UDC: 004.774.6.051
Professional paper

ENHANCING WEBSITE SPEED AND SECURITY WITH CLOUDFLARE CDN: A CASE STUDY ON WORDPRESS WEBSITES

Enes BAJRAMI [1*], Florim IDRIZI [2], Agim RUSHITI [3]

[1*] *Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University*
[2] *Faculty of Natural Sciences and Mathematics, University of Tetova*
[3] *Faculty of Business Administration, University of Tetova*
[*] *Corresponding author e-mail: enes.bajrami@students.finki.ukim.mk*

Abstract

One of the vital components of an organization's prosperity is data. Through true sites that are explicitly intended for showcasing, data might be spread. The created site should satisfy speed and security measures. Cloudflare is an organization that offers content conveyance network administrations, cloud online protection, DDoS relief, and ICANN-licensed space enrollment administrations. Cloudflare typically facilitates the transport of data from website pages so it ends up being faster with splendid execution. Cloudflare confines bots and blocks dangers. Cloudflare fundamentally diminishes spam and dangers while additionally improving quality paces by up to 95%. Cloudflare's savvy framework reserving saves transmission capacity, and that implies less work for the server and less cash. Cloudflare cuts down bandwidth by a typical 60%. Cloudflare decreases open time by half on each site page, bringing about speeding up.

Keywords: CDN, Speed, Security, Website, Cloudflare.

1. Introduction

An unyieldingly typical example for destinations with around the world high appearance is to use content delivery network (CDN) to host or store their resources. According to Cisco, CDNs will serve 71% of all traffic in approaching years, up from 52% in 2016 [1]. Likely the most eminent CDNs consolidate Akamai, Cloudflare, Fastly, and Amazon CloudFront. These CDNs routinely house server ranches across the globe, suggesting that induction to locales is advanced by serving from regions geographically near requests. On top of this, CDNs regularly offer protection organizations to hold clients back from having their destinations brought someplace close to scattered refusal of organization (DDoS) attacks, or vandalized by spam. Security of this sort takes different designs, yet an ordinary technique is to use public IP-set up standing checking regarding requests that target defended destinations. Before giving access, these checks look at whether approaching IP addresses have been used for noxious action previously. If an IP address is considered to have a 'poor' reputation existing CDNs could use one of the following decisions for observing defended destinations:

- block access totally;
- impose human proof-of-work challenges to stop bots from gaining access. (such as CAPTCHA);
- forward requests through the web application firewall [2].

2. Literature Review

As indicated by the researcher [3], the primary cause of cloud server attacks is inadequate security from the start. The attackers worked on several security problems to resolve these problems. They talked about a variety of strategies for protecting the cloud infrastructure, such as security models, cloud server concerns, and threats. Every technology, in the author's

https://doi.org/10.62792/ut.jnsm.v9.i17-18.p2824

opinion, has two stages. There are two stages: one leads to difficulties and the other to wealth. Users of the cloud encounter several security issues in addition to cloud computing. Standardization, lack of assistance, and insider attacks are a few of the causes of security problems. Subsequently, the researchers talked about the hazards and vulnerabilities connected to data stored on the cloud, as well as the security concerns and privacy breaches that cloud users encounter. In paper [4], to defend the cloud server against both internal and external assaults, a program was created. Numerous strategies have been put into practice to defend the cloud server against pattern matching and brute force attacks, and numerous strategies have been suggested to defend the cloud server against internal attacks such as denial-of-service attacks. Following the acquisition of distinct outcomes from external attacks, these outcomes were applied to identity property and commutative law. Furthermore, it has been stated that all effective algorithms should be practically applied to the cloud server to protect it from both internal and external attacks. This would greatly lower the likelihood of an attack. In the paper [5], the researcher developed a research methodology that used three processes to represent the work breakdown structure application of Cloudflare. As a means of obtaining data regarding the organizational requirements necessary to deploy Cloudflare, the researcher employed the following steps: Basic Analysis: Information is gathered to determine whether Cloudflare will be beneficial for the website. viewed via the live webpage The results of the Gap Analysis show that there are variations in access speeds when compared to comparable websites.

3. Cloudflare

Cloudflare, a prominent entity in the domain of cloud computing, specializes in cloud security and content delivery network (CDN) services, aimed at enhancing website performance, fortifying security measures, and optimizing overall functionality. Serving as an intermediary link between a website's server and its visitors, Cloudflare endeavors to expedite website loading times and bolster reliability while concurrently shielding against various online threats. With a primary focus on enhancing the security, performance, and dependability of internet-connected devices, Cloudflare's overarching goal revolves around augmenting the efficiency and safety of the global internet infrastructure. Notably, Cloudflare extends the majority of its core functionalities without charge, facilitating seamless setup procedures and accessibility for users. Both a user-friendly interface and an Application Programming Interface (API) are furnished by Cloudflare, empowering website administrators with versatile tools for the management and maintenance of their online platforms. [6]. To understand how Cloudflare works, we need to consider common mistakes websites have made in the past. When you visit a website without Cloudflare, website visitors request content from your server [7]. However, if you have too many visitors on your server at the same time, it will overload your server and your website will slow down or stop working. As a website owner, you don't want to see this. That's why Cloudflare has come up with a solution for this [8].

