Assessing the Impact of Malicious Bots on Cloud Web Applications

Vijay Raj
Research Scholar,
College of Computer Science and Information Science, Srinivas University
Mangalore
vijayrajbv@gmail.com

Dr. Subramanya Bhat
Research Scholar
College of Computer Science and Information Science, Srinivas University
Mangalore

ABSTRACT - Malicious bots pose a significant threat to cloud web applications. They can overwhelm servers with traffic, leading to denial-of-service attacks that disrupt legitimate user access and cause revenue loss. These bots actively scrape sensitive data like customer information and intellectual property, giving competitors an unfair advantage and jeopardizing user privacy. Furthermore, they exploit vulnerabilities to hijack user accounts through credential stuffing, enabling them to spread malware, launch further attacks, and engage in fraudulent activities. The consequences extend beyond operational disruptions, impacting brand reputation, eroding user trust, and incurring substantial costs associated with increased infrastructure needs, enhanced security measures, and the remediation of data breaches and reputational damage. This research assesses the impact of malicious bots on cloud web applications and also explores popular mitigation strategies.

Keywords: Malicious Bots, Cloud Web Applications, Security, Vulnerabilities, Mitigation Strategies.

1. INTRODUCTION

Cloud web applications have become the backbone of modern computing, providing scalable, on-demand access to resources and services. However, their increased adoption has also made them a prime target for malicious actors [1]. Malicious bots, in particular, pose a significant threat to cloud web applications, exploiting vulnerabilities to compromise security, disrupt services, and steal sensitive data. Lack of awareness of security concepts and the procedures to defend for such malware leads to a significant threat which the botmaster can exploit it to launch a huge damage in the target [2]. The common activities that the intruder performed with the bots are the DDoS attack, phishing attack, flooding attack, gathering information such as keyloggers to obtain the financial information about the user, and click fraud attack. These automated threats can lead to devastating consequences, including financial losses, reputational damage, and legal liabilities [3]. "Malicious bots are becoming a big problem because they're easy to create, spread, and control. Hackers can even buy or rent botnets on the dark web, making it simple for them to launch massive attacks without much effort. Additionally, the widespread use of cloud services and content delivery networks (CDNs) makes it harder to tell the difference between genuine website traffic and fake bot activity. Despite the growing threat, there is a lack of comprehensive research on the impact of malicious bots on cloud web applications [4]. This study aims to bridge this gap by assessing the effects of malicious bots on cloud web application performance, security, and availability. By understanding the impact of malicious bots, we can develop effective mitigation strategies to protect cloud web applications from these automated threats.

2. OBJECTIVES

a) To investigate the prevalence and characteristics of malicious bots targeting cloud web applications.
b) To analyze the impact of malicious bots on cloud web application performance, security, and user experience.

c) To explore the most popular mitigation strategies to secure cloud web applications from malicious bots.

3. RELATED WORKS

The threat posed by malicious bots to cloud web applications has garnered significant attention in recent years. As the complexity and frequency of these attacks continue to escalate, researchers and practitioners have proposed various solutions to detect, prevent, and mitigate their impact. This section provides an overview of the existing literature on assessing the impact of malicious bots on cloud web applications, highlighting the key findings, methodologies, and limitations of previous studies.

Singh, S. P., & Afzal, N. (2024) [5], the author demonstrates the significant impact of malicious bots on cloud web application performance and highlights the need for effective bot mitigation strategies to ensure cloud web application reliability and scalability. The study focuses only on performance metrics, ignoring security and availability aspects. The testbed setup may not accurately represent real-world cloud web application environments.

Guo, Y., et al. (2019) [6], this paper provides insights into the characteristics of malicious bot traffic in cloud web applications, enabling the development of more effective bot detection and mitigation strategies. But this paper relies on a single cloud web application's traffic data, which may not be representative of all cloud web applications.

Attou, H., et al. (2018) [7], paper highlights the significant security risks posed by malicious bots to cloud web applications, emphasizing the need for robust security controls, monitoring, and incident response strategies to mitigate these threats. The paper focuses solely on security aspects, ignoring performance and availability impacts.

Shang, Y., et al. (2018) [8], The paper demonstrates the effectiveness of machine learning in detecting malicious bots in cloud web applications, highlighting the potential for automated bot detection and mitigation. The study relies on a single dataset, which may not generalize well to other cloud web applications.

