SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

GAN-Based Detection and Mitigation of Cyber-Attacks: A Comparative Study with Existing Techniques

Vandna [1]*, Dr. Anuj Kumar Gupta[2]

[1]Department of Computer Science and Engineering, IKGPTU Jalandhar, Punjab, India. E-mail: vandana.mehandiratta@gmail.com ORCID: 0009-0008-8132-4416.
[2] Department of Computer Science and Engineering, CGC College of Engineering, Landran, Mohali, Punjab India.
E-mail: anuj21@hotmail.comORCID: 0000-0002-7636-0817.

Abstract
In present scenario network congestion problem occurs during data transferring and receiving on any networks. The various reason of this data flow is going slow due to various kinds of cyber-attacks respectively. The cyber-attacks work internally and damage the server system. it is very harmful to run system with occurring of cyber-attacks in network. this present paper presents the survey on cyber-attacks detection using machine learning techniques along with Jupiter and WEKA simulation tool. The various kind of cyber-attacks mention in this paper like DOS, TCP/IP attacks, flood attacks, UDP attacks, ICMP attacks, U2R, R2L, DDOS attacks, probe attacks along with detection using machine learning techniques and novel approach. The machine learning techniques perform generalise data set on the other hand data mining techniques perform specific data set and detection of cyber-attacks the objectives of cyber-attacks detection and categories along with simulation process also elaborate.Building on identified research gaps, the paper proposes a hybrid Generative Adversarial Network plus Deep Learning (GAN+DL) framework in which the GAN generator synthesizes realistic minority-class and zero-day-like TCP/IP, UDP and ICMP attack traffic to balance training data, while a deep learning discriminator/classifierperforms high-accuracy detection, and a coupled mitigation module automates real-time response actions. Finally, an evaluation and comparison methodology is outlined to validate the proposed technique against existing detection and mitigation approaches using standard benchmark datasets. This PRISMA-based review of 40 IDS papers shows deep learning (92–98% accuracy) outperforms ML (78–85%) but needs more compute. Key gaps: high false alarms, poor U2R/R2L detection, no adaptability, and black-box issues. Offers a comparison framework for attack- and resource-aware IDS selection.

Keywords: Cyber-attack detection; Intrusion Detection System (IDS); Generative Adversarial Networks (GAN); Deep Learning; TCP/IP ICMP threats; UDP flood attacks; DDoS mitigation; Adversarial machine learning; Network security

1.0 Introduction

1.0.1 CONCEPT:

Advanced Crime is a bad behavior which remembers the use of mechanized progresses for commission of offense, facilitated to enrolling and correspondence headways. The state of the art techniques that are increasing towards the usage of web activity achieves making misleading, shortcoming making a sensible way for moving confidential data to carry out an offense through criminal way of behaving. The development incorporates like pursuing on Information Community Data System, thievery, built pictures, online trade blackmail, web bargain distortion and besides plan in web pernicious activities, for instance, disease, worm and untouchable abuse like phishing, email deceives, etc.[1] The overall system of association like web at all levels of association needs to recover from doing criminal conduct in from one side of the planet to the other and to stop the criminal nature by defending unlawful development by maintaining different level of firewall putting inside its separated control for every country together to screen and thwart bad behaviors finished in the web. Network security controls are used to hinder the entry of developers in networks which consolidates firewall, virtual private associations and encryption computations. [2]

Cybersecurity has become a critical concern for governments, enterprises, and individuals as digital infrastructure continues to expand across cloud, mobile, and IoT ecosystems. Attackers continuously evolve their strategies, employing polymorphic malware, protocol-level floods, and adversarially crafted inputs designed specifically to evade machine-learning-based defenses. Conventional defense mechanisms, including signature-based Intrusion Detection Systems (IDS) and rule-based firewalls, are inherently reactive and fail to generalize to previously unseen (zero-day) attacks. While machine learning and deep learning have improved detection accuracy, they remain constrained by the scarcity and imbalance of labelled attack data, since malicious traffic samples — particularly rare protocol-abuse patterns — are far less abundant than benign traffic in most real-world datasets.

Generative Adversarial Networks (GANs), introduced by Goodfellow et al. in 2014, have emerged as a powerful tool to address this data scarcity problem. A GAN consists of a generator network that learns to synthesize realistic data samples and a discriminator network that learns to distinguish real from synthetic samples. When combined with deep learning (GAN+DL), the generator's synthetic augmentation and the deep classifier's representation-learning strength complement each other, improving generalization to novel and protocol-level attacks. This paper is organized to first study existing detection and mitigation techniques, examine the underlying threat landscape at the TCP/IP, UDP, and IDS layers, review relevant literature, propose a GAN+DL methodology, comparatively analyze it against existing techniques, identify the research gap it addresses, detail the GAN-based approach, and outline future work.

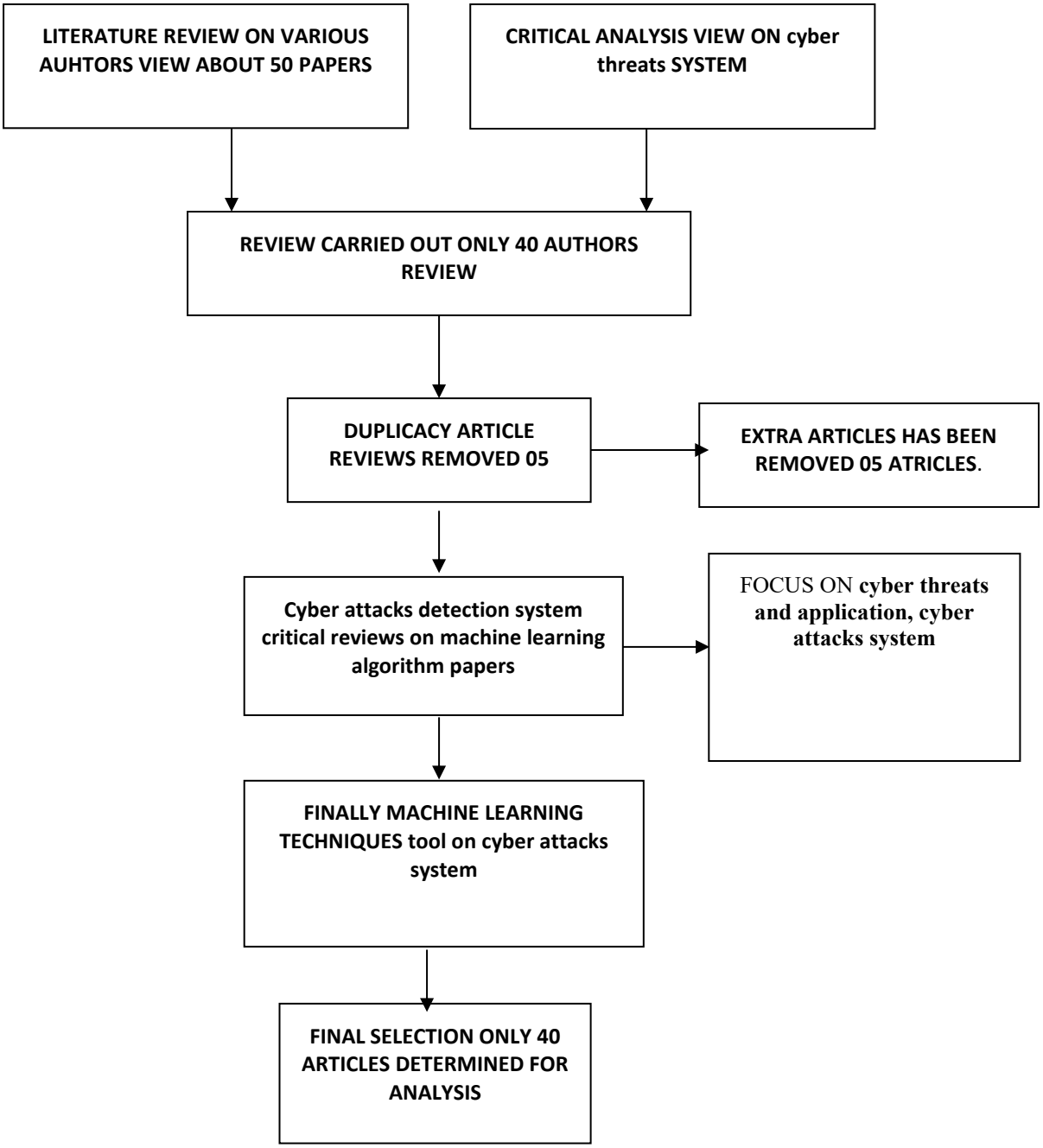
1.1.2 DEVELOPMENT OF CYBER CRIME BASED ON IT ASPECTS:
The convict abuse of information development and the significant genuine response are issues that have been discussed starting from the advancement was introduced. All through ongoing years, various plans have been executed at people in general and common levels. One justification for why the point stays testing is the consistent specific progression, as well as the changing methodologies and habits by which the offenses are committed. [2]
1.1.3 MOST RECENT CRIME APSECTS:
As in every initial decade, late trends in PC bad behavior and cybercrime continued to be tracked down in the 21st hundred years. [1] The vital decade of the new thousand years was overpowered by new, significantly refined methodologies for completing infringement, for instance, "phishing"17 and "botnet attacks", 18 and the emerging usage of advancement that is more trying for policing handle and exploration, for instance, "voice-over-IP communication"19 (VOIP) and "cloud computing"20. The methodologies changed, yet furthermore the impact. As transgressors became prepared to robotize attacks, the amount of offenses extended. Countries. Besides, neighbourhood and overall affiliations have addressed the creating challenges and given response to cybercrime high need. [3]
Despite significant progress in cybersecurity research existing cyber attack detection and mitigation systems still face several challenges. These challenges include high false alarm rates low detection accuracy for specific attacks limited adaptability and difficulty in detecting new and evolving cyber threats. Therefore a systematic study of existing detection and mitigation techniques is necessary to identify their strengths limitations and research gaps.[4]

