# Real-Time Threat Intelligence Integrated Ethical Hacking for DoS Threats Detection: A Systematic Literature Review

Anuprita Joshi[1], Sandhya Kaprawan[2]
[1]*M.S. Cyber Security Student, University of Mumbai*
[2]*Assistant Professor, University of Mumbai*
*doi.org/10.64643/IJIRTV12I12-201292-459*

***Abstract*— The complexity in the new variants of DoS attacks is rising immensely, making it more challenging to detect emerging DoS attacks and mitigate them in real-time. This requires transitioning from reactive security approaches to proactive intelligence-driven defense strategies combined with offensive validation to bridge the gap in existing methods. This research dedicates its focus to an intensive literature review on Real-Time Threat Intelligence Integrated Ethical Hacking especially for DoS (Denial of Service) Threats by also mapping it to MITRE ATT&CK matrix and utilizing BAS (Breach and Attack Simulation). A Systematic Literature Review methodology was adopted in analyzing 29 core studies by implementing qualitative as well as quantitative synthesis. This literature review states its results that despite various advancements are made in AI driven DoS detection, there are high failure rates against unknown TYPE-A attacks, false-positives in TYPE-B attacks (new variants of known threats) and a data grounding problem due to the use of outdated and static databases. This paper concludes that pivoting an automated bridge between Cyber Threat Intelligence and Real-time Offensive validation is essential to close the research gap and build a new, resilient, and automated defense framework.**

***Index Terms*— Real time threat intelligence, Cyber threat intelligence, DoS, Denial of Service, Ethical hacking, DoS threat detection.**

## I. INTRODUCTION

The surging refinement of multi-vector Denial-of-Service (DoS) attacks needs a transition from reactive security to proactive, intelligence-driven defense architectures [10]. The rapid emergence of new vulnerabilities has failed to be encompassed due to the traditional yearly penetration tests being increasingly inadequate, creating a security gap [17]. Modern cybersecurity environments, specifically concerning the Critical Information Infrastructure and Software-Defined Networks, remain highly vulnerable to protocol-specific exploits that current defenses which are often reliant on outdated datasets and static signatures fail to detect, that lead to high false-positive rates [15], [21], [25]. Hence, a significant disconnect exists between the gathering of global Cyber Threat Intelligence (CTI) and the tactical execution of offensive testing [10], [12]. To address this issue, AI-augmented frameworks like PenTest++ can automate reconnaissance, while AI-driven Breach and Attack Simulation (BAS) mimics adversary behaviors to identify deep-seated vulnerabilities [7], [16]. By mapping intelligence to the MITRE ATT&CK matrix and utilizing Snort-based detection to validate friendly simulations, organizations can develop a closed-loop, threat-informed offensive lifecycle that transforms reactive measures into a resilient, automated defense framework [20], [29], [13].

The subsequent sections of this paper are structured as: Section II evaluates the existing research through a Systematic Literature Review, Section III outlines the Research Methodology with a detailed PRISMA flow protocol, Section IV discusses the findings from the review while Section V reports the results obtained from this research. At the end, Section VI concludes the study and suggests future research directions.

## II. LITERATURE REVIEW

### A. Analysis of Existing Literature Work

#### 1) Architectures for Real-Time Threat Intelligence and Adaptive Defense

In the modern cybersecurity landscape, a transition from static perimeters to real-time threat intelligence integrated systems is needed to inform adaptive defense mechanisms [10]. High-fidelity intelligence feeds are essential for detecting sophisticated attack vectors and evolving malicious behaviors before they manifest as full-scale breaches [10]. These intelligence-driven frameworks allow the automated correlation of incidents and coordinated governance across borderless networks, which is quite critical for national and organizational resilience [3]. Furthermore, the systematic mapping of intelligence against standardized matrices, such as ATT&CK, provides a rigorous method for assessing the severity and tactical nature of incoming threats [20]. This intelligence-led approach makes sure that defensive configurations remain dynamic and capable of handling modern adversary tactics [10].

