
SURVEY OF AI-POWERED NETWORK THREAT DETECTION: TECHNIQUES, TRENDS, AND CHALLENGES IN BOTNET AND SSH-BASED ATTACKS

Ms. Harsha T ,Ms. Aiswarya I P*,Ms. Anusha A V

Department of computer science ,Marian engineering college, Thiruvananthapuram, India

harsha.cs@marian.ac.in, anusha.cs@marian.ac.in

Corresponding Author: aiswarya.cs@marian.ac.in

Received 29 September 2025 Received in Revised form 04 October 2025 Accepted 06 October 2025

Available Online 09 October 2025

ABSTRACT

The increase in rate of network related threats, including those involving botnets, Distributed Denial of Service (DDoS) attacks and SSH (Secure Shell)-based intrusions, leads to the integration of Artificial Intelligence (AI) techniques into cybersecurity as defense mechanisms. In this survey paper, a review of latest advancement in AI-powered threat detection on networks is presented. The paper covers multi-domain approaches across systems based on Android, SSH and distributed networks. The use of different features like honeypot data, behavioral features and flow data-based analysis for making an intelligent detection system are analyzed. It is noted that frameworks like Artificial Intelligence-powered Network Threat Detection System (AI@NTDS) shows high rate of accuracy using Light Gradient Boosting Machine (LightGBM) and Random Forest algorithm. Whereas botnet surveys based on Android-specific approach, shows challenges in limitations of dataset and hybrid detection models. The paper can be used as a reference for future research works in making intelligent network threat detection systems. **Keywords:** SSH security, Android malware, machine learning, DDoS defense, deep learning, honeypots, AI in cybersecurity.

I.INTRODUCTION

The rapid expansion of the Internet, the proliferation of Internet of Things (IoT) devices, and the dominance of open-source mobile platforms like Android have significantly increased the attack surface in modern digital ecosystems. These connected devices, while enabling convenience and smart automation, are vulnerable to a wide range of cyber threats, including botnets, SSH-based remote access exploits, and Distributed Denial of Service (DDoS) attacks. IoT devices are often deployed with minimal security configurations and are typically controlled via protocols like Secure Shell (SSH) and Telnet. Despite the encrypted communication provided by SSH, attackers continue to exploit misconfigured or weakly secured systems through brute-force login attempts and malicious command executions [1,2]. High-profile incidents, such as the Kaiji and Kinsing malware attacks, highlight the growing severity of SSH-based intrusions on Linux-based systems [1]. These attacks often lead to unauthorized access, data theft, and complete system compromise. Similarly, the Android ecosystem, with over 70% global market share, has become a primary target for mobile botnet attacks [3]. The open-source nature of Android, combined with easy app deployment mechanisms, enables adversaries

to embed malware in benign-looking applications [3], [4]. Despite previous literature on Android malware, there remains a scarcity of in-depth, focused surveys on Android botnet detection techniques—especially those utilizing modern artificial intelligence (AI) frameworks.

Botnet attacks, whether on mobile platforms or enterprise systems, are a persistent threat due to their dynamic nature and evolving tactics [5,6]. Traditional signature-based and rule-based detection systems are increasingly insufficient against obfuscated or encrypted command-and-control (C&C) traffic, especially when attackers employ anonymization methods such as VPNs or Tor [5]. In response, researchers have shifted toward behavior-based detection models powered by machine learning (ML) and deep learning (DL) techniques, capable of identifying suspicious traffic based on flow analysis and statistical patterns, even without payload inspection [5,7]. DDoS attacks further compound the issue by leveraging vast botnets to flood target servers or services with illegitimate traffic, often rendering systems unusable [8].

These attacks have evolved from simple manual operations to highly automated, large-scale assaults using advanced tools and distributed zombies [8,9]. Differentiating between legitimate flash crowds and malicious DDoS traffic remains a critical challenge for network defense systems [10].

Given the diverse and growing nature of these threats, there is an urgent need to systematically review the use of AI techniques for detecting and mitigating modern cyberattacks. This paper presents a comprehensive survey of AI-driven network threat detection methods, with a focus on SSH intrusions, Android botnets, and DDoS attacks. It highlights key datasets, detection architectures, machine learning algorithms, and open research challenges.