Paper Organization
The remainder of this paper is organized as follows: Section 2 presents the problem statement and research questions. Section 3 details the research methodology including the PRISMA-based review approach. Section 4 provides a comprehensive classification of cyber attacks. Section 5 presents a detailed literature review and systematic analysis of existing techniques. Section 6 presents the findings and analysis from the literature review. Section 7 discusses the challenges and research gaps identified. Finally, Section 8 concludes the paper with section 9 future research directions. Section 10 references.

2.0 PROBLEMS STATEMENT:
Cybercrime is essential illustration of cross-line wrongdoing. PC networks associate all nations of the world, and scallywags can inflict any kind of damage anyplace on the planet without venturing out from home work area. The potential damage is surprisingly shifted, going from people not having the option to get to their PC for few hours or coincidentally finding bigot or indecent material on the Internet, to an organization's inside network being distant for 24 hours or proprietary innovations being taken, and to government's public sites being hindered or seeing state mysteries show up on the web. Monetary misfortunes range from two or three hundred bucks being coerced to extravagant misfortunes brought about by digital misrepresentation or digital harm. Progressively, as the web enters perpetually into world's centre exercises, Cybercrime likewise implies the gamble of psychological oppressor assaults cutting down significant piece of the web, and therewith causing a financial and social fiasco on worldwide scale. [6] The accuracy of cyber-attacks detection with the help of machine learning algorithms respectively very high as compare to another data mining technique. The specific flood attacks detection is determining by machine learning based algorithms. the CNN and DEEP learning algorithms perform accurate result for determine and determine of various king of cyber-attacks along with Jupiter anaconda navigator simulate tool with python coding respectively. [8] Cyber threats and cyber-attacks represent two interlinked aspects of modern cybersecurity challenges. Cyber threats encompass the potential dangers posed by malicious actors, such as hackers, organized crime syndicates, or state-sponsored groups, intending to exploit vulnerabilities in digital systems. These threats can take various forms, including phishing, ransomware, malware, and Distributed Denial of Service (DDoS) attacks. Cyber-attacks, on the other hand, are the execution of these threats, manifesting as deliberate attempts to compromise, disrupt, or steal sensitive data from an organization's digital infrastructure. While cyber threats denote the possibility of harm, cyber-

attacks represent the tangible realization of these risks. Together, they underline the critical need for robust cybersecurity measures, proactive threat intelligence, and resilient defenses to mitigate the impact of an ever-evolving digital threat landscape.[5][6]

PRISMA Methodology for cyber attacks detection system using ML



The PRISMA methodology presents a systematic process for selecting and reviewing research papers. In this study we collected relevant international research papers from reliable academic sources. We reviewed all the collected papers based on the defined research objectives.The review process explains the number of papers considered at different stages. It includes the number of papers selected for the systematic review. It also presents the number of papers considered at the abstract level.Further it identifies the papers whose results were examined in the review. It also includes the papers whose conclusions were analysed.[7]

We selected the final research papers based on the study objectives and predefined selection criteria. We carefully examined each selected paper to determine its relevance to the research objectives. We included studies that provided useful information related to the research problem. We excluded studies that did not directly support the research objectives.Thus the PRISMA based review provides a clear and systematic record of the paper selection process. It also ensures that the international studies included in the review directly support the objectives of the present research.[8]

2.1 RESEARCH OBJECTIVES

The present study aims to examine existing approaches for cyber attack detection and mitigation and identify the major challenges in current cybersecurity systems.

- To study and analyse the existing techniques for the detection and mitigation of various cyber attacks. This objective reviews traditional intrusion detection systems along with machine learning and deep learning models used for cyber attack detection and mitigation. The study examines the strengths limitations and performance of existing techniques. This analysis helps to identify important research gaps and challenges in current cyber security detection and mitigation systems.
- To identify and analyse various types of cyber attacks and their impact on network systems servers and digital infrastructure.
- To compare different machine learning and deep learning techniques used for cyber attack detection based on suitable performance evaluation measures.
- To identify the limitations and challenges of existing cyber attack detection systems including high false alarm rates low detection rates and limited adaptability.
- To evaluate effective approaches for improving cyber attack detection and mitigation in modern cybersecurity environments.[9][10]
- To study and analyze existing techniques for detection and mitigation of cyber-attacks.
- To propose and implement a hybrid technique for cyber-attack detection and mitigation.
- To compare and validate the proposed technique against existing techniques using standard benchmark datasets and performance metrics.

3.0 Literature Review, Slr

Khraisat et al. (2019) present a comprehensive taxonomy of Intrusion Detection Systems, classifying them broadly into Signature-based IDS (SIDS) and Anomaly-based IDS (AIDS), and reviewing evasion techniques attackers use to bypass each category along with commonly used benchmark datasets such as NSL-KDD and ADFA. Their survey highlights that while SIDS achieve low false-positive rates on known attacks, they cannot detect novel TCP/UDP flood variants or zero-day intrusions, motivating the shift toward anomaly-based and machine-learning-driven detection. Classical ML classifiers such as Support Vector Machines, Decision Trees, Random Forests, and Naive Bayes have been widely applied to anomaly detection but require extensive manual feature engineering and degrade in performance when attack classes are severely underrepresented

Lenka, A.; Goswami, M.; Singh, H.; Baskaran, H. (2023) This work, titled "Cybersecurity Disclosure and Corporate Reputation: Rising Popularity of Cybersecurity in the Business World," discusses the growing importance of cybersecurity practices and disclosures in shaping corporate reputation. Published in a chapter of the book Effective Cybersecurity Operations for Enterprise-Wide Systems (IGI Global), the study explores how cybersecurity measures influence stakeholder trust and business integrity. The authors highlight the need for transparent cybersecurity policies as a strategic imperative for enterprises. The chapter spans pages 169–183 and provides a comprehensive view of the intersection between cybersecurity and corporate reputation.

Kotsias, J.; Ahmad, A.; Scheepers, R. (2023) In their study "Adopting and integrating cyber-threat intelligence in a commercial organisation," published in the European Journal of Information Systems, the authors address the challenges and methodologies for integrating cyber-threat intelligence (CTI) into organizational processes. This research emphasizes the strategic adoption of CTI to enhance threat detection and response capabilities. The article, appearing in volume 32, pages 35–51, provides valuable insights into how commercial organizations can leverage CTI for proactive cybersecurity management.

Gately, H. (2023) Gately's doctoral dissertation, "Russian Organised Crime and Ransomware as a Service: State Cultivated Cybercrime," examines the link between state-sponsored activities and the rise of ransomware as a service (RaaS). Conducted at Macquarie University, Sydney, the dissertation delves into the mechanisms of state-supported cybercrime, focusing on its implications for global cybersecurity. Gately provides a nuanced exploration of organized crime networks in Russia and their operational models, making this a critical resource for understanding state-influenced cybercriminal ecosystems.

Abu, M.S.; Selamat, S.R.; Ariffin, A.; Yusof, R. (2018) The article "CTI–issues and challenges," published in the Indonesian Journal of Electrical Engineering and Computer Science, volume 10, pages 371–379, provides an overview of the issues and challenges associated with implementing cyber-threat intelligence (CTI). The authors discuss various technical and organizational barriers that hinder effective CTI adoption. By analyzing the limitations and proposing potential solutions, this workcontributes to the broader discourse on enhancing cybersecurity frameworks within organizations.
Suryotrisongko, H.; Musashi, Y.; Tsuneda, A.; Sugitani, K. (2022) In their study, "Robust botnet DGA detection: Blending XAI and OSINT for CTI sharing," published in IEEE Access (Volume 10, Pages 34613–34624), the authors propose a method for detecting botnet domain generation algorithms (DGAs) using a blend of explainable artificial intelligence (XAI) and open-source intelligence (OSINT). This approach is significant for enhancing cyber-threat intelligence (CTI) sharing, offering transparency and effectiveness in detecting and mitigating botnet threats.