2) AI-Driven Breach Simulation and Automated Penetration Testing

Automated Breach and Attack Simulation (BAS) has emerged as a crucial link for ethical hacking, allowing for the continuous validation of security controls with the help of AI-driven methodologies [16]. By mimicking the specific tactics, techniques, and procedures (TTPs) of known threat actors, BAS tools identify deep-seated vulnerabilities that traditional manual testing might overlook [16]. Professional frameworks like PenTest++ further elevate this process by integrating AI to automate the reconnaissance and scanning phases of vulnerability assessments [7]. These automated simulations provide immediate feedback on network weaknesses, enforcing rapid remediation and hardening of the attack surface [17]. Such continuous testing is important for maintaining a strong security posture in rapidly changing cloud and hybrid environments [16].

3) Real-Time Detection and Mitigation of DoS in SDN and Smart Grids

Denial-of-Service (DoS) attacks pose a significant threat to Critical Information Infrastructure (CII), particularly in smart grid applications where communication vulnerabilities can lead to physical disruptions [15]. Within Software-Defined Networks (SDN), specialized modules like DoSGuard offer scalable, protocol-independent defense by monitoring OpenFlow messages for anomalies [21]. DoSGuard maintains a consistency map between switches and hosts to filter malicious packets with minimal CPU overhead, making sure the defense does not become a performance bottleneck [21]. Similarly, trust-based detection models are essential in smart business environments to identify and block DoS traffic before it saturates network resources [4]. These real-time mitigations are critical for maintaining service availability during active, high-volume attack campaigns [21].

4) Machine Learning Approaches for Anomaly and Pattern Recognition

Advanced detection of DoS threats increasingly relies on hybrid deep learning models that capture both spatial and temporal traffic features simultaneously [15]. Innovative research even utilizes computer vision techniques to convert network traffic into image-based representations, allowing for the application of high-speed visual recognition algorithms to detect attack signatures [28]. To ensure these models remain accurate in real-time, feature selection techniques like the Slime Mould Algorithm are used to identify the most relevant network parameters and reduce data noise [18]. This dimensionality reduction is necessary for achieving the low latency required for an effective real-time security response [2]. These models are specifically effective at identifying multi-vector attacks that attempt to blend in with legitimate traffic bursts [15].

5) Holistic Management of Open-Source Cyber Threat Intelligence (CTI)

A holistic approach to CTI management involves the automated gathering of open-source intelligence through systems like ThreatKG, which builds AI-powered knowledge graphs of emerging threats [12]. Integrating these knowledge graphs with risk assessment frameworks allows organizations to prioritize vulnerabilities based on their exploitability in current global scenarios [11]. Collaborative intrusion detection networks further boost the quality of CTI by allowing different entities to share threat signatures and attack patterns in real-time [19]. This shared intelligence is vital for detecting large-scale, coordinated DoS attacks that target multiple infrastructure sectors simultaneously [13]. Such frameworks ensure that organizations maintain visibility over a broader threat landscape than they could achieve through internal monitoring alone [19].

6) Explainable AI (XAI) and Automated Mitigation for Critical Infrastructure

In critical infrastructure, the use of AI for threat mitigation must be accompanied by explainability to make sure that automated actions are transparent and justifiable [6]. Explainable AI (XAI) frameworks allow security analysts to interpret the logic behind an automated "block" or "quarantine" command, significantly reducing the risk of costly false positives [5]. This is especially important for DoS analysis, where legitimate traffic surges must be distinguished from malicious flooding attempts [5]. AI-powered systems can also automate the patching of identified vulnerabilities, closing the window of opportunity for attackers in real-time [1]. This "closed-loop" security model—from detection to explanation to remediation—represents the next generation of cybersecurity defense for essential services [6].

7) VAPT and Systematic Penetration Testing

Systematic reviews of penetration testing taxonomies reveal that standardized frameworks and scoring methods are essential for consistent and repeatable security evaluations [14]. Integrated Vulnerability Assessment and Penetration Testing (VAPT) for web applications utilize tools like Kali Linux and the Metasploit framework to simulate realistic and complex attack scenarios [23]. These assessments are increasingly based on threat modeling, ensuring that the testing focus is placed on the most likely and high-impact attack paths [24]. For educational and research purposes, the use of packet generators and snort rules allows for the controlled simulation of DoS attacks to train defense systems and personnel [29]. These methodologies ensure that ethical hacking remains a disciplined, rigorous, and professional practice [26].