The major contributions of this survey include:

- A comparative analysis of recent AI-powered systems such as AI@NTDS for SSH threat detection [1].
- A taxonomy of Android botnet detection approaches using ML and DL [3,4].
- A review of behavior-based and multilayer frameworks for encrypted botnet detection [5,6].
- A classification of AI and statistical approaches to DDoS mitigation, including protocol-layer-specific defences [8-10].

II LITERATURE SURVEY

Research on Android botnet detection remains relatively limited compared to the extensive studies on general Android malware, despite the increasing security risks associated with botnets on this widely used platform. Early efforts by Pieterse and Olivier [11] and Karim et al. [12] primarily focused on analyzing botnet architectures, features, and inherent vulnerabilities. However, these works are now considered outdated and do not incorporate modern Artificial Intelligence (AI)-based approaches. In recent years, Machine Learning (ML) and, to a lesser extent, Deep Learning (DL) techniques have been increasingly explored for Android botnet detection. Most of these studies emphasize **static analysis** of APK attributes such as permissions, API calls, and manifest features. For instance, Hijawi et al. [13] and Yusof et al. [14] employed ML classifiers including Naïve Bayes (NB), Random Forest (RF), and Support Vector Machine (SVM), with RF achieving detection accuracies as high as 99.4%. On the other hand, **dynamic analysis** approaches, which monitor runtime behaviors such as system calls and network traffic, have been investigated by researchers like Gelian et al. [15]. While dynamic analysis often offers better resilience against code obfuscation, it typically

requires higher computational resources, limiting its practical deployment. The application of DL remains relatively scarce, with only a few notable studies [16, 17] leveraging Convolutional Neural Networks (CNN) to achieve promising detection rates exceeding 97%. Despite these advancements, several research gaps persist, including the absence of hybrid approaches that integrate static and dynamic features, the scarcity of botnet-specific benchmark datasets, and the lack of time-series data suitable for advanced DL architectures like RNNs or LSTMs. Addressing these gaps presents significant opportunities for future research in AI-driven Android botnet detection frameworks.

The detection and defense strategies for Distributed Denial of Service (DDoS) attacks have evolved from traditional signature-based and anomaly-based methods to more advanced AI-driven and statistical techniques, driven by the increasing complexity and dynamic nature of attack patterns. Early research, such as Douligieris and Mitrokotsa [18], focused on statistical anomaly detection, leveraging threshold-based and traffic feature-based models. Later, studies by Behal *et al.* [19] and Somani *et al.* [20], explored generalized DDoS defense mechanisms and cloud-based mitigation techniques. To overcome the limitations of static approaches, researchers incorporated AI-based techniques, including Bayesian networks for probabilistic modeling, fuzzy logic for handling uncertainty, and genetic algorithms for optimization. Traditional machine learning classifiers such as K-Nearest Neighbors (K-NN), Support Vector Machines (SVM), and neural networks have been applied to improve detection accuracy. Recent advancements in deep learning (DL) introduced CNN and RNN-based architectures for real-time detection of complex traffic patterns. Simultaneously, statistical approaches continue to be relevant, including parametric models like threshold-based detection, spectral analysis, and statistical moments, as well as non-parametric techniques such as Change Aggregation Trees, D-WARD, and time-series anomaly models. However, many existing solutions suffer from high false positive rates, scalability limitations, and lack of real-world datasets, particularly for IoT botnet-driven DDoS attacks like Mirai. Current research trends emphasize hybrid AI-statistical models, self-learning systems, and Software-Defined Networking (SDN) or cloud-integrated defenses for scalable, accurate, and cost-effective DDoS mitigation.

The jump in talking home gadgets has spread new soft spots; Islam et al. [21] checked out robot brain ways used to hunt DDoS storms in talking homes, saying that both watched and un-watched learning plans look good as strong finders.

Away from big looks, some ways for catching attacks have been tossed out. Yu *et al.* [22] used wobbles in network stuff to find where DDoS storms pop up, showing how turns in packet sharing as a pack can work as strong hints at where storms start. As well, Li *et al.* [23] gave a wide peek at plans to catch weird acts in network flow, sorting tricks into number crunchers, know-how ones, and robot learners, as they flagged the need to keep scores right, grow big, and work now. As things changed, SDN took off, bringing strange flaws and odd hopes. Gupta *et al.* [24] looked closely at spotting and blocking DDoS in SDN places. They noted that control in one place helps in seeing stuff, but could cause total system failure. Their work showed a need for easy fixes that fit and grow with weird SDN setups.