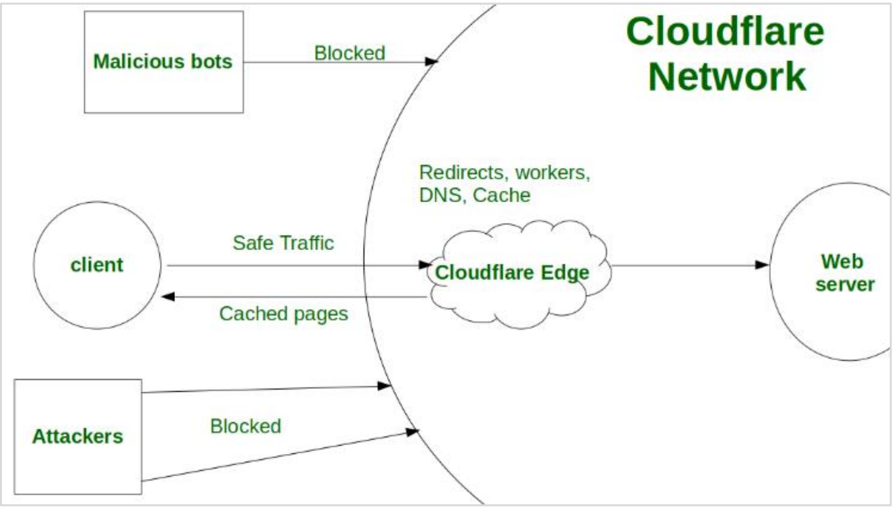


Figure 1: Cloudflare schema[5]

Between the website and the web server, Cloudflare set up its server in the form of a huge global network. Site guests don't discuss straightforwardly with the server any longer, however with the Cloudflare network which as of now has put away the site content and loads this through a server relying upon the area of the guest [9]. For example: You have a site that is facilitated in Germany, and somebody from the US attempts to interface with your site. The solicitation needs to cover a major distance (between the site and the web server). Cloudflare tackles this by offering an immense organization of servers all over the planet. The American doesn't need to make an association with the German server any longer, however, he will interface with the closest Cloudflare server some place in the US [10].

4. The DNS market over time

DNS is crucial for the working of the Web. DNS maps space names that clients can recollect to Web Convention (IP) addresses that PCs use to find the data they are searching for. Cloud administrations and content conveyance networks are completely founded on DNS, so the web insight as far as we might be concerned today depends vigorously on specialized highlights, which are as yet secret in specialized layers, and are generally muddled in open conversation [11]. Other than the political discussions encompassing the space name enlistment framework, which incorporated the foundation of the Web Company for Relegated Names and Numbers (ICANN) and its resulting change, the DNS is overseen by a private, non-benefit association in the US [12], researchers have not given enough attention to the dynamics of the domain name market and its recent tendency toward concentration. Starting around 2009, numerous players have offered other options (additionally called "public") DNS resolvers. Of these, some spend significant time on DNS goals, e.g., Noticing changes in the general Web economy, the Web Affiliation's 2019 World Web Report takes note that DNS goal is presently performed by a few players. Besides, "DNS conventions are in any event, developing in manners that build up this pattern [13]. "One of eight companies that now handle half of the world's Internet traffic" is the description of Google. Google's DNS takes the best position with around 13% of DNS traffic in the measurement. OpenDNS is in runner-up with around 2% piece of the pie. The most up-to-date market passages, Quad9, sent off in November 2017, and Cloudflare (which sent off its 1. 1. 1. 1 assistance on April 1, 2018), both record for around 0. 12% of absolute utilization [14].

[5] https://www.geeksforgeeks.org/what-is-cloudflare/

5. Content delivery network (CDN)

A content delivery network is a network of geographically dispersed proxy servers and associated data centers. By spreading the help spatially according to end clients, the goal is to convey high accessibility and execution. Many big video websites use content delivery network (CDN) technology to improve service quality meet user needs and enhance user viewing experiences. CDN is a speed-increasing innovation by directing the clients to the closest server. Focus servers and edge servers set in various geographic areas comprise the CDN organization [15]. The load balancing mechanism is implemented by special nodes among them. Utilizing CDN innovation can address the organization's transmission capacity bottleneck and reaction time issue of video business. Additionally, large, well-known websites like Alibaba, Facebook, and Twitter make use of CDN. However, CDNs have some issues to worry about: With the explosive growth of network traffic, current CDN systems also face a lack of IT infrastructure and storage space [16]. It has become monetarily for more modest suppliers to contend for a huge scope following the conventional model by building new data centers [17].

