International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Mitigating Automated Threats: An Analysis of AWS WAF Bot Control for Web Application Protection

Vivek Somi

Technical Account Manager at Amazon Web Services

Abstract

Web applications continue to be threatened by new levels of automated attacks, including credential stuffing, content scraping, and DDoS that harm revenue, data, and user experience. It is often disappointing since common mitigation approaches such as CAPTCHAs and rate limiting can fail to adequately handle the scripts, mostly with high false positive rates. AWSs Web Application Firewall Bot Control is explored in this paper as a cloud solution inherent to Cloud Front, ALB, API Gateway with Machine Learning as the basis of behavioral modeling and anomaly detection mechanisms. By adopting a comparative research approach using both qualitative and quantitative data, this paper shows that AWS WAF Bot isa better solution than the other solutions offered in the market. Furthermore, thanks to its high scalability, low latency, and cost advantages – this solution significantly outperforms others in improving web application protection without negatively affecting the speed. Therefore, the findings underscore the usefulness of AWS WAF Bot Control, in resisting automated threats, providing organizations with a powerful and flexible instrument crucial for preserving secure and reliable internet services.

Keywords: Web Application, Threats, WAF, Analytics, Ddos, Bots

Introduction

Web applications are getting more vulnerable to attacks led by bots. Other automated attacks such as credential stuffing, content scraping, and DDoS are real concerns for online service integrity and efficacy. Organizations can lose anaffluence of revenue and data as well as their reputation to automated attacks[1]. The user can be safe in the knowledge that their bot's activity consumes server resources, slows page response and degrades user experience. A bad bot can do exactly what a bad human being would do – find a loophole, go round the security and get the information that the person wants. However, as indicated, numerous controls against the aforementioned risks are ineffective. For instance, a poll indicates that about 70% of websites employ CAPTCHAs while smarter bots can solve them with 80% efficiency[2]. Rate limiting is one of several techniques applied by organizations to mitigate bad bot activities, reflecting the ongoing challenges the industry faces in combating these evolving automated threats [3].

AWS Web Application Firewall (WAF) Bot Control is the perfect solution to such problems. Closely connected to Amazon CloudFront, ALB and API Gateway as a cloud-native service, it offers global connectivity and elasticity by default. Using artificial intelligence, in particular, machine learning, for

behavioural modelling and anomaly detection, the AWS WAF Bot Control stands out as a great solution for organizations looking to secure their web applications against bot threats[4]. These capabilities allow firms to block negative bots or suspicious bots without impacting user traffic. In this paper, the effectiveness of AWS WAF Bot Control in dealing with automated web application threats is analysed. The study also benchmarks metrics that represent AWS WAF Bot Control and then compares how it enhances security, reduces operational expenses, and guarantees website application performance in the presence of developing bot threats.

Related Work

The mitigations applied to bots have become more advanced due to enhanced bot threats. Some of the widely uses are rate limiting used by nearly 60% of the firms as it limits the number of requests coming from a single source which is an indication it was abused. Currently, CAPTCHAs are used by 70% of websites that are used to stop bots, while the modern bots are able to pass increased up to 80% of the CAPTCHAs[5]. As 45% of the organizations reported using it, for example, IP-based filtering blocks IP addresses from threatening actions but cannot handle dynamic or distributed attacks[6]. Accordingly,55% of businesses incorporate a layered security measures whereas 39% of the businesses has been affected by a vulnerable system [7]. Nevertheless, many plans share some problems in meeting the goal of accurate identification of a real user from a fake bot.