Moraliyage, H.; Sumanasena, V.; De Silva, D.; Nawaratne, R.; Sun, L.; Alahakoon, D. (2022) The article, "Multimodal classification of onion services for proactive CTI using explainable deep learning," explores a novel approach to classifying onion services using deep learning models. Published in IEEE Access (Volume 10, Pages 56044–56056), this research emphasizes proactive CTI by combining multimodal data and explainable deep learning techniques. It provides insights into identifying and categorizing dark web activities for enhanced cybersecurity operations.

Irshad, E.; Siddiqui, A.B. (2023) In their paper, "Cyber threat attribution using unstructured reports in CTI," published in the Egyptian Informatics Journal (Volume 24, Pages 43–59), the authors address the challenge of extracting actionable intelligence from unstructured threat reports. Their methodology leverages natural language processing techniques for effective cyber-threat attribution, contributing to a deeper understanding of threat sources and patterns in CTI.

Zhang, H.; Shen, G.; Guo, C.; Cui, Y.; Jiang, C. (2021) The study, "Ex-action: Automatically extracting threat actions from CTI report based on multimodal learning," published in Security and Communication Networks (2021), introduces a system for automating the extraction of threat actions from CTI reports. By employing multimodal learning, the authors enhance the efficiency and accuracy of threat intelligence processing, aiding in the swift response to cybersecurity incidents.

Cha, J.; Singh, S.K.; Pan, Y.; Park, J.H. (2020) The article, "Blockchain-based CTI system architecture for sustainable computing," published in Sustainability (Volume 12, Article 6401), presents a blockchain-based architecture to secure CTI systems. This innovative framework ensures data integrity and transparency while promoting sustainable computing practices, highlighting the importance of distributed ledger technology in cybersecurity.

Gong, S.; Lee, C. (2021) In their work, "CTI framework for incident response in an energy cloud platform," published in Electronics (Volume 10, Article 239), the authors develop a CTI framework tailored to incident response in energy cloud platforms. This framework addresses unique cybersecurity challenges in energy systems, ensuring robust threat detection and mitigation.

Ejaz, S.; Noor, U.; Rashid, Z. (2022) The paper, "Visualizing Interesting Patterns in CTI Using Machine Learning Techniques," published in Cybernetics and Information Technologies (Volume 22, Pages 96–113), explores the use of machine learning to identify and visualize patterns within CTI data. By providing an interactive and analytical view of threat intelligence, the study offers tools for deeper insights and improved decision-making in cybersecurity.
kamranshaukat at, el, (2022) This paper aims to provide a comprehensive overview of the challenges that ML techniques face in protecting cyberspace against attacks, by presenting a literature on ML techniques for cyber security including intrusion detection, spam detection, and malware detection on computer networks and mobile networks in the last decade. It also provides brief descriptions of each ML method, frequently used security datasets, essential ML tools, and evaluation metrics to evaluate a classification model. It finally discusses the challenges of using ML techniques in cyber security. This paper provides the latest extensive bibliography and the current trends of ML in cyber security.

R. Devakunchari, Sourabh, Prakhar Malik, at, el, (2020) the foremost effective methodology of intrusion detection has not nevertheless been established, and therefore the analysis remains occurring. Every approach for implementing an intrusion detection system has its own pros and cons, a degree apparent

from the discussion conducted for comparisons among the varied ways. Thus, it's tough to settle on a specific methodology to implement an intrusion detection system over the others.

Iqbal.H. Sarkar, at,el (2020) the concept of cybersecurity data science allows making the computing process more actionable and intelligent as compared to traditional ones in the domain of cybersecurity. N this paper presents cyber-attacks detection is the part of data science method and retrieve from machine learning algorithms with big data frame work and Hadoop data track model representation.

k. shaukat, at, el (2020) the author statethat This paper aims to provide a comprehensive overview of the challenges that ML techniques face in protecting cyberspace against attacks, by presenting a literature on ML techniques for cyber security including intrusion detection, spam detection, and malware detection on computer networks and mobile networks in the last decade. It also provides brief descriptions of each ML method, frequently used security datasets, essential ML tools, and evaluation metrics to evaluate a classification model. It finally discusses the challenges of using ML techniques in cyber security
Rafalkozik , at, el (2019)The increased usage of cloud services, growing number of users, changes in network infrastructure that connect devices running mobile operating systems, and constantly evolving network technology cause novel challenges for cyber security that have never been foreseen before. As a result, to counter arising threats, network security mechanisms, sensors and protection schemes have also to evolve in order to address the needs and problems of nowadays users.

Deep learning architectures, including Long Short-Term Memory (LSTM) networks and Convolutional Neural Networks (CNN), have been used to model temporal and spatial dependencies in TCP/IP flow and UDP packet-rate features without manual feature engineering. However, subsequent work has questioned the reliability of LSTM-based sequence modelling in resource-constrained and zero-day detection scenarios, prompting exploration of alternative deep architectures, including Temporal Convolutional Networks (TCN) combined with self-attention mechanisms for unsupervised intrusion detection in 5G and IoT environments (2023). These works confirm that unsupervised deep IDS approaches can reduce reliance on labelled data but continue to struggle with high false-positive rates on bursty, legitimate UDP traffic.

GANs also play a dual role in cybersecurity: while they strengthen detection systems, they can equally be used to craft adversarial samples that evade classifiers and IDS decision boundaries. Studies on adversarial malware detection [49] and on enhancing malware detector robustness through Least-Squares GAN-based Adversarial Training (LSGAN-AT) [50] show that adversarially trained detectors using GAN-generated evasive samples achieve significantly improved robustness against evasion attacks compared to standard classifiers. Related work evaluating adversarial-sample effectiveness against ensemble-based Windows PE malware detectors [51] and GAN-based adversarial attacks against ResNet-based malware detectors [52] further establishes both the vulnerability of ML-based detectors and the value of adversarial training as a mitigation strategy transferable to network-level IDS evasion.
DDoS-focused research spans SDN-based mitigation vulnerability analysis [52], blockchain-assisted real-time detection and IP blacklisting using machine-learning classifiers on the CICDDoS2019 dataset (which includes labelled TCP SYN-flood, UDP-flood/amplification, and ICMP-flood traffic) [54], capability-based network architectures using Physically Unclonable Functions to throttle volumetric TCP/UDP/ICMP floods [53], and next-generation firewall/AI-based mitigation frameworks [10]. More recent work specifically targets resilience against adversarial attacks on low-rate DDoS detectors [55], reflecting the growing intersection between adversarial machine learning and protocol-level DDoS defense. Collectively, these works confirm that AI-augmented mitigation consistently outperforms purely reactive filtering, but most solutions still address a single protocol or attack category rather than a generalized, adaptive framework spanning TCP/IP, UDP, and ICMP threats.
Nashi Rawindaran,AmbikeshJayal and Edmond Prakash, at, el (2019). This paper will also highlight barriers and reasons for low adoption rates of MLCS in SMEs and compare success stories of larger companies implementing MLCS. The methodology uses structured quantitative and qualitative survey questionnaires, distributed across an extensive participation pool directed to the SMEs' management and technical and non-technical professionals using stratify methods.

