Intrusion Detection System-Based Network Behavior Analysis: A Systemic Literature Review

Mohammed Janati[1], Fayçal Messaoudi[2]
National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, Fez, Morocco[1]
National School of Business and Management, Sidi Mohamed Ben Abdellah University, Fez, Morocco[2]

***Abstract*—An Intrusion Detection System (IDS) in cyberspace, as of now, plays primarily as a means of detecting illegal access and activity in a network. Due to the rapidly evolving cyber threats, the traditional signature-based IDS have started losing their effectiveness, leading to the emergence of advanced alternatives to these traditional technologies, such as Network Behavior Analysis (NBA). Unlike conventional signature-based systems, NBA monitors behavioral patterns for deviations and potential threats, which is a far more flexible and powerful way of detecting intrusion. While NBA-based IDS is a growing field of interest, the existing research in this area is mostly disoriented, mostly concentrating on single features like machine learning, deep learning algorithms, specific detection processes, or unique environments such as IoT and cloud systems. This systematic literature review (SLR) follows the guidelines proposed by Kitchenham to collect various studies, highlights research gaps, and provides an overview of the existing evidence. Spanning literature from January 2014 to April 2024, it comprehensively highlights the methods, datasets, types of detectable cyber-attacks, performance metrics, and the challenges that besiege existing NBA-based IDS. This shows the urgency for much more flexible and robust solutions, i.e., providing solutions through advanced Artificial Intelligence (AI) techniques in response to the increasing cyberspace complexities. Therefore, this review provides fundamental perspectives for researchers and practitioners and makes an important contribution towards stimulating future research efforts to design more effective and robust IDS solutions.**

Keywords*—*Artificial Intelligence (AI); deep learning; machine learning; cybersecurity; Intrusion Detection System; Network Behavior Analysis (NBA); Systematic Literature Review (SLR)

I. Introduction

In the context of cybersecurity frameworks, Intrusion Detection Systems (IDS) are essential for detecting unauthorized access and malicious activities aimed at networks. Historically, IDS development began with simple signature-based detection methods, which relied on matching known threat signatures to identify malicious activities [1]. Although effective for known threats, these traditional signature-based methods have significant limitations in classifying new and emerging cyber threats, particularly zero-day vulnerabilities, due to their dependency on predefined signatures [13].

In response to these limitations, Network Behavior Analysis (NBA) has gained prominence as an innovative alternative. NBA fundamentally differs from traditional approaches by monitoring and analyzing network traffic patterns rather than relying on known threat signatures. This behavior-oriented approach allows NBA to detect anomalies and unusual activities that signal potential threats, making it particularly effective against evolving threats that frequently change their characteristics and behaviors [2, 3]. Consequently, NBA-based IDS are uniquely capable of identifying sophisticated attacks, including insider threats and Advanced Persistent Threats (APTs), which traditional IDS may fail to detect [4].

Despite growing interest and numerous studies investigating NBA's integration within IDS, the research field remains fragmented, with a lack of comprehensive, integrated evaluations. The value-added of this paper lies precisely in addressing this fragmentation. Unlike previous studies, this Systematic Literature Review (SLR), guided by Kitchenham's systematic review methodology [5], systematically synthesizes a broad range of existing research from reputable databases such as Scopus and Clarivate Web of Science, covering a decade of recent developments from January 2014 to April 2024. This approach enables a more holistic and coherent overview of methodologies, datasets, detectable cyber-attacks, performance metrics, and existing challenges, clearly delineating areas that require deeper investigation.

Motivated by the growing inadequacies of traditional IDS in handling complex and evolving cyber threats, this study underscores the critical need for comprehensive re-evaluation and advancement of NBA techniques. By consolidating scattered research insights and clearly identifying gaps, this paper significantly advances the state-of-the-art understanding of NBA-based IDS. Consequently, it provides innovative insights for researchers and practitioners, uniquely contributing to developing more robust, adaptive, and efficient intrusion detection systems capable of effectively confronting emerging cybersecurity threats.

II. Related Work

For network security at scale, especially given the complexity of new systems, it is crucial to deploy Intrusion Detection Systems (IDS). Several review studies have investigated different techniques of IDS, among which are anomaly-based, signature-based, or hybrid detection approaches. However, very few of these reviews looked specifically at the new-generation IDSs that were based on Network Behavior Analysis (NBA)—the concept of detection in deviations from how network traffic normally behaves as a way of identifying possible security threats. The fact is that there is very little concentration on NBA-based IDSs in the extant literature, which serves as an important gap that needs to be addressed by this paper.

S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour [6] present a survey of IDS solutions for IoT environments, highlighting the necessity of a lightweight and scalable IDS. Though the findings of their work demonstrate the drawbacks in standard IDS techniques when applied to IoT networks, it is not centered on NBA-based IDS, which has its own specific advantages for the dynamic and heterogeneous nature of IoT traffic. In the same way, J. Kaur, A. Agrawal, and R. A. Khan [7] explained the security problems in fog computing environments that have many common constraints with IoT, whereas it has not been discussed how an NBA-based IDS could be utilized to tackle these scenarios more effectively using network behavior patterns to detect intrusions.

On the other hand, despite being denoted as a comprehensive review, M. Ozkan-Okay, R. Samet, O. Aslan, and D. Gupta [8] fail to fulfill all of the strictly required standards for being called a systematic literature review (SLR). It is a general claim, and it gives just some brief information about patent detection mechanisms for the NBA, but it cannot include this with detecting patents on an overall level. Given that no dedicated IDS concerning the NBA is available, a systematic review is still indispensable in this aspect.

O. H. Abdulganiyu, T. Ait Tchakoucht, and Y. K. Saheed [9] conducted a systematic review of the literature, following all the steps in a fully comprehensive manner: formulating a review protocol, searching and selecting studies systematically, extracting data carefully, and synthesizing it thoroughly. Nevertheless, even with the methodological rigor, their review is still very limited to a technical aspect of anomaly detection and provides no insight about the behavioral aspect. Though the analysis does provide an extensive summary of different IDS approaches, it does not concentrate on discussing how network behavior analysis (NBA) can be used to extend detection functionalities. This is quite a major shortcoming of their investigation, as NBA-based solutions are crucial for spotting APTs that the old legacy technology cannot detect.

Finally, existing literature gains important insights into the overall landscape of IDS research, yet no systematic reviews were found that primarily targeted NBA-based IDS. This void is particularly important, as NBA-based IDS have the capability to fill in the gaps that earlier versions of IDS have been unable to identify on innovative and advanced threats. The objective of this article is to address this need by performing a structured systematic literature review (SLR) to systematically assess the NBA-based IDS methodologies critically, find some deficiencies in these studies, and suggest future research directions. This research work, therefore, aims to better appreciate the ability of NBA-based IDS in improving network security in various environments by concentrating on network behavior analysis.

III. Methodology

A. Method of Reviewing

In conducting a literature review on IDS, particularly regarding behavior analysis, a systematic literature review (SLR) is conducted following Kitchenham's [5] guidelines, which consist of three main stages: planning, conducting, and reporting.