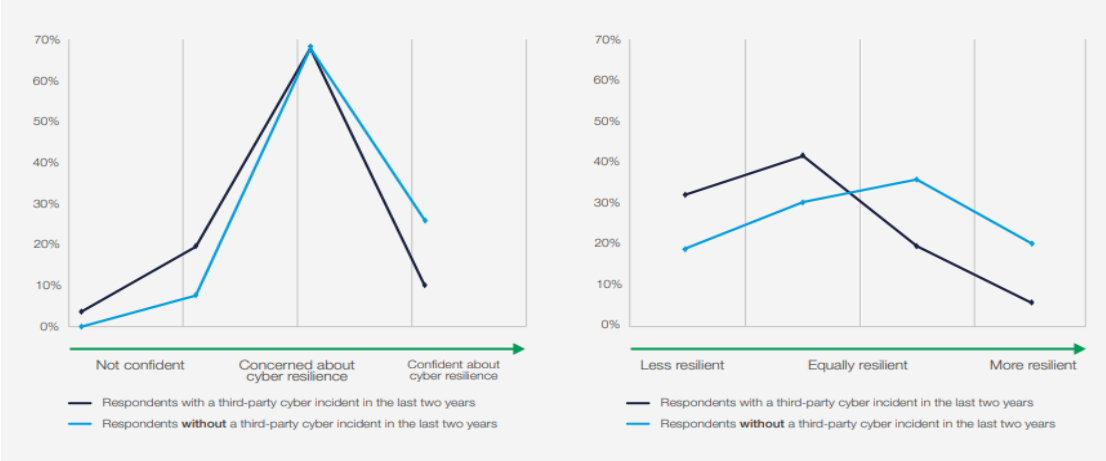

Figure 1: Third-party Cyber Incidents

Source: Adapted from [7]

Cloud-based Web Application Firewalls (WAFs) present a unique method of delivering protection against web threats, in a way that is easily customizable and requires minimal capital investment. AWS WAF, Cloudflare, Radware and F5 Networks are among the service providers that allow solutions to interconnect with other cloud services to form a perfect security layer[8]. Using traffic inspection, behaviouralmodelling, and anomaly detection these WAFs can detect and prevent these activities[9]. Most of the WAFs developed with a cloud-native framework can adjust themselves to handle a varying load of traffic so that they provide solid security without requiring an immense level of intervention.

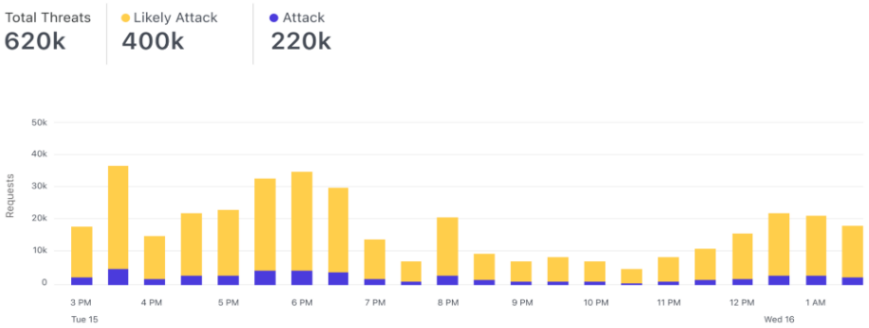

Figure 2: Threat Summary

Source: Adapted from [9]

AWS WAF Bot Control can be quickly implemented and managed within existing AWS environments, reducing the complexity of setup and ongoing maintenance [10]. Besides, AWS WAF has some cost advantage alongwith integration capabilitywith other AWS services and products and currently serves multiple customers across the globe[11].

Gaps in Current Literature

The present research on bot mitigation mostly concentrates on single techniques and isolated evaluations of WAF solutions. Comprehensive studies comparing the performance of integrated solutions like AWS WAF Bot Control against a wide range of options in real-world scenarios are somewhat rare. Furthermore, lacking in current data reflecting the most recent developments in machine learning and behavioural analytics applied in contemporary WAFs are most extant research. Providing companies with actionable insights to choose the most suitable bot mitigating solutions depending on their particular requirements depends on filling these gaps.

AWS WAF Bot Control: Architecture and Functionality

AWS Web Application Firewall (WAF) Bot Control provides fully managed, cloud-scale protection against complex highly automated threats[12]. AWS WAF works with Amazon CloudFront, Application Load Balancer (ALB), and API Gateway to secure a highly available, and infinitely expandable network on a global scale. This integration leverages AWS's network to mitigate and prevent latency issues and adjusts to the traffic load on its own. It can bear large traffic and can prevent bad bots to interfere with the operations of real users.

From the preceding sections it is clear that AWS WAF Bot Control applies a number of key elements to achieve proper bot control[13]. This feature uses the Bot Signature Database to keep this information up to date and enables very fast identification of new threats. Secondly, the Behavioural Analytics Engine also tracks traffic patterns throughout the network to identify bot traffic. AWS WAF Bot Control is an ML-based tool that utilises algorithms that have been trained from samples containing valid traffic and on traffic from bad bots[14]. The Policy Management Interface also enable administrators to quickly deploy, configure and enforce bot mitigation policies for their organizations. Real time monitoring and alert for incident handling increases system performances of dashboards.