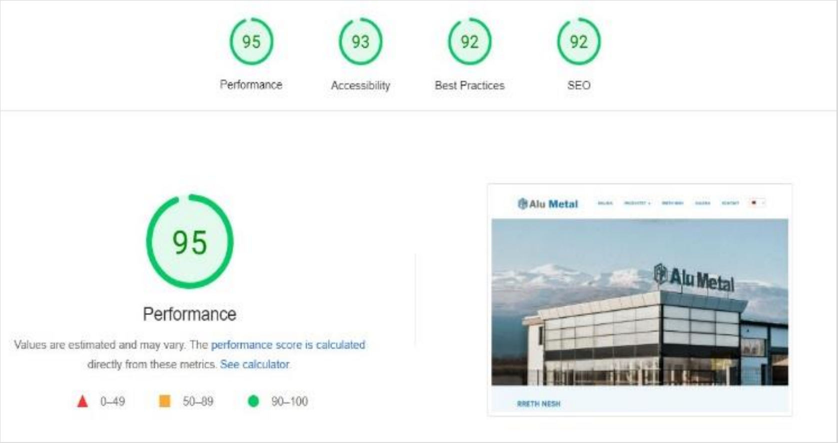
6. Encrypted DNS and its Penetration

6.1.Encrypted DNS: Beginning from the initiation of DNS, the shortfall of decency of Do53 has allowed control tries, e.g., changing the DNS objective for organizations like electronic banking, shopping, and online diversion, or redirecting visitors to phishing destinations. DNSSEC [18] permits the legitimate name server liable for a particular space to cryptographically sign DNS reactions, consequently guaranteeing DNS trustworthiness; however, it doesn't give an assurance of privacy. DNSCrypt [19] aims to encrypt and authenticate the DNS channel using elliptic curve cryptography. However, because its specification has not yet been submitted to the IETF, it is neither standardized nor widespread [18]. In 2015, the IETF defined DNS-over-TLS [20] to encode DNS correspondences in a normalized manner. However, ISPs can easily identify DoT traffic (to a remote resolver) and filter it out because it uses a designated port number (853). Through such interruptions, ISPs can drive the requester to minimize Do53, and this might happen flawlessly as per the pioneering protection profiles [21] that most stub resolvers adapt. In 2017, DNS-over HTTPS was characterized by the IETF, which utilizes a similar degree of encryption and the notable objective port number 443 utilized for encoded Web correspondences. Consequently, other than being uninterpretable by a busybody, DNS questions (and reactions) over HTTPS can undoubtedly sidestep firewalls [22].

6.2.Penetration: DoH, in light of HTTPS, was first carried out (as a client) as a component of Mozilla's Firefox program. [23], therefore, there is no underlying operating system requirement for encrypted DNS communications. The first major step since then was taken by Mozilla (in 2018) by introducing full functional support for Trusted Recursive Resolvers (TRR) in its browser, Firefox [24]. Google rolled out comparable improvements to Chrome browser in 2019 [25]. Moreover, in 2020, Mozilla declared that it would utilize DoH, explicitly Cloudflare's TRR, as a matter of course for US clients (even though clients can change these settings). Comparative endeavors have caused worry among ISPs (particularly in the UK), as virtually every one of their administrations will ultimately fizzle if DoH is utilized and outsider resolvers are depended upon. After Mozilla was selected as "Web Antagonist of the Year", Mozilla didn't empower DoH of course for UK inhabitants [26]. However, this is not an obstacle to the adoption of DoH, which although still in its infancy, continues to slowly gain popularity. For example, Microsoft recently announced the addition of OS-level DoH support for Windows 10 Insiders [27]. Additionally, DoH is not only supported natively on iOS and macOS platforms but also provides APIs to customize the use of DoH (and DoT) in any application, e.g. to connect to a DoH service if you are using a WiFi router [28]. Comparable applications are likewise accessible for Android. Furthermore, Comcast as of late joined Cloudflare and NextDNS in Mozilla's TRR program as the initial ISP to offer DoH administrations through the program [29].