8) The Growing Threat of Underrated Denial-of-Service Vectors

Despite the focus on sophisticated data breaches, Denial-of-Service remains a growing and often underrated threat to global digital stability and service continuity [22]. Analysis of various DoS types shows that even simple flooding techniques can be devastating if not met with real-time prevention and mitigation strategies [27]. Modern DoS threats have evolved to target application layers, requiring deep packet inspection and behavioral analysis to mitigate effectively [27]. Real-time response systems must, therefore, be capable of identifying "low and slow" attacks that attempt to bypass traditional volume-based triggers [2]. Continuous monitoring and the integration of adaptive intelligence remain the primary defenses against this persistent and evolving threat landscape [10].

9) Detection of Unknown Security Attacks

A significant challenge in the literature is the detection of "unknown" security attacks—those that do not match predefined categories during the machine learning model's training phase [25]. Research distinguishes between Type-A unknown attacks (completely new categories) and Type-B (new variations within known categories) [25]. Evaluations of nearly 100 different deep learning models revealed that many struggle with Type-A attacks, often exhibiting significant error rates [25]. This highlights a critical need for innovative techniques, such as unsupervised learning and ensemble methods, to address the problem of unknown security threats in real-time [25].

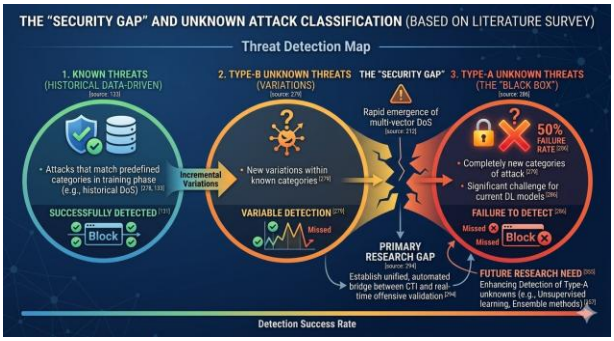


Fig. 1. Security gap of Unknown Attacks (Author generated using reviewed literature)

*B. Comparative Analysis*

TABLE I. Existing VS Proposed Work

| Feature | Existing Work | Proposed Work |
|---|---|---|
| **Data Foundation** | Relies on static vulnerability databases and manual log analysis [17]. | Built on dynamic, real-time Cyber Threat Intelligence (CTI) feeds [10]. |
| **Attack Framework** | Generic testing often lacks a structured adversary behavioral model [26]. | Strictly mapped to the MITRE ATT&CK matrix for tactical adversary emulation [20]. |
| **Simulation Trigger** | Manual or scheduled penetration tests triggered by human intervention [24]. | Automated CTI-integrated DoS attack simulations triggered by incoming threat indicators [16]. |

| | | |
|---|---|---|
| **Detection Engine** | Standard firewalls or basic AI models are often susceptible to high false positives [5]. | Real-time detection using Snort with custom rulesets [29]. |
| **Response Loop** | Disconnected; results are manually reported to SOC teams [1]. | Closed loop; simulation results directly inform and suggest defensive policies [21]. |

The current literature builds a clear tension between modern DoS (Denial of Service) attacks and limitations of existing defense mechanisms. While this paper prioritizes the Real-Time Threat Intelligence (RTII) Integration necessary to inform adaptive defenses, a disconnect continues to persist between the intelligence acquisition and its application during offensive validation [10]. While the Automated Breach and Attack Simulation (BAS) and PenTest++ frameworks provide notable advances made in continuous security validation, both of them are often considered as independent entities from Real-Time Detection modules used in SDN (Software-Defined Networks) or Smart Grids [16], [7], [21], [15]. Although high-level Machine Learning (ML) and Computer Vision models have improved detection speeds, they frequently are hurdled by TYPE-A unknown attacks and lack Explainable AI (XAI) transparency necessary for critical information infrastructure [15], [28], [25], [6]. After comparing; Threat Intelligence, Attack Simulation and Detection are individually quite robust but lack a unified technical feedback loop. By failing to translate unstructured, real-source CTI into quick, actionable DoS simulations that validate Snort-based detection rules in real-time; the data grounding problem of outdated data failed to be bridged by current existing work [29], [1].