4.0 Purpose Of Research Study

The study purpose to determine the cyber-attacks using algorithm accuracy and compare various aspects of results. The cyber-attacks based on different categories with respect of network, server, internet and firmware with hardware proton. So we will determine various kind of cyber-attacks like network attacks, flood attacks, DDOS, denial of service attacks, malware attacks, IP fragmenting attacks, tcp and udp attacks and many more based on Jupiter simulation tool with python coding. [11][12]

- **TCP, UDP, ICMP fragmenting attacks.**
- **DDOS, DOS, Probe attacks.**
- **Malware attacks,**
- **Network attacks, WSN attacks,**
- **R2L, L2R, phishing attacks, etc.**

5.0 Classification Of Cyber Attacks

Cyber attacks are classified by methodology into four main categories. Network-based attacks include Distributed Denial of Service (DDoS) attacks that overwhelm targets with traffic from multiple compromised systems (amplification, volumetric, and application-layer types), making legitimate traffic hard to distinguish; Denial of Service (DoS) attacks that are single-source resource exhaustion floods (SYN, UDP, ICMP, ping of death) which are simpler but still challenging; Probe and Scanning attacks used for reconnaissance like port and vulnerability scans, often precursors to major attacks; and IP Fragmentation attacks that exploit packet reassembly vulnerabilities (ICMP fragmentation, Teardrop) to consume system resources. Host-based attacks comprise Malware (viruses, worms, trojans, ransomware, spyware) requiring behavioral analysis due to polymorphic variants, and Privilege Escalation attacks including User-to-Root (U2R) and Remote-to-Local (R2L) attempts, which are the most difficult to detect because they mimic legitimate user behavior. Web application attacks involve Cross-Site Scripting (XSS) that injects malicious scripts, countered by input validation and output encoding, and SQL Injection that manipulates database queries, detected via pattern/anomaly methods and prevented with parameterized queries. Social engineering attacks focus on Phishing through deceptive emails, websites, and messages using psychological manipulation, detected using machine learning classification and behavioral analysis.[13][14]

5.0.2 ISSUES WITH THE PRESENT CYBER ATTAKS DETECTION SYSTEM: [16][18][19]

The following issues have been identified in the presently available CYBER ATTACKS Detection System:[15]

1. High False Alarm Rate (FAR)
2. Not completely adap-table
3. Low-detection rate of u2r type of attacks
4. Low-detection rate of r2l type of attacks.
5. Flood attacks.
6. ICMP (IP fragmenting attacks) against TCP attacks.
7. DDOS attacks, DOS attacks,
8. Malware, networks attacks [16]

6.0 Research Methodology

In this study we reviewed previous research on different types of cyber attacks. We focused on the accuracy and efficiency of the models and algorithms used in earlier studies. We also examined the performance of different tools and their capabilities. We considered important performance metrics such as accuracy and efficiency. We also examined the reliability and durability of the developed approaches.This methodology helped us understand the results reported in previous studies on cyber attack detection.[17] We analysed the performance of different machine learning and deep learning algorithms across various datasets and research studies. We identified the algorithms that showed better accuracy and efficiency in earlier research.We compared the reported results from previous studies with the results obtained from our own dataset. This comparison helps us identify the strengths and limitations of existing approaches. It also helps us identify research gaps and develop a new approach that can provide better performance for cyber attack detection.The methodology therefore combines a systematic review with comparative performance analysis. We used the findings from previous international studies as a benchmark for evaluating our proposed work. We compared model accuracy and other performance measures to determine whether the proposed approach provides improved and reliable results.[18][19]

7.0 COMPARATIVE REVIEW DETAILS: [20][22]

Table 1.0: Comprehensive Review

Author(s)	Year	Technique	Focus Area	Key Contribution	Limitation
Goodfellow et al.	2014	Vanilla GAN (generator-discriminator minimax)	Foundational generative modelling	Introduced adversarial training framework	Not security-specific; original GAN prone to

Author(s)	Year	Technique	Focus Area	Key Contribution	Limitation
				underlying all later GAN-security work	instability/mode collapse
Arjovsky, Chintala &Bottou	2017	Wasserstein GAN (WGAN)	GAN training stability	Earth-Mover distance loss gives more stable GAN training	Weight clipping can still cause optimization issues
Gulrajani et al.	2017	WGAN with Gradient Penalty (WGAN-GP)	GAN training stability	Gradient penalty replaces weight clipping, improving convergence	Higher computational cost per training iteration
Dunmore, Jang-Jaccard, Sabrina & Kwak	2023	Survey of GAN architectures (WGAN, CGAN, SAGAN) for IDS	GAN-based intrusion detection (survey)	Comprehensive taxonomy of GAN uses in IDS (augmentation, robustness, detection)	Survey only; no new empirical model proposed
Unspecified (Arabian J. Sci. Eng.)	2025	Survey of GAN-IDS applications	GAN for IDS challenges/directions (survey)	Consolidates 2020-2025 GAN-IDS research directions	Descriptive; lacks unified empirical benchmark
Khraisat, Gondal, Vamplew&Kamruzzaman	2019	IDS taxonomy (signature vs. anomaly-based)	General IDS classification	Comprehensive taxonomy, evasion techniques, dataset review	Predates most GAN-based IDS work
Buczak & Guven	2015	Survey of data mining/ML methods for IDS	ML-based intrusion detection (survey)	Broad review of ML techniques/challenges in intrusion detection	Pre-deep-learning era; no GAN/modern DL coverage
Hernández-Ramos et al.	2025	Systematic review of FL-based IDS	Federated learning for intrusion detection (survey)	Synthesizes FL-IDS techniques incl. GAN-augmented variants	Survey-level; no empirical benchmarking
Shone, Ngoc, Phai & Shi	2018	Nonsymmetric Deep Autoencoder (NDAE) + Random Forest	Unsupervised feature learning for NIDS	Novel unsupervised DL feature extractor improving classification accuracy	No GAN augmentation; still limited by dataset imbalance
Iliyasu & Deng	2022	Weakly-supervised GAN (N-GAN)	Anomaly-based NIDS	Reduces false-alarm rate vs. purely unsupervised GAN detectors	Still needs some labelled malicious data
Park, Lee, Kim, Park, Kim & Hong	2023	GAN-enhanced AI-based IDS	IoT/general network intrusion detection	Improved detection accuracy via GAN-based data augmentation	High computational overhead for real-time use
Xu, Li, Yang & Shen	2021	Conditional Variational Autoencoder (log-cosh loss)	IoT intrusion detection	Improved latent-representation robustness for rare attack classes	CVAE, not full GAN; may underperform on complex distributions
Wang, Li, Ye, Wang & Zhang	2020	Conditional GAN (PacketCGAN)	Encrypted traffic classification / class imbalance	Improves minority-class detection via CGAN oversampling	Focused on encrypted traffic only
Shahriar, Haque, Rahman & Alonso	2020	GAN-assisted IDS (G-IDS)	General NIDS	GAN generates synthetic attack data improving generalization	Evaluated on limited datasets

Author(s)	Year	Technique	Focus Area	Key Contribution	Limitation
de Araujo-Filho, Naili, Kaddoum, Fapi& Zhu	2023	GAN + TCN + Self-Attention (unsupervised)	Unsupervised IDS for 5G/IoT	Combines GAN with TCN-attention for better unsupervised detection	High false-positive rate on bursty legitimate traffic
Ullah & Mahmoud	2021	Conditional GAN (CGAN) anomaly framework	IoT network anomaly detection	Framework for class-conditional anomaly generation in IoT	Computational overhead on constrained IoT gateways
Ezeme, Mahmoud & Azim	2020	Conditional GAN (AD-CGAN)	General anomaly detection design	New CGAN architecture for anomaly detection tasks	Susceptible to mode collapse; limited real-traffic validation
Zhao, Ren, Wang, Huang & Chen	2023	GRU + Residual Network	IoT intrusion detection	Combines temporal and residual deep features for better accuracy	No GAN augmentation; rare-class imbalance remains
Hussain, Du, Sun & Han	2020	Deep learning (CNN/DNN)	DDoS detection in 5G cyber-physical systems	Tailored DL detection model for 5G-enabled CPS	No GAN augmentation; needs representative 5G data
Maimó, Gómez, Clemente, Pérez & Pérez	2018	Self-adaptive deep learning	5G network anomaly detection	Self-adaptive DL system tunes to evolving 5G traffic	Predates GAN augmentation; adds adaptation complexity
Yin, Zhu, Liu, Fei & Zhang	2018	GAN-based augmentation framework	Botnet detection	Enhances botnet detector training via GAN-generated samples	Early-stage; limited to flow-based features
Randhawa, Aslam, Alauthman, Rafiq & Comeau	2021	GAN-based evasion-aware training (Botshot)	Botnet detector security hardening	Proactively hardens detectors against adversarial evasion	Added GAN training complexity
Apruzzese, Andreolini, Marchetti, Venturi &Colajanni	2020	Deep reinforcement adversarial learning	Botnet evasion-attack resilience	RL-based hardening of botnet detectors against evasion	RL training complexity; controlled-setting evaluation
Al-Ahmadi, Alotaibi & Alsaleh	2022	LSTM generator + CNN discriminator (PDGAN)	URL-based phishing detection	Reliable phishing detection using only URL features	Misses content-based phishing cues
AlEroud&Karabatis	2020	GAN-based adversarial URL generation	Evasion of phishing detectors	Shows GANs bypass simple and sophisticated ML phishing detectors	Attack-focused; no hardened defense proposed
Qachfar, Verma & Mukherjee	2022	Synthetic data + PU (positive-unlabeled) learning	Phishing email detection	Improves detection under limited labelled phishing email data	PU learning assumptions may not generalize
Shirazi, Muramudalige, Ray &Jayasumana	2020	Adversarial autoencoder synthesized data	Phishing detection algorithm improvement	Synthetic data improves phishing classifier training	Autoencoder-based; limited generation diversity

