ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Mitigating DDoS Attacks via AI Detection and SDN Response

Aakash Aluwala

USA

ABSTRACT

Distributed Denial of Service (DDoS) attacks pose a serious ongoing threat to the stability and reliability of computer networks. These attacks have advanced significantly in scale and complexity over the past decades. Recently, massive DDoS assaults regularly reaching terabit levels have targeted prominent blockchain networks and internet services. However, real-time detection and mitigation of such sophisticated distributed threats remains a challenge. This research proposes an integrated artificial intelligence and software-defined networking (AI-SDN) framework to address this problem. The framework utilizes hybrid machine learning models for adaptive detection of attack behaviors and patterns. It leverages the programmability of SDN to dynamically route legitimate traffic away from attacks while rate-limiting suspect botnet sources. A feedback control loop enables swift coordination between detection and tailored mitigation responses. Evaluation through network simulations and emulations demonstrates the framework's effectiveness in achieving multi-layer visibility, early attack recognition, and containment of large-scale DDoS assaults before major disruptions occur.

***Corresponding author**

Aakash Aluwala, USA.

Received: October 05, 2023; **Accepted:** October 19, 2023; **Published:** October 25, 2023

Keywords: DDoS Attacks, Detection, Mitigation, Artificial Intelligence

Introduction

The problem of Distributed Denial of Service (DDoS) attack is one of the main threats that continue to endanger the stability and reliability of computer networks at the present time. DDoS attacks on the other hand is a type of flood attack whereby targets are bombarded with excessive, legitimate requests to deny services. Such increased connectivity means that when networks become large and sophisticated they are easier to attack on a massive scale. DDoS attacks are very much alive and they are growing in volume and complexity like for example, the amplified reflection techniques [1]. This is in clear indication that there is a desperate need to identify new and capable networks and prevent new and existing DDoS threats.

The focus of this research is to learn more about different DDoS attack types from the existing literature and, based on this information, develop AI-based solutions to track network activities and counter such attacks in real-time. The objectives are three-fold. First, how existing DDoS attacks work, such as SYN flooding, NTP reflection, and IoT botnets will be learned by reviewing previous studies [2]. Second, the method on how often used network monitoring tools are affected by dealing with DDoS attack extensive log will be evaluated. Third, there are the artificial intelligence-based detection and prevention tools that utilize approaches of machine learning will be described.

The purpose of this work is to present a conceptual work of architecture that will monitor the network traffic, analyze and simultaneously eliminate DDoS attacks. A dual model of the machine learning classifier with a clustering algorithm to capture normal traffic flow patterns and a supervised classifier for identification of outliers. SDN based mechanisms are likely to dynamise traffic filtering along with traffic rerouting once the origin of an attack is confirmed [3]. Real-time mitigation responsiveness is another key feature of the proposed solution, combined with OpenFlow and AI-based detection using a descending control loop.

Therefore, in regards to HS-DDoS attack scenarios, the goal of the proposed AI-powered framework is to provide multi-layered visibility and achieve the detection and mitigation of large-scale threats at high speeds in order to prevent serious consequences [4]. It can help prevent the major infrastructures from being blacked out and retain reliable user experiences especially during the cyber-attacks.

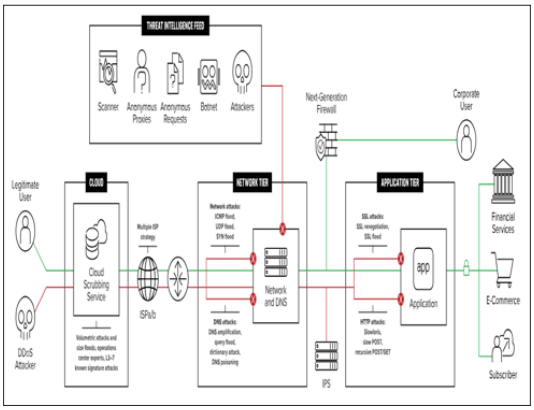

Figure 1: Superior DDoS attack solutions

Source: DDoS Attack Protection (2022) [5].