Bazm, M., et al. (2019) [9] The paper demonstrates the effectiveness of rate limiting in mitigating malicious bot attacks on cloud web applications, highlighting its potential as a simple yet effective defense mechanism. The evaluation was conducted on a single cloud web application, which may not represent all scenarios.

R. Kumar et al. (2020) [10] The paper highlights the significant impact of malicious bots on cloud web application availability and cloud resource utilization, emphasizing the need for effective bot mitigation strategies to ensure application reliability and scalability. The study focused on a single cloud web application and may not generalize to other applications.

Ahmed, J.,. et.al (2022) [11], provides a comprehensive review of botnets and botnet detection techniques in cloud computing, highlighting the need for more effective and efficient detection methods to address the unique challenges of cloud environments.

Veeraiah et al. (2022) [12], The paper demonstrates the effectiveness of machine learning techniques in detecting malicious cloud bandwidth consumption, highlighting their potential in ensuring cloud security and optimizing resource utilization. The paper relies on a single dataset from a cloud service provider, which may not be representative of all cloud environments.

4. BOTNET LIFECYCLE

A typical botnet can be created and maintained in five phases including initial infection, secondary injection, malicious command and control, update and maintenance [13]. This life-cycle is depicted in Figure 1

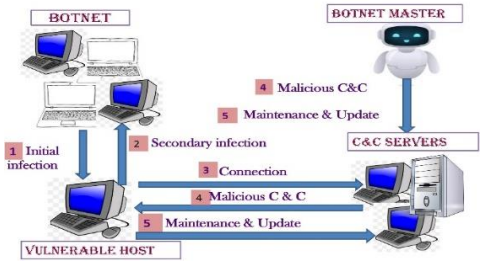

Figure 1: Typical Malicious Botnet Lifecycle [14]

During the initial infection phase, the attacker scans a target subnet for known vulnerability and infects victim machines through different exploitation method [15]. Then, in secondary injection phase, the infected hosts execute a script known as shell-code. The shell-code fetches the image of the actual bot binary from the specific location via FTP, HTTP, or P2P [16]. The bot binary installs itself on the target machine. Once the bot program is installed, the victim computer turns to a Zombie and runs the malicious code [17]. The bot application starts automatically each time the zombie is rebooted. n connection phase, the bot program establishes a C&C channel and connects the zombie to the C&C serve [18]. Upon the establishment of C&C channel, the zombie becomes a part of attacker's botnet army. After connection phase, the actual botnet command and control activities will be started [19]. The botmaster uses the C&C channel to disseminate commands to his bot army. Bot programs receive and execute commands sent by botmaster [20]. The C&C channel enables the botmaster to remotely control the action of large number of bots to conduct various illicit activities [21]. The last phase is to maintain bots live and updated. In this phase, bots are commanded to download an updated binary. Bot controllers may need to update their botnets for several reasons [22]. For instance, they may need to update the bot binary to evade detection techniques, or they may intend to add new functionality to their bot army. Moreover, sometimes the updated binary moves the bots to a different C&C server. This process is called server migration and it is very useful for botmasters to keep their botnet alive [23].

5. BOTNET ARCHTECTURE AND ITS CHARACTERSTICS

BOTNET uses four types of architectures to control network and to be invisible from detection i.e. Centralized Botnet Architecture, Peer to Peer Botnet Architecture (P2P), Hybrid, and Combination of Hyper Text Transfer Protocol with Peer to Peer (HttP2P).

a. Centralized Botnet Architecture:

A **centralized botnet architecture** is one of the primary types of botnet structures used by attackers to control and coordinate a large network of compromised computers, often referred to as "bots" or "zombies."[24]. In this architecture, all the compromised machines (bots) communicate with and receive instructions from a single, centralized command and control (C&C) server. This server acts as the "brain" of the botnet, issuing commands to bots and managing the overall botnet operations.