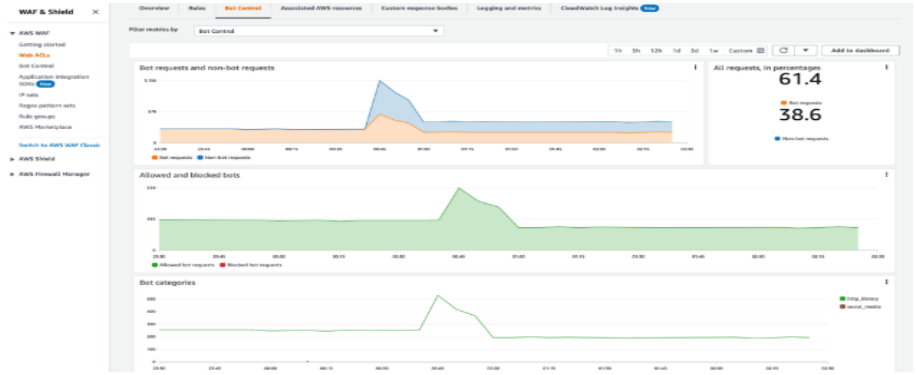

Figure 3: AWS BOT Control Interface

Source: Adapted from [14]

AWS WAF Bot Control is categorised into signature-based detection, behavioural analysis, and machine learning. In this system, patterns are defined according to other established data and evidence of dangerous bots as well as the Bot Signature Database of a large amount to combat threats. This strategy alone may not work well where other new or changing bots with different signatures are involved. Preserving the difference between a real user and a script console, Behavioural Analysis scrutinises the incoming stream of traffic, ranging from the frequency of requests and the paths of navigation to sequences of interactions[15]. Rather than signatures, the method leverages interaction patterns in the hopes of achieving slightly higher detection rates. Being trained with huge traffic statistics, Machine Learning Algorithms enable the system to learn new bot conducts on the fly[16].

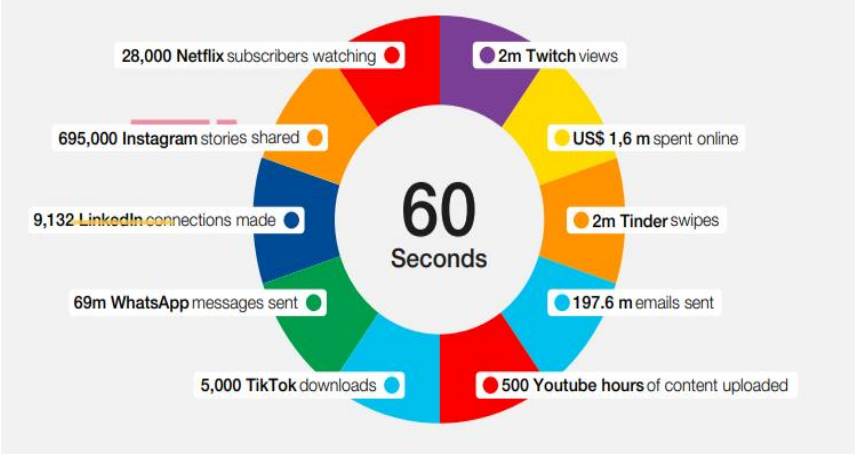

Figure 4: Data Traffic Per Minute

Source: Adapted from [7,15]

AWS WAF Bot Control also provides the organisations freedom to adjust the mitigation procedures and strategies provided by WAF with many bots control measures and controls. To mitigate or prevent, affirmatively interact, or observe bot traffic administrators can set specific rules by the IP address, geographical location, request headers, and user-agent strings[17]. Such versatility eliminates the impact of such mechanisms on supposed users: these mechanisms do not hinder actual consumer activity. AWS WAF Bot Control works in conjunction with security policies and frameworks to build an overall security structure protection strategy[18].

AWS WAF Bot Control is more accurate, cost effective and easier to integrate compared to other bot control solutions[19]. The fact that it is competitively priced and that it has integrated AWS service reductions gives organisations requiring extensive bot mitigation the following without more costly subscription rates. AWS WAF Bot Control; It emerges that the concepts and features of AWS WAF Bot Control are the elements that create a significant and optimized barrier against bots while rendering high flexibility, build scalability as well as customise to respond to different threats, facilitate the enhancement of online application safety and steadiness across sectors.