B. Research Questions

In a systematic literature review (SLR), the research question is of paramount importance. It serves as the foundation for the entire study and guides every subsequent step of the research process. This SLR investigates the following research questions:

- RQ1: What methods and techniques are commonly employed in network behavior analysis-based intrusion detection systems?
- RQ2: Which datasets are predominantly used for testing and training network behavior analysis-based intrusion detection system?
- RQ3: What types of cyberattacks are detectable by the current network behavior analysis-based intrusion detection system?
- RQ4: Which performance metrics are most commonly used to evaluate the effectiveness of a network behavior analysis-based intrusion detection system?
- RQ5: What are the common challenges and limitations faced by intrusion detection systems using network behavior analysis-based intrusion detection systems?

C. Search Strategy

The process of constructing search terms in systematic literature reviews (SLRs), as discussed in [5], involves several steps. This includes breaking down each question into key concepts, identifying synonyms and related terms, and combining them with Boolean operators.

D. Search Process

The study refers to two of the most recognized academic databases (Scopus and Clarivate's Web of Science) for collecting relevant references that facilitate an analysis. Table I provides search queries for the data retrieval from both databases, which were developed with a view to capturing relevant research articles on the topic of study.

By executing the given queries in Scopus and Web of Science, 468 papers were captured. These papers are used as the main data discovery, which ensures a well-rounded basis for answering this study's research questions. The choice course guaranteed that the papers replicate high-quality and relevant publications from both significant databases, which greatly helps in increasing the trustworthiness of the research findings.

E. Study Selection

We applied both inclusion and exclusion criteria to select the primary studies. The inclusion and exclusion criteria are as follows:

Inclusion Criteria:

- Study Focus: Studies that specifically focus on methods, techniques, and datasets used in intrusion detection.
- Systems use either Network Behavior Analysis or Behavior Analysis.
- Relevance to Questions: Articles that address at least one of the specific research questions listed above.

- Type of Publication: Peer-reviewed journal articles, conference proceedings, chapters of books, and comprehensive reviews.
- Recent Publications: Studies published within the last 10 years to ensure relevance to current technologies.
- Language: Studies published in English to ensure comprehensibility and accessibility.

Exclusion Criteria:

- Beyond Scope: Studies that do not focus on intrusion detection systems or network behavior analysis, such as general cybersecurity or other types of network monitoring unrelated to security.
- Preliminary Reports: Short communications, abstracts, posters, and presentations that do not provide.
- Comprehensive analysis or findings.
- Non-English Publications: Articles not available in English, unless significant findings are relevant and no.
- English studies are available.
- Non-Peer Reviewed Material: Grey literature, editorials, opinion pieces, and non-peer-reviewed articles.
- Unless they provide crucial insights or data not available in peer-reviewed sources.
- Outdated Research: Studies that were conducted more than 10 years ago unless they are seminal works.
- Finally, after filtering for full-text availability, only 32 papers were found to be relevant and address issues related to the NBA-based IDS, as shown in Fig. 1.

F. Data Extraction

Data was extracted to answer the research questions from the primary studies in an iterative manner to address data issues. For this purpose, the extraction addressed these five main properties: (a) NBA-based IDS methods and techniques (to answer RQ1), (b) NBA-based IDS datasets (to answer RQ2), (c) types of cyberattacks are detectable by NBA-based IDS (to answer RQ3), (d) performance metrics to evaluate the effectiveness of NBA-based IDS (to answer RQ4), and (e) common challenges and limitations faced by NBA-based IDS (to answer RQ5).

G. Study Quality Assessement and Data Synthesis

In addition, assessment of the quality of studies is required to ensure an adequate interpretation of synthesis findings and confirm conclusions [5]. The purpose of the data synthesis is to address all research questions. Finally, we tabulated the data according to individual research questions and presented it in pie charts, bar charts, or tables.

H. Threats to Validity

Threats to the validity of this review exist. These are conditioned by the fact that papers were not searched for manually by reading the title of each eligible journal paper. Therefore, this study may have missed a few papers during its filtering process.

TABLE I. RESEARCH QUESTIONS AND RELATED SEARCH STRATEGIES

Research question	Key concepts	Synonyms and Related Terms	Search String
RQ1: What methods and techniques are commonly employed in Intrusion Detection Systems using Network Behavior Analysis?	• Methods • Techniques • Network Behavior Analysis • Intrusion Detection Systems	• Methods: approaches, strategies, algorithms • Techniques: tactics, methodologies • Network Behavior Analysis: NBA, network monitoring, behavioral detection • Intrusion Detection Systems: IDS, network security systems	("methods" OR "techniques" OR "approaches" OR "strategies" OR "algorithms") AND ("Network Behavior Analysis" OR "NBA" OR "network monitoring" OR "behavioral detection "OR" Behavior-based") AND ("Intrusion Detection Systems" OR "IDS" OR "network security systems")
RQ2: Which datasets are predominantly used for testing and training Intrusion Detection Systems using Network Behavior Analysis?	• Datasets • Testing • Training • Network Behavior Analysis • Intrusion Detection Systems	• Datasets: data sets, benchmark data, sample data • Testing: evaluation, assessment • Training: learning, development	("dataset" OR "data sets" OR "benchmark data" OR "sample data") AND ("Network Behavior Analysis" OR "NBA") AND ("Intrusion Detection Systems" OR "IDS")
RQ3: What types of cyber-attacks are detectable by current Intrusion Detection Systems using Network Behavior Analysis?	• Cyber-attacks • Detectable • Network Behavior Analysis • Intrusion Detection Systems	• Cyber-attacks: network attacks, security breaches, malware, hacking • Detectable: identifiable, recognizable	("cyber-attacks" OR "network attacks" OR "security breaches" OR "malware" OR "hacking") AND ("Network Behavior Analysis" OR "NBA") AND ("Intrusion Detection Systems" OR "IDS")
RQ4: Which performance metrics are most commonly used to evaluate the effectiveness of Intrusion Detection Systems using Network Behavior Analysis?	• Performance metrics • Evaluate • Effectiveness • Network Behavior Analysis • Intrusion Detection Systems	• Performance metrics: evaluation metrics, performance indicators • Evaluate: assess, measure	("performance metrics" OR "evaluate" OR "assess" OR "measure" OR "effectiveness") AND ("Network Behavior Analysis" OR "NBA") AND ("Intrusion Detection Systems" OR "IDS")
RQ5: What are the common challenges and limitations faced by Intrusion Detection Systems using Network Behavior Analysis in detecting sophisticated cyber threats?	• Challenges • Limitations • Network Behavior Analysis • Intrusion Detection Systems • Sophisticated cyber threats	• Challenges: issues, problems • Limitations: constraints, shortcomings • Sophisticated cyber threats: advanced threats, complex threats	("sophisticated cyber threats" OR "advanced threats" OR "complex threats" OR "challenges" OR "issues" OR "problems" OR "limitations" OR "constraints" OR "shortcomings") AND ("Network Behavior Analysis" OR "NBA") AND ("Intrusion Detection Systems" OR "IDS")