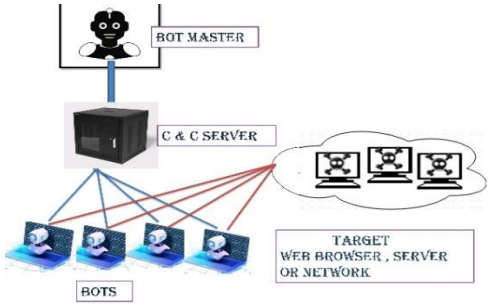

Figure 2 : Centralized Botnet Architecture [25]

a. Components of Centralized Botnet Architecture

- ***Command and Control (C&C) Server***: The C&C server is the central entity in this architecture. It is controlled by the attacker. Distributes malware updates or instructions to bots (e.g., to start DDoS attacks, send spam, or steal data). Receives data from infected machines, such as stolen credentials or keylogged information[26].
- ***Bots (Compromised Machines):*** Bots are the computers or devices infected by malware and controlled remotely by the C&C server. Once compromised, these machines communicate with the C&C server for instructions and carry out malicious activities as directed. Execute commands like launching DDoS attacks, sending spam emails, or performing click fraud. Report back status updates or stolen data to the C&C server. ++ [27]
- ***Botmaster (Attacker):*** The botmaster is the person or entity who controls the botnet via the C&C server. The botmaster typically remains anonymous and hidden, using sophisticated techniques to evade detection. Issues commands to the C&C server. Updates malware or changes instructions to adapt to detection efforts or increase the potency of attack[28]

b. Peer *to Peer (P2P) Botnet Architecture*

A Peer-to-Peer (P2P) botnet architecture is a more decentralized approach to controlling a botnet compared to the centralized architecture [29]. In a P2P botnet, the botmaster does not rely on a single Command and Control (C&C) server to issue commands to the bots. Instead, each bot in the network acts both as a client and a server, sharing commands and data with other bots in a distributed manner [30]. P2P architecture is more resilient to takedowns, as there is no single point of failure like a centralized C&C server [31].

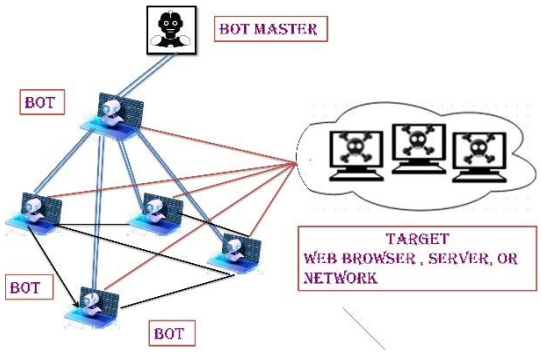

Figure 2: Peer to Peer (P2P) Botnet Architecture [32]

Components of p2p Architecture

- ***Peer Nodes (Bots):***

In a P2P botnet, each infected machine (bot) functions as both a server and a client. Bots communicate directly with each other rather than relying on a central server [. Each bot can pass commands to others, making the system decentralized. Bots discover other infected machines through various peer discovery mechanisms (e.g., via IP addresses or specific protocols). Commands and updates are propagated through the network by hopping from bot to bot [33].

- **Botmaster (Attacker):**

The botmaster injects commands into the botnet through one or more entry points, which then propagate through the peer-to-peer network. The botmaster can inject updates or new instructions into the network from any bot rather than relying on a central C&C server. This allows the botmaster to control the botnet from any node in the network, which enhances the botnet's stealthiness and resilience [34].

- **Peer Communication:**

Bots communicate with each other to receive and relay commands, distribute updates, and share stolen data. Bots use peer discovery mechanisms to identify and communicate with other bots in the network. Communication can be encrypted or disguised to make detection difficult. Data is often fragmented and passed in small packets to avoid detection by network monitoring tools [35].

The P2P botnet architecture offers attackers a resilient and scalable network for launching cyberattacks, making it harder to detect and shut down. However, the decentralized structure also introduces complexities and slower command propagation, providing opportunities for defenders to infiltrate and disrupt the botnet's operations.

b. Hybrid Botnet Architecture

A hybrid botnet architecture combines elements from both centralized and peer-to-peer (P2P) botnet architectures to create a more resilient and flexible control system for botnets [36]. This design leverages the strengths of both architectures to overcome some of their inherent weaknesses, such as the single point of failure in centralized systems and the complexity of managing a pure P2P network [37]. In a hybrid botnet, bots may use a centralized Command and Control (C&C) server for efficient management and control while utilizing P2P communication for resilience and redundancy [37]. This structure makes it more challenging for security teams to take down the botnet, as it can adapt to the loss of the centralized server by falling back on P2P mechanisms.