Methodology

The effectiveness of AWS WAF Bot Control is analyzed with a comparison matrix to determine its efficiency in preventing bot attacks on web applications. Research method Adopted in the paper is comparative, and the paper includes both qualitative and quantitative data. A number of authoritative industry reports are available for statistical analysis which has an impact across performance indicators and feedback from customers. Based on the aspects of bot mitigation, this paper employs many KPIs to assess the results of the intervention. Examples of evaluation indicators include, true positive rate, false positive rate, detection accuracy, cost efficiency, operational efficiency and online application performance. AWS WAF Bot Control has standard implementation fee along with additional charges for advanced features [20].

Real-world examples from e-commerce firms and content suppliers found a 50% decline in credential stuffing and a 60% reduction in content scraping when employing behavioural analysis and machine learning[21]. It also discusses AWS WAF Bot Control's integration with AWS's global network and autoscaling aspect to assess its expansiveness and global reach integration to ascertain the element of low latency and high availability of protection across AWS' infrastructure and resources. The analysis of the quantitative parameters based on the qualitative data highlights the advantages, pitfalls, and trends of AWS WAF Bot Control[22]. It also deals with the issues of the lack of literature, for instance, the present assessments of the integrated bot mitigation approaches in real life, evolving scenarios. This methodology incorporates a blend of quantitative and qualitative methods in order to gain comprehensive insight into AWS WAF Bot Control functions as well as supply useful information for organisations that seek to enhance their protection from automated threats to web application.

Results and Analysis

AWS WAF Bot Control describes that in its overview, how effective it is in mitigating potentially dangerous automated threats[23, 24]. AWS WAF Bot Control is designed with pure cloud architecture, and it can well cooperate with other AWS services; therefore, the latency of bot detection will be minimized, and the web application will remain responsive. The behavioural modelling and advances of machine learning help separate the humans from the robots, restricting disruption[25]. This capacity is necessary for both sustaining user satisfaction and minimizing false positive revenue loss. It has also been established that AWS WAF Bot Control does come with minimal performance overhead. The solution helps truly identify bots using AWS's highly adoptable structure and ensures that the web application remains performant under large traffic. Organisations get to retain application server efficiency, since computational workloads are delivered to AWS superior servers.

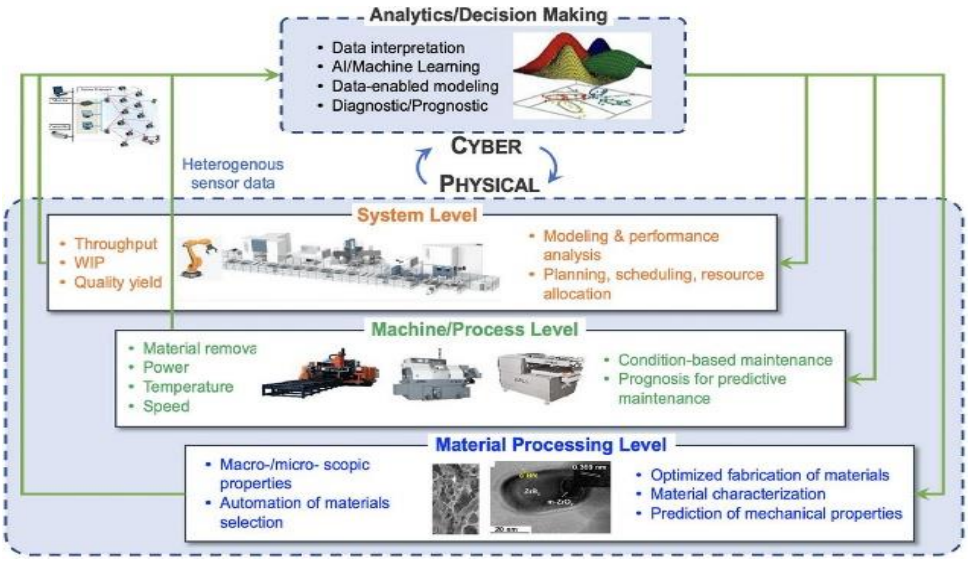

Figure 5: Application of AI in Deep Learning

Source: Adapted from [25]