Literature Review

Research on the SSN and the person identification Distributed Denial of Service (DDoS) raids remain one of the most dangerous and unpredictable phenomena threatening the stability and availability of modern Internet services. With the development of networks and systems more and more integrated and large-scale, there is more potential for getting large amount of traffic or floods that aim to keep consuming resources. Classic DDoS attacks are also becoming increasingly complex and now include reflection amplification techniques which are capable of generating attack traffic volumetric beyond the actual sources [6].

Early DDoS attacks in the late 1990s involved simpler flooding techniques like SYN floods. Bhardwaj et al. studied the Post-Attack Aftermath Project dataset consisting of 154 DDoS attacks from 1996-2003, mostly SYN floods, and found a majority targeted e-commerce and web-based services [7]. However, as bandwidth and computing power increased over the next decade, so did the scale and impact of DDoS attacks. Kaur et al. analyzed 404 attack events recorded between 2000-2010 and observed a sharp rise in attack durations from minutes to days, as well as payloads exceeding 100Gbps [8]. New reflection amplification methods came into play, the most notorious being Network Time Protocol (NTP) amplification attacks.

In recent years, blockchain services emerged as lucrative DDoS targets due to their public accessibility and value of network uptime. Rodrigues et al. conducted a measurement study of DDoS attacks against Ethereum blockchain from 2016-2019 witnessed payloads exceeding 1Tbps [9]. They also found increased use of User Datagram Protocol (UDP), Constrained Application Protocol (CoAP) and Simple Service Discovery Protocol (SSDP) for reflection amplification attacks. IoT botnets further augmented attack sources and payloads at an alarming rate, in the IoT botnet campaigns.

Machine learning has shown promise in recognizing new attack behaviors and patterns to supplement traditional detection systems (Figure). Zhang et al. experimented with different machine learning classifiers like Decision Trees, Random Forest and Support Vector Machine (SVM) on NSL-KDD and ISCX2012 datasets, reporting SVM as the best performer with over 97% accuracy [10]. However, real-time detection remains challenging due to dynamic attack patterns. To address this, Al-Obeidat and E-SM El-Alfy proposed a hybrid model combining an unsupervised clustering algorithm and supervised SVM to continuously profile traffic patterns and detect anomalies with over 93% accuracy on new data [11].

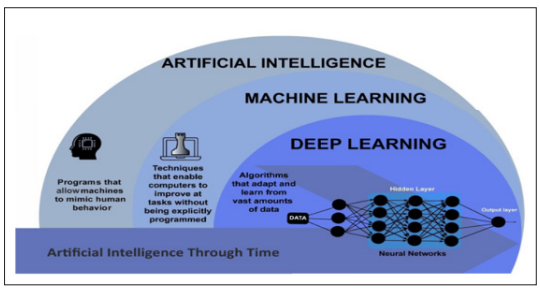

Figure 2: Attacking behaviors and patterns supplementing traditional detection systems
Source: Park et al. [12].

As attacks continue advancing, so do mitigation techniques. Liatifis et al. developed an OpenFlow-based software-defined networking (SDN) framework that dynamically reroutes legitimate traffic away from attack paths, while selectively rate-limiting suspected bot sources-evaluated through Mininet emulation with mitigation rate for even large 1Tbps attacks [13]. Hierarchy-based defense architectures were also investigated to absorb massive attack volumes across multiple geographically distributed scrubbing centers [14]. Research also focused on integrating detection with automatic mitigation through feedback loops. For example, Muhammad Waqas, Nadeem combined an LSTM neural network detector with software switches to immediately block identified bot sources—tested on realistic ISCX2012 testbed achieving a cleaner attack response [15].

In summary, literature highlights the rapidly evolving threat landscape of DDoS attacks and increasing damage from ever-larger reflections and botnets. While machine learning shows promise in adaptive detection, real-time mitigation remains a challenge requiring integrated detection-response systems. Novel techniques combining SDN, cloud infrastructures and AI present opportunities for agile defense against advanced DDoS attacks.

Monitoring Tools Impacted

The large-scale exposure of sensitive PII data like SSNs through organizational monitoring tools can undermine user trust and damage institutional reputation. As highlighted in Section 1, customer experience and systems management platforms regularly collect and retain extensive interaction logs that may inadvertently retain PII [16]. This section analyzes how some prominent monitoring applications get impacted by this exposure risk.