7. Research results and discussion

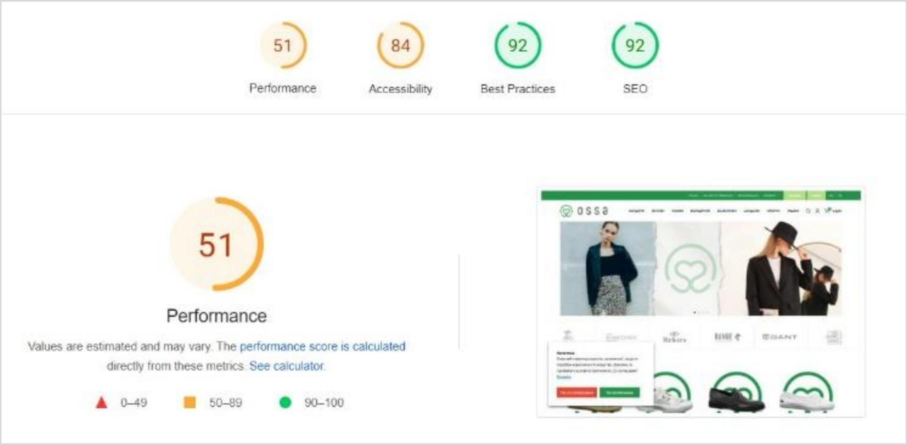
7.1. Research results: In this part, we will elucidate the findings derived from an investigation conducted on two distinct websites that were developed using same technology. The hosting infrastructure for both websites remains consistent, as they are both hosted by the same hosting provider. Additionally, one of the websites has been seamlessly integrated into the Cloudflare content delivery network to gauge the potential impact on its performance metrics. The comprehensive evaluation and comparison of these websites' overall performance and speed across a variety of geographical locations is the primary goal of this study. To achieve this, a meticulous analysis of various performance indicators, such as page load times, server response times, and overall user experience, will be undertaken. The selected websites have been meticulously crafted using the widely utilized WordPress platform, complemented by the integration of the Elementor website builder to enhance design flexibility and functionality. By examining the performance metrics of these websites under different conditions and configurations, this study aims to provide valuable insights into the factors influencing website speed and user experience. This comparative analysis will contribute to a nuanced understanding of the interplay between hosting environments, content delivery networks, and website construction tools in shaping the digital landscape.



Values are estimated and may vary. The performance score is calculated directly from these metrics. See calculator

Figure 2: Alumetal.mk website and data results from PageSpeed Insights

Alumetal.mk was the initial website employed in our research. As depicted in Figure 2, the performance results reveal a 95% improvement when utilizing Cloudflare.



51
Performance

84
Accessibility

92
Best Practices

92
SEO

51
Performance

Values are estimated and may vary. The performance score is calculated directly from these metrics. See calculator.

▲ 0–49 ■ 50–89 ● 90–100

Figure 3: Ossa.mk website and data results from PageSpeed Insights

Ossa.mk is the second website incorporated in our study. While both websites are hosted on the same hosting provider, there is a distinction in performance, with Ossa displaying a 44% lower performance rate. Both websites were tested using Google tools.

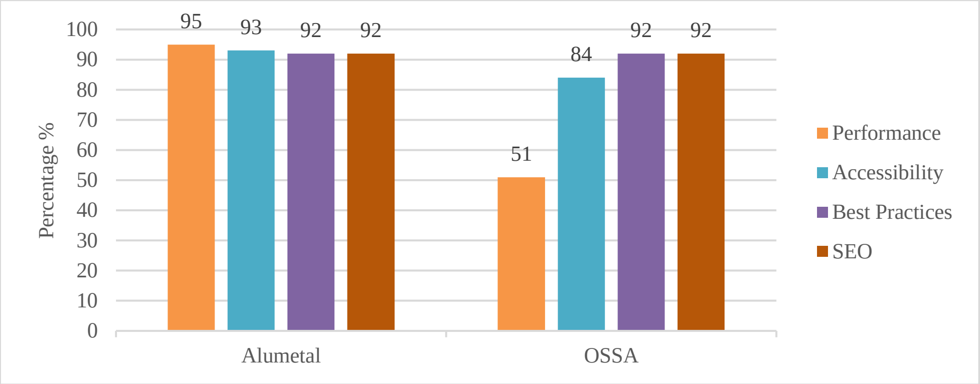


Figure 4: Alumetal vs Ossa

In the Figure 4, we have presented the data to enhance clarity for future readers. The subsequent examination involves the web page speed index, where we initially evaluated the loading speed of the web page in Virginia, USA, followed by Frankfurt, DE.

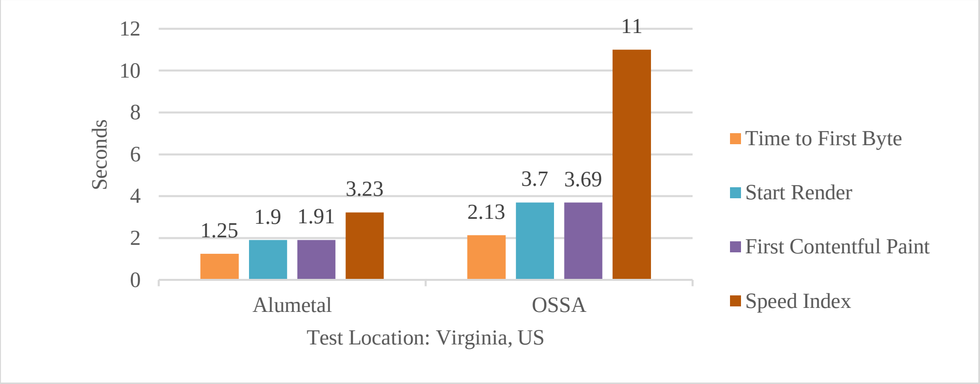


Figure 5: Testing conducted from Virginia, USA

Following the results, a distinction is evident between the website integrated with Cloudflare and the one utilizing the standard provider's DNS, particularly in the speed index. The testing was conducted from Virginia, USA.