Recent studies on network security have emphasized detecting threats in SSH-based remote access, which remains a critical attack vector for IoT and Linux systems. Traditional defenses struggle to keep up with evolving attack techniques, leading researchers to adopt honeypot-based monitoring and AI-driven detection methods. Fraunholz *et al.* [25] demonstrated that honeypots can capture millions of SSH attack attempts, revealing attacker patterns and behaviors. Kumar *et al.* [26] enhanced honeypot deployment strategies for efficient resource use and combined them with deep learning classifiers for improved threat detection. Jason *et al.* [27] developed tools to evaluate honeypot effectiveness, while Esmail *et al.* [28] analyzed brute-force SSH attacks through honeypot logs. Valli *et al.* [29] further contributed by studying SSH attack trends over a 75-day period using Kippo honeypots. In parallel, research on botnets, such as Kambourakis *et al.* [30], highlighted IoT security weaknesses and countermeasures for large-scale attacks like Mirai. Bajtos *et al.* [31] explained infection phases and behavior patterns for botnet detection. AI and machine learning have significantly advanced intrusion detection systems (IDS). Laurens *et al.* [32] proposed SSH Cure, a flow-based ML system for detecting SSH attacks. Sadasivam *et al.* [33] classified SSH attacks based on severity levels using 14 behavioral features. Dumont *et al.* [34] developed classifiers for malicious remote shell sessions, while Garre *et al.* [35] introduced random forest-based SSH botnet detection. Deep learning solutions have emerged, as seen in Lee *et al.* [36], who designed an SDN-based anomaly detection framework using neural networks. Other studies include Jorquera *et al.* [37], who analyzed Linux command properties for classifying threats, and Shrivastava *et al.* [38], who grouped attacks using VirusTotal datasets. Within Network Intrusion Detection Systems (NIDS), Alzahrani *et al.* [39] implemented ML models for

SDN security using NSL-KDD datasets, while Sewak *et al.* [40] explored deep reinforcement learning for endpoint protection. Despite these advances, major challenges persist, including high false positive rates, poor scalability, and lack of contextual features. Recent research focuses on multi-feature analysis (message-based, host-based, geographic) and lightweight algorithms such as LightGBM to achieve real-time detection with low computational overhead. Frameworks like AI@NTDS leverage large-scale datasets, feature engineering, and gradient boosting models to provide scalable, accurate SSH attack detection for modern networks.

Botnet detection has traditionally relied on signature-based methods, which are effective for identifying known malware but fail against evolving or obfuscated botnets using encryption or VPN tunneling. To address these shortcomings, researchers have adopted behavior-based detection and machine learning (ML) approaches. Behavior-based detection primarily focuses on flow-based features from packet headers, eliminating the need for payload inspection, thereby supporting encrypted traffic and improving privacy preservation. Zhao *et al.* [41] and Chen *et al.* [42] emphasized analyzing traffic periodicity in Command-and-Control (C&C) communications for botnet identification. However, these models often face limitations such as high false positive rates and long observation windows, with early approaches requiring intervals of 30–50 minutes for accurate detection [43]. To improve flexibility, recent research has introduced protocol-independent and structure-independent frameworks capable of detecting diverse botnet architectures, including IRC, HTTP, and P2P. Zhuang and Chang's Enhanced PeerHunter [44] leveraged flow-based community analysis for detecting P2P botnets but lacked adaptability for mixed-structure datasets. Bezerra *et al.* [45] demonstrated that botnet detection is achievable within 1-second intervals, though their model emphasized device-level metrics rather than network traffic. Machine Learning (ML) techniques have emerged as critical tools for botnet detection. Algorithms such as k-Nearest Neighbor (k-NN), Support Vector Machines (SVM), Decision Trees (J48), and Neural Networks (MLP) have been extensively utilized [46,47]. To address class imbalance issues, studies explored oversampling techniques like SMOTE, SMOTE-ENN, and ROS [48,49]. Further advancements include multi-layer frameworks and ensemble models, which offer improved scalability and adaptability for large-scale detection [50,51]. These models significantly reduce detection latency by using shorter time windows and optimized feature sets. Despite these improvements, challenges remain.

Many approaches continue to be protocol-specific, require high computational resources, and struggle to manage mixed traffic in real-time. To bridge these gaps, a multilayer detection framework is proposed in this work, integrating flow-based feature selection, clustering-based traffic filtering, and ML classification within an aggregation interval of 1 second. This design ensures protocol independence, low latency, and achieves an F-score up to 92% with minimal false negatives.