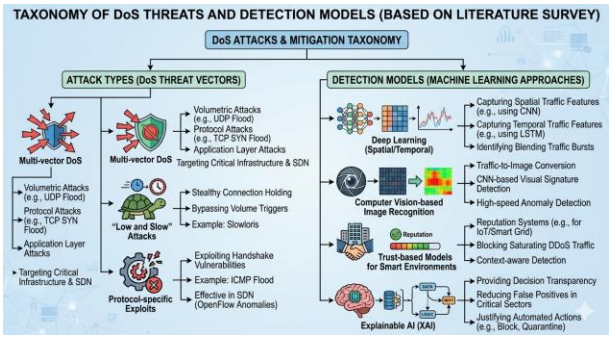


Fig. 2. DoS Threats and Detection Models Taxonomy (Author generated using reviewed literature)

### *C. Limitations of Current Literature*

#### 1) Technical Constraints

Current systems struggle with Type-A unknown attacks, showing failure rates near 50% [25]. Many AI models function as "black boxes", lacking the interpretability required for high-stakes decisions in critical infrastructure [6]. Additionally, legacy system integration remains computationally expensive, often adding significant latency [10].

#### 2) Scope and Scarcity

Existing frameworks are often siloed within specific domains like Smart Grids [15] or SDN [21]. Furthermore, there is a "data-grounding problem" caused using outdated datasets like NSL-KDD, which fail to reflect 2025-era multi-vector DoS tactics [1].

### *D. Identification of Research Gaps*

The research gap identified from the above literature review is the absence of a unified and automated bridge between CTI and real-time offensive validation. Even though threat intelligence, offensive testing and DoS detection have been addressed independently, there is a crucial need for a system that can:

1) Automate Intelligence-to-Attack-Pipeline which directly translates unstructured CTI into actionable DoS simulations using MITRE ATT&CK framework [10].

2) Implements Real-time Rule Validation which uses Snort-based detection to get immediate feedback if a friendly simulation, modeled on current global threats can bypass existing defenses or not [29].

3) Creates a Technical Feedback Loop that bridges the gap between knowing about a threat and justifying why a defense mechanism works; through continuous, automated integration of threat intelligence and ethical hacking [16].

## II. METHODOLOGY

To ensure a rigorous, transparent, and reproducible synthesis of existing knowledge, this study employs a Systematic Literature Review (SLR) methodology; which investigates the intersection of Real-Time Threat Intelligence (CTI) and Ethical Hacking specifically within the domain of Denial-of-Service (DoS) detection and mitigation.

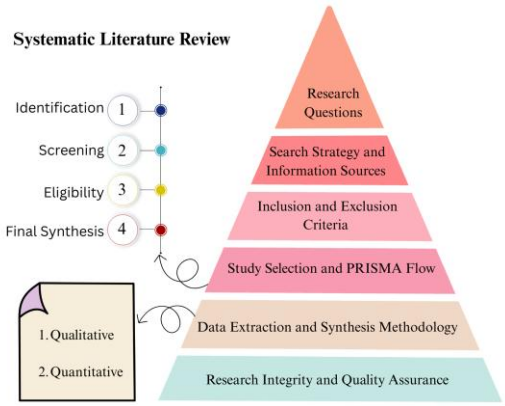


Fig. 3. *Systematic Literature Review Methodology (Author generated using reviewed literature)*

### A. *Research Questions*

The research question that this paper aims to find answers are:

1) What are the existing works related to this area?
2) What methodologies have been used for DoS Detection?
3) How does the paper title bridge the research gap identified?
4) How real-time threat intelligence integrated ethical hacking detects DoS Threats?

### B. *Search Strategy and Information Sources*

The literature review analyzed 29 research papers collected from various repositories, databases, and journals. This search captured high-impact, peer-reviewed, and open access published journals as well as preprints and specifically published between 2013 and 2026. The primary databases were ACM Digital Library, IEEE Xplore, MDPI, Wiley Online Library, and ProQuest. Other Aggregators, Repositories and Search Engines include Google Scholar, arXiv.org and ResearchGate.