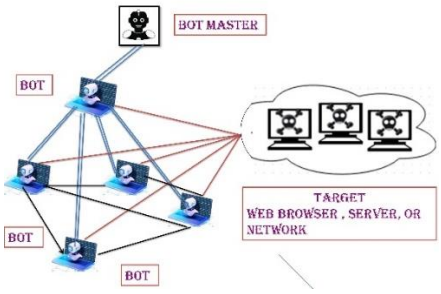

Figure 3: Hybrid Botnet Architecture

Components of Hybrid Botnet Architecture

- **Centralized Command and Control (C&C) Server:** In hybrid botnets, the C&C server still plays a crucial role in issuing commands and coordinating attacks. This is similar to the centralized architecture, where a single or small number of servers control the botnet [38]. The C&C server provides instructions, malware updates, and attack coordination. Bots may initially connect to the C&C server to join the botnet

and receive their first set of commands. The C&C server is typically used for high-level control to keep the network organized [39].

- **Peer-to-Peer (P2P) Communication: In** addition to communicating with a central server, bots in a hybrid architecture can also communicate directly with each other, similar to a P2P botnet. This provides resilience if the C&C server is taken down or becomes inaccessible. Bots share commands and updates with each other in a decentralized manner, ensuring that the botnet continues functioning even if the C&C server is offline.P2P communication allows the botnet to propagate malware updates, commands, or stolen data among infected machines, maintaining control even in a fragmented network [40].
- **Bots (Compromised Machines):** Each bot in the hybrid botnet can communicate with the C&C server or its peers depending on the situation. Bots are more autonomous and capable of both following centralized instructions and acting as peers in a decentralized network. Bots relay commands between each other when necessary, ensuring that instructions propagate even if the C&C server is down. Bots may store lists of peers, update their malware autonomously, or report stolen data back through either centralized or decentralized channels [41].
- **Botmaster (Attacker):** The attacker (botmaster) can issue commands through the C&C server or directly into the P2P network. The hybrid structure gives the botmaster flexibility in how they manage and control the botnet [42]. The botmaster can switch between centralized and decentralized control depending on the needs of the attack, making it harder for defenders to detect or take down the entire botnet. They can use the C&C server for organized attacks and updates but rely on the P2P network for resilience [43].

5. IMPACT OF MALICIOUS BOTS ON CLOUD APPLICATIONS

Malicious bots have a significant and multifaceted impact on cloud web applications, threatening their security, performance, and financial stability. These bots exploit vulnerabilities, degrade services, and consume resources, causing a range of harmful effects.

b. Performance Impact: Performance Impact refers to the measurable degradation of cloud web application performance, resulting from malicious bot attacks, resource-intensive requests, or other malicious activities. Cloud web applications are increasingly vulnerable to performance degradation due to malicious bot attacks. Performance impact, a critical consequence of these attacks, can have far-reaching effects on user experience, business productivity, and revenue. Malicious bots can significantly degrade the performance of cloud web applications, leading to:

- **Reduced Application Response Time**: Increased latency and slower response times, frustrating users and impacting business operations.
- **Increased Resource Utilization**: Malicious bots consume CPU, memory, and bandwidth resources, leading to CPU overload Memory exhaustion Bandwidth saturation.
- **Resource Exhaustion:** Malicious bots can exhaust resources by sending large volumes of requests to the application, causing the cloud provider to provision additional resources (such as storage, CPU, or bandwidth). This results in higher operational costs for the company.

b. **Security Impact:** Security Impact refers to the potential harm or exploitation of cloud web application security vulnerabilities, resulting from malicious bot attacks, unauthorized access, or data breaches. Cloud web applications are vulnerable to security threats from malicious bots, compromising data integrity, confidentiality, and availability. Security impact, a critical consequence of these attacks, can have devastating effects on business operations, reputation, and compliance.

- **Data Theft and Breaches** Bots can scrap sensitive or proprietary data from cloud web applications, including customer details, intellectual property, product pricing, or other valuable information. Data theft

can lead to intellectual property loss, competitive disadvantage, or violations of data protection regulations like GDPR or HIPAA. It can also expose sensitive customer information, resulting in potential lawsuits and reputational damage.

- **Credential Stuffing and Brute Force Attacks**: Bots often use stolen or weak credentials to perform credential stuffing attacks, gaining unauthorized access to user accounts in cloud web apps. These bots systematically test username-password combinations across large numbers of accounts. Account takeovers (ATOs) allow bots to perform fraudulent actions, such as stealing sensitive data, conducting financial transactions, or making unauthorized changes. This leads to significant financial losses, legal consequences, and a loss of customer trust.

