm Intelligence. In this paper, we have undertaken an in-depth review of the machine-learning-based classification methods for anomaly detection that have been introduced by different researchers over the span of nearly two decades, from 2003 to 2022. By meticulously examining and analyzing these methods, we aimed to provide a comprehensive understanding of their strengths, limitations, and applicability in real-world scenarios. Moreover, we have gone beyond the confines of the study itself and delved into a bibliometric analysis. Leveraging data from the top 10 renowned databases, we have shed light on the publication landscape of this field. Remarkably, our analysis has revealed that Science Direct stands as the prominent platform for publications related to anomaly detection using machine learning techniques. The aim of this paper is to offer invaluable insights to fellow researchers who share a passion for exploring diverse models. We aspire to ignite their curiosity and inspire them to develop integrated models that push the boundaries of automated system-level anomaly detection. By fostering a deeper understanding of the research landscape and by presenting a comprehensive overview of cutting-edge methodologies, we aim to accelerate progress in this vital field of study.

Author Contributions: N.K.G., conducted the study and analysis and is the corresponding author. N.G., provided suggestions to the data analysis. D.C., provided the AWSCTD data and assistance in the data analysis. H.A.Č., provided suggestion on the structure for the analysis. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare that they have no conflict of interest either financially or non-financially.

References

1. Mengist, W.; Soromessa, T.; Legese, G. Method for conducting systematic literature review and meta-analysis for environmental science research. *MethodsX* **2020**, *7*, 100777. [CrossRef]
2. Zhen, R.; Jin, Y.; Hu, Q.; Shao, Z.; Nikitakos, N. Maritime Anomaly Detection within Coastal Waters Based on Vessel Trajectory Clustering and Naïve Bayes Classifier. *J. Navig.* **2017**, *70*, 648–670. [CrossRef]
3. Niranjan, M.; Saipreethy, M.S.; Kumar, T.G. An intelligent question answering conversational agent using Naïve Bayesian classifier. In Proceedings of the IEEE International Conference on Technology Enhanced Education, Amritapuri, India, 3–5 January 2012; pp. 1–5. [CrossRef]
4. Swarnkar, M.; Hubballi, N. OCPAD: One class Naive Bayes classifier for payload based anomaly detection. *Expert Syst. Appl.* **2016**, *64*, 330–339. [CrossRef]
5. Rabenoro, T.; Lacaille, J.; Cottrell, M.; Rossi, F. Anomaly detection based on aggregation of indicators. *arXiv* **2014**, arXiv:1407.0880.
6. Yao, Y.; Liang, S.; Li, X.; Chen, J.; Liu, S.; Jia, K.; Zhang, X.; Xiao, Z.; Fisher, J.B.; Mu, Q.; et al. Improving global terrestrial evapotranspiration estimation using support vector machine by integrating three process-based algorithms. *Agric. For. Meteorol.* **2017**, *242*, 55–74. [CrossRef]
7. Akpinar, K.; Ozcelik, I. Anomaly detection on EtherCAT based water level control automation. In Proceedings of the 2020 5th International Conference on Computer Science and Engineering (UBMK), Diyarbakir, Turkey, 9–11 September 2020; pp. 79–82.
8. Shon, T.; Kim, Y.; Lee, C.; Moon, J. A machine learning framework for network anomaly detection using SVM and GA. In Proceedings of the Sixth Annual IEEE SMC Information Assurance Workshop, West Point, NY, USA, 15–17 June 2005. [CrossRef]
9. Salem, A.; Mohsen, H.; El-Dahshan, E.; El-Horbaty, E. Brain tumor type classification based on support vector machine in magnetic resonance images. *Ann. "Dunarea De Jos" Univ. Galati Math. Phys. Theor. Mech. Fascicle II* **2017**, *40*, 75–88.