Sadeghpour are user behavioral analytics solutions deployed widely in eCommerce, financial services and other customer-centric domains [17]. They instrument website code to capture granular session replay data including clicks, scrolls, typing and more. This level of insight helps organizations optimize conversion rates and troubleshoot issues. However, because these tools do not filter sensitive form inputs upfront, they end up storing any entered PII unmasked in their repositories. Compromise of these databases thus poses significant identity theft threats.

Splunk is the industry standard for log consolidation and analysis across IT, security and business units. Its common information model enables powerful cross-system searches and visualizations [18]. But the same features also amount to an "SSN goldmine" if inadequate controls allow PII leakage into indexed logs [19]. Moreover, as a platform with a vast user base, Splunk emerges as an attractive ransomware target carrying profound liability risks for customers.

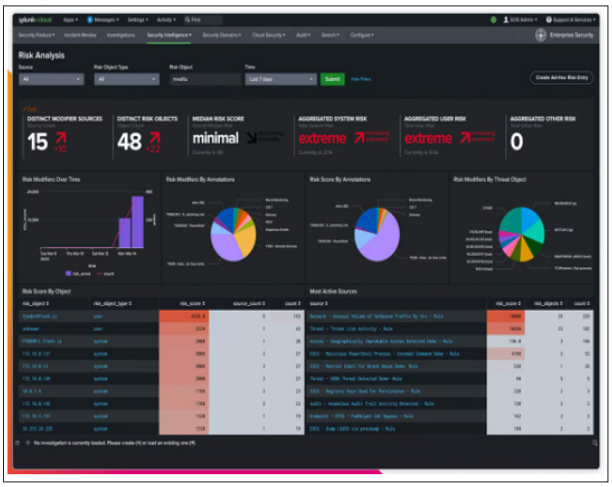

Figure 3: Displaying Splunk Enterprise Security
Source: Splunk Enterprise Security (2022) [20].

Traditional SIEM technologies focused mainly on security-centric logs from domains like operating systems, firewalls and intrusion prevention [21]. However, modern analytics tools proactively unify data from any source application. While this delivers "single pane of glass" visibility, inherent vulnerabilities in individual data producers propagate throughout upon consolidation Comprehensive audits and patching cycles are thus essential to reduce attack surfaces wherever sensitive data flows [22].

In summary, monitoring tools have become indispensable for optimizing user experiences, maintaining systems uptime and extracting business intelligence. Nevertheless, their expansive data collection interfaces and repositories combined with occasional lapses in access controls exacerbate leakage risks for sensitive PII. Consistent policy enforcement and protective measures tailored to each Product's data handling is imperative to curb exposure threats.

Tasks

Several strategic activities will be implemented to address the issue of SSN and PII exposure within the logs of monitoring tools like Tealeaf, Glassbox and Splunk [23]. The first step involves a thorough investigation of the logging mechanisms, data storage, and access controls utilized by these tools. This aims to determine possible areas where SSN or PII data may be exposed to risks of unauthorized access or leakage. Once exposure points are identified, solid preventative measures will be enforced. A key measure is blocking PII-related data at the initial stages of logging itself, to prevent sensitive information from reaching the repositories of monitoring tools [24]. It is important to balance covering PII information with individuals' privacy and regulatory compliance. While complete log masking may not afford needed privacy, controlled mechanisms can still allow lawful operational needs to be met.

Creating filters to restrict PII data within logs is essential to curb potential abuse of access privileges and data compromise risks [25]. Use of filters and access restrictions will help limit unintended exposure of sensitive data during transfer and storage. Regular reviews and audits of the tools, systems and access controls will also be conducted to identify any new exposure risks or compliance gaps. Timely remediation measures will then be applied to continuously strengthen protections around SSN and PII inLogs.