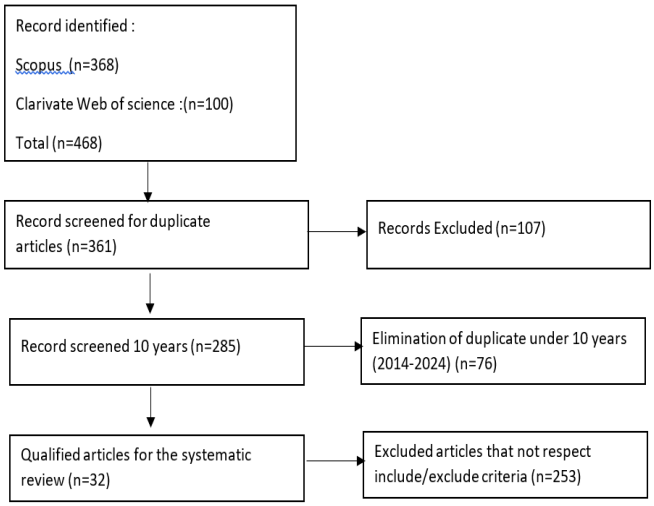

Fig. 1. Study selection flowchart.

IV. Research Result

A. RQ1: Methods and Techniques for NBA-Based IDS

Intrusion Detection Systems (IDS) based on Network Behavior Analysis (NBA) employ various methods and techniques to effectively identify and mitigate security threats. Feature Engineering (FE) and Supervised Machine Learning, including Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Random Forest (RF), Gradient Boosting (GB), and Naive Bayes (NB), along with Logistic Regression (LR), are key techniques for behavior-based IDS to detect intranet attacks, reconnaissance, and post-stage attacks through network traffic classification and prediction [4].

Another approach is the Subtractive Center Behavior Model (SCBM), applied with machine learning techniques like Random Forest, J48, and Logistic Model Trees (LMT) to focus on system call analysis and detect malware like ransomware, Trojans, and rootkits by analyzing behavioral patterns [10]. Similarly, behavior-based detection combined with dynamic analysis using the Virtual Machine Introspection (VMI) technique is used to detect evolving malware. Random Forest, LMT, C4.5, SLR, SMO, and KNN improve detection accuracy in cloud environments [11].

SQL Query Abstraction and Behavior-Based Anomaly Detection systems utilize context-centric Hybrid Techniques and Concolic Testing to identify insider threats, SQL injections, and masquerader attacks in database intrusion detection [12]. For large-scale network environments, deep learning techniques such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and autoencoders, combined with Principal Component Analysis (PCA), help reduce data dimensions and improve the detection of DoS, DDoS, and brute force attacks [13].

Ensemble learning techniques, including decision trees, random forests, and neural networks, along with data augmentation methods like ADASYN, balance datasets and enhance botnet and infiltration attack detection [14]. Bio-inspired algorithms like CLONALG, Learning Vector Quantization (LVQ), and Multilayer Perceptrons (MLP) are also used for behavior-based detection, particularly for DoS and DDoS attacks, with the Majority Voting Strategy improving accuracy [15].

Cloud-based intrusion detection systems often use PCA and NBA combined with Genetic Algorithms (GA) to reduce false positives and detect User-to-Root (U2R) and Remote-to-Local (R2L) attacks [16]. Time series analysis techniques, including Lyapunov's exponent and chaos theory, model network traffic behavior to identify botnets and advanced evasion techniques [17].

Multi-stage attacks like Eternal Blue are predicted using Hidden Markov Models (HMM) supported by the Baum-Welch and Forward-Backward Algorithms, which analyze network behavior over time [18].

Anomaly-based detection methods using SVM are widely applied in mobile ad hoc networks (MANETs), detecting attacks like blackhole, grayhole, wormhole, and flooding through normalization, discretization, and feature selection [20]. Advanced methods like Extreme Learning Machines (ELM) with Prefix Trees, Hierarchical Heavy Hitters (HHH), and Probability Space Mapping are used to detect DDoS, SQL Injection, and Cross-Site Scripting (XSS) attacks, reducing false positives [21].

Aggregation Measure and Logistic Regression are often used to model user behavior and detect abnormal or unauthorized access [24]. Recursive Feature Elimination (RFE), along with feature selection and dimensionality reduction, optimizes machine learning models for detecting complex network threats [3].

Cognitive cybersecurity models leverage Symbolic Deep Learning (SDL), Model Tracing, and Reinforcement Learning to predict attacker behavior, using expert analyst data to enhance cybersecurity defenses [27]. The Capturing-the-Invisible (CTI) Algorithm, designed for IoT-centric Industrial Control Systems (ICS), applies process mining and event log analysis to detect flooding and injection attacks [22]. Abnormal behavioral pattern detection systems in closed-loop environments use multi-level information analysis and similarity metrics to detect zero-day deceptive threats [26].

Deep learning models such as ResNet and Bidirectional RNN, combined with attention layers and time-series pattern detection, are used to detect network anomalies and masquerading users; this method is named the superior behavior-based anomaly detection system (SuperB) [28]. Snort Rule Extension, FP-Growth Association Analysis, and Data Mining help detect advanced persistent threats (APTs) [29]. Adaptive Trust Management Schemes and Outlier Detection in dynamic networks help detect on-off and zero-day attacks [30].

Immunity-Inspired Algorithms, including Artificial Immune System (AIS) and Behavioral-Scripted Event-Schema (BSES), are used for behavior-based anomaly detection in IoT systems [31]. Particle Swarm Optimization (PSO) and K-Means Clustering, along with behavior analysis models like ActBehavior and FailBehavior, help detect botnets in network traffic [32]. NBA, combined with statistical and behavioral analysis, detects obfuscated attacks in HTTPS traffic using naive Bayes classification [33] (Table II).

TABLE II. COMPARATIVE ANALYSIS OF CYBERSECURITY THREAT DETECTION METHODS: TECHNIQUES, GOALS, AND SUCCESS RATES (2015-2024)