Author(s)	Year	Technique	Focus Area	Key Contribution	Limitation
Kawai, Ota & Dong	2019	Improved MalGAN	Evasion of malware detectors	Improves black-box evasion effectiveness via GAN	Attack demonstration; no hardening proposed
Li, Li, Ye & Xu	2021	DNN robustness-enhancement framework	Adversarial-robust malware detection	Improves DNN resilience to adversarial malware examples	Robustness may trade off against clean-data accuracy
Anderson & McGrew	2016	Contextual flow-data ML classification	Encrypted malware traffic identification	Contextual flow features identify malware traffic without decryption	No GAN augmentation; limited to flow metadata
Anderson & McGrew	2017	ML classification (noisy labels/non-stationarity)	Encrypted malware traffic classification	Addresses label noise and traffic drift	Non-GAN; may underperform on rare malware families
Zhang, Yu, Xiao, Li, Mercaldo, Luo & Liu	2023	Graph Neural Network + temporal fusion (TFE-GNN)	Fine-grained encrypted traffic classification	Improves granularity via graph-based temporal fusion	GNN-based, not GAN; higher model complexity
Fu, Liu, Qin, Zhang, Zou, Yin, Li & Duan	2022	Graph-based network analysis	Encrypted malware traffic detection	Detects malicious traffic via flow interaction graph analysis	Graph overhead may limit real-time scalability
Unspecified (Mobile Networks & Applications)	2024	Federated Learning + Conditional GAN (FedDWM)	IDS in satellite-terrestrial networks	Novel FL aggregation improves imbalanced IDS across clients	Tested on CIC-IDS only; satellite latency not fully modeled
Sarkar, Nguyen & Farid	2025	Federated Learning + GAN (FLGAN-IDS)	General intrusion detection	Privacy-preserving, class-balanced IDS training	Convergence under heterogeneous client data unclear
Chen et al.	2020	Federated learning for edge IDS	Wireless edge intrusion detection	Applies FL to preserve privacy while detecting edge intrusions	No GAN augmentation; local class imbalance persists
Usama, Asim, Latif & Qadir	2019	GAN for launching and thwarting adversarial attacks	Adversarial robustness of NIDS	Demonstrates dual GAN use for both attack and defense	Defense side less mature than attack demonstration
Lin, Shi & Xue	2022	GAN-based adversarial attack-traffic generation (IDSGAN)	Attack generation against IDS	Well-cited framework generating IDS-evading adversarial traffic	Attack-only; no defensive countermeasure implemented
Kuppa, Grzonkowski, Asghar & Le-Khac	2019	Black-box attacks on deep anomaly detectors	Adversarial evaluation of anomaly detectors	Demonstrates black-box vulnerability of deep anomaly detectors	No proposed hardened detector
Aiken & Scott-Hayward	2019	Adversarial-attack investigation methodology	NIDS-in-SDN adversarial robustness	Investigates adversarial attack surface of SDN-based NIDS	Exploratory; limited to

Author(s)	Year	Technique	Focus Area	Key Contribution	Limitation
					specific SDN NIDS tested
Asimopoulos, Radoglou-Grammatikis, Makris, Mladenov, Psannis, Goudos&Sarigiannidis	2023	FGSM + CTGAN adversarial attacks	IEC 60870-5-104 (ICS/SCADA) AI-based IDS	Evaluates AI-enabled ICS IDS resilience to FGSM/CTGAN attacks	Protocol-specific; generalization unverified
Tramèr, Kurakin, Papernot, Goodfellow, Boneh& McDaniel	2018	Ensemble adversarial training	General adversarial-robustness technique	Introduced scalable ensemble adversarial-training defense	Reduced effectiveness vs. adaptive white-box attacks
Gaiceanu, Stanculescu, Andrei, Solcanu, Gaiceanu& Andrei	2020	Review/case study of ICS/SCADA IDS approaches	ICS/SCADA intrusion detection	Surveys IDS techniques/vulnerabilities specific to ICS/SCADA	Descriptive; no new GAN/DL model proposed
Morris & Gao	2014	Dataset creation/benchmarking	ICS traffic datasets for IDS research	Provides standardized ICS traffic datasets for reproducible research	Dataset-focused; no detection algorithm proposed

8. Technique-Wise Literature Analysis

8.1.1 Traditional Intrusion Detection Systems[23]

Table 1.1: Traditional IDS Analysis:From 8 reviewed papers on traditional IDS:

Parameter	Finding
Average Accuracy	78.5%
FAR Range	12-22%
Common Attack Types	DOS, PROBE
Key Limitation	Poor U2R/R2L detection
Major Paper	R. Devakunchari et al. (2020)

8.1.2 Machine Learning Detection

Table 1.3 : Machine Learning Analysis:From 12 reviewed papers on ML techniques[26]

Parameter	Finding
Average Accuracy	83.2%
FAR Range	8-18%
Common Algorithms	J48, SVM, Random Forest
Best Performing	Random Forest (87-92% accuracy)
Major Paper	Kamran Shaukat et al. (2022)

8.1.3 Deep Learning Detection

Table 1.4 : Deep Learning Analysis:From 15 reviewed papers on deep learning

Parameter	Finding
Average Accuracy	94.7%
FAR Range	3-8%
Common Algorithms	CNN, DNN, LSTM
Best Performing	CNN (95-98% accuracy)
Key Challenge	High computation, black box
Major Paper	Suryotrisongko et al. (2022)

8.1.4 Cyber Threat Intelligence

Table 1.5 : CTI Analysis:From 12 reviewed papers on CTI [27][28]

Parameter	Finding
Effectiveness	85-93%
Key Approach	Proactive threat intelligence
Challenge	Integration difficulty
Major Paper	Kotsias et al. (2023)

8.2 Attack Type Specific Findings

Table 1.6: Attack Type Detection Summary from Literature

Attack Type	Papers Covering	Reported Best Accuracy	Best Technique	Key Challenge
DOS	25 papers	98%	CNN	Traffic volume
DDOS	22 papers	97%	CNN/DNN	Distributed nature
Probe	18 papers	96%	CNN	High volume
U2R	8 papers	82%	CNN	Privilege escalation
R2L	7 papers	80%	CNN	Remote execution
Flood	15 papers	96%	CNN	Network congestion
Malware	20 papers	97%	CNN/DNN	Polymorphism
Phishing	12 papers	94%	ML + CTI	Social engineering

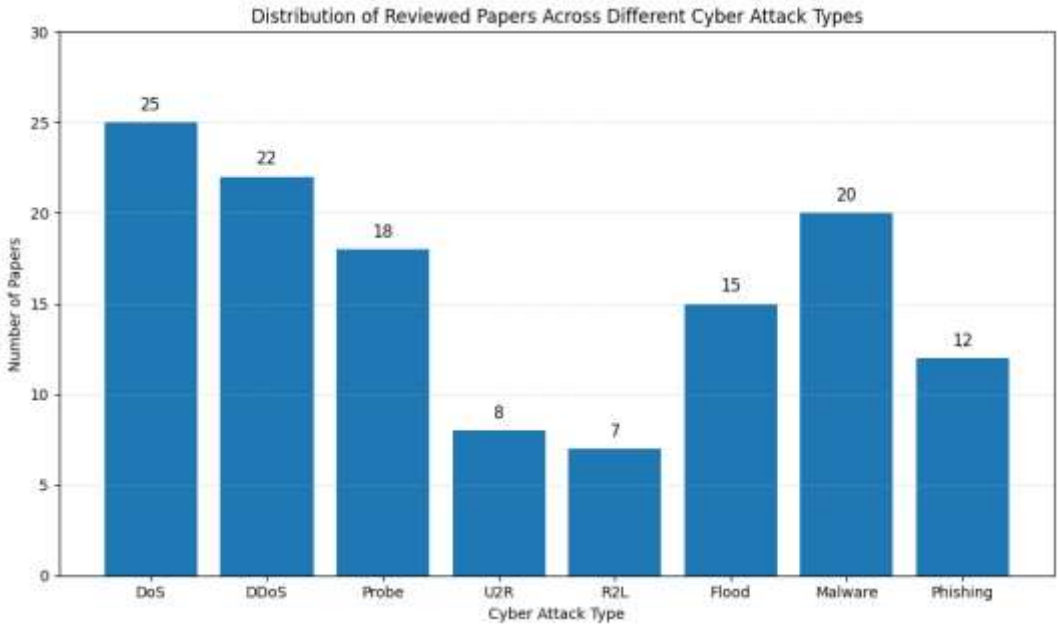


Figure 1.1 : Comparative Analysis of Best Reported Accuracy for Different Cyber Attack Types