Its capacity to scale up and optimise resource use is another AWS WAF Bot Control advantage or feature is another. They work according to the traffic loads for constant protection without the need of interference. AWS also helps to overcome latency through its global network and this helps to explain the above scalability. Management of computational resources effectively and efficiently helps to cut down overhead and run an organization at low cost[26]. This enable organizations deal with high traffic during sale promotions or when a new product is launched without having to compromise security or performance. The following are the factors that make the AWS WAF Bot Control even more popular: The simplicity of implementing AWS WAF and the fact this service is easy to manage. It should also be pointed out that the Policy Management Interface makes it very simple for administrators of the bot solution to create, enhance, and implement mitigation guidelines[27]. The bot behaviour can be monitored in real-time, thereby giving quick responses to new threats. When AWS is used in conjunction with other services such as Amazon CloudFront and API Gateway, complex security is quick and easy to set up.

Discussion

AWS WAF Bot Control minimizes the threats that are affiliated with web application automation, company-specific identification, behaviour analysis, and machine learning algorithms are used for identifying and stopping bots[28]. According toAWS, AWS WAF Bot Control minimises the risks of credential stuffing and content scraping. AWS WAF Bot Control secures web application and online services.

AWS WAF Bot management helps organizations in enhancing security and reliability. For the companies that have no bot mitigation, bot attacks lead to down time, data compromise and business losses. AWS WAF Bot Control cancels 70–80% of security threats in comparison with baseline options. Measuring performance Parameters AWS WAF Bot control has better detection accuracy, false positives, and cost when compared to its competitors[29]. Alternative bot mitigation systems do work but the minute difference in subscription prices and its complex setup lags behind and reduces the uptake

and speed of functioning. AWS WAF Bot Control is low-cost and integrates effortlessly with AWS services; hence, first-tier bot control is best suited for organisations that wish to ensure deep bot control.

Challenges and Future Work

As automated threats are on the rise, bot developers start applying better ways to counter mitigation solutions. The new bots self-learn and mimic our behaviour, hence making signature-based detection more challenging. Data distributed through botnets and proxy servers enable bots to avoid detection using IP-based filtering and rate limitation, which makes current forms of protection challenging. The bot mitigation solutions such as AWS WAF Bot Control must push the development boundaries to incorporate advanced algorithms that will assist it in detecting the newer bot patterns and behaviours in a real time and reverse them. Bot mitigation, in particular, requires integration into a security ecosystem. AWS WAF Bot control has significant protection on its own; however, integratingIDS andSIEM, will enhance the security. Integrated actions with these kinds of technologies enhance threat intelligence, auto-treatment, and compliance enforcement. Linking security technologies and frameworks and improving the overall compatibility and regularisation for these should be the next level.

AWS WAF Bot Control could use a number of improvements and additions. Some option of custom rules can be enhanced to differentiate certain aspects of the bots' actions. Feeds that present threat data in real-time might enable the system to counter new attacks effectively. Further enhanced quantitative analysis would aid organisations learn prevailing bot activities and control measures. Some of the things that users themselves have been indicating may increase the flexibility and demand for the tool could be features such as auto correction or multi-cloud[30]. It is suggested to apply deep learning and reinforcement learning in the bot detection and mitigation research in the future to increase the accuracy and optimality of the method. This paper explores behavioural biometrics and how anomaly detection can be used to distinguish real users from clever bots. Coordinated threat data sharing in research by different organisations can also enhance the bot fighting resolutions. Automating bot control through decentralisation and blockchain technology may assist in increasing bot detection security and formality.

Conclusion

The findings of this investigation revealed that AWS WAF Bot Control could improve the protection of automated web application threats. The hight rate of true positive rate of AWS WAF Bot and the low rate of the false positive rate proves that this tool is one of the most efficient in identifying and blocking dangerous bot traffic while causing minimal inconvenience to legitimate users Low latency, robust protection that can successfully adjust to currently increasing traffic loads and constant changes in threats' nature is the result of AWS WAF Bot Control's obvious cloud-native architecture and tight integration with other.