Paper	Proposed Method	Goal/Success	Year
[4]	Feature Engineering (FE) & Supervised Machine Learning (SVM, KNN, RF, GB, NB, LR)	Detection of intranet attacks, reconnaissance, and post-stage attacks	2024
[10]	Subtractive Center Behavior Model (SCBM) + Machine Learning (Random Forest, J48, LMT)	Malware detection (ransomware, Trojans, rootkits) through system call analysis	2023
[11]	Behavior-Based Detection + Dynamic Analysis (Random Forest, LMT, C4.5, SLR, SMO, KNN)	Malware detection and accuracy enhancement in cloud environments	2023
[12]	SQL Query Abstraction & Behavior-Based Anomaly Detection	Detection of insider threats, SQL injections, masquerader attacks	2022
[13]	Deep Learning (CNN, LSTM, Autoencoders) + PCA	Detection of DoS, DDoS, Brute Force attacks	2022
[14]	Ensemble Learning (Decision Trees, RF, Neural Networks) + ADASYN	Improved detection of botnet and infiltration attacks	2022
[15]	Bio-Inspired Algorithms (CLONALG, LVQ, MLP)	Detection of DoS and DDoS attacks with enhanced accuracy	2021
[16]	PCA + NBA + Genetic Algorithms (GA)	Reduction of false positives and detection of U2R and R2L attacks	2021
[17]	Abnormal Behavioral Pattern Detection + Multi-Level Information Analysis,Time Series Analysis + Lyapunov's Exponent & Chaos Theory	Detection of zero-day deceptive threats, Botnet detection and advanced evasion technique identification	2021
[18]	Hidden Markov Models (HMM) + Baum-Welch & Forward-Backward	Prediction of multi-stage attacks like Eternal Blue,	2021
[22]	Algorithms, Capturing-the-Invisible (CTI) Algorithm + Process Mining	Detection of flooding and injection attacks in ICS	2020
[23]	RUBRA + Weighted Sequential Pattern Mining & Temporal Analysis	Detection of SQL injection, Detection of malicious insider transactions and threats	2020
[26]	Multi-Layered Behavior-Based IDS + Ensemble Learning & Data Augmentation	Detection of DDoS and Botnet attacks with imbalanced datasets	2020
[27]	Cognitive Cybersecurity Models (SDL, Model Tracing, Reinforcement Learning)	Prediction of attacker behavior to improve defense strategies	2020
[28]	Deep Learning Models (ResNet, Bidirectional RNN) + Attention Layers	Detection of network anomalies and masquerading users	2020
[20]	Anomaly-Based Detection (SVM)	Detection of MANETs attacks (Blackhole, Grayhole, Wormhole, Flooding)	2019
[30]	Adaptive Thresholding & Outlier Detection, v	Zero-day and on-off attack detection in dynamic networks	2019
[24]	Aggregation Measure & Logistic Regression	Detection of abnormal activities and unauthorized access	2019
[29]	Snort Rule Extension + FP-Growth Association Analysis	Detection of advanced persistent threats (APTs)	2019
[3]	Behavior-based Network Intrusion Detection (BNID)	Detect the intrusions	2018
[19]	Sonification Techniques (SoNSTAR)	Real-time detection of botnet activities, DDoS, phishing	2018
[21]	Extreme Learning Machines (ELM) + Prefix Trees, HHH, Probability Space Mapping	Detection of DDoS, SQL Injection, Cross-Site Scripting (XSS) attacks with reduced false positives	2018
[31]	Immunity-Inspired Algorithms (AIS, BSES)	Behavior-based anomaly detection in IoT systems	2016
[25]	Hybrid Intrusion Detection Systems (Anomaly & Signature-Based), DTrojan Model + Bayes Classification + Traffic Detection	Enhanced protection against known and unknown threats,Detection of malware (Trojans, spyware)	2015
[32]	Particle Swarm Optimization (PSO) + K-Means Clustering + Behavior Analysis (ActBehavior, FailBehavior)	Botnet detection in network traffic	2015
[33]	Network Behavior Analysis (NBA) + Statistical & Behavioral Analysis	Detection of obfuscated attacks in HTTPS traffic using Naive Bayes	2015

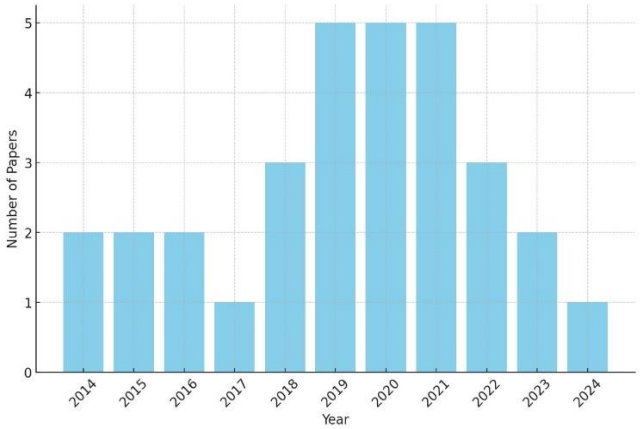

Fig. 2. Distribution of cybersecurity research papers over time (2014-2024).

Finally, techniques like the DTrojan Model, Bayes Classification, and Traffic Detection are used to detect malware, including Trojans and spyware, by analyzing network behavior [25]. Role and User Behavior-Based Risk Assessment (RUBRA), combined with Weighted Sequential Pattern Mining and Temporal Analysis, detects malicious insider transactions and threats in database systems [23]. Additionally, Sonification Techniques, as used in the SoNSTAR system, convert network traffic into auditory signals for real-time botnet detection [19]. Fig. 2 shows the distribution of cybersecurity research papers over time.

B. RQ2: Dataset Used for NBA-Based IDS

The task of training algorithms for NBA-based IDS necessitates vast and varied datasets. These datasets help bring about the accuracy and reliability of IDS models by recording attack incidents and other benign traffic in a realistic environment. One of the more often used datasets, the CIC-IDS2017[15], also has labeled network traffic data in a range of different types of attacks, like DDoS, brute force attacks, botnet activity, and infiltration. It has been a widely used dataset in the Behavior-Based Intrusion Detection System for machine learning model training.

CSE-CIC-IDS2018 is another well-known dataset, which covers a wide array of attack categories, including DoS, DDoS, brute force, and web-based attacks. It is preferred in the deep learning-based IDS applications due to its detailed attack patterns and large labeling. CSE-CIC-IDS2018 [13] is another well-known dataset, which covers a wide array of attack categories, including DoS, DDoS, brute force, and web-based attacks. It is preferred in the deep learning-based IDS applications due to its detailed attack patterns and large labeling.

Another classic dataset for the evaluation of machine learning and deep learning models is the NSL-KDD dataset [34], which is an improved version of the older KDD 99. One of the most common attack types is control tests; this includes DOS (Denial of Service), R2L (Remote-to-Local), U2R (User-to-Root), and probe-type testing, making this essential for anomaly detection system testing.

Despite being outdated, the KDD-Cup 1999 dataset [16] remains to be used in IDS research, as it is a large collection of simulated network traffic with labels for DoS, probing, and R2L attacks. It establishes a base to benchmark new models over the legacy datasets.

ISCX IDS 2012 for HTTP-based DoS, DDoS attacks, and botnet activities; normal and abnormal network traffic [21]. It is because of the fully provided traffic scenario-based simulation that this dataset is generally used to evaluate anomaly-based detection techniques like Extreme Learning Machines (ELM).

The CTU-Malware-Capture-Botnet-254-1 dataset [17] is popular for botnet detection due to the fact that it includes legitimate network traffic taken from a real-world, business-class network trace with malware and botnet infection. Thus, this dataset is also indispensable for benchmarking behavior-based IDS, which are aimed at detecting botnets with behaviors within network traffic.

Conventionally, malware detection systems utilize the artifacts observed, such as IRP hooking and the sticky keys backdoor persistence method, to detect ransomware while drawing corpus samples from malware repositories such as MalwareBazaar and VirusShare, which contain a diverse range of malware, including ransomware samples with other related differences [11]. These repositories are critical for the training of dynamic analysis-based IDS that identify malware behaviors in real-time.