- **Insider threats:** Insider threats refer to security risks posed by individuals with authorized access to an organization's assets, systems, or data, intentionally or unintentionally compromising security.

c. **Economic Impact:** Economic Impact refers to the financial consequences of malicious bot attacks on cloud web applications, including revenue loss, increased operational costs, compliance penalties, and reputational damage. Malicious bots pose a significant threat to cloud web applications, resulting in substantial economic losses and reputational damage. The economic impact of these attacks can be devastating, compromising business continuity, customer trust, and market value

- **Revenue Loss:** Revenue Loss refers to the financial losses incurred by cloud web applications due to malicious bot attacks, resulting in reduced sales, decreased conversion rates, and lower average order value. Malicious bots can significantly impact cloud web applications, resulting in substantial revenue loss and financial instability.
- **Increased Operational Costs:** Increased Operational Costs refer to the additional expenses incurred by cloud web applications due to malicious bot attacks, including incident response, security personnel, technology upgrades, and compliance fees.
- **Operational Impact:** Operational Impact refers to the effects of malicious bot attacks on cloud web application operations, including downtime, performance degradation, and resource exhaustion. Malicious bot attacks can significantly disrupt cloud web application operations, compromising business continuity, productivity, and efficiency.
- **Downtime and unavailability**: Downtime and Unavailability refer to periods when cloud web applications are inaccessible or non-functional, resulting in lost productivity, revenue, and customer trust. Cloud web applications rely on continuous availability to serve users and drive business success. However, malicious bot attacks can disrupt operations, causing devastating downtime and unavailability.
- **Service Disruption**: Service Disruptions refer to interruptions or degradation of cloud web application services, resulting in compromised user experience, revenue loss, and reputational damage. Cloud web applications rely on uninterrupted service delivery to meet user expectations and drive business success.

6. CONCLUSION

This study has demonstrated the significant threat posed by malicious bots to cloud web applications. Through our research, we have shown that bots can cause substantial damage, including: Increased latency and resource consumption, Decreased application performance and availability, Compromised data security and integrity financial losses due to fraud and abuse. Our findings highlight the need for effective bot detection and mitigation strategies in cloud web applications. We recommend that organizations implement a multi-layered approach, incorporating: Advanced bot detection techniques, such as machine learning and behavioral analysis Robust security measures, including firewalls, intrusion detection systems, and encryption Regular security audits and penetration testing Incident response planning and disaster recovery strategies. By taking proactive measures to address the threat

of malicious bots, organizations can protect their cloud web applications and ensure the security, availability, and performance of their online services.

7. FUTURE ENHANCEMENT

To further strengthen the assessment of malicious bots' impact on cloud web applications, future works include Leverage AI/ML techniques to develop predictive models for proactive bot threat detection and mitigation.

REFERENCES

[1] Jabeen, G., Rahim, S., Afzal, W., Khan, D., Khan, A. A., Hussain, Z., & Bibi, T. (2022). Machine learning techniques for software vulnerability prediction: a comparative study. *Applied Intelligence*, *52*(15), 17614-17635.Google Scholar

[2] Subramanian, E. K., & Tamilselvan, L. (2019). A focus on future cloud: machine learning-based cloud security. *Service Oriented Computing and Applications*, *13*(3), 237-249. Google Scholar

[3] Chen, H., & Babar, M. A. (2024). Security for Machine Learning-based Software Systems: A Survey of Threats, Practices, and Challenges. *ACM Computing Surveys*, *56*(6), 1-38. Google Scholar

[4] Krishnaveni, S., Prabakaran, S., & Sivamohan, S. (2016). Automated vulnerability detection and prediction by security testing for cloud SAAS. *Indian Journal of Science and Technology*, *9*(1). Google Scholar

[5] Singh, S. P., & Afzal, N. (2024, June). Effective Bot Management Strategies for Web Applications. *2024 International Symposium on Intelligent Robotics and Systems (ISoIRS)* (pp. 314-322). IEEE. Google Scholar

[6] Guo, Y., Shi, J., Cao, Z., Kang, C., Xiong, G., & Li, Z. (2019, August). Machine learning based cloud bot detection using multi-layer traffic statistics. In *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 2428-2435). IEEE. Google Scholar

[7] Attou, H., Mohy-eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., Alabdultif, A., & Almusallam, N. (2023). Towards an intelligent intrusion detection system to detect malicious activities in cloud computing. *Applied Sciences*, *13*(17), 9588. Google Scholar