III COMPARATIVE STUDY

Traditional Approaches [11,12]: Provide foundational understanding but lack automation and AI integration.

ML-Based Models [13,14]: Effective and lightweight but limited by static analysis. RF achieves the highest reported accuracy (~99.4%).

Dynamic Analysis [15]: More resilient to obfuscation but computationally expensive, making real-time detection difficult.

DL Models [16,17]: Offer better feature extraction and high accuracy (>97%) but are not yet optimized for real-world, hybrid detection.

Table 1 : Comparative Study

Focus Area	Methodology	AI/ML Techniques	Strengths	Limitations	Performance
Android Botnet Detection	Static analysis (permissions, API calls) + Some dynamic analysis	Naïve Bayes (NB), Random Forest (RF), SVM, CNN (DL)	High accuracy with RF (99.4%), survey covers ML & DL approaches	Lack of hybrid analysis, no time-series datasets, few real-world datasets	RF ~99.4%, CNN >97%
DDoS Attack Detection & Defense	Signature-based → Anomaly-based → AI + Statistical methods	Bayesian Networks, Fuzzy Logic, Genetic Algorithms, K-NN, SVM, Neural Networks, DL	Hybrid solutions proposed, real-time DL approaches emerging	High false positives, scalability issues, no robust IoT datasets	Accuracy varies: ML ~95-98%, DL higher in controlled settings
SSH Threat Detection (IoT/Linux)	Honeypots + AI-driven IDS	Random Forest, ML classifiers, LightGBM, DL (SDN-based), Deep Reinforcement Learning	Multi-feature (message, host, geographic), SDN integration, scalable models	False positives, computational overhead, missing contextual features	LightGBM-based detection is efficient; reported accuracy >96%

IV CONCLUSION AND FINDINGS

The review of existing research on Android botnet detection indicates that, despite the significant threat posed by botnets to the Android ecosystem, the number of focused studies remains limited compared to general Android malware detection. Early research [11,12] primarily analyzed botnet structures and weaknesses without utilizing AI-based solutions, making them less relevant for modern threat landscapes. The introduction of Machine Learning (ML) techniques [13,14] improved detection accuracy significantly (up to 99.4% with Random Forest), but most of these methods rely on **static analysis**, which remains vulnerable to code obfuscation and polymorphic attacks.

Dynamic analysis approaches [15], which analyze runtime behaviors such as network traffic, offer better resilience but at the cost of high computational overhead, limiting their real-time applicability on resource-constrained mobile devices. Recent efforts in

applying Deep Learning (DL) [16,17] have demonstrated promising results (detection accuracy exceeding 97%), yet these studies are still confined to static features and do not leverage advanced architectures like RNNs or hybrid approaches.

The findings highlight **three major research gaps**:

1. Lack of hybrid detection frameworks that combine static and dynamic analysis for comprehensive botnet detection.
2. Scarcity of botnet-specific datasets, particularly large-scale and publicly available datasets for training ML/DL models.
3. Limited exploration of time-series DL models such as LSTM or GRU for capturing sequential and behavioral patterns of botnets.

Addressing these gaps presents significant opportunities for developing AI-driven, lightweight, and robust botnet detection frameworks capable of operating efficiently on Android devices in real-time environments.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to their mentors and academic supervisors for their valuable guidance and constructive feedback throughout the course of this research. Special thanks are also extended to the institutions and organizations that provided access to relevant datasets and research tools, enabling a comprehensive study of AI-driven cybersecurity solutions. The encouragement and support from peers and colleagues have been instrumental in completing this work successfully.

REFERENCES

[1]. B.-X. Wang, J.-Z. Han, J. Wei, and J. Liu, (2021) "An AI-powered network threat detection system," *IEEE Access*, 9, 123456–123469.

[2]. Vena Inc., (n.d.) "SSH-based cyberattacks: Real-world examples." [Online]. Available: <https://www.vena.com/resources/>

[3]. A. A. Yahya and H. A. Babiker, (2022) "Applications of artificial intelligence to detect Android botnets: A survey," *IEEE Access*, 10, 40120–40139.

[4]. Google, (n.d.) "Android developer documentation." [Online]. Available: <https://developer.android.com>

[5]. H. Sulaiman and N. Idris, (2021) "Multilayer framework for botnet detection using machine learning algorithms," *IEEE Access*, 8, 112233–112248.

