International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 2.102

Security and Performance in Modern CDN Caching: A Study of Akamai's Caching Infrastructure

Mohit Thodupunuri

Charter Communications Inc

Abstract: ***Modern CDNs are at the heart of web performance optimization and security by caching and delivering content closer to the user. It examines Akamai's content delivery mechanism concerning caching, detailing how various levels of sophisticated caching mechanisms further performance enhancement and robust security. The multi-tiered caching approach of Akamai with intelligent request-routing mechanisms and smart content replication is carefully examined herein. This study has demonstrated that Akamai caching reduces latency in page loading speed. In addition, Akamai includes security features such as DDoS protection, bot management, and data encryption, showing how caching can play a very defensive role in many applications. This paper provides insight into the symbiotic relationship between performance and security in CDN caching. It gives an understanding of how Akamai's infrastructure meets modern web application demands for speed, resiliency, and security.***

Keywords: security, performance, CDN caching, Akamai's Caching, infrastructure, encryption

1. Introduction

The continuous evolution of network distribution and web services brings the requirement of reliable, scalable, optimized, and secured content delivery, and therefore appropriate methods are required to achieve this objective. Content Delivery Networks (CDN) with Akamai's Caching methods are the best ways to handle these aspects as they provide the best performance while keeping the system secure from any malicious activities. This is why it is a leading network technology as it utilizes advanced caching methods and updated security methods to provide a smooth secure experience.

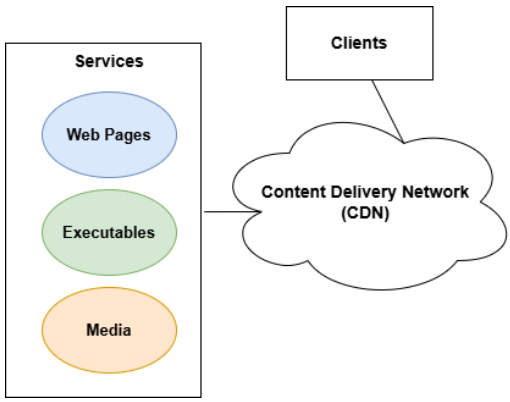

Figure 1: CDN Architecture

The presented research document explores Akamai's caching methods to highlight its role and importance in both the performance and security of the web applications distributed over a network. The performance metrics include, reliability, scalability, reduced latency, and bandwidth optimization. Moreover, for security, attack protection, bot management, firewalls, and data encryption methods are significantly considered. The study explores the detailed data encryption methods that are utilized and how they help to achieve the overall objective of a secured user experience over a network.

The basic architecture of CDN is given in Figure 1 above which shows how CDN interacts with Clients to provide continuous services of different types. The Figure 2 however shows the architecture of Akamai conceptual model for complete Content Delivery Network as efficient provider. Client is responsible to interact with the most closely available cache to make requests and get responses in return. The response provider has to interact with the origin to generate responses that are needed to be added in the caching. The cloud has the servers to store the data, get data from databases and execute any processes against the user requirements. The complete working method is shown below,

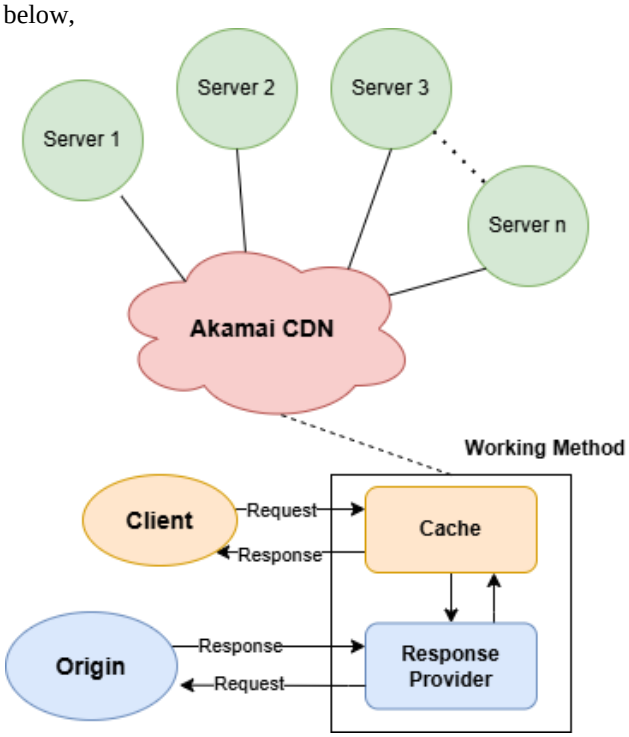

Figure 2: Akamai's CDN Architecture

Caching is one of the main aspects of Content Delivery Network as it helps place the content closer to the user access. The resource requirement is reduced and performance is enhanced by caching content at distributed edge servers. Thus, the distance of data travel is reduced with an overall impact on performance. The latency reduction is achieved by serving content from the nearest

cache and load time is reduced. The edge caches are utilized rather fully taking the resources of original servers and therefore bandwidth is less required with reduced server load. The page load time is reduced and so the user experience is enhanced which is why continuous engagement is achieved.