These datasets were generated from Siemens S7-1200 and National Instruments NI-cRIO-9074 to assess IDS in IoT environments. These datasets are used when identifying anomalies in Industrial Control Systems (ICS) networks, particularly for injection and flooding attacks, targeting a vulnerable environment [22]. Cloud-based IDS evaluations can use the ITOC Attack Dataset [3], which simulates different types of flooding and DDoS attacks on cloud infrastructure. This dataset is essential for evaluating cloud-based Intrusion Detection Systems and solving these challenges unique to the cloud.

The University of Rhode Island Network Flows (2014) dataset is employed to evaluate the adaptive thresholding and outlier detection methods for academic networks. It belongs to a dataset of real-world traffic in educational environments and is built with the aim of simulating on-off and zero-day attack detection [30]. The datasets that are mainly utilized for testing and training the IDS on NBA cover a wide range of attack types, such as DoS, DDoS, brute force, malware, and botnets.

The most popular datasets include CIC-IDS2017, CSE-CIC-IDS2018, NSL-KDD, KDD-Cup 1999, and ISCX IDS 2012, all of which are significantly important to improve the performance of machine learning-based and deep learning-based IDS. These datasets provide a rich set of attack profiles along with legitimate traffic needed for reliable detection and classification (Table III).

TABLE III. COMPARATIVE ANALYSIS OF CYBERSECURITY INTRUSION DETECTION DATASETS: FEATURES, ATTACK TYPES, AND DATA CHARACTERISTICS

Number	Dataset Name	Year	Features	Attack Types	Labeled/ Unlabeled	Number of Instances
1	KDD-CUP	1999	41	DoS, R2L, U2R, Probing	Labeled	4,898,431
2	NSL-KDD	2009	41	DoS, R2L, U2R, Probing	Labeled	148,517
3	ISCX IDS 2012	2012	25	DoS, DDoS, SSH brute force, and HTTP DoS	Labeled	2,540,044
4	CICIDS2017	2017	80	DoS, DDoS, Brute Force, Heartbleed, Botnet, Web Attacks	Labeled	Varies
5	CTU-13	2011	Varies	Botnet	Labeled	Varies

C. RQ3 Cyber-Attacks Detectable by NBA-Based IDS

Network behavior analysis-based IDS excel in identifying a wide range of cyberattacks due to their extensive operational scope. Attacks like Denial of Service (DoS), Distributed Denial of Service (DDoS) attacks, Bot, FTP-patator, Heartbleed, Infiltration, Portscan, SSH-patator, and Web Attack, can be detected using ensemble learning techniques [14]. Along with nature-inspired algorithms like CLONALG to detect these attacks. GoldenEye, Slowloris, SlowHTTPTest, Hulk, HOIC, and LOIC-UDP are a few of the many DoS and DDoS tools used to perform such attacks [15].

When IDS detects bot-like behavior in the network traffic pattern, it can also detect botnet attacks [19]. In order to identify botnets, many methods have been developed for training them using datasets like CTU-Malware-Capture-Botnet-254-1 and ISCX IDS 2012 [17].

Insider threats, when someone within the company begins to act oddly, are also something that can be tracked by monitoring unusual behavior. Methods such as weighted sequential pattern mining and risk assessment are used to discover these risks [23].

APTs are more cumbersome; however, IDSs using NBA can also be effective at identifying them. These systems have a longer-term focus with more advanced capabilities and frequently escape detection by traditional methods. IDS-based NBA can help organizations spot such threats hiding in encrypted traffic, incorporating features such as Snort Rule Extension and FP-Growth Association Analysis [29]. They are skilled at spotting those attacks where hackers attempt unauthorized access, like User-to-Root (U2R) or Remote-to-Local (R2L). Attack trees are targeted toward the NBA-based hybrid cloud intrusion detection system, and Principal Component Analysis (PCA) captures these attacks [16].

The NBA-based IDS are also very useful for malware detection. Similar to the previous examples, use machine-learning algorithms in addition to dynamic analysis but for known malware only, as well as run a classification over different types of malware (e.g., ransomware, rootkits at the kernel level) [11].

These systems can also intercept injection attacks in the form of flooding in IoT environments. Process mining and event log analysis create a vision of what is going on in the industrial areas where this kind of attack is most common, observing network traffic to gain insight [22]. Finally, NBA-based IDS can also find more intricate attacks, such as multi-stage ones (for example, the one using Eternal Blue). Hidden Markov Models (HMM) and sequential analysis are some of the methodologies used to catch these complex attacks [18].

In summary, NBA-based IDS are highly capable of detecting a variety of cyber-attacks, from DoS and DDoS to brute force, botnets, SQL injection, insider threats, and APTs up through multi-stage attack types. They notice not only already existing threats but also emerging ones (though they cannot always avoid mistakes of the past and occasionally presume new unlawful actions). The distribution of the occurrence of attack types in papers presented in this study is shown in the chart in Fig. 3.

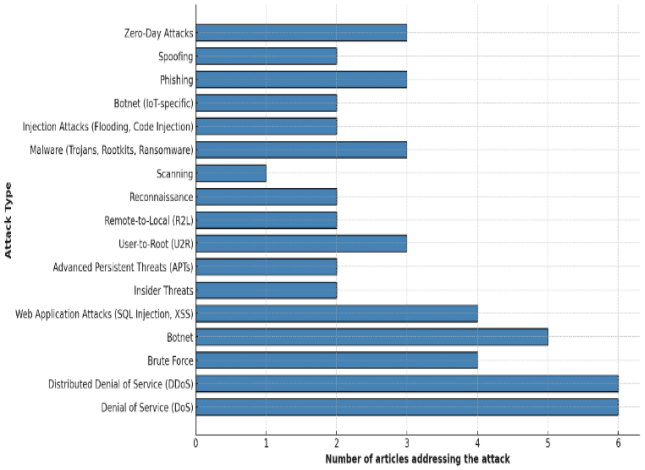

Fig. 3. Frequency of cybersecurity research articles addressing various attack types.

D. RQ4: Metrics Commonly Used to Evaluate the Effectiveness of NBA-Based IDS

Evaluating the effectiveness of Network Behavior Analysis-based Intrusion Detection Systems requires various performance metrics to determine the capability of IDS as a defense system for identifying and preventing cyber threats. These metrics include accuracy, precision, recall, F1-score, false positive rate (FPR), true positive rate (TPR), detection rate, area under the curve (AUC), time complexity, detection time, confusion matrix, and fitness value (PSO).

One of the fundamental metrics to evaluate what percentage of benign and malicious traffic was identified is accuracy. The metric has been commonly used in the field of measuring the performance of machine learning models for classifying different types of cyberattacks, where it was evaluated for detection behavior-based intranet attacks using machine learning techniques [4].

The precision measures the proportion of detections that were true positives (how well does an IDS do in correctly identifying threats without tagging too many benign activities as malign). This is particularly important for a malware detection system since ‘false alarms are common’ [11].