[8] Shang, Y., Yang, S., & Wang, W. (2018, June). Botnet detection with hybrid analysis on flow based and graph based features of network traffic. In *International Conference on Cloud Computing and Security* (pp. 612-621). Cham: Springer International Publishing. Google Scholar

[9] Bazm, M., Khatoun, R., Begriche, Y., Khoukhi, L., Chen, X., & Serhrouchni, A. (2015, June). Malicious virtual machines detection through a clustering approach. In *2015 International Conference on Cloud Technologies and Applications (CloudTech)* (pp. 1-8). IEEE. Google Scholar

[10] Ahmed, J., Gharakheili, H. H., Russell, C., & Sivaraman, V. (2022). Automatic detection of DGA-enabled malware using SDN and traffic behavioral modeling. *IEEE Transactions on Network Science and Engineering*, *9*(4), 2922-2939. Google Scholar

[11] Burton, R. (2020). Unsupervised learning techniques for Malware characterization: Understanding certain DNS-based DDoS attacks. *Digital Threats: Research and Practice*, *1*(3), 1-26. Google Scholar

[12] Veeraiah, D., Mohanty, R., Kundu, S., Dhabliya, D., Tiwari, M., Jamal, S. S., & Halifa, A. (2022).Detection of malicious cloud bandwidth consumption in cloud computing using machine learning techniques. *Computational Intelligence and Neuroscience*, *2022*(1), 4003403. Google Scholar

[13] Ismail, Z., Jantan, A., Yusoff, M. N., & Kiru, M. U. (2021). The effects of feature selection on the classification of encrypted botnet. *Journal of Computer Virology and Hacking Techniques*, *17*, 61-74. Google Scholar

[14] Yang, H. W., Huang, L. C., & Hwang, M. S. (2021). Research on detection and prevention of mobile device botnet in cloud service systems. *International Journal on Network Security*, *23*(3), 371-378. Google Scholar

[15] Sadeghpour, S., Vlajic, N., Madani, P., & Stevanovic, D. (2021, January). Unsupervised ML based detection of malicious web sessions with automated feature selection: Design and real-world validation. In *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1-9). IEEE. Google Scholar

[16] Rovetta, S., Suchacka, G., & Masulli, F. (2020). Bot recognition in a Web store: An approach based on unsupervised learning. *Journal of Network and Computer Applications*, *157*, 102577. Google Scholar

[17] Sadqi, Y., & Maleh, Y. (2022). A systematic review and taxonomy of web applications threats. *Information Security Journal: A Global Perspective*, *31*(1), 1-27. Google Scholar

[18] Chissingui, H. J., Pando, H. D., Espino, M. M., & Pérez, N. C. (2022). Bot detection algorithms: a systematic literature review. *Revista Cubana de Ciencias Informáticas*, *16*(4). Google Scholar

[19] Hemmatpour, M., Zheng, C., & Zilberman, N. (2024, March). E-commerce bot traffic: In-network impact, detection, and mitigation. In *2024 27th Conference on Innovation in Clouds, Internet and Networks (ICIN)* (pp. 179-185). IEEE. Google Scholar

[20] Qazi, F. (2022). Application Programming Interface (API) Security in Cloud Applications. *EAI Endorsed Transactions on Cloud Systems*, *7*(23), e1-e1. Google Scholar

[21] Thanh Vu, S. N., Stege, M., El-Habr, P. I., Bang, J., & Dragoni, N. (2021). A survey on botnets: Incentives, evolution, detection and current trends. *Future Internet*, *13*(8), 198. Google Scholar

[22] Martins, S. L., Cruz, F. M. D., Araújo, R. P. D., & Silva, C. M. R. D. (2024). Systematic literature review on security misconfigurations in web applications. *International Journal of Computers and Applications*, 1-13 Google Scholar

[23] Srinivasan, K., Mubarakali, A., Alqahtani, A. S., & Dinesh Kumar, A. (2020). A survey on the impact of DDoS attacks in cloud computing: prevention, detection and mitigation techniques. In *Intelligent Communication Technologies and Virtual Mobile Networks: ICICV 2019* (pp. 252-270). Springer International Publishing. Google Scholar

[24] Senecal, D. (2024). *The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet*. John Wiley & Sons. Google Scholar