### C. *Inclusion and Exclusion Criteria*

To maintain high technical standards and focus on the specific problem definition, the following criteria were applied:

TABLE II. Inclusion/ Exclusion Criteria

| Criteria | Inclusion (Accepted) | Exclusion (Rejected) |
|---|---|---|
| Focus | DoS detection, MITRE ATT&CK, Threat Intelligence Integration frameworks, Ethical Hacking. | Unrelated networking or malware, irrelevant DDoS attack only focused work. |
| Type | Pre-prints, Peer-reviewed journals and conferences. | Blog posts, editorials, or posters. |
| Method | Empirical studies or architectural models. | Subjective opinion pieces without data. |
| Timeline | July 2013 – January 2026. | Research older than 2013 (unless seminal). |

### D. *Study Selection and PRISMA Flow*

The selection process was in accordance with the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol. This process involved - Identifying initial papers through database search engines like Google Scholar, Screening the papers based on the relevance to the topic, checking Eligibility of Full-text articles by assessing against the inclusion/exclusion criteria and Final Synthesis where 29 core studies were selected for thematic and quantitative analysis.

### E. *Data Extraction and Synthesis Methodology*

The review utilizes a Mixed-Methods Synthesis approach to process the findings from the selected papers. Quantitative Synthesis in which technical performance metrics were extracted and compared. Qualitative Thematic Analysis in which findings were categorized into key integration strategies. Technical taxonomies and conceptual frameworks were visualized using Gemini and Canva.

### F. *Research Integrity and Quality Assurance*

In compliance with modern academic standards for research, the following measures were taken - Originality Verification via Paperpal, PaperOwl, and Grammarly to ensure a low similarity index and verify human-led synthesis; along with Quillbot and Scribbr were utilized for citation cross-referencing.

## III. DISCUSSION

The limitation of tradition often fosters the inadequacy of scheduled penetration testing, which becomes a recurring theme. This creates a security gap that fails to accommodate the rapid surfacing of new vulnerabilities and growing threats. AI enables less complex and classified types of automated attack simulations, which makes it resemble a double-edged sword. The use of AI in DoS attack detection can grant spatial and temporal traffic analysis often needed to detect low and slow DoS attacks missed by volume-based triggers. Explainable AI (XAI) might be required due to the nature of AI being a Black Box, to

justify automated blocking or other actions in a critical sector. AI is referred to as a Black box since you can see what data is fed inside and what decision is generated but not the entire exact logic that goes behind it. The discussion also reveals that specialized environments such as Smart Grid Systems or SDN (Software-Defined Networks) need specialized modules to maintain consistency maps and filter out malicious packets without causing congestion points in the performance. The most significant finding in the discussion is the disconnect between knowing - CTI feeds and proving - Ethical Hacking in an automated environment for quick assessment or penetration testing. It's very rare to find both in a real-time and automated framework, which this research paper identifies the gap and addresses it.

## IV.RESULTS

Deep Learning Models being incorporated with dimensionality reduction techniques like Slime Mould Algorithm results in acquiring low latency required for the real-time response, simultaneously keeping high accuracy against multi-vector DoS Attacks. The above analysis depicts that existing deep learning models cater for almost half of the failure rates against TYPE-A (completely new) attacks. Threat Intelligence mapped to MITRE ATT&CK matrix improves the overall effectiveness for assessment, in comparison with unstructured testing. A crucial result of this paper identified is the "data grounding problem". For example, a student reading the wrong reference book for the exam. If the data used is anchored in old databases like NSL-KDD, it won't be able to detect new attack vectors. This leads to Data Aging Issues.

## V. CONCLUSION AND FUTURE WORK

### *A. Conclusion*

This paper concludes even though plenty of the advances are being made in AI-driven DoS detection, machine learning algorithms-based DoS patterns detection, and automated penetration testing, there is a lack for a centralized orchestrator between real-time threat intelligence and ethical hacking for offensive validation. In complex environments, static signatures, high false-positive rates, and a lack of interoperability in automated decisions cause frequent obstruction in the existing defense strategies or framework. There is also a need to address that volume-based alerts might miss identification of low and slow attacks. Organizations can hugely cut down the benefit of doubt to create an opportunity for attackers by pivoting a closed-loop system where real-time CTI (Cyber Threat Intelligence) informed automated simulations can validate and provide updated detection rules or suggest patches to be implemented.

### *B. Future Work*

The future work majorly involves using SOAR (Security Orchestration, Automation and Response) in building a centralized orchestrator that integrates Real-time threat intelligence and MITRE ATT&CK Framework metric into feeds and triggering automated simulations based on those feeds to detect if there exists a vulnerability for TYPE-B attacks (known attack patterns with new variants) along with updating Snort rules or suggesting patches. Another scope of work can focus on investigating unsupervised learning and ensemble methods or algorithms to reduce the volume of failure rates associated with TYPE-A attacks (completely new and unknown threats). Along with this, developing and implementing updated datasets that reflect 2026 latest attack vectors to resolve the data grounding problem.