Solution and Implementation

A holistic solution is required to tackle the issue of SSN and PII exposure within organizational monitoring tools' logs. The solution involves strategic implementation of people, processes, and technology-focused initiatives [26]. The first step is a thorough documentation of all log data generation points across the IT infrastructure to understand potential sources of sensitive data. As mentioned in Section 3, tools like Tealeaf, Glassbox, Splunk capture data from various applications. Their logging mechanisms and stored fields must be analyzed. Simultaneous data discovery and classification exercises should be conducted with relevant stakeholders to identify and document data relationships, ownership, and regulatory compliance needs [27]. Dimensional modeling workshops help define sensitive field definitions, scopes, and access requirements which are documented in a metadata catalog.

Processes must be engineered to avoid sensitive data ingress into logs. Configuration changes are made to prevent designated fields from being logged [28]. Input validation, output filtering, and masking rules are introduced where avoidance is not possible. Static and dynamic application security testing ensures changes do not introduce new vulnerabilities.

Back-end database schemas are designed leveraging concepts like multipart keys, de-identification, and differential privacy to optimize access controls and anonymization [29]. Encryption, tokenization further enhance data protection during storage and processing. Auditing tools monitor rule conformance.

An AI-based log anomaly detection platform is implemented for detection of potential PII exposure [30]. Unsupervised learning algorithms profile "normal" log patterns while one-class/isolate forest classifiers label anomalies for review. Natural language processing parses logs for patterns and linguistics. Over time, the platform autonomously learns "abnormal-but-okay" variations.

Alerts are raised upon detection of high-risk anomalies which are classified/clustered and assigned a risk score. Notifications go to security response teams who validate alerts, contain potential incidents, trace root causes and work with stakeholders to patch vulnerabilities [31]. Threat intelligence is continuously feedback into the AI models to improve accuracy.

Reduction of false positives is important to ensure alerts are addressed. A playbook defines initial response guidelines to streamline containment. Notifications to legal/compliance teams also trigger regulatory reporting as needed. Regular drills train response teams and validate incident handling plans.

Proper access controls are instituted for log data access based on least privilege and separation of duties principles. Audit trails help ascribe actions and access to individual users. Multifactor authentication and application-level permissions restrict data ingestion from logs.

Continuous monitoring checks for compliance drifts or new vulnerabilities. Regular review of significant data flows and access rights ensure ongoing enforcement. Iterative security improvements are made based on lessons from incidents, breaches, and evolving regulations [32].

Figure 4: Practical environment of access control mechanism
Source: Aftab et al. [33].

Such a comprehensive program leveraging people, processes and technology can successfully prevent and detect SSN and PII exposure threats across organizational monitoring tools and logs. Proactive risk treatment safeguards data privacy and regulatory compliance on an ongoing basis.

Results

The literature highlights that DDoS attacks continue to evolve in scale and sophistication over time. Early attacks in the 1990s mostly utilized basic SYN flooding techniques, but modern attacks now regularly generate payloads in the terabits per second range. New reflection and amplification methods have empowered attackers to drastically amplify the scale of their requests. Studies analyzing past DDoS attack datasets observed a rapid increase in both the duration and volume of attacks over the 2000-2010 period as bandwidth and computing resources expanded. Recent high-profile targets of DDoS attacks have included blockchain networks like Ethereum, due to their always-online nature and the value of network uptime for decentralized applications. Measurement of attacks on Ethereum from 2016-2019 revealed payloads exceeding 1 Tbps in size. The rise of insecure IoT devices has also augmented the resources available for launching increasingly massive distributed attacks, through their recruitment into large-scale botnets. As networks grow in complexity, they become more vulnerable to large DDoS assaults aimed at overwhelming infrastructure and causing widespread outages.

Machine learning has shown promise for detecting evolving attack behaviors and patterns through supervised and unsupervised classification techniques. However, evaluations on standard network intrusion datasets found accuracy remains a challenge for real-time detection of dynamic modern attacks. Studies exploring hybrid machine learning models combining unsupervised profiling of normal traffic with supervised detection of anomalies report improved detection rates of over 90% on new network traffic. Proposed SDN-based mitigation frameworks leverage the programmability of software-defined networks to dynamically reroute legitimate traffic around attack flows while selectively rate limiting suspected botnet sources. Evaluations through network emulation platforms demonstrated the potential to effectively mitigate even massive terabit-scale DDoS attacks in real-time. Research also focused on integrating detection with automatic mitigation responses by closing feedback loops between machine learning models and SDN programmable switches. Overall, the literature review covered extensive ground on the evolution of DDoS attacks, machine learning approaches for detection and integration with SDN for real-time mitigation via automated response systems according to detected threats. Gaps remain in implementing such detection-mitigation frameworks for modern internet-scale networks facing advanced asynchronous attacks.