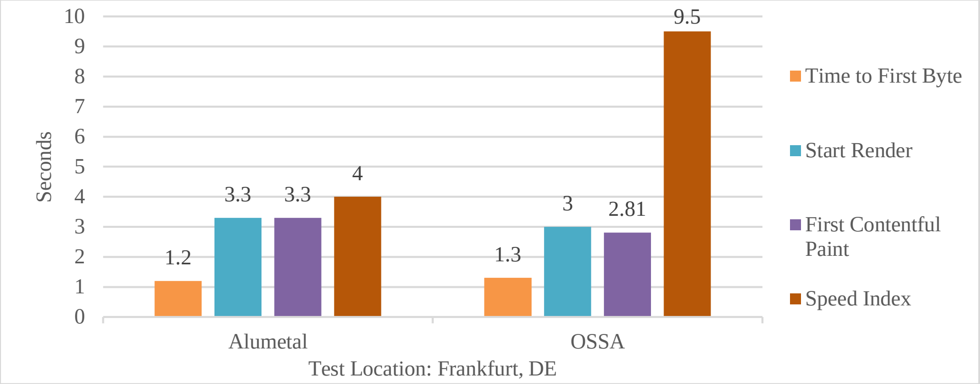
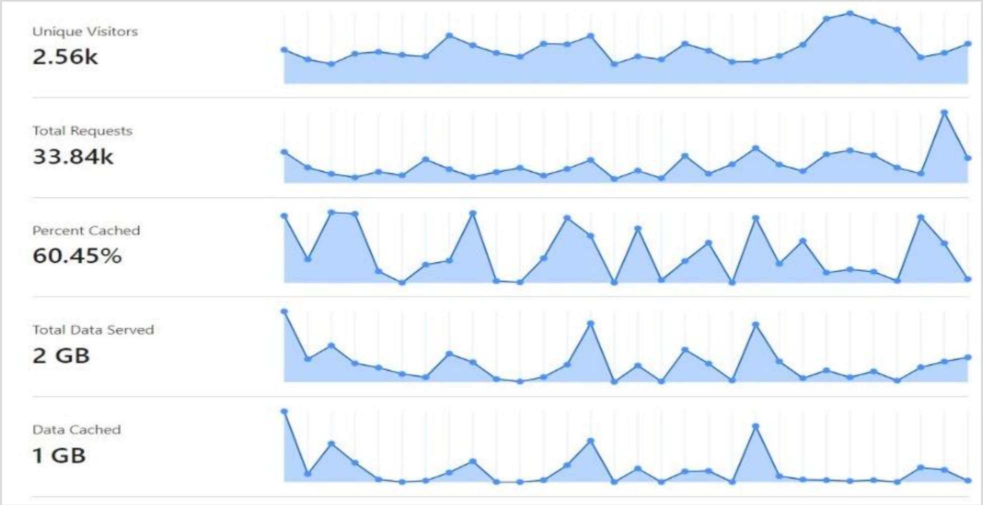


Figure 13: Testing conducted from Frankfurt, DE

In contrast to the test outcomes in the United States, there is minimal disparity when compared to those in Europe. Nevertheless, the website that has been incorporated into Cloudflare exhibits superior performance compared to the alternative website lacking Cloudflare integration.



Unique Visitors
2.56k

Total Requests
33.84k

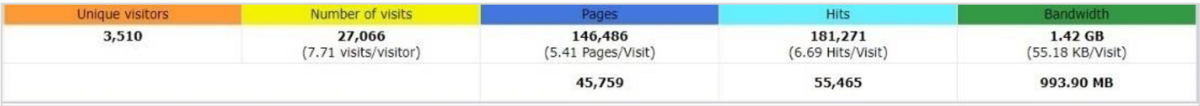
Percent Cached
60.45%

Total Data Served
2 GB

Data Cached
1 GB

Figure 7: Analytics data for the period of December to January for the alumetal.mk website (Cloudflare dashboard)

In Figure 7, we have displayed data for a one-month period, extracted from the Cloudflare panel for the Alumetal.mk website. As indicated, during the period from December 1 to January 1, there were 33.84K requests, a notably high number for a one-month timeframe.