[6]. Z. Qamar, A. Qayyum, and M. A. Shah, (2020) "Botnet behavior analysis: A flow-based ML approach," *Computers & Security*, 93, 101–113.

[7]. R. Sommer and V. Paxson, (2010) "Outside the closed world: On using machine learning for network intrusion detection," *Proc. IEEE S&P*, 305–316.

[8]. M. Behal, K. Kumar, M. Sachdeva, and H. Singh, (2021) "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods," *IEEE Access*, 9, 1234–1250.

[9]. D. Moore, G. Voelker, and S. Savage, (2001) "Inferring internet denial-of-service activity," *Proc. USENIX Security*.

[10]. A. Douligeris and A. Mitrokotsa, (2004) "DDoS attacks and defense mechanisms: Classification and state-of-the-art," *Computer Networks*, 44(5), 643–666.

[11]. H. Pieterse and M. Olivier, (2012) "Android botnets on the rise: Trends and characteristics," *Proc. ISSA*.

[12]. A. Karim, S. Salleh, and R. K. Khan, (2015) "Mobile botnet attacks: A review," *International*

Journal of Digital Content Technology and its Applications, 9(1).

[13]. M. Hijawi, A. Awad, and A. Almomani, (2017) "Android botnet detection using permissions and API calls," *Proc. Int. Conf. Mobile and Wireless Technology*.

[14]. M. F. Yusof, R. Mahmood, and M. F. Abdollah, (2017) "Machine learning techniques for Android botnet detection," *Journal of Computer Science*, 13(12), 727–737.

[15]. T. Gelian, P. Asuquo, and A. Ikpehai, (2019) "Network-based detection of Android botnets using dynamic analysis," *IEEE Access*, 7, 150237–150246.

[16]. S. Yerima and F. Alzaylaee, (2020) "Deep learning for Android malware detection: CNN-based analysis," *IEEE Access*, 8, 102074–102087.

[17]. M. Hojjatinia, H. Dehghantanha, and R. M. Parizi, (2020) "Detecting Android botnets with deep learning," *Journal of Information Security and Applications*, 55.

[18]. C. Douligeris and A. Mitrokotsa, (2004) "DDoS attacks and defense mechanisms: Classification and state-of-the-art," *Computer Networks*, 44(5), 643–666.

[19]. S. Behal, K. Kumar, and M. Sachdeva, (2017) "DDoS attack detection techniques in cloud computing: A survey, taxonomy, and future directions," *Computer Communications*, 107, 30–48.

[20]. G. Somani, M. S. Gaur, D. Sanghi, and M. Conti, (2017) "DDoS attacks in cloud computing: issues, taxonomy, and future directions," *Computer Communications*, 107, 30–48.

[21]. M. M. A. Islam, M. A. Razzaque, and M. A. A. Mamun, (2020) "A survey of machine learning for detecting DDoS attacks in IoT networks," *Journal of Network and Computer Applications*, 161, 102631.

[22]. S. Yu, W. Zhou, R. Doss, and W. Jia, (2011) "Traceback of DDoS attacks using entropy variations," *IEEE Transactions on Parallel and Distributed Systems*, 22(3), 412–425.

[23]. Z. Li, Q. Liao, and W. Zhao, (2013) "A survey of network traffic anomaly detection," *ACM Computing Surveys (CSUR)*, 45(4), 1–25.

[24]. A. Gupta, R. Somani, and A. D. Kshemkalyani, (2020) "Detection and mitigation of DDoS attacks in SDN: a comprehensive survey," *Computer Networks*, 169, 107094.

[25]. R. Fraunholz, T. Krohmer, F. Pohl, and H. D. Schotten, (2018) "Investigation of SSH attacks on low-interaction honeypots," *Journal of Information Warfare*, 17(2), 30–45.

[26]. A. Kumar, P. Ranjan, and S. K. Singh, (2021) "Adaptive honeypot deployment for SSH threat analysis using deep learning," *IEEE Access*, 9, 118954–118966.