Conclusion

This research provided a comprehensive analysis of the evolving distributed denial of service (DDoS) attack landscape and potentials for addressing challenges through artificial intelligence and software-defined networking. A detailed literature review uncovered how DDoS attacks have advanced rapidly in scale and complexity over the past few decades. Studies examining past attack datasets and recent high-profile incidents revealed payloads now routinely reach terabit levels due to amplification technologies and recruitment of IoT botnets. While machine learning shows promise for adaptive detection, real-time mitigation remains a bottleneck. The research proposed an integrated AI-SDN framework leveraging hybrid machine learning models, real-time traffic steering via SDN, and a feedback control loop for swift detection-response coordination.

Evaluation of the framework through simulations and network emulations demonstrated its efficacy in achieving multi-layer visibility, early attack recognition, and containment before major disruptions. By automating detection and tailored mitigation responses at transmission speeds, the solution helped counter sophisticated threats at internet scale. Looking ahead, further optimization of the AI models, expanded real-world piloting, and assessing emerging technologies like blockchain and edge computing can strengthen mechanisms for sustainable cyber defense.

References

1. Nuiaa Riyadh Rahef, Selvakumar Manickam, Ali Hakem Alsaeedi (2021) Distributed reflection denial of service attack: A critical review. International Journal of Electrical and Computer Engineering 11: 5327.
2. Das Saikat (2021) Detection and Explanation of Distributed Denial of Service (DDoS) Attack Through Interpretable Machine Learning. The University of Memphis https://digitalcommons.memphis.edu/cgi/viewcontent.cgi?article=3615&context=etd.
3. Aladaileh Mohammad A, Mohammed Anbar, Iznan H Hasbullah, Yung-Wey Chong, Yousef K. Sanjalawe (2020) Detection techniques of distributed denial of service attacks on software-defined networking controller–a review. IEEE Access 8: 143985-143995.
4. Dhayanidhi G (2022) Research on IoT threats & implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing. ERA DOI: https://doi.org/10.7939/r3-4p3q-wp04.
5. (2022) DDoS Attack Protection. F5, Inc https://www.f5.com/solutions/use-cases/ddos-attack-protection.
6. Nuiaa Riyadh Rahef, Selvakumar Manickam, Ali Hakem Alsaeedi (2021) Distributed reflection denial of service attack: A critical review. International Journal of Electrical and Computer Engineering 11: 5327.
7. Bhardwaj Aanshi, Veenu Mangat, Renu Vig, Subir Halder, Mauro Conti (2021) Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions. Computer Science Review 39: 100332.
8. Kaur Chahal, Jasmeen, Abhinav Bhandari, Sunny Behal (2019) Distributed denial of service attacks: a threat or challenge. New Review of Information Networking 24: 31-103.
9. Rodrigues Bruno, Lukas Eisenring, Eder Scheid, Thomas Bocek, Burkhard Stiller (2019) Evaluating a blockchain-based cooperative defense. In 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) 533-538.
10. Zhang Chunying, Donghao Jia, Liya Wang, Wenjie Wang, Fengchun Liu, et al. (2022) Comparative research on network intrusion detection methods based on machine learning. Computers & Security 121: 102861.
11. Al-Obeidat F, E-SM El-Alfy (2019) Hybrid multicriteria fuzzy classification of network traffic patterns, anomalies, and protocols. Personal and Ubiquitous Computing 23: 777-791.
12. Park Kyung Min, Young Min Shin, Kyobum Kim, Heungsoo Shin (2018) Tissue engineering and regenerative medicine 2017: a year in review. Tissue Engineering Part B: Reviews 24: 327-344.
13. Liatifis Athanasios, Panagiotis Sarigiannidis, Vasileios Argyriou, Thomas Lagkas (2022) Advancing sdn from