Unique visitors	Number of visits	Pages	Hits	Bandwidth
3,510	27,066 (7.71 visits/visitor)	146,486 (5.41 Pages/Visit)	181,271 (6.69 Hits/Visit)	1.42 GB (55.18 KB/Visit)
		45,759	55,465	993.90 MB

Figure 8: Analytics data for the period of December to January for the ossa.mk website (cPanel dashboard)

On another website where Cloudflare has not been integrated, the monthly visits totaled 27K. This number of visitors is considered quite high for the site in question.

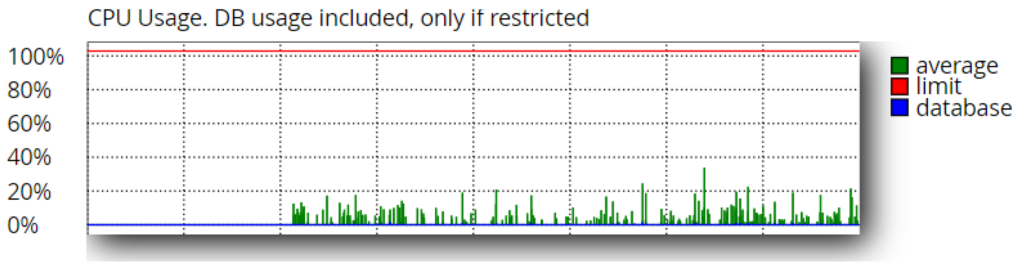


Figure 9: Analytics on CPU usage for alumetal.mk

As evident in the Figure 9, the server's CPU usage is notably low, resulting in swift website performance, thanks to the integration of Cloudflare. Despite the high traffic, the server has not exhausted all available resources.

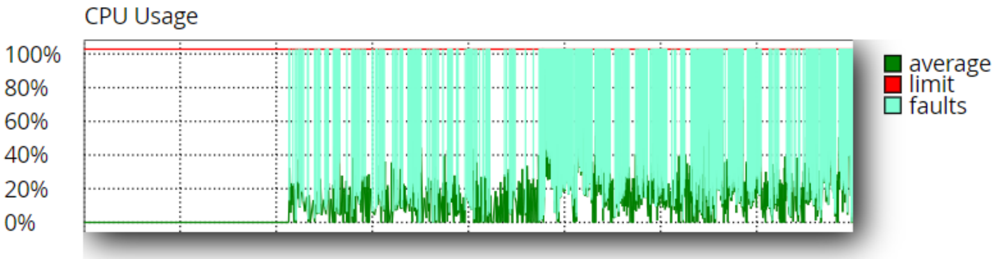


Figure 10: Analytics on CPU usage for ossa.mk

On the other website, illustrated in Figure 10, the CPU resources consistently consume a significant amount, leading to frequent faults almost every day. This compels the hosting provider to restart the server to restore the site to normalcy.

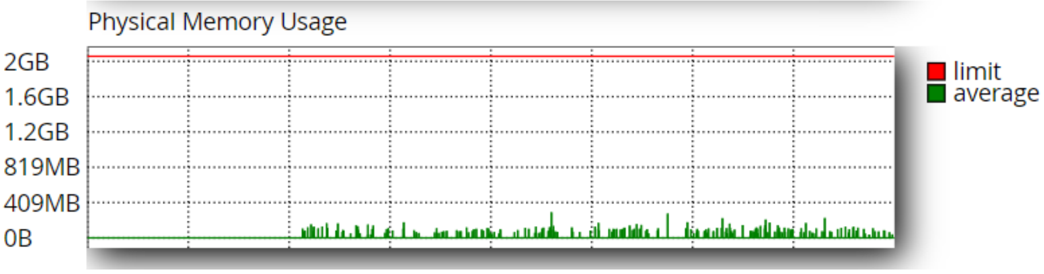


Figure 11: Physical Memory Usage for alumetal.mk

In the website integrated with Cloudflare, it's observed that the physical memory remains stable, and there's no need for the server to consume extensive resources, as illustrated in Figure 11, with physical memory usage peaking at 400MB.

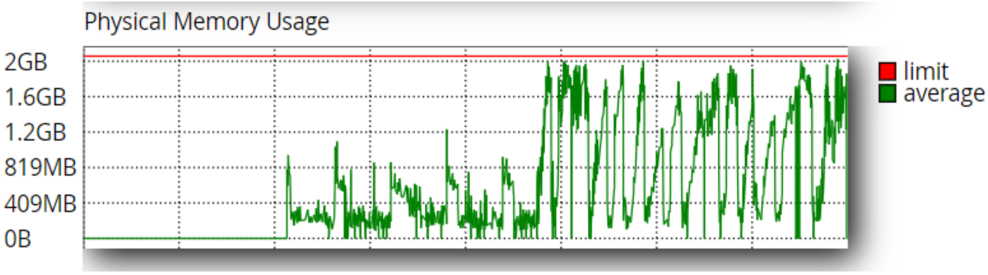


Figure12: Physical Memory Usage for ossa.mk

On the other website, as illustrated in Figure 12, the physical memory occasionally reaches its limit, causing the server to become blocked. To address this issue, the server must be restarted to return to normal operation, either manually or automatically, until the memory is normalized and there are no requests on the website.