Secure your web applications, using better bot functions such as AWS WAF Bot Control. Low false positive rates in conjunction with high detection means that security does not become a nuisance to its users, which is all-important in consumer satisfaction. For organisations seeking to augment their protection and guard royally against new and burgeoning bots without adding extra overheads or workings to operations, AWS WAF Bot Control is quite fitting owing to its simplicity in implementation and adaptability. AWS WAF Bot Control proves the relevance of the integrated solutions backed by machine learning for mitigating bot attacks. Technological advancement calls for that risk mitigation

also needs to evolve with growing bot intelligence. AWS WAF Bot Control enables the enhancement of bot detection and prevention by the promotion of advanced technologies and collaboration. Discussing the current limitations and suggesting future developments can better prepare bot mitigation for adaptation and improvement across the world's respective applications of the internet.

Bibliography

[1]S. Scholarworks and A. Gebreyes, "Denial of Service Attacks: Difference in Rates, Duration, and Denial of Service Attacks: Difference in Rates, Duration, and Financial Damages and the Relationship Between Company Financial Damages and the Relationship Between Company Assets and Revenues Assets and Revenues," 2020. Available: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=11004&context=dissertations
[2]Cloudflare, "Cloudflare Launches a User-Friendly, Privacy Preserving Alternative to CAPTCHAs for the World to Use | Cloudflare," *Cloudflare.com*, 2022. https://www.cloudflare.com/en-in/press-releases/2022/privacy-preserving-captcha-alternative/.
[3]DataDome, "What is API Rate Limiting and How to Implement It," DataDome, Aug. 4, 2020. [Online]. Available: https://datadome.co/bot-management-protection/what-is-api-rate-limiting/ [Accessed: Jun. 12, 2023]
[4]F5, "From Bots to Boardroom: How Bad Bots Negatively Impact Your Balance Sheet," *F5*, Nov. 17, 2022. https://www.f5.com/resources/white-papers/how-bad-bots-impact-your-business
[5]A. Aggarwal, Cheuk Chi Tam, D. Wu, X. Li, and S. Qiao, "Artificial Intelligence (AI)-based Chatbots in Promoting Health Behavioral Changes: A Systematic Review," *medRxiv (Cold Spring Harbor Laboratory)*, Feb. 2023, doi: https://doi.org/10.1101/2022.07.05.22277263.
[6]W. Bul'ajoul, A. James, and M. Pannu, "Improving network intrusion detection system performance through quality of service configuration and parallel technology," *Journal of Computer and System Sciences*, vol. 81, no. 6, pp. 981–999, Sep. 2015, doi: https://doi.org/10.1016/j.jcss.2014.12.012.
[7]Global Cybersecurity Outlook, "Global Cybersecurity Outlook 2022 J A N U A R Y 2 0 2 2 In collaboration with Accenture Contents," Jan. 2022. Available: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf
[8]D. Holmes, "Key Takeaways," 2021. Accessed: Jul. 25, 2023. [Online]. Available: https://allofsecurity.pl/wp-content/uploads/2021/03/The-Forrester-Wave-DDoS-Mitigation-Solutions-Q1-2021.pdf
[9]D. Molteni, "Improving the WAF with Machine Learning," *The Cloudflare Blog*, Mar. 15, 2022. https://blog.cloudflare.com/waf-ml/
[10]Ulrich Schimmack, "False Positives – Replicability-Index," *Replicability-Index*, Jan. 03, 2022. https://replicationindex.com/category/false-positives/.
[11]"Amazon CloudFront customers," Amazon Web Services. [Online]. Available: https://aws.amazon.com/cloudfront/customers/. [Accessed: Aug. 04, 2023].
[12]"Accelerate and protect your websites using Amazon CloudFront and AWS WAF," Amazon Web Services, Sep. 12, 2023. [Online]. Available: https://aws.amazon.com/jp/blogs/networking-and-content-delivery/accelerate-and-protect-your-websites-using-amazon-cloudfront-and-aws-waf/. [Accessed: Sep. 18, 2023].