## REFERENCES

[1] M. Malkawi and R. Alhajj, “AI-Powered Vulnerability Detection and Patch Management in Cybersecurity: A Systematic review of techniques, challenges, and emerging trends,” Machine Learning and Knowledge Extraction, vol. 8, no. 1, p. 19, Jan. 2026, doi: 10.3390/make8010019.

[2] M. K. Mahto, “Dynamic Threat Intelligence,” Wiley Online Library, pp. 107–136, Jan. 2026, doi: 10.1002/9781394305698.ch5.

[3] K. A. Olakojo, “Strengthening Cross-Border cybersecurity resilience through federated threat intelligence sharing, Real-Time incident correlation, and coordinated governance mechanisms,” International Journal of Computer Applications Technology and Research, Dec. 2025, doi: 10.7753/ijcatr1312.1011.

[4] O. Okporokpo, F. Olajide, N. Ajienka, and X. Ma, “A novel Trust-Based DDOS cyberattack detection model for smart business

environments," arXiv (Cornell University), Dec. 2025, doi: 10.48550/arxiv.2512.04855.

[5] P. B. Yakubu, L. Santana, M. Rahouti, Y. Xin, A. Chehri, and M. Aledhari, "Automated and explainable denial of service analysis for AI-Driven intrusion detection systems," arXiv (Cornell University), Nov. 2025, doi: 10.48550/arxiv.2511.04114.

[6] J. Paulraj, B. Raghuraman, N. Gopalakrishnan, and Y. Otoum, "Autonomous AI-based cybersecurity framework for critical infrastructure: Real-Time threat mitigation," arXiv (Cornell University), Jul. 2025, doi: 10.48550/arxiv.2507.07416.

[7] H. S. Al-Sinani and C. J. Mitchell, "PenTest++: Elevating Ethical Hacking with AI and Automation," arXiv (Cornell University), Feb. 2025, doi: 10.48550/arxiv.2502.09484.

[8] A. Spyros et al., "AI-Based Holistic Framework for Cyber Threat Intelligence Management," IEEE Access, vol. 13, pp. 20820–20846, Jan. 2025, doi: 10.1109/access.2025.3533084.

[9] S. Shah and F. K. Parast, "AI-Driven Cyber Threat Intelligence Automation," arXiv (Cornell University), Oct. 2024, doi: 10.48550/arxiv.2410.20287.

[10] M. Aminu, A. Akinsanya, D. A. Dako, and O. Oyedokun, "Enhancing Cyber Threat Detection through Real-time Threat Intelligence and Adaptive Defense Mechanisms," International Journal of Computer Applications Technology and Research, Jul. 2024, doi: 10.7753/ijcatr1308.1002.

[11] V. V. Ríos, F. Zaidi, A. R. Cavalli, and A. Rego, "Towards the adoption of automated cyber threat intelligence information sharing with integrated risk assessment," ACM Digital Library, pp. 1–9, Jul. 2024, doi: 10.1145/3664476.3670444.

[12] P. Gao, X. Liu, E. Choi, S. Ma, X. Yang, and D. Song, "ThreatKG: An AI-Powered System for Automated Open-Source Cyber Threat Intelligence Gathering and Management," ACM Digital Library, pp. 1–12, Nov. 2023, doi: 10.1145/3689217.3690613.

[13] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," Sensors, vol. 23, no. 16, p. 7273, Aug. 2023, doi: 10.3390/s23167273.

[14] K. U. Sarker, F. Yunus, and A. Deraman, "Penetration Taxonomy: A systematic review on the penetration process, framework, standards, tools, and scoring methods," Sustainability, vol. 15, no. 13, p. 10471, Jul. 2023, doi: 10.3390/su151310471.

[15] M. K. Hasan, A. K. M. A. Habib, S. Islam, N. Safie, S. N. H. S. Abdullah, and B. Pandey, "DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments," Energy Reports, vol. 9, pp. 1318–1326, Jun. 2023, doi: 10.1016/j.egyr.2023.05.184.