7.2. Discussion: In today's digital environment., website performance plays a critical role in user satisfaction and engagement. With the increasing demand for fast and reliable web experiences, website owners are constantly seeking ways to optimize their platforms. In this paper, we compare and contrast two websites hosted on the same hosting provider, one of which has been integrated with Cloudflare, a popular content delivery network (CDN) and internet security service. Our study aims to evaluate the impact of Cloudflare integration on various aspects of website performance. We conducted a comparative analysis of two websites with similar traffic volumes, ranging from 25 to 33K monthly visitors, both hosted on the same hosting provider. One website was integrated with Cloudflare, while the other operated without it. We measured performance metrics including Performance, Accessibility, Best Practices, SEO, as well as time to first byte, start render, and speed index using standardized tools and methodologies. Our results demonstrate the significant performance enhancements achieved by the website integrated with Cloudflare. Across all measured metrics, the Cloudflare-integrated website outperformed its counterpart. Specifically, the website with Cloudflare integration exhibited superior Performance, Accessibility, Best Practices, and SEO scores. Moreover, crucial indicators such as time to first byte, start render, and speed index showed remarkable improvements compared to the website without Cloudflare integration. Importantly, despite both websites experiencing high traffic volumes, the server hosting the Cloudflare-integrated website demonstrated stability, with no faults or resource limitations observed. The findings of our study underscore the tangible benefits of integrating Cloudflare into website infrastructure. By leveraging Cloudflare's robust CDN and internet security services, website owners can effectively enhance performance, user experience, and overall site reliability. The superior performance metrics observed in the Cloudflare-integrated website highlight the efficacy of CDN in optimizing content delivery and mitigating latency issues. Furthermore, the stability of the hosting server hosting the Cloudflare-integrated website reinforces the scalability and resilience offered by Cloudflare's distributed infrastructure. Our experiment provides compelling evidence that integrating Cloudflare significantly improves website performance compared to traditional hosting setups. With the ever-growing importance of speed and reliability in the online ecosystem, we strongly recommend website owners consider integrating Cloudflare into their infrastructure. By doing so, they can deliver faster, more secure, and more accessible web experiences to their users, ultimately driving greater engagement and satisfaction.

8. Conclusion

In conclusion, this manuscript provides a comprehensive review of key elements in the digital infrastructure, specifically focusing on Cloudflare, the evolving DNS market, CDN dynamics, and the penetration of encrypted DNS. A significant aspect of this study involves a meticulous comparison between two websites, both created using WordPress and hosted on the same provider's server. The evaluation encompassed performance metrics, speed differentials, and resource utilization, revealing a pronounced advantage for the website integrated with Cloudflare. Through a detailed examination of total requests, CPU usage, and physical memory consumption using both Cloudflare and cPanel dashboards, our findings underscore the tangible benefits of incorporating Cloudflare services. The discernible disparities affirm Cloudflare's efficacy in enhancing website performance, emphasizing its role as a pivotal component in optimizing the online experience.

References

[1] Cisco, "Cisco Annual Internet Report (2018–2023) White Paper," 9 March 2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. [Accessed 15 January 2024].

[2] Alex Davidson, Ian Goldberg, Nick Sullivan, George Tankersley, and Filippo Valsorda, "Privacy Pass: Bypassing Internet Challenges Anonymously," *Proceedings on Privacy Enhancing Technologies,* vol. 3, pp. 164-180, 2018.

[3] Narendra Rao Tadapaneni, "Cloud Computing Security Challenges," *International Journal of Innovations in Engineering Research and Technology,* vol. 7, no. 6, pp. 1-6, 2020.

[4] Muhammad Nadeem, Ali Arshad, Saman Ria, Shahab S. Band, and Amir Mosavi, "Intercept the Cloud Network From Brute Force and DDoS Attacks via Intrusion Detection and Prevention System," *IEEE,* vol. 9, pp. 1-10, 2021.

[5] Dewi, Estri JH, Rusydi, Umar, Imam, Riadi, "Implementation of Cloudflare Hosting for Speeds and Protection on The Website," 2019. [Online]. Available: https://eprints.uad.ac.id/15251/. [Accessed 03 02 2024].

[6] "GeeksforGeeks | A computer science portal for geeks," 2023. [Online]. Available: https://www.geeksforgeeks.org/what-is-cloudflare/. [Accessed 06 01 2024].

[7] Miller Charles,Pelosi Michael,Brown Michael Scott, "Domain Fronting Through Microsoft Azure and CloudFlare: How to Identify Viable Domain Fronting Proxies," *Def Con,* pp. 1-12, 2023.