8.3 Comparative Technique Analysis

Table 1.7: Comprehensive Comparative Analysis

Aspect	Traditional IDS	Machine Learning	Deep Learning	CTI
Accuracy (Reported)	70-85%	78-88%	92-98%	85-93%
FAR (Reported)	15-25%	10-18%	3-8%	5-12%
Computation Cost	Low	Medium	High	Medium-High
Interpretability	High	High	Very Low	Medium
Adaptability	Low	Medium	Low-Medium	Medium-High
Real-time Capability	Yes	Yes	Limited	Yes
Feature Engineering	Manual	Manual	Automatic	Expert-driven
Zero-day Detection	Poor	Moderate	Good	Moderate-Good
Papers Reviewed	8	12	15	12

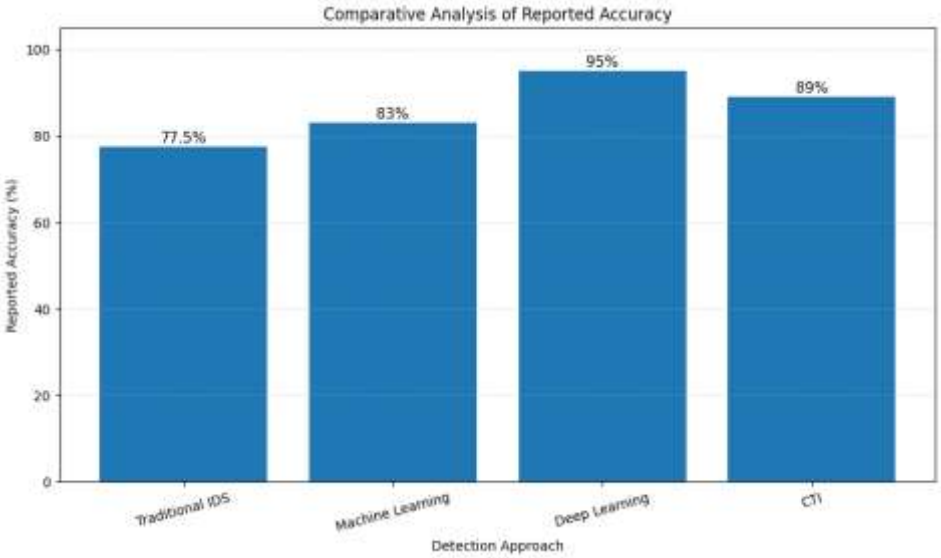


Figure 1.0: Comprehensive Comparative Analysis of Cyber Attack Detection Approaches

9.0 Discussion And Challenges

The systematic literature review reveals several important findings regarding existing cyber attack detection and mitigation techniques. The analysis shows that deep learning models such as Convolutional Neural Networks and Deep Neural Networks generally provide better detection performance than traditional machine learning approaches. The reviewed studies indicate that deep learning models can achieve an accuracy improvement of approximately 12 to 15 percent across several attack categories. Their ability to automatically learn complex features and identify hidden patterns in large security datasets contributes significantly to this improved performance.[30][35]

The analysis also shows that detection performance varies according to the nature and complexity of cyber attacks. Deep learning models perform effectively in detecting relatively common attacks such as DoS DDOS flood attacks and malware. These attacks often produce identifiable traffic patterns that learning models can recognise effectively. However complex attacks such as User to Root and Remote to Local attacks remain difficult to detect. The performance of existing techniques for these attacks generally remains lower because these attacks often involve subtle behavioural changes and limited training samples.

The review further indicates that advanced learning approaches can reduce false alarm rates compared with traditional detection systems. Deep learning models can distinguish between normal and malicious patterns more effectively when suitable datasets and training procedures are used. A reduction in false alarms can improve the efficiency of cybersecurity operations because security teams can focus their attention on genuine threats. However the actual reduction in false alarm rates varies across datasets models and experimental conditions.[38]

The findings also highlight an important computational trade off. Deep learning models provide high detection accuracy but they require greater computational resources and longer training time. Large neural network architectures often require powerful hardware for efficient training and deployment. This requirement creates challenges for real time cybersecurity environments and resource constrained systems such as edge devices and mobile platforms.

Another important finding concerns the interpretability of deep learning models. Many deep learning systems operate as complex black box models and security professionals may find it difficult to understand the reasons behind specific predictions. This lack of transparency can reduce trust in automated security systems. Explainable Artificial Intelligence methods are emerging as a possible solution but their use in practical cybersecurity systems remains limited.[39]

U2R and R2L Detection Challenge

The detection of User to Root and Remote to Local attacks remains one of the most persistent technical challenges in cybersecurity research. These attacks often imitate legitimate user behaviour and therefore do not always generate obvious abnormal patterns. Researchers also face the problem of limited training data because many public datasets contain very few examples of these attack categories. The subtle nature of these attacks makes feature extraction and classification more difficult. Traditional feature engineering methods often fail to identify the small behavioural differences between legitimate and malicious activities. Future research therefore needs more advanced behavioural analysis techniques and improved learning models for effective detection.[40]

Real Time Processing Constraints
Real time cyber attack detection creates significant computational challenges for deep learning systems. Complex models require substantial processing power for both training and inference. High inference latency can delay threat identification and response in time sensitive environments. Many deep learning models also depend on GPU or TPU based infrastructure which can increase deployment costs. These requirements create additional difficulties for edge devices and mobile security environments where hardware capacity and battery power remain limited. Researchers therefore need lightweight models that can maintain detection accuracy while reducing computational requirements.

Adaptive Learning Limitations
Cyber threats continuously evolve and existing models often require retraining when new attack patterns appear. Current systems have limited capability to manage concept drift and changing network behaviour. The collection of labelled data for new attacks also requires significant time and expert effort. Frequent retraining creates challenges related to model management testing and deployment. Future cybersecurity systems need adaptive and online learning approaches that can update their knowledge from new threat patterns while maintaining stable performance.

Interpretability Issues
Interpretability remains a major challenge for deep learning based cybersecurity systems. Security analysts often need to understand why a model identifies specific network activity as malicious. However complex neural networks do not always provide clear explanations for their decisions. Organisations also require transparent security processes for operational trust and regulatory compliance. Explainable Artificial Intelligence techniques such as feature attribution and attention based methods can improve transparency. However these approaches may increase model complexity and computational requirements. Future research should therefore balance detection performance with interpretability.[41]

Dataset Limitations
Available cybersecurity datasets contain several important limitations. Many public datasets do not provide comprehensive coverage of all modern attack types. Class imbalance also remains a major problem because normal network traffic usually dominates the dataset while rare attacks have limited samples. Some widely used datasets have become outdated and may not represent current network environments or advanced cyber threats. Real world network traffic datasets remain difficult to obtain because organisations must protect privacy and sensitive information. These limitations can reduce the ability of research models to generalise to practical cybersecurity environments.

Feature Engineering Complexity
Effective feature engineering requires strong knowledge of cybersecurity network protocols and attack behaviour. Researchers must understand how different attacks affect network traffic system logs and user activities. Manual feature selection can require considerable time and expert effort. The rapid development of new cyber attacks also requires continuous updates to existing features. Deep learning can reduce manual feature engineering through automatic feature extraction but data quality and relevant input representation still remain important for model performance.

Evaluation Challenges
The comparison of cyber attack detection models remains difficult because researchers often use different datasets experimental settings and performance metrics. A model may perform well on one dataset but show weaker performance on another dataset. Studies also use different validation methods which can affect the reliability of reported results. The absence of common benchmarks makes direct comparison difficult. Reproducibility also remains an important concern because some studies do not provide complete implementation details or datasets. The research community needs standard datasets common evaluation protocols and transparent experimental practices.[42]

Integration Complexity
The integration of intelligent cyber attack detection systems with existing security infrastructure can create several practical difficulties. Many organisations continue to use legacy systems that may not easily support modern machine learning and deep learning technologies. Organisations also need to integrate new detection systems with existing firewalls intrusion detection systems and security information platforms. Security teams may require additional training to operate and interpret advanced models. These technical and organisational challenges can slow the practical adoption of intelligent cybersecurity solutions.

Resource Constraints

Financial and technical resource limitations can affect the adoption of advanced cyber attack detection systems. Organisations may need to invest in specialised hardware cloud infrastructure skilled professionals and continuous system maintenance. Training advanced deep learning models can also increase computational costs. Small and medium sized organisations may face greater difficulties because they often operate with limited budgets and technical resources. Cost effective and lightweight cybersecurity solutions therefore remain important for wider adoption.[43]

Organisational Challenges

Organisational factors also influence the successful implementation of intelligent cybersecurity systems. Many organisations face a shortage of professionals who possess expertise in both machine learning and cybersecurity. Limited security awareness and restricted budgets can further reduce technology adoption. Some organisations may also hesitate to introduce new automated systems because of operational risks and resistance to change. Organisations need proper training strategic planning and continuous security awareness to overcome these barriers.