[16] C. Ubagaram, N. R. Dyavani, B. S. Jayaprakasam, R. R. Mandala, V. Garikipati, and V. K. R, "Ethical Hacking and Penetration Testing: Strengthening Cyber Defense with AI-Driven Breach and Attack Simulation," International Journal of Information Technology & Computer Engineering, vol. 11, no. 1, pp. 230–236, 2023, [Online]. Available: https://www.academia.edu/129873601/Ethical_Hacking_and_Penetration_Testing_Strengthening_Cyber_Defense_with_AI_Driven_Breach_and_Attack_Simulation

[17] P. Lachkov, L. Tawalbeh, and S. Bhatt, "Vulnerability assessment for applications security through penetration simulation and testing," Journal of Web Engineering, Dec. 2022, doi: 10.13052/jwe1540-9589.2178.

[18] S. Sokkalingam and R. Ramakrishnan, "An intelligent intrusion detection system for distributed denial of service attacks: A support vector machine with hybrid optimization algorithm based approach," Concurrency and Computation Practice and Experience, vol. 34, no. 27, Sep. 2022, doi: 10.1002/cpe.7334.

[19] M. Guarascio, N. Cassavia, F. S. Pisani, and G. Manco, "Boosting Cyber-Threat intelligence via collaborative intrusion detection," Future Generation Computer Systems, vol. 135, pp. 30–43, Apr. 2022, doi: 10.1016/j.future.2022.04.028

[20] S. Zhang et al., "An Automatic Assessment Method of Cyber Threat Intelligence Combined with ATT&CK Matrix," Wireless Communications and Mobile Computing, vol.

2022, no. 1, Jan. 2022, doi: 10.1155/2022/7875910

[21] J. Li, T. Tu, Y. Li, S. Qin, Y. Shi, and Q. Wen, "DOSGuArd: Mitigating Denial-of-Service Attacks in Software-Defined Networks," Sensors, vol. 22, no. 3, p. 1061, Jan. 2022, doi: 10.3390/s22031061.

[22] W. Bonasera, M. M. Chowdhury, and S. Latif, "Denial of service: a growing underrated threat," 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Oct. 2021, doi: 10.1109/iceccme52200.2021.9591062.

[23] M. Tabassum, S. Mohanan, and T. Sharma, "Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework," International Journal of Innovation in Computational Science and Engineering, vol. 2, no. 1, May 2021, [Online]. Available: https://www.researchgate.net/profile/Mujahid-Tabassum/publication/353320995_Ethical_Hacking_and_Penetrate_Testing_using_Kali_and_Metasploit_Framework/links/60f3a46cfb568a7098b94fe5/Ethical-Hacking-and-Penetrate-Testing-using-Kali-and-Metasploit-Framework.pdf

[24] G. Salzillo, M. Rak, and F. Moretta, "Threat Modeling based Penetration Testing: The Open Energy Monitor Case study," ACM Digital Library, pp. 1–8, Nov. 2020, doi: 10.1145/3433174.3433181.

[25] M. Al-Zewairi, S. Almajali, and M. Ayyash, "Unknown security attack detection using shallow and deep ANN classifiers," Electronics, vol. 9, no. 12, p. 2006, Nov. 2020, doi: 10.3390/electronics9122006.

[26] K. S. Prasad, K. R. Sekhar, and P. Rajarajeswari, "An Integrated Approach Towards Vulnerability Assessment & Penetration Testing for a Web Application," International Journal of Engineering & Technology, vol. 7, no. 2.32, p. 431, May 2018, doi: 10.14419/ijet.v7i2.32.15733.

[27] K. Thakur, "Analysis of Denial of Services (DOS) Attacks and Prevention Techniques," International Journal of Engineering Research & Technology (IJERT), vol. 4, no. 7, Sep. 2015, [Online]. Available: https://www.ijert.org/research/analysis-of-denial-of-services-dos-attacks-and-prevention-techniques-IJERTV4IS070164.pdf

[28] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu, and J. Hu, "Detection of Denial-of-Service attacks based on computer vision techniques," IEEE Transactions on Computers, vol. 64, no. 9, pp. 2519–2533, Nov. 2014, doi: 10.1109/tc.2014.2375218.

[29] Z. Trabelsi and L. Alketbi, "Using network packet generators and snort rules for teaching denial of service attacks," ACM Digital Library, pp. 285–290, Jul. 2013, doi: 10.1145/2462476.2465580