[8] Ian Pye, "Locks, deadlocks and abstractions: experiences with multi-threaded programming at CloudFlare, Inc.," *SPLASH '11 Workshops,* pp. 129-132, 2011.

[9] S. Looney, "Content moderation through removal of service: Content delivery networks and extremist websites," *Policy & Internet,15,* pp. 544-558, 2023.

[10] "Hipex," Cloudflare: what is it? And what can you do with it?, January 2023. [Online]. Available: https://www.hipex.io/en/cloudflare/. [Accessed January 2024].

[11] M. L. Mueller, Ruling the Root: Internet Governance and the Taming of Cyberspace, The MIT Press, 2004.

[12] R. Radu, Negotiating Internet Governance, Oxford University Press, 2019.

[13] A. Sullivan, "Internetsociety," 2022. [Online]. Available: https://www.internetsociety.org/wp-content/uploads/2022/12/2019-Internet-Society-Global-Internet-Report-Consolidation-in-the-Internet-Economy.pdf. [Accessed 2023].

[14] N. Z, "Medium," 2018. [Online]. Available: https://medium.com/@nykolas.z/dns-resolvers-performance-compared-cloudflare-x-google-x-quad9-x-opendns-149e803734e5. [Accessed 2023].

[15] Zhenyun Zhuang;Chun Guo, "Building cloud-ready video transcoding system for Content Delivery Networks (CDNs)," *Communications Software, Services and Multimedia Symposium ,* pp. 2048-2053, 2013.

[16] Lin, Chia-Feng; Leu, Muh-Chyi; Chang, Chih-Wei; Yuan, Shyan-Ming, " The Study and Methods for Cloud based CDN," *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery,* pp. 466-475, 2011.

[17] Fangfei Chen;Katherine Guo;John Lin;thomas La Porta, "Intra-cloud Lightning - Building CDNs in the Cloud," *IEEE INFOCOM,* pp. 1-9, 2012.

[18] Samuel Weiler; David Blacka, "Clarifications and Implementation Notes for DNS Security (DNSSEC)," *Internet Engineering Task Force (IETF) ,* pp. 1-21, 2013.

[19] "DNSCrypt.info," [Online]. Available: https://dnscrypt.info/protocol/. [Accessed 2023].

[20] Z. Hu; L. Zhu; J. Heidemann; A. Mankin; D. Wessels; P. Hoffman, " Specification for DNS over Transport Layer Security (TLS)," *Internet Engineering Task Force (IETF) ,* pp. 1-18, 2013.

[21] S. Dickinson; D. Gillmor; T. Reddy, " Usage Profiles for DNS over TLS and DNS over DTLS," *Internet Engineering Task Force (IETF) ,* pp. 1-26, 2018.

[22] Qing Huang;Deliang Chang;Zhou Li, "A Comprehensive Study of DNS-over-HTTPS Downgrade Attack," *10th USENIX FOCI. USENIX Association,* pp. 1-8, 2020.

[23] C. Cimpanu, "Bleeping Computer," Mozilla Is Testing "DNS over HTTPS" Support in Firefox, 2018. [Online]. Available: https://www.bleepingcomputer.com/news/software/mozilla-is-testing-dns-over-https-support-in-firefox/. [Accessed January 2024].

[24] M. Erwin, "Trusted Recursive Resolvers – ProtectingYour Privacy with Policy and Technology.," 2019. [Online]. Available: https://blog.mozilla.org/netpolicy/2019/12/09/trusted-recursiveresolvers-protecting-your-privacy-with-policy-technology/. [Accessed 2023].

[25] C. Catalin, "ZDNet," 2019. [Online]. Available: https://www.zdnet.com/article/google-to-run-dns-over-https-doh-experiment-in-chrome/. [Accessed 2023].

[26] "ISPreview," 2019. [Online]. Available: https://www.ispreview.co.uk/index.php/2019/09/firefox-says-no-dns-over-https-doh-by-default-for-uk.html. [Accessed 2023].

[27] S. Gatlan, "Bleeping Computer," Microsoft adds Windows 10 DNS over HTTPS settings section, 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/microsoft-adds-windows-10-dns-over-https-settings-section/. [Accessed 2023].

[28] Lindsey O'Donnell, "Threat Post," Microsoft Adds DNS-Over-HTTPS Support for Windows 10 Insiders, 2020. [Online]. Available: https://threatpost.com/microsoft-dns-over-https-windows-10/155746/. [Accessed 2023].

[29] Skanda Hazarika, "XDA Developers," BraveDNS is an open-source DNS-over-HTTPS client, firewall, and adblocker for Android, 2020. [Online]. Available: https://www.xda-developers.com/bravedns-open-source-dns-over-https-client-firewall-adblocker-android/. [Accessed 2023].