10. Tian, J.; Azarian, M.H.; Pecht, M. Anomaly detection using self-organizing maps-based k-nearest neighbor algorithm. In Proceedings of the PHM Society European Conference, Nabtes, France, 8–10 July 2014; p. 2.
11. Li, W. Using genetic algorithm for network intrusion detection. In Proceedings of the United States Department of Energy Cyber Security Group, Kansas City, KS, USA, January 2004; pp. 1–8.
12. Sarmadi, H.; Karamodin, A. A novel anomaly detection method based on adaptive Mahalanobis-squared distance and one-class kNN rule for structural health monitoring under environmental effects. *Mech. Syst. Signal Process.* **2019**, *140*, 106495. [CrossRef]
13. Ingre, B.; Yadav, A. Performance analysis of NSL-KDD dataset using ANN. In Proceedings of the 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, India, 2–3 January 2015; pp. 92–96.
14. Jadidi, Z.; Muthukkumarasamy, V.; Sithirasenan, E.; Sheikhan, M. Flow-based anomaly detection using neural network optimized with GSA algorithm. In Proceedings of the 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops, Philadelphia, PA, USA, 8–11 July 2013; pp. 76–81.
15. Koustubh, B.P.; Nair, V.V.; Kumaravel, S. Anomaly Detection in Hybrid Electric Vehicles Using ANN Based Support Vector Data Description. In Proceedings of the International Conference on Power, Energy, Control and Transmission Systems, Chennai, India, 22–23 February 2018; pp. 14–20. [CrossRef]
16. Jain, R.; Shah, H. An anomaly detection in smart cities modelled as a wireless sensor network. In Proceedings of the 2016 International Conference on Signal and Information Processing (IConSIP), Nanded, India, 6–8 October 2016; pp. 1–5.
17. Vargaftik, S.; Keslassy, I.; Orda, A.; Ben-Itzhak, Y. RADE: Resource-efficient supervised anomaly detection using decision tree-based ensemble methods. *Mach. Learn.* **2021**, *110*, 2835–2866. [CrossRef]
18. Lakshminarasimhan, N.; Subramanya, S.R. Computer viruses. *IEEE Potentials* **2001**, *20*, 16–19.
19. Yasami, Y.; Mozaffari, S.P. A novel unsupervised classification approach for network anomaly detection by k-means clustering and id3 decision tree learning methods. *J. Supercomput.* **2010**, *53*, 231–245. [CrossRef]
20. Primartha, R.; Tama, B.A. Anomaly detection using random forest: A performance revisited. In Proceedings of the 2017 International Conference on Data and Software Engineering (ICoDSE), Palembang, Indonesia, 1–2 November 2017; pp. 1–6.
21. Puggini, L.; Doyle, J.; McLoone, S. Fault Detection using Random Forest Similarity Distance. *IFAC-PapersOnLine* **2015**, *48*, 583–588. [CrossRef]
22. Prashanth, G.; Prashanth, V.; Jayashree, P.; Srinivasan, N. Using Random Forests for Network-based Anomaly detection at Active routers. In Proceedings of the 2008 International Conference on Signal Processing, Communications and Networking, Chennai, India, 4–6 January 2008; pp. 93–96. [CrossRef]
23. Yao, D.; Yin, M.; Luo, J.; Zhang, S. Network anomaly detection using random forests and entropy of traffic features. In Proceedings of the 2012 Fourth International Conference on Multimedia Information Networking and Security, Nanjing, China, 2–4 November 2012; pp. 926–929.
24. Usman, M.; Muthukkumarasamy, V.; Wu, X.-W. Mobile agent-based cross-layer anomaly detection in smart home sensor networks using fuzzy logic. *IEEE Trans. Consum. Electron.* **2015**, *61*, 197–205. [CrossRef]
25. Feizollah, A.; Shamshirband, S.; Anuar, N.B.; Salleh, R.; Kiah, M.L.M. Anomaly detection using cooperative fuzzy logic controller. In Proceedings of the Intelligent Robotics Systems: Inspiring the NEXT: 16th FIRA RoboWorld Congress, FIRA 2013, Kuala Lumpur, Malaysia, 24–29 August 2013; pp. 220–231.
26. Linda, O.; Manic, M.; Vollmer, T.; Wright, J. Fuzzy logic-based anomaly detection for embedded network security cyber sensor. In Proceedings of the 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), Paris, France, 12–13 April 2011; pp. 202–209.
27. Nakano, T.; Kourai, K. Secure Offloading of Intrusion Detection Systems from VMs with Intel SGX. In Proceedings of the 2021 IEEE 14th International Conference on Cloud Computing (CLOUD), Chicago, IL, USA, 5–10 September 2021; pp. 297–303. [CrossRef]
28. Hamamoto, A.H.; Carvalho, L.F.; Sampaio, L.D.H.; Abrão, T.; Proença, M.L. Network Anomaly Detection System using Genetic Algorithm and Fuzzy Logic. *Expert Syst. Appl.* **2018**, *92*, 390–402. [CrossRef]
29. Yang, Z.; Abbasi, I.; Mustafa, E.; Ali, S.; Zhang, M. An anomaly detection algorithm selection service for IoT stream data based on fresh tool and genetic algorithm. *Secur. Commun. Netw.* **2021**, *2021*, 1–10.
30. Benaicha, S.; Saoudi, L.; Guermeche, S.; Lounis, B. Intrusion detection system using genetic algorithm. In Proceedings of the 2014 Science and Information Conference, London, UK, 27–29 August 2014; pp. 564–568.
31. Ngo, P.C.; Winarto, A.A.; Kou, C.K.L.; Park, S.; Akram, F.; Lee, H.K. Fence GAN: Towards better anomaly detection. In Proceedings of the IEEE 31st International Conference on Tools with Artificial Intelligence, Portland, OR, USA, 4–6 November 2019; pp. 141–148.
32. Kim, J.; Jeong, K.; Choi, H.; Seo, K. GAN-based anomaly detection in imbalance problems. In Proceedings of the European Conference on Computer Vision, Glasgow, UK, 23–28 August 2019; pp. 128–145.
33. Zenati, H.; Romain, M.; Foo, C.; Lecouat, B.; Chandrasekhar, V. Adversarially Learned Anomaly Detection. In Proceedings of the 2018 IEEE International Conference on Data Mining (ICDM), Singapore, 17–20 November 2018; pp. 727–736.
34. Cho, S.-B.; Park, H.-J. Efficient anomaly detection by modeling privilege flows using hidden Markov model. *Comput. Secur.* **2003**, *22*, 45–55. [CrossRef]
35. Chen, C.M.; Guan, D.J.; Huang, Y.Z.; Ou, Y.H. Anomaly network intrusion detection using hidden Markov model. *Int. J. Innov. Comput. Inf. Control* **2016**, *12*, 569–580.