Recall, or True Positive Rate (TPR)—The proportion of actual threats that were correctly identified by the system. It is an important metric that helps to prevent IDS from missing potential security attacks. J. K. Samuel, M. T. Jacob, M. Roy, S. P M, and A. R. Joy [11] demonstrated the significance of high recall rates for discerning advanced malware within cloud computing solutions.

This is especially useful for the F1-score, which is ideal in systems where there is a cost associated with both false positives and false negatives. This gives a unique metric on how good the system is at separating malicious and benign traffic. M. Antunes et al. [13] evaluated deep learning-based intrusion detection systems using the F1-score.

The most important Achilles heel of these systems operating in real-time environments is the False Positive Rate (FPR), which tells you how many times an IDS incorrectly classifies

benign traffic as malicious. Yet high FPRs swamp security teams with alerts that cannot be responded to in a timely manner and make the entire detection system less efficient. This was targeted by M. Debashi and P. Vickers [19] in their botnet detection system, where they used a sonification technique to reduce false positives.

The True Positive Rate (TPR), also called Sensitivity, measures the success of the IDS to detect actual attacks. It helps in ensuring that the system detects various threats and supports both known and unknown attacks and sophisticated attacks. P. Ferreira and M. Antunes [15] utilized this to access bio-inspired algorithms to identify DDoS attacks.

Another important metric is the detection rate: the percentage of detected attacks across all the total attacks. This metric illustrates how well an IDS functions (in general). M. Nazari, Z. Dahmardeh, and S. Aliabady [17] argued that this was a critical property when studying botnet detection.

The receiver operating characteristic (ROC) curve is a plot of false positives against true positives; the area under this figure, abbreviated as AUC, is often used to assess the trade-offs. This is a rough gauge of how the system itself works, primarily around benign and malicious traffic. V. Agate et al. [15] looked over ensemble learning-based IDS with AUC.

The two important parameters in real-time systems are time complexity and detection time, as it is required to respond to an active attack as soon as possible. An IDS needs to be able to reliably scan significant amounts of traffic without sacrificing accuracy in order to function. Y. Cui, J. Xue, Y. Wang, Z. Liu, and J. Zhang [29] have stressed the need for lower time complexity in various advanced persistent threat (APT) detection mechanisms.

One of the other essential tools to examine IDS performance is the confusion matrix, which shows the relationships between true positives, true negatives, false positives, and false negatives. Check out its detailed assessment of the ability of the IDS to differentiate between various genres of traffic. Z. S. Malek et al. [25] used a confusion matrix to design a user behavior-based intrusion detection system in their research.

Fitness Value (PSO), a performance metric, is a measure of how well a system is performing. This includes measuring how close the algorithm has converged to an optimal method to detect attacks such as botnets. S.-H. Li et al. [33] used the fitness value in their network behavior-based botnet detection system.

Finally, the evaluation of network behavior analysis-based IDS modules is typically done with a combination of accuracy, precision, recall, F1-score, false positive rate (FP), true positive rate (TP), detection rate, area under the ROC curve (AUC), time complexity, detection time, confusion matrix, and fitness value. Each of these metrics is required to provide the most accurate evaluation while using an IDS to detect, classify, and respond (where suitable) to cyber threats.

E. RQ5: Common Challenges and Limitations Faced by NBA-Based IDS

An Intrusion Detection System (IDS) that is based on network behavior analysis faces some major challenges, and they do suffer many limitations, which in turn diminish the system's performance, leading to poor detection of advanced cyber-attacks. Most of these problems stem from the dynamic evolution of cyberthreats and the overall complexity of current network technologies, as well as the technical overhead that goes hand in hand with cutting-edge deep learning and machine learning algorithms.

One of the main challenges is a high false positive rate for behavior-based IDS, which makes them less effective. Behavior-based IDS produce false positives when benign activities are misclassified as malicious; thus, they generate alerts and require further investigation. This is less of a problem when neural networks are fine-tuned to the network environment, because overfitting can lead to false alarms with machine learning models. An example of such a limitation is shown by Jang and Lee [4] on greeting fall detection systems, wherein overfitting resulted in extremely high false positives while detecting in the real-time environment. While work such as V. Pai, A. S. Rao, Devidas, and B. Prapthi [10] is applied to creating systems that prioritize detecting malware variants using machine learning, part of dealing with this struggle arises from the similar complexity in determining benign vs. malicious behaviors.

One other downside is the balance of data sets, as related to the number of benign traffic known when compared to that attributed to attack, which embarks on quite an unfavorable incentive for machine learning algorithms, which will have a hard time figuring out attacks. This skew greatly hurts the detection capability, especially for rare and more damaging types of attacks. M. Antunes et al. [13] found that the asymmetrical attack dataset used in their study on deep learning methods for network intrusion detection posed challenges due to the skewed distribution of different types of intrusions, which made it difficult for the system to accurately detect anomalies.

Zero-day attacks are also a significant constraint in network behavior analysis-based IDS detection. Zero-day attacks, by which vulnerabilities are exploited that have yet to be patched, are especially difficult to detect due to their distinct behavior patterns. Due to the nature of behavior-based IDS, they will only be able to detect attacks that deviate from the behavior norms and would not be able to recognize entirely new or fundamentally different attack vectors. V. Agate et al. [14] pointed out that the ensemble learning methods were inefficient in identifying zero-day attacks, especially when there are no specific patterns in the training data. P. Ferreira and M. Antunes [15] also found bio-inspired algorithms to be inefficient for tackling novel threats in another study.

Another major challenge is high computational costs. In some IDS systems, which are mainly based on machine/deep learning models, data needs to be preprocessed and features need to be extracted, and then training the model accordingly requires a very high computational resource. However, this requirement incurs a computational burden, which can hinder scalability and render IDS unusable in large-scale or resource-constrained environments. For instance, Y. Cui, J. Xue, Y. Wang, Z. Liu, and J. Zhang [29] explained the high resource usage of Snort Rule Extensions for APTs (Advanced Persistent Threats) detection that was not near real-time. Similarly, J. K. Samuel, M. T. Jacob, M. Roy, S. P. M., and A. R. Joy [11]

observed that performing a dynamic analysis to identify zero-day malware in the cloud environment drained computational resources.

Another major drawback is low real-time detectability. As network traffic gets bigger and more organized, the attacks to inflict get more elaborate: IDS needs to process data easily without making mistakes. But many of the ML algorithms are afflicted with long-run time complexity, which prevents them from performing in real-time traffic analysis. Y. Cui, J. Xue, Y. Wang, Z. Liu, and J. Zhang [29] have brought the issue of time complexity with detection accuracy trade-offs to the fore in APT detection.