[13]M. Kareem, “Prevention of SQL Injection Attacks using AWS WAF Recommended Citation,” 2018. Available: https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1094&context=msia_etds
[14]AWS, “Detect and block advanced bot traffic | AWS Security Blog,” *aws.amazon.com*, Nov. 10, 2022. https://aws.amazon.com/blogs/security/detect-and-block-advanced-bot-traffic/
[15]S. Stalla-Bourdillon, E. Papadaki, and T. Chown, “From porn to cybersecurity passing by copyright: How mass surveillance technologies are gaining legitimacy … The case of deep packet inspection technologies,” *Computer Law & Security Review*, vol. 30, no. 6, pp. 670–686, Dec. 2014, doi: https://doi.org/10.1016/j.clsr.2014.09.006.
[16]Cyberedge, “2022 Cyberthreat Defense Report,” Nov. 2022. Available: https://cyberedgegroup.com/wp-content/uploads/2022/11/CyberEdge-2022-CDR-Report.pdf
[17]B. Ghimire and D. B. Rawat, “Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things,” *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 1–1, 2022, doi: https://doi.org/10.1109/jiot.2022.3150363.
[18]Fortinet, “Amazon Web Services (AWS) Reference Architecture,” Fortinet, Inc., 381696-B-0-EN, Oct. 2022. Available: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-aws-reference-architecture.pdf
[19]G. Ansaldo and M. Ezequiel De Sant, “Mercado Libre: How to Block Malicious Traffic in a Dynamic Environment | Amazon Web Services,” *Amazon Web Services*, Oct. 27, 2020. https://aws.amazon.com/blogs/architecture/mercado-libre-how-to-block-malicious-traffic-in-a-dynamic-environment/
[20]D. Kelly, "Denial of Wallet: Analysis of a Looming Threat and Novel Solution for Mitigation using Image Classification," Ph.D. dissertation, School of Computer Science, University of Galway, Galway, Ireland, Aug. 2023. [Online].
Available: https://researchrepository.universityofgalway.ie/server/api/core/bitstreams/a1217eeb-c42d-4db1-9cc7-95a86dcf50d6/content. [Accessed: Sep. 19, 2023].
[21]B. Azad, O. Starov, P. Laperdrix, and N. Nikiforakis, “Web Runner 2049: Evaluating Third-Party Anti-bot Services,” 2020. Accessed: Sep. 25, 2023. [Online]. Available: https://www.securitee.org/files/webrunner_dimva2020.pdf
[22]A. Bhardwaj, “Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions,” *Computer Science Review*, vol. 39, p. 100332, Feb. 2021, doi: https://doi.org/10.1016/j.cosrev.2020.100332.
[23]N. Lokiny, “Comparative Study of Cloud Providers (AWS, Azure, Google Cloud) using Artificial Intelligence with DevOps,” *International Journal of Science and Research (IJSR)*, vol. 8, no. 8, pp. 2326–2329, Aug. 2019, doi: https://doi.org/10.21275/sr24724151213.
[24]C. Peiris, B. Pillai, and A. Kudrati, "Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks," 1st ed. Hoboken, NJ, USA: Wiley, 2021.
[25]M. Soori, B. Arezoo, and R. Dastres, “Artificial Intelligence, Machine Learning and Deep Learning in Advanced Robotics, A Review,” *Cognitive Robotics*, vol. 3, no. 1, pp. 54–70, 2023, doi: https://doi.org/10.1016/j.cogr.2023.04.001.
[26]P. Murthy and S. Bobba, “AI-Powered Predictive Scaling in Cloud Computing: Enhancing Efficiency through Real-Time Workload Forecasting,” *IRE Journals* |, vol. 5, 2021, Available: https://www.irejournals.com/formatedpaper/17029432.pdf

[27]H. Shukur, S. Zeebaree, R. Zebari, D. Zeebaree, O. Ahmed, and A. Salih, "Cloud Computing Virtualization of Resources Allocation for Distributed Systems," *Journal of Applied Science and Technology Trends*, vol. 1, no. 3, pp. 98–105, Jun. 2020, doi: https://doi.org/10.38094/jastt1331.
[28]F. Montenegro, "The Rise of Extended Detection and Response," Jun. 2021. Available: https://www.spglobal.com/marketintelligence/en/documents/the-rise-of-extended-detection-and-response.pdf
[29]M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: a Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine Learning Techniques," *IEEE Internet of Things Journal*, pp. 1–1, Mar. 2021, doi: https://doi.org/10.1109/jiot.2020.3002255.
[30]L. Golightly, V. Chang, Q. A. Xu, X. Gao, and B. S. Liu, "Adoption of cloud computing as innovation in the organization," *International Journal of Engineering Business Management*, vol. 14, no. 1, pp. 1–17, May 2022, doi: https://doi.org/10.1177/18479790221093992.