[25] Kumar, K. C., Reddy, B. M., Tahaseen, N., Bista, B. B., & Devi, S. G. (2024). A cloud based honeyclo system for malicious detection using machine learning techniques. *Educational Administration: Theory And Practice*, *30*(4), 152-158. Google Scholar

[26] Bin Sulaiman, R., & Rahi, M. A. (2021). A Framework to Mitigate Attacks in Web Applications. *IUP Journal of Computer Sciences*, *15*(1). Google Scholar

[27] Chimuco, F. T., Sequeiros, J. B., Lopes, C. G., Simões, T. M., Freire, M. M., & Inácio, P. R. (2023). Secure cloud-based mobile apps: attack taxonomy, requirements, mechanisms, tests and automation. *International Journal of Information Security*, *22*(4), 833-867. Google Scholar

[28] Nadeem, M., Arshad, A., Riaz, S., Zahra, S. W., Rashid, M., Band, S. S., & Mosavi, A. (2023). Preventing Cloud Network from Spamming Attacks Using Cloudflare and KNN. *Computers, Materials & Continua*, *74*(2). Google Scholar

[29] Hatzivasilis, G., & Kunc, M. (2020). Chasing Botnets: A Real Security Incident Investigation. In *Model-driven Simulation and Training Environments for Cybersecurity: Second International Workshop, MSTEC 2020, Guildford, UK, September 14–18, 2020, Revised Selected Papers 2* (pp. 111-124). Springer International Publishing. Google Scholar

[30] Sangeetha Prabhu, & Subramanya Bhat. (2020). Cyber Attacks Mitigation: Detecting Malicious Activities in Network Traffic–A Review of Literature. International journal of case studies in business, IT, and education (IJCSBE), 4(2), 40-64. Google Scholar

[31] Khalaf, O. I., Ogudo, K. A., & Sangeetha, S. K. B. (2022). Design of graph-based layered learning-driven model for anomaly detection in distributed cloud IoT network. *Mobile Information Systems*, *2022*(1), 6750757. Google Scholar

[32] Pahal, S., & Saroha, A. (2023). Distributed Denial of Services attacks on cloud servers: Detection, Analysis, and Mitigation. *Mapana Journal of Sciences*, *22*(1), 121-145. Google Scholar

[33] Dawadi, B. R., Adhikari, B., & Srivastava, D. K. (2023). Deep learning technique-enabled web application firewall for the detection of web attacks. *Sensors*, *23*(4), 2073. Google Scholar

[34] Rahman, R. U., & Tomar, D. S. (2021). Threats of price scraping on e-commerce websites: attack model and its detection using neural network. *Journal of Computer Virology and Hacking Techniques*, *17*, 75-89. Google Scholar

[35] Potluri, S., Mangla, M., Satpathy, S., & Mohanty, S. N. (2020, July). Detection and prevention mechanisms for ddos attack in cloud computing environment. In *2020 11th international conference on computing, communication and networking technologies (ICCCNT)* (pp. 1-6). IEEE Google Scholar

[36] Memos, V. A., & Psannis, K. E. (2020, October). AI-powered honeypots for enhanced IoT botnet detection. In *2020 3rd World Symposium on Communication Engineering (WSCE)* (pp. 64-68). IEEE. Google Scholar

[37] Kaur, P., Sharma, I., & Kaur, A. (2021, October). Web Application Vulnerabilities & Countermeasures. In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-6). IEEE. Google Scholar

[38] Agarwal, A., Prasad, A., Rustogi, R., & Mishra, S. (2021). Detection and mitigation of fraudulent resource consumption attacks in cloud using deep learning approach. *Journal of Information Security and Applications*, *56*, 102672. Google Scholar

[39] Ellaky, Z., Benabbou, F., & Ouahabi, S. (2023). Systematic literature review of social media bot detection systems. *Journal of King Saud University-Computer and Information Sciences*, *35*(5), 101551. Google Scholar

[40] Rahal, B. M., Santos, A., & Nogueira, M. (2020). A distributed architecture for DDoS prediction and bot detection. *IEEE Access*, *8*, 159756-159772. Google Scholar

[41] Quezada, V., Astudillo-Salinas, F., Tello-Oquendo, L., & Bernal, P. (2023). Real-time bot infection detection system using DNS fingerprinting and machine-learning. *Computer Networks*, *228*, 109725. Google Scholar

[42] Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 129-171. Google Scholar