36. Sukhwani, H.; Sharma, V.; Sharma, S. A Survey of Anomaly Detection Techniques and Hidden Markov Model. *Int. J. Comput. Appl.* **2014**, *93*, 26–31. [CrossRef]
37. Kolias, C.; Kambourakis, G.; Maragoudakis, M. Swarm intelligence in intrusion detection: A survey. *Comput. Secur.* **2011**, *30*, 625–642. [CrossRef]
38. Abadi, M.; Jalili, S. An ant colony optimization algorithm for network vulnerability analysis. *Iran. J. Electr. Electron. Eng.* **2006**, *2*, 106–120.
39. Forestiero, A.; Mastroianni, C.; Spezzano, G. QoS-based dissemination of content in Grids. *Futur. Gener. Comput. Syst.* **2008**, *24*, 235–244. [CrossRef]
40. Franco, G.A.; Romero, A.H. Firefly algorithm for structural search. *J. Chem. Theory Comput.* **2016**, *12*, 3416–3428. [CrossRef] [PubMed]
41. Čeponis, D.; Goranin, N. Towards a Robust Method of Dataset Generation of Malicious Activity for Anomaly-Based HIDS Training and Presentation of AWSCTD Dataset. *Balt. J. Mod. Comput.* **2018**, *6*, 217–234. [CrossRef]
42. Liao, Q.; Stanczak, S. Network State Awareness and Proactive Anomaly Detection in Self-Organizing Networks. In Proceedings of the 2015 IEEE Globecom Workshops (GC Wkshps), San Diego, CA, USA, 6–10 December 2015; pp. 1–6. [CrossRef]
43. Wei, J.T.; Zhihong, Y.L.; Dong, L. A digital evidence fusion method in network forensics systems with Dempster-shafer theory. *China Commun.* **2014**, *11*, 91–97.
44. Su, M.Y. Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest-neighbor classifiers. *Expert Syst. Appl.* **2011**, *38*, 3492–3498. [CrossRef]
45. *IEEE Std 802.11-2016*; IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE: Washington, DC, USA, 2016; pp. 1–3534. [CrossRef]