2. Literature Review

To handle frequent request changes and shortage of storage, a new architecture can be used. This architecture uses hierarchical adaptive caching strategy which predicts the consumption of network resources in advance both for edge devices and cloud. This is especially helpful when dealing with large-scale multimedia content delivery networks [1]. Dynamic request routing is achievable in hierarchical caching for content that requires large resources [2]. For instance, multi-tier caching can be used in CDN-based services for resources with high requirements such as video streaming systems. The focus for these kinds of systems is to reduce the metrics such as stall duration tail probability (SDTP) [3].

Content Delivery Network helps identify security issues through automated systems. The TLS or HTTPS methods in the backend systems can be analyzed which verifies in appropriate access through certificate validation and TLS configurations [4]. To tackle the attacks like Distributed Denial of Service Attack (DDOS), there are two factors to be considered. So, CDN collects the information about intensity of the attack and the method to handle the attack [5]. The encryption is used in CDN to hide the contents of user requests taken by the Content Providers (CPs) [6].

3. Problem Statement

Earlier web applications were simple and easy to maintain but the complexity of modern web applications has increased over time. These complex systems have created some challenges not only for the developer but for the network handlers. The content delivery is required to be faster therefore optimized and secure for a better user experience. Factors like latency, bandwidth distribution, and malicious attacks are significant to consider.

Caching is the only possible solution that is presented overtime to tackle these performance resolutions but it has not been fully explored to present a model solution to all problems [7]. The Akamai's CDN caching can be a possible solution but the problem is how to utilize this for both better performance and system security. The presented study considers the security of the system using Akamai's caching while maintaining the efficiency of the system.

4. Akamai's Caching Infrastructure

The Akamai's multi-tiered caching infrastructure can resolve the problem of performance as well as security during content delivery. This multi-tiered infrastructure is based on,

- Akamai's servers are distributed largely across the countries (more than half) which helps to assign the closest server to the users. Thus, caching is improved. A large number of servers approximately 350,000 can be deployed which is present in more than 100 countries in CDN services [8].
- The user requests are dynamically directed to the respective servers considering factors like geolocation, operated network health, and the load distribution of servers within the network.
- The availability of servers is ensured with a distributed approach as the origin server remains free. The popular content is placed even closer for quick access.
- The hierarchical approach is used for the distribution of content to the respected servers either on regional or end servers. This provides large scalability of handling a greater number of applications as well as efficient resource utilization.

5. Performance Impacts

The modern system requires efficiency in their outputs but with improved performance in all measures. A quick response with reliable results is mandatory to distribute the project on a large scale. The following performance factors show the impact of Akamais' CDN caching on web applications to achieve better system performance,

5.1. Scalability

The traffic is controlled effectively during peak times and the large servers are utilized to provide the uninterrupted service to the users. This therefore ensures scalability to large and complex web applications with a greater number of requests. The Akamai's infrastructure handles these large numbers of requests efficiently to ensure scalability in the network.

5.2. Optimized Bandwidth

The effective caching methods used in Akamai's infrastructure help in load reduction by keeping the data closest to the required places. This also helps reduce the resource requirements from the user side as well as provide fast results against the requests. So, even under a high demand period, it becomes easy to provide a smooth experience to users.

5.3. Reliability

The Akamais' architecture ensures that the user is getting appropriate results against the requests made without any interruption. Moreover, large web applications can rely on this infrastructure considering the performance advantages like bandwidth optimization, scalable solutions, and reduced latency as well as the security implications.

5.4. Low Latency

The page loading time of web applications is reduced by more than half most of the time with the use of Akamais' CDN caching. The matrix such as Time To First Byte (TTFB) indicates a clear improvement in the performance. Therefore, the overall latency of the complex systems is reduced with the efficient use of this architecture. User experience is directly connected with the response time and

so this is the most important factor to consider in the network design.

6. Security Aspects

Following are some of the security advantages that are equipped with Akamai's infrastructure as it uses modern methods of CDN caching,

6.1. Attacks Protection

The attacks are defended by Akamai's strong and protected infrastructure keeping the servers available without any interruption. The most famous attack is the Denial of Service or the Distributed Denial of Services attack. These are defended by distributing the traffic across a large network and providing immediate resolutions against attacking methods.

6.2. Bot Management

The Akamai's infrastructure is strong enough to identify the bots and block these malicious activities either with the use of state-of-the-art methods or machine learning algorithms. This however does not make any impact on the users with authentication. This helps to achieve secure web applications with restricted access to unauthorized requests.

6.3. Web Applications Firewalls

The potential malicious security attacks like SQL injections, web scraping, script installation, and other relevant threats are protected with the firewalls built into the CDN architecture with Aakamai's integration at the edge of the network [9]. It ensures a secure experience for users and defense against unwanted activities.

6.4. Data Encryption

The most protective method against the attacks is data encryption which is provided by the Akamai's architecture in the network. The TLS or SSL protocols are installed in the architecture which provides easy transmission of sensitive data between servers and end nodes of users and also to achieve better performance [10]. The man-in-the-middle attacks are therefore prevented with appropriate data encryption.