In addition, evasion methods used by cybercriminals present a significant headache for IDS systems. Malicious activity can be obfuscated via techniques such as traffic obfuscation, encryption, and polymorphism to avoid detection by IDS. I. Homoliak, D. Ovsonka, M. Gregr, and P. Hanacek [33] proposed how obfuscation techniques are able to circumvent detection mechanisms, especially when disguised within HTTPS traffic. M. Nazari, Z. Dahmardeh, and S. Aliabady [17] Botnet detection is further a problem for IDS due to the advanced evasion techniques used by different bots, which were hard for IDS to detect. Another significant problem is the integration with existing systems. Most behavior-based IDSs need to operate with existing network infrastructure and security systems, which can complicate deployment. J. K. Samuel, M. T. Jacob, M. Roy, S. P M, and A. R. Joy [11] identified this challenge in the context of cloud computing, showing that the integration of IDS into cloud environments was challenging with respect to scalability and performance requirements. From another side, M. Debashi and P. Vickers [19] have also shown the complexity of deploying botnet detection systems into current infrastructures, especially in large-volume traffic.

In cases of large and dynamic network environments, which are common in distributed enterprises, scalability becomes an ongoing problem. Performance often degrades as the network grows in size and complexity; this is the problem many IDS solutions face. This problem is more common in systems that rely on computationally expensive algorithms, such as deep learning models. S. Raja et al. [16] have shown that the scalability of IDS becomes challenging in cloud-based settings, and as the network size grows, the detection rate drastically decreases.

Lastly, IDS also confronts mimicry and polymorphic attacks. The signatures or behaviors of these attacks are modified so as not to be detected, which further makes them very tough for pattern-recognition-based systems. M. I. Khan, S. N. Foley, and B. O'Sullivan [12] highlighted the dangers of mimicry attacks in behavior-based anomaly detection systems because attackers can modify their behavior to evade these detection mechanisms.

V. Conclusion and Future Works

In this study, we have reviewed the main barriers encountered by Intrusion Detection Systems (IDS) using network behavior analysis. Though several advancements have been made in using machine learning and deep learning. There are some problems that are still not fully solved. There are still many challenges in creating an effective IDS system, like high false positive rates, dataset imbalances, zero-day attack detection, and computational complexities. Furthermore, there are practical challenges in the integration of IDS within large-scale real-time environments due to high network traffic volumes and also because of evasion techniques used by attackers. Additionally, in cloud-based as well as IoT environments where threat vectors are dynamic and change over time, there is this concern of scalability with IDS systems adaptable to be scalable to such threats. On a high level, the review identifies three main areas in which better algorithms or data (or perhaps both) will be required to address these issues moving forward.

In the future, it will be beneficial for those who are carrying out research in IDS (Intrusion Detection System) based on network behavior analysis to work upon a few areas critical to improving the performance and scalability of these systems. To start, we need to create better machine learning models that can cope with the inherent imbalance and decrease false positives. It could also be beneficial to investigate hybrid models that combine anomaly-based detection with signature-based techniques, which may be used in detecting zero-day attacks. Furthermore, there should be more universal datasets (i.e., capturing a broader range of attack patterns) specially focused on emerging threats like advanced persistent threats (APTs) and sophisticated botnets. For future work, efforts should also be made to minimize the computational delays of IDS systems using either better algorithms or by offloading processing tasks onto edge computing systems and distributed ones. In the end, it also remains necessary to improve the real-time detection features of IDS, especially for such challenging environments, including those encountered in IoT and cloud computing. Future research may also wish to consider ways of more easily embedding IDS in the existing network infrastructure, particularly in complex and larger-scale environments, so that they are actually working properly.

References

[1] X. Sun, Z. Wang, B. Lv, and J. Ou, A Review on Behavior-Based Detection for Network Threats, Beijing, China: IEEE, May 2017, pp. 127–132. doi: 10.1109/BigDataSecurity.2017.30.

[2] K. Xu, Network Behavior Analysis: Measurement, Models, and Applications. Singapore: Springer, 2022. doi: 10.1007/978-981-16-8325-1.

[3] K. K. Ghanshala, P. Mishra, R. C. Joshi, and S. Sharma, BNID: A Behavior-based Network Intrusion Detection at Network-Layer in Cloud Environment, in 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar,India: IEEE, Dec. 2018, pp. 100–105. doi: 10.1109/ICSCCC.2018.8703265.

[4] M. Jang and K. Lee, An Advanced Approach for Detecting Behavior-Based Intranet Attacks by Machine Learning, IEEE Access, vol. 12, pp. 52480–52495, 2024. doi: 10.1109/ACCESS.2024.3387016.

[5] B. Kitchenham and P. Brereton, A systematic review of systematic review process research in software engineering, Information and Software Technology, vol. 55, no. 12, pp. 2049–2075, Dec. 2013. doi: 10.1016/j.infsof.2013.07.010.

[6] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, Intrusion detection systems in the Internet of things: A comprehensive investigation, Computer Networks, vol. 160, pp. 165–191, Sep. 2019. doi: 10.1016/j.comnet.2019.05.014.

[7] J. Kaur, A. Agrawal, and R. A. Khan, Security Issues in Fog Environment: A Systematic Literature Review, Int. J. Wireless Inf. Networks, vol. 27, no. 3, pp. 467–483, Sep. 2020. doi: 10.1007/s10776-020-00491-7.

[8] M. Ozkan-Okay, R. Samet, O. Aslan, and D. Gupta, A Comprehensive Systematic Literature Review on Intrusion Detection Systems, IEEE Access, vol. 9, pp. 157727–157760, 2021. doi: 10.1109/ACCESS.2021.3129336.

[9] O. H. Abdulganiyu, T. Ait Tchakoucht, and Y. K. Saheed, A systematic literature review for network intrusion detection system (IDS),Int. J. Inf. Secur., vol. 22, no. 5, pp. 1125–1162, Oct. 2023. doi: 10.1007/s10207-023-00682-2.

[10] V. Pai, A. S. Rao, Devidas, and B. Prapthi, An Intelligent Behavior-Based System to Recognize and Detect the Malware Variants Based on Their Characteristics Using Machine Learning Techniques, in Advanced Network Technologies and Intelligent Computing, vol. 1797, I. Woungang et al., Eds., Cham: Springer Nature Switzerland, 2023, pp. 73–88. doi: 10.1007/978-3-031-28180-8-6.

[11] J. K. Samuel, M. T. Jacob, M. Roy, S. P M, and A. R. Joy, Intelligent Malware Detection System Based on Behavior Analysis in Cloud Computing Environment, in 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT), Kollam, India: IEEE, Aug. 2023, pp. 109–113. doi: 10.1109/ICCPCT58313.2023.10245065.

[12] M. I. Khan, S. N. Foley, and B. O'Sullivan, Database Intrusion Detection Systems (DIDs): Insider Threat Detection via Behaviour-Based Anomaly Detection Systems - A Brief Survey of Concepts and Approaches, in Emerging Information Security and Applications, vol. 1403, W. Meng et al., Eds., Cham: Springer, 2022, pp. 178–197. doi: 10.1007/978-3-030-93956-4-11.

[13] M. Antunes, L. Oliveira, A. Seguro, J. Ver´ıssimo, R. Salgado, and T. Murteira, Benchmarking Deep Learning Methods for Behaviour- Based Network Intrusion Detection, Informatics, vol. 9, no. 1, p. 29, Mar. 2022. doi: 10.3390/informatics9010029.