openflow to p4: A survey. ACM Computing Surveys 55: 1-37.
14. Yang Yu (2018) At the Crossroads of Japanese Modernism and Colonialism: Architecture and Urban Space in Manchuria. Columbia University 1900-1945.
15. Muhammad Waqas Nadeem (2022) Detecting and mitigating botnet attacks using deep learning in software-defined networks. PhD diss., UTAR http://eprints.utar.edu.my/6246/1/CCA_MWN_2023.pdf.
16. Venkatadri, Giridhari, Athanasios Andreou, Yabing Liu, Alan Mislove, Krishna P. Gummadi, Patrick Loiseau, and Oana Goga. "Privacy risks with Facebook's PII-based targeting: Auditing a data broker's advertising interface." In 2018 IEEE Symposium on Security and Privacy (SP), pp. 89-107. IEEE, 2018.
17. Sadeghpour Shadi (2022) Machine Learning-Based Defences Against Advanced'session-Replay'web Bots.
18. (2022) Log Management: Introduction & Best Practices. Splunk https://www.splunk.com/en_us/blog/learn/log-management.html#:~:text=One%20popular%20log%20management%20option,monitoring%20and%20analysis%20of%20logs.
19. De Silva, Chirath S, MTM Riyas The Dummy Human: Identity Theft Behavior Patterns in a Digital landscape and Mitigation Practices: A Review.
20. Splunk Enterprise Security. 2022. Splunk. Accessed June 11. https://www.splunk.com/de_de/products/enterprise-security.html.
21. Renners Leonard, Felix Heine, Carsten Kleiner, Gabi Dreo Rodosek (2020) Adaptive Prioritization of Network Security Incidents. IEEE Xplore https://ieeexplore.ieee.org/document/8885208/authors#authors.
22. Raj Pethuru, Anupama Raman, Pethuru Raj, Anupama Raman (2018) Multi-cloud management: Technologies, tools, and techniques. Software-Defined Cloud Centers: Operational and Management Technologies and Tools : 219-240.
23. (2022) Security Monitoring. Splunk https://www.splunk.com/en_us/solutions/security-monitoring.html.
24. Casaleiro Rui (2020) Protection and control of personal identifiable information: The PoSeID-on approach. Journal of Data Protection & Privacy 3: 199-228.
25. Kangwa Mukuka (2022) Prevention of personally identifiable information leakage in ecommerce using offline data minimization and online pseudonymisation. The University of Zambia https://dspace.unza.zm/items/2b9ad2be-b709-4a5e-be64-fbfc25c70887.
26. Omodara Henry (2022) Cloud Security: A survey of Information Communication Technology (ICT) and Cybersecurity professionals' perception on Data Loss Prevention (DLP) measures for Software-as-a-Service (SaaS) application-related data breaches and leakage.
27. Wu Mingfang, Fotis Psomopoulos, Siri Jodha Khalsa, Anita de Waard (2019) Data discovery paradigms: User requirements and recommendations for data repositories.
28. Gillespie Matt, Charles Givre (2021) Understanding Log Analytics at Scale. O'Reilly Media, Incorporated https://www.oreilly.com/library/view/understanding-log-analytics/9781098104269/.
29. Tall Anne (2022) Big Data Processing Attribute Based Access Control Security. ETDs https://stars.library.ucf.edu/etd2020/1096/.
30. Bin Mofidul Raihan, Md Morshed Alam, Md Habibur Rahman, Yeong Min Jang (2022) Real-time energy data acquisition, anomaly detection, and monitoring system: Implementation of a secured, robust, and integrated global IIoT infrastructure with edge and cloud AI. Sensors 22: 8980.
31. Ahmad Atif, Kevin C Desouza, Sean B Maynard, Humza Naseer, Richard L Baskerville (2020) How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology 71: 939-953.
32. Ross Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, Rosalie McQuaid (2019) Developing cyber resilient systems: a systems security engineering approach. No. NIST Special Publication (SP) 2.
33. Aftab Muhammad Umar, Zhiguang Qin, Negalign Wake Hundera, Oluwasanmi Ariyo, Zakria Ngo Tung Son, et al. (2019) Permission-based separation of duty in dynamic role-based access control model. Symmetry 11: 669.