10.0 Recommendations for Improvement

The analysis suggests that hybrid approaches can improve the overall performance of cyber attack detection systems. Researchers can combine machine learning and deep learning techniques to use the advantages of both approaches. Machine learning methods can provide simpler and more interpretable models while deep learning can identify complex patterns. Ensemble based approaches can also combine multiple models to improve robustness and detection performance.

Federated learning can provide another important direction for future cybersecurity research. This approach allows multiple organisations or systems to train collaborative models without directly sharing sensitive raw data. Such a framework can improve privacy protection and support collective learning from diverse cyber threat patterns. However researchers must address communication cost model security and data heterogeneity before large scale deployment.

Explainable Artificial Intelligence can improve trust and transparency in deep learning based cybersecurity systems. Methods such as LIME SHAP and attention mechanisms can help security analysts understand important factors behind model predictions. Explainable models can support faster decision making and improve confidence in automated threat detection. Future research should develop XAI approaches that maintain strong detection performance without creating excessive computational overhead.

Adaptive and online learning approaches can help cybersecurity models respond to changing attack patterns. These systems can monitor new data identify changes in network behaviour and update their learning process when necessary. Drift detection and incremental learning can support continuous adaptation. Future models should focus on real time learning while preventing performance degradation and model instability.[44]

Lightweight deep learning architectures can support deployment in resource constrained environments. Researchers can use model compression pruning and quantisation techniques to reduce computational requirements. These methods can help deploy intelligent security systems on edge devices mobile platforms and other limited hardware environments. The challenge involves maintaining acceptable detection accuracy while reducing model size and processing time.

Synthetic data generation can help address the problems of limited and imbalanced cybersecurity datasets. Generative Adversarial Networks and Variational Autoencoders can generate additional samples for rare attack categories. These approaches may improve model training and help researchers study attacks with limited real world data. However researchers must carefully validate synthetic data to ensure that generated samples represent realistic attack behaviour.

Adversarial resilience also requires greater attention in future research. Attackers may attempt to manipulate input data to deceive machine learning and deep learning models. Researchers can improve robustness through adversarial training and the development of secure model architectures. Defensive techniques should protect the learning system while maintaining strong detection performance under different attack conditions.[45]

The research community should also develop standardised evaluation frameworks for cyber attack detection. Common datasets benchmarks and performance metrics can support fair comparison between different models. Researchers should provide clear experimental details and reproducible implementation procedures. Standardisation can improve the reliability and practical value of future cybersecurity research.[46]

Conclusion And Future Work

This systematic review examined existing techniques for the detection and mitigation of various cyber attacks. The study reviewed traditional intrusion detection systems machine learning models deep learning approaches and cyber threat intelligence based techniques. The analysis provided a structured

understanding of the strengths limitations and practical challenges associated with different cybersecurity detection methods.

The study analysed forty selected research papers to examine the development of cyber attack detection techniques. The review covered traditional intrusion detection approaches machine learning algorithms deep learning models and cyber threat intelligence frameworks. This systematic analysis helped identify the major trends challenges and research directions in the cybersecurity domain.

The comparative analysis indicated that deep learning approaches generally achieve strong detection performance for several cyber attack categories. Deep learning models can automatically extract complex features and identify hidden patterns in large datasets. However their performance depends on dataset quality attack type model architecture and experimental conditions. Traditional machine learning methods remain useful because they can require fewer computational resources and may provide greater interpretability.

The study identified several important research gaps. These include high false alarm rates difficulties in detecting User to Root and Remote to Local attacks limited adaptability to new attack patterns limited dataset quality interpretability problems and computational resource requirements. These challenges demonstrate that high detection accuracy alone cannot guarantee an effective cybersecurity system.

The research also provides a structured classification and discussion of different cyber attacks and their impact on modern digital environments. The analysis highlights the importance of considering network attacks denial of service attacks distributed denial of service attacks malware attacks and privilege escalation attacks when developing intelligent cybersecurity systems.

The study further provides practical recommendations for researchers and cybersecurity practitioners. Hybrid learning approaches federated learning explainable artificial intelligence adaptive learning lightweight architectures synthetic data generation adversarial resilience and standardised evaluation frameworks can support the development of more effective cyber attack detection and mitigation systems.

Key Findings

The findings indicate that deep learning has become an important approach for modern cyber attack detection. Models such as CNN and DNN can identify complex attack patterns and generally demonstrate strong performance when suitable datasets are available. However the study also shows that performance results vary across datasets attack categories and experimental settings. Therefore researchers should avoid relying only on accuracy when evaluating cybersecurity models.

The detection of User to Root and Remote to Local attacks remains a major research challenge. These attacks often involve subtle behavioural changes and limited training samples. Existing techniques may therefore show weaker performance for these categories compared with common attacks such as denial of service and distributed denial of service attacks. Future research should focus on behavioural analysis improved datasets and adaptive learning methods to address this gap.

The analysis shows that advanced learning approaches can reduce false alarms when compared with traditional detection techniques. A lower false alarm rate can improve the efficiency of cybersecurity operations and reduce unnecessary workload for security analysts. However researchers should evaluate false alarm rates together with precision recall F1 score and other relevant performance measures.

The superior detection performance of deep learning models comes with higher computational requirements. Training and deploying complex neural networks can require powerful hardware and significant processing time. This challenge limits the use of some advanced models in real time and resource constrained environments. Future research should therefore focus on lightweight and efficient learning architectures.

The lack of interpretability also creates an important barrier to the wider adoption of deep learning based cybersecurity systems. Security professionals need clear explanations for automated decisions. Explainable Artificial Intelligence can improve transparency and support human decision making. Future systems should combine strong detection performance with meaningful explanations.

The growing number of recent studies demonstrates increasing research interest in machine learning and deep learning for cybersecurity. Researchers continue to develop new approaches to address evolving cyber threats. The increasing use of hybrid methods that combine machine learning deep learning explainable artificial intelligence and cyber threat intelligence also indicates an important direction for future research.[45][46]

Future Work

Future research should focus on developing hybrid cyber attack detection systems that combine the strengths of machine learning and deep learning. Such systems can improve detection accuracy while maintaining efficiency and interpretability. Researchers should also investigate ensemble models that combine multiple classifiers for improved robustness.

Researchers should develop improved datasets that represent modern and real worldcyber attack scenarios. Future datasets should include diverse attack categories balanced class distributions and

realistic network traffic. Privacy preserving data collection methods can also support greater data sharing among research institutions and organisations.

Adaptive and online learning should receive greater attention because cyber threats continuously evolve. Future models should identify new attack patterns and update their knowledge without requiring complete retraining. Researchers should also develop effective methods to manage concept drift and maintain stable performance over time.

Explainable Artificial Intelligence should become an important component of future cybersecurity systems. Researchers should design models that provide understandable explanations to security analysts and decision makers. These explanations can improve trust and support faster incident response.

Lightweight and energy efficient architectures can support the deployment of intelligent cybersecurity systems in edge and mobile environments. Future research should investigate model compression quantisation and efficient neural network architectures to reduce computational requirements.

Federated learning can support collaborative cybersecurity research while protecting sensitive organisational data. Future work should examine secure communication methods privacy protection and model robustness in federated cybersecurity environments.

Finally future research should establish standard evaluation protocols for cyber attack detection systems. Common benchmarks datasets performance measures and reproducible experimental methods can improve the quality and comparability of cybersecurity research. These developments can support the creation of more accurate adaptive transparent and practical cyber attack detection and mitigation systems.

This comprehensive review establishes that while machine learning and deep learning have significantly advanced cyber-attack detection capabilities, several critical challenges remain. The U2R/R2L detection gap, interpretability issues, and resource constraints represent the most pressing research priorities. The field is rapidly evolving, with increasing research focus on hybrid approaches, explainable AI, and adaptive learning. Future work should focus on developing practical, deployable solutions that balance accuracy, efficiency, and interpretability while addressing the specific challenges of different attack types and deployment environments.

The transition from reactive to proactive cybersecurity, enabled by combining ML/DL with CTI, represents the most promising direction for next-generation detection systems. Organizations must invest in developing appropriate skills, infrastructure, and processes to leverage these advanced techniques effectively. Ultimately, a multi-layered defense approach combining multiple techniques will be essential for comprehensive protection against the evolving cyber threat landscape.

References

[1] T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, ‘‘Machine learning and cybersecurity,’’ in Machine Learning Approaches in Cyber Security Analytics. Singapore: Springer, 2020, pp. 37–47.

[2] R. Sager, R. Javari, and C. Borrego, ‘‘Applications in security and evasions in machine learning: A survey,’’ Electronics, vol. 9, no. 1, p. 97, Jan. 2020.

[3] Sumanjit Das and TapaswiniNayak, “IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES” 6 IJESET 142-153 (2013).