[14] V. Agate, F. M. D'Anna, A. D. Paola, P. Ferraro, G. L. Re, and M. Morana, A Behavior-Based Intrusion Detection System Using Ensemble Learning Techniques, in Advanced Network Technologies and Intelligent Computing, vol. 1797, Cham: Springer Nature, 2022.

[15] P. Ferreira and M. Antunes, Benchmarking Behavior-Based Intrusion Detection Systems with Bio-inspired Algorithms, in Security in Computing and Communications, vol. 1364, S. M. Thampi et al., Eds., Singapore: Springer, 2021, pp. 152–164. doi: 10.1007/978-981-16-0422-5 11.

[16] S. Raja, S. Pran, N. Pandeeswari, P. Kiruthiga, D. Nithya, and G. MuthuPandi, Contemporary PCA and NBA based Hybrid Cloud Intrusion Detection System, EAI Endorsed Trans. Energy Web, p. 168727, Feb. 2021. doi: 10.4108/eai.19-2-2021.168727.

[17] M. Nazari, Z. Dahmardeh, and S. Aliabady, A Novel Approach of Botnets Detection Based on Analyzing Dynamical Network Traffic Behavior, SN Comput. Sci., vol. 2, no. 4, p. 247, Jul. 2021. doi: 10.1007/s42979-021-00634-4.

[18] S. Jing, M. Li, Y. Sun, and Y. Zhang, Research on Prediction of Attack Behavior Based on HMM, in 2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China: IEEE, Jun. 2021, pp. 1580–1583. doi: 10.1109/IMCEC51613.2021.9482334.

[19] M. Debashi and P. Vickers, Sonification of Network Traffic for Detecting and Learning About Botnet Behavior, IEEE Access, vol. 6, pp. 33826–33839, 2018. doi: 10.1109/ACCESS.2018.2847349.

[20] R. Meddeb, F. Jemili, B. Triki, and O. Korbaa, Anomaly-based Behavioral Detection in Mobile Ad-Hoc Networks, Procedia Comput. Sci., vol. 159, pp. 77–86, 2019. doi: 10.1016/j.procs.2019.09.162.

[21] B. G. Atli, Y. Miche, A. Kalliola, I. Oliver, S. Holtmanns, and A. Lendasse, Anomaly-Based Intrusion Detection Using Extreme Learning Machine and Aggregation of Network Traffic Statistics in Probability Space, Cogn. Comput., vol. 10, no. 5, pp. 848–863, Oct. 2018. doi: 10.1007/s12559-018-9564-y.

[22] A. Bhardwaj, F. Al-Turjman, M. Kumar, T. Stephan, and L. Mostarda, Capturing-the-Invisible (CTI): Behavior-Based Attacks Recognition in IoT-Oriented Industrial Control Systems, IEEE Access, vol. 8, pp. 104956–104966, 2020. doi: 10.1109/ACCESS.2020.2998983.

[23] I. Singh, N. Kumar, S. K.G., T. Sharma, V. Kumar, and S. Singhal, Database intrusion detection using role and user behavior based risk assessment, Journal of Information Security and Applications, vol. 55, p. 102654, Dec. 2020. doi: 10.1016/j.jisa.2020.102654.

[24] Z. S. Malek, B. Trivedi, and A. Shah, User Behavior-Based Intrusion Detection Using Statistical Techniques, in Advanced Informatics for Computing Research, vol. 956, A. K. Luhach, D. Singh, P.-A. Hsiung, K. B. G. Hawari, P. Lingras, and P. K. Singh,Eds., in Communications in Computer and Information Science, vol. 956, Singapore: Springer Singapore, 2019, pp. 480–489. doi:10.1007/978-981-13-3143-5 39.

[25] L. Xue and G. Sun, Design and implementation of a malware detection system based on network behavior, Security Comm Networks, vol. 8, no. 3, pp. 459–470, Feb. 2015. doi: 10.1002/sec.993.

[26] A. Gorbenko and V. Popov, Abnormal Behavioral Pattern Detection in Closed-Loop Robotic Systems for Zero-Day Deceptive Threats, in 2020 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Sochi, Russia: IEEE, May 2020, pp. 1–6. doi: 0.1109/ICIEAM48468.2020.9112054.

[27] V. D. Veksler, N. Buchler, C. G. LaFleur, M. S. Yu, C. Lebiere, and C. Gonzalez, Cognitive Models in Cybersecurity: Learning From Expert Analysts and Predicting Attacker Behavior, Front. Psychol., vol. 11, p. 1049, Jun. 2020. doi: 10.3389/fpsyg.2020.01049.

[28] D. Y. Karasek, J. Kim, V. Y. Kemmoe, M. Zakirul Alam Bhuiyan, S. Cho, and J. Son, SuperB: Superior Behavior-based Anomaly Detection Defining Authorized Users' Traffic Patterns, in 2020 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA: IEEE, Aug. 2020, pp. 1–9. doi: 10.1109/ICCCN49398.2020.9209657.

[29] Y. Cui, J. Xue, Y. Wang, Z. Liu, and J. Zhang, Research of Snort Rule Extension and APT Detection Based on APT Network Behavior Analysis, in Trusted Computing and Information Security, vol. 960, H. Zhang, B. Zhao, and F. Yan, Eds., in Communications in Computer and Information Science, vol. 960, Singapore: Springer Singapore, 2019, pp. 51–64. doi: 10.1007/978-981-13-5913-2 4.

[30] Y. Chae, N. Katenka, and L. DiPippo, An Adaptive Threshold Method for Anomaly-based Intrusion Detection Systems, in 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA: IEEE, Sep. 2019, pp. 1–4. doi: 10.1109/NCA.2019.8935045.

[31] B. Arrington, L. Barnett, R. Rufus, and A. Esterline, Behavioral Modeling Intrusion Detection System (BMIDS) Using Internet of Things (IoT) Behavior-Based Anomaly Detection via Immunity-Inspired Algorithms, in 2016 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, HI, USA: IEEE, Aug. 2016, pp. 1–6. doi:10.1109/ICCCN.2016.7568495.

[32] S.-H. Li, Y.-C. Kao, Z.-C. Zhang, Y.-P. Chuang, and D. C. Yen, A Network Behavior-Based Botnet Detection Mechanism Using PSO and K-means, ACM Trans. Manage. Inf. Syst., vol. 6, no. 1, pp. 1–30, Apr. 2015. doi: 10.1145/2676869.

[33] I. Homoliak, D. Ovsonka, M. Gregr, and P. Hanacek, NBA of Obfuscated Network Vulnerabilities' Exploitation Hidden into HTTPS Traffic, 2014.

[34] A. M. V. Bharathy, N. Umapathi, and S. Prabaharan, An Elaborate Comprehensive Survey on Recent Developments in Behaviour Based Intrusion Detection Systems, in 2019 International Conference on Computational Intelligence in Data Science (ICCIDS), Chennai, India: IEEE, Feb. 2019, pp. 1–5. doi: 10.1109/ICCIDS.2019.8862119.