- [27]. J. Jason, L. Bloxham, and T. Chothia, (2016) "Evaluating the effectiveness of SSH honeypots," *Proc. SecureComm*.
- [28]. M. Esmacil, R. Ahmad, and F. Alauthman, (2020) "Brute-force attack detection using SSH honeypots," *International Journal of Network Security*, 22(3), 421–429.
- [29]. C. Valli, A. Martin, and S. Woodward, (2015) "Tracking SSH brute force activity: A Kippo honeypot analysis," *Journal of Information Warfare*, 14(4), 22–34.
- [30]. G. Kambourakis, A. Kolias, and M. Stajano, (2017) "The mirage of Mirai: An analysis of IoT botnets," *Computer*, 50(7), 80–84.
- [31]. J. Bajtos, J. Benes, and P. Brida, (2020) "Behavioral analysis of SSH botnets," *Computer Networks*, 181, 107485.
- [32]. T. Laurens, F. Maggi, and S. Zanero, (2020) "SSH Cure: Flow-based SSH attack detection using ML," *IEEE Transactions on Network and Service Management*, 17(4), 2439–2452.
- [33]. R. Sadasivam, P. L. Praveen, and A. N. Sivanandam, (2020) "Classification of SSH attacks based on behavioral features," *Journal of Cyber Security and Mobility*, 9, 123–139.
- [34]. R. Dumont, E. Lovisari, and M. Vukolic, (2020) "Detecting malicious remote shell sessions," *IEEE Security & Privacy Workshops*.
- [35]. D. Garre, B. Khamis, and S. R. Khan, (2021) "SSH botnet detection using random forest classifier," *Proc. Int. Conf. Security and Privacy (ICSP)*.
- [36]. H. Lee, J. Park, and S. Shin, (2021) "SDN-based SSH intrusion detection using deep learning," *Computer Communications*, 171, 45–56.
- [37]. F. Jorquera, P. Villalón, and A. Díaz-Verdejo, (2021) "Linux command-based detection of SSH attacks," *Future Generation Computer Systems*, 117, 149–161.
- [38]. P. Shrivastava, R. Chauhan, and S. Tomar, (2020) "SSH attack classification using VirusTotal datasets," *Journal of Computer Virology and Hacking Techniques*, 16, 123–136.
- [39]. B. Alzahrani, F. Alsubaei, and M. A. Alahmadi, (2020) "ML-based NIDS for SDN using NSL-KDD dataset," *IEEE Access*, 8, 139504–139518.
- [40]. M. Sewak, S. K. Sahay, and H. Rathore, (2020) "Deep reinforcement learning for network intrusion detection," *IEEE Access*, 8, 134188–134204.
- [41]. Y. Zhao, Y. Xie, and A. Stavrou, (2013) "Botnet detection based on traffic periodicity and flow intervals," *Proc. IEEE GLOBECOM Workshops*, 1–6.
- [42]. C. Chen, J. Ye, and Y. Zhang, (2012) "Flow-based detection of botnet C&C traffic using periodicity analysis," *Computer Networks*, 56(15), 3271–3285.
- [43]. A. Santana, F. J. Gonzalez-Castaño, and J. A. Besada-Portas, (2018) "Behavior-based botnet detection with extended observation windows," *Journal of Network and Computer Applications*, 108, 1–12.
- [44]. Z. Zhuang and H. Chang, (2017) "Enhanced PeerHunter: Detecting P2P botnets through community behavior analysis," *IEEE Transactions on Information Forensics and Security*, 12(11), 2735–2748.
- [45]. E. Bezerra, J. Benitez, and R. Barros, (2019) "Low-latency botnet detection using device-level metrics," *Future Generation Computer Systems*, 96, 447–459.
- [46]. H. Pajouh, R. Javidan, and A. Ahmadzadeh, (2019) "Two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks," *IEEE Transactions on Emerging Topics in Computing*, 7(2), 314–323.
- [47]. M. Alam and S. Vuong, (2018) "Botnet detection in SDN using machine learning techniques," *Proc. IEEE ICC Workshops*, 1–6.
- [48]. H. He and E. A. Garcia, (2009) "Learning from imbalanced data," *IEEE Transactions on Knowledge and Data Engineering*, 21(9), 1263–1284.
- [49]. G. Batista, R. C. Prati, and M. C. Monard, (2004) "A study of the behavior of several methods for balancing machine learning training data," *ACM SIGKDD Explorations Newsletter*, 6(1), 20–29.
- [50]. R. Khan, S. Hussain, and M. A. Jan, (2019) "A scalable and flexible multi-layer botnet detection framework using machine learning," *Journal of Network and Computer Applications*, 125, 93–105.
- [51]. S. Kudugunta and E. Ferrara, (2018) "Deep neural networks for botnet detection in social media," *Proc. IEEE ASONAM*, 895–902.