7. Data Encryption

The security of users is ensured in the app with the use of encrypted data wherever required. It is not limited to the payment section only but security is provided throughout the app from general account security to booking a service. The sensitive information is secured according to the privacy policy provided to users. The data encryption is provided with the help of the following ways that are adapted:

- **Rest Data Encryption:** The data that is stored in the database or servers should be encrypted before it gets stored. The methods like Advanced Encryption Standards (AES) are used to protect data from external attacks.
- **Transfer Data Encryption:** The intercepted malicious attacks while transferring data between end users and servers must be blocked with strong encryption techniques. Encryption protocols like SSL should be used to encrypt data during transmission between systems.
- **User Authentication:** User authentication is closely monitored, along with data encryption, to ensure user security. The Akamai's encryption protocols ensure that users are connected to legitimate servers. The TSL or SSL certificates are tied to these encryption protocols.
- **Encrypted Keys:** The keys should be encrypted and generated securely before storing them. The measures are taken to protect keys from unauthorized external access.
- **Secure Third-Party Integration:** Ensure using third-party securely and encrypted data is used before any transfer. Third-party services can be used while maintaining encryption.
- **Regular Testing:** The software services should be regularly tested and manipulation effort must be restricted on the first attempt. The encryption techniques can be tested periodically and to be validation according to the market requirements.
- **Continuous Encryption Updates:** The loopholes in the network can be identified and the malicious activities can be performed by the attackers. The modern attack methods are challenging to address completely and therefore there is a need for continuous security updates. There is ongoing research on new strategies to stay one step ahead of the attackers as part of the security updates.

8. Future Development

Following are some of the future developments that can be forecasted based on the current ongoing research methodologies in the field,

- Utilizing large machine learning models, it is predicted to achieve proactive caching and next-stage user experience.
- With the evolution of edge computing, processing capabilities can be added to edge servers for personalized experience.
- Quantum computing will open the way to continuous data security by using correct encryption protocols.
- In the future, every request is predicted to be authenticated and verified from either external or internal resources to achieve zero trust architecture.

9. Conclusion

The modern CDN technologies are inspired by the latest infrastructures like Akamai's caching for better performance and security to correctly meet the growing demand in the updated web applications. It provides reduced latency, better scaling, optimized bandwidth, enhanced performance, secure infrastructure, and modern security measures. Performance and security are the two main factors to study.

The presented study therefore reflects the importance of Akamai's infrastructure and the growing importance of

CDN for optimized, reliable, and secure web experiences. The encryption methods in the latest CDN developments provide a secure experience to users. However, the continuous development in the field is exploring more ways to enhance user experience in all domains.

References

[1] J. Ni, D. Tsang, I. Yeung and X. Hei, "Hierarchical content routing in large-scale multimedia content delivery network," in *IEEE International Conference on Communications, 2003. ICC '03*, Anchorage, AK, 20 Jun, 2003.

[2] J. Dai, Z. Hu, B. Li, J. Liu and B. Li, "Collaborative hierarchical caching with dynamic request routing for massive content distribution," in *2012 Proceedings IEEE INFOCOM*, Orlando, FL, 10 May, 2012.

[3] A. O. Al-Abbasi, V. Aggarwal and M.-R. Ra, "Multi-Tier Caching Analysis in CDN-Based Over-the-Top Video Streaming Systems," *IEEE/ACM Transactions on Networking*, vol. 27, no. 2, pp. 835 - 847, 25 Mar, 2019.

[4] B. Shobiri, M. Mannan and A. Youssef, "CDNs' Dark Side: Security Problems in CDN-to-Origin Connections," *Digital Threats: Research and Practice*, vol. 4, no. 1, pp. 1-22, 07 Mar, 2023.

[5] Z. Al-Qudah, B. Al-Duwairi and O. Al-Khaleel, "DDoS protection as a service: hiding behind the giants," *International Journal of Computational Science and Engineering*, vol. 9, no. 4, 28 Apr, 2014.

[6] S. Cui, M. R. Asghar and G. Russello, "nternational Journal of Computational Science and Engineering Vol. 9, No. 4," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 984 - 999, 04 May, 2018.

[7] G. Haßlinger and F. Hartleb, "Content delivery and caching from a network provider's perspective," vol. 55, no. 18, pp. 3991-4006, 29 Dec, 2011.

[8] J. Chen, N. Sharma, T. Khan, S. Liu, B. Chang, A. Akella, S. Shakkottai and R. K. Sitaraman, "Darwin: Flexible Learning-based CDN Caching," *ACM SIGCOMM '23: Proceedings of the ACM SIGCOMM 2023 Conference*, pp. 981-999, 01 Sep, 2023.

[9] M. Jiang, "Developing a platform strategy for Akamai Cloudlet applications," Massachusetts Institute of Technology, 2015.

[10] K. Moriarty, "Encryption," *Transforming Information Security*, pp. 73-100, 02 Jul, 2020.