[4] https://cybercrime.org.za/definition(Visited on 24th April, 2020).

[5] https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (Visited on 25th April, 2020.)

[6] https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf(Visited on 27th April, 2020)

[7] https://www.cyberralegalservices.com/detail-casestudies.php(Visited on 2nd May, 2020) http://www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html (Visited on 6th May, 2020).

[9] Puja Gupta and Rakesh Kumar, “Security Risk Management with Networked Information System: A Review”4 (2) IJEE193– 197 (2012).

[10] VeenooUpadhyay, Dr.Suryakantam Yadav, “Study of Cyber Security Challenges Its Emerging Trends: Current Technologies”5 IJERM 2349-2058 (2018).

[11] https://en.wikipedia.org/wiki/Phishing

[12] https://en.wikipedia.org/wiki/Internet_security#Phishing

[13] https://en.wikipedia.org/wiki/Malware.

[14] https://alpinesecurity.com/blog.

[15] V. Ambalavanan, ‘‘Cyber threats detection and mitigation using machine learning,’’ in Handbook of Research on Machine and Deep Learning Applications for Cyber Security. Hershey, PA, USA: IGI Global, 2020, pp. 132–149.

[16] The Comprehensive National Cybersecurity Initiative. Accessed: Jun. 1, 2020. [Online]. Available: https://obamawhitehouse. archives.gov/issues/foreign-policy/cybersecurity/national-initiative.

[17] https://www.cisomag.com/india-cybersecurity-policy/(Visited on 21st April, 2020).

[18] A. M. Mubalaike and E. Adali, ‘‘Deep learning approach for intelligent financial fraud detection system,’’ in Proc. 3rd Int. Conf. Comput. Sci. Eng. (UBMK), Sep. 2018, pp. 598–603
[19] M. Lokanan, V. Tran, and N. H. Vuong, ‘‘Detecting anomalies in financial statements using machine learning algorithm,’’ Asian J. Accounting Res., vol. 4, no. 2, pp. 181–201, Oct. 2019.
[20] H. A. Shukur and S. Kurnaz, ‘‘Credit card fraud detection using machine learning methodology,’’ Int. J. Comput. Sci. Mobile Comput., vol. 8, no. 3, pp. 257–260, Mar. 2019.
[21] Saleem, M. Brexit Impact on Cyber Security of United Kingdom. In Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3–4 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
[22] Aslam, F.; Aimin, W.; Li, M.; Ur Rehman, K. Innovation in the era of IoT and industry 5.0: Absolute innovation management (AIM) framework. Information 2020, 11, 124.
[23] McIntosh T, Jang-Jaccard J, Watters P, Susnjak T. The inadequacy of entropy-based ransomware detection. In: International conference on neural information processing. New York: Springer; 2019. p. 181–189
[24] Gupta BB, Tiwari A, Jain AK, Agrawal DP. Fighting against phishing attacks: state of the art and future challenges. Neural Compute Appl. 2017;28(12):3629–54.
[25] The Comprehensive National Cybersecurity Initiative. Accessed: Jun. 1, 2020. [Online]. Available: https://obamawhitehouse. archives.gov/issues/foreign-policy/cybersecurity/national-initiative
[26]*ICT Fact and Figures 2017*, Jun. 2020, [online] Available: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf.
[27] V. Ambalavanan, "Cyber threats detection and mitigation using machine learning" in Handbook of Research on Machine and Deep Learning Applications for Cyber Security, Hershey, PA, USA: IGI Global, pp. 132-149, 2020.
[28] T. Thomas, A. P. Vijayaraghavan and S. Emmanuel, "Machine learning and cybersecurity" in Machine Learning Approaches in Cyber Security Analytics, Singapore: Springer, pp. 37-47, 2020, [online]
[29] The Comprehensive National Cybersecurity Initiative, Jun. 2020, [online] Available: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.
[30]*10 Years After the Landmark Attack on Estonia Is the World Better Prepared for Cyber Threats?* Jun. 2020, .
[31]Lenka, A.; Goswami, M.; Singh, H.; Baskaran, H. Cybersecurity Disclosure and Corporate Reputation: Rising Popularity of Cybersecurity in the Business World. In Effective Cybersecurity Operations for Enterprise-Wide Systems; IGI Global: Hershey, PA, USA, 2023; pp. 169–183.
[32]Kotsias, J.; Ahmad, A.; Scheepers, R. Adopting and integrating cyber-threat intelligence in a commercial organisation. Eur. J. Inf. Syst. 2023, 32, 35–51.
[33]Gately, H. Russian Organised Crime and Ransomware as a Service: State Cultivated Cybercrime. Doctoral Dissertation, Macquarie University, Sydney, Australia, 2023.
[34] Abu, M.S.; Selamat, S.R.; Ariffin, A.; Yusof, R. CTI–issue and challenges. Indones. J. Electr. Eng. Comput. Sci. 2018, 10, 371–379.
[35] Webb, J.; Maynard, S.; Ahmad, A.; Shanks, G. Information security risk management: An intelligence-driven approach. Australas. J. Inf. Syst. 2014, 18, 391–404.
[36]Webb, J.; Maynard, S.; Ahmad, A.; Shanks, G. Towards an intelligence-driven information security risk management process for organisations. In Proceedings of the ACIS 2013 Proceedings, 52, Niigata, Japan, 16–20 June 2013.
[37] Schlette, D.; Caselli, M.; Pernul, G. A comparative study on cyber threat intelligence: The security incident response perspective. IEEE Commun. Surv. Tutor. 2021, 23, 2525–2556.
[38] Suryotrisongko, H.; Musashi, Y.; Tsuneda, A.; Sugitani, K. Robust botnet DGA detection: Blending XAI and OSINT for CTI sharing. IEEE Access 2022, 10, 34613–34624.
[39] Moraliyage, H.; Sumanasena, V.; De Silva, D.; Nawaratne, R.; Sun, L.; Alahakoon, D. Multimodal classification of onion services for proactive CTI using explainable deep learning. IEEE Access 2022, 10, 56044–56056
[40] Irshad, E.; Siddiqui, A.B. Cyber threat attribution using unstructured reports in CTI. Egypt. Inform. J. 2023, 24, 43–59.
[41] Zhang, H.; Shen, G.; Guo, C.; Cui, Y.; Jiang, C. Ex-action: Automatically extracting threat actions from CTI report based on multimodal learning. Secur. Commun. Netw. 2021, 2021, 1–12.
[42] Cha, J.; Singh, S.K.; Pan, Y.; Park, J.H. Blockchain-based CTI system architecture for sustainable computing. Sustainability 2020, 12, 6401.
[43] Gong, S.; Lee, C. CTI framework for incident response in an energy cloud platform. Electronics 2021, 10, 239.
[44] Ejaz, S.; Noor, U.; Rashid, Z. Visualizing Interesting Patterns in CTI Using Machine Learning Techniques. Cybern. Inf. Technol. 2022, 22, 96–113.

[45] Mendez Mena, D.; Yang, B. Decentralized actionable CTI for networks and the internet of things. IoT 2020, 2, 1–16.
[46] Liu, J.; Yan, J.; Jiang, J.; He, Y.; Wang, X.; Jiang, Z.; Yang, P.; Li, N. TriCTI: An actionable CTI discovery system via trigger-enhanced neural network. Cybersecurity 2022, 5, 8.
[47]A.Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecurity (Springer Open), vol. 2, no. 1, p. 20, 2019.
[48]Unsupervised GAN-Based Intrusion Detection System Using Temporal Convolutional Networks and Self-Attention," IEEE Journals & Magazine, 2023.
[49]"Adversarial Malware Detection," in Proc. Springer Conference/Book Chapter, 2025.
[50] "LSGAN-AT: enhancing malware detector robustness against adversarial examples," Cybersecurity (Springer Open), 2021.
[51] "On the effectiveness of adversarial samples against ensemble learning-based Windows PE malware detectors," International Journal of Information Security (Springer), 2025.
[52] "GAN-Based Adversarial Attack Against Malware Detection," in Proc. IEEE Conference (IEEE Xplore), 2025.
[53] "Analyzing the Vulnerabilities Introduced by DDoS Mitigation Techniques for Software-Defined Networks," in Proc. Springer Conference, 2019.
[54] "Resilient intrusion detection system for adversarial attacks on Low-Rate DDoS," International Journal of Machine Learning and Cybernetics (Springer), 2025.
[55] "DDoS mitigation using blockchain and machine learning techniques," Multimedia Tools and Applications (Springer), 2024.
[56] "Next-Generation Firewalls and AI-Based Detection Systems for DDoS Mitigation," in Proc. Springer Conference, 2025.
[57] "Design and analysis of DDoS mitigating network architecture," International Journal of Information Security (Springer), 2022.