# بررسی قابلیت اطمینان در شبکه های توزیع محتوا

**آریا فاضلی**

**Aryafazeli6@gmail.com**

**خلاصه**

امروزه پردازش اطلاعات و ارائه خدمات در راستای درخواست های کاربران اینترنت و وب به یکی از چالش های بزرگ مدیران و توسعه دهندگان این بستر جهانی تبدیل شده است. با رشد فناوری رایانش ابری و پردازش اطلاعات تحت وب، مسیر عرضه این خدمات برای مدیران پایگاه های اینترنتی و وبسایت ها هموارتر از گذشته شده است. شبکه های توزیع محتوا تبدیل به زیرساختی پرسرعت با بازدهی بالا شد که متشکل از زنجیره بزرگ سرورها و شبکه های بهینه سازی شده برای پاسخ به درخواست های کاربران وبسایت های مختلف است. این شبکه ها با هدف ارائه خدمات با سرعت بیشتر و کیفیت بالاتر در نقاط مختلف جغرافیایی توزیع شده اند و میتوانند پاسخگوی رقم بالایی از درخواست ها در سرتاسر جهان باشند. قابلیت اطمینان و پایایی این شبکه های در حال توسعه میتواند بسته به شرایطی باشد و فرایند پردازش و پاسخ به کاربران وابسته به این شرایط تغییر کند. مسائل مربوط به جغرافیای شبکه و فواصل، ظرفیت و گنجایش سرور ها، تعادل بار وارد شده و بسیاری از موارد دیگر میتوانند چالش های مربوط به قابلیت اطمینان در شبکه های توزیع محتوا را مورد توجه قرار دهند. این مقاله به بررسی و ارزیابی قابلیت اطمینان در شبکه های توزیع محتوا میپردازد.

کلمات کلیدی : قابلیت اطمینان، توزیع محتوا،شبکه های کامپیوتری، بهینه سازی خدمات

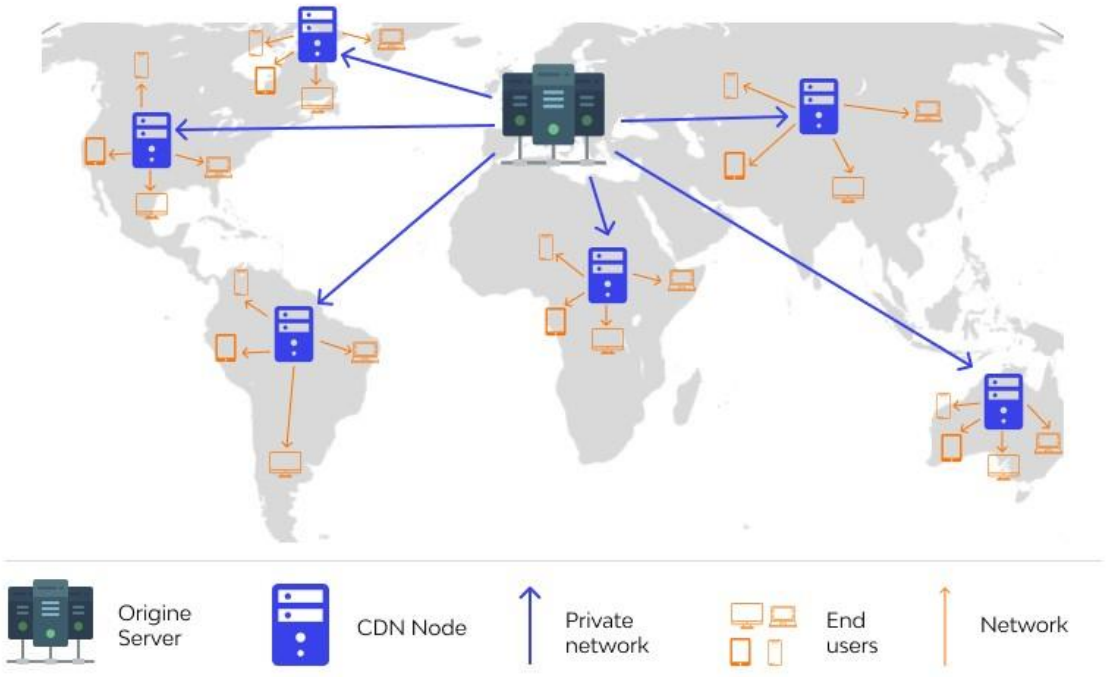
**مقدمه**

شبکه های توزیع محتوا، شبکه های کامپیوتری بزرگ متشکل از سرورهای بهینه سازی شده در سرتاسر نقاط جهان هستند که به واسطه موارد مختلفی گردآوری شده اند. هدف اصلی این زنجیره افزایش سرعت بارگیری سرویس ها و بهبود تجربه کاربران است. این سرورهای میزبان در نقاط مختلف جغرافیایی توزیع شده اند و نسخه های کپی شده از داده های سایت را درون خود ذخیره میکنند. هنگامی که کاربر درخواست اتصال به یک وبسایت مجهز به شبکه توزیع محتوا را دارد، سیستم بطور خودکار به نزدیکترین سرور به کاربر از لحاظ جغرافیایی وظیفه پاسخ را واگذار میکند. فاصله جغرافیایی کم بین سرور میزبان و کاربر وب باعث کم شدن زمان " پینگ " یا تاخیر و در نتیجه افزایش سرعت میشود. علاوه بر سرعت، شبکه های توزیع محتوا به عنوان سپر امنیتی و ماشین های مجازی وبسایت ها نیز عمل میکنند که به جلوگیری از حملات منع سرویس و تخریبگری کاربران سودجو کمک فوق العاده بالایی میکنند.

هنگامی که کاربر پیامی مبنی بر اتصال، بارگیری و هر درخواست دیگری را به شبکه ارسال میکند، آن را به نزدیکترین و البته خلوت ترین سرور موجود در شبکه ارسال میکند و سرور انتخاب شده وظیفه پردازش و در نهایت ایجاد خروجی مناسب را به عهده دارد. این انتخاب بر اساس مواردی مثل ادرس IP کاربر، فاصله جغرافیایی و ظرفیت سرور متغیر است. قابلیت اطمینان خاصیتی از سیستم یا هر عنصری است که بوسیله آن میتوان احتمال انجام وظیفه، تحت شرایط مشخص و از پیش تعریف شده را پیش بینی کرد. به بیان واضح تر، پتانسیل سیستم که به واسطه آن ایجاد اعتماد نسبت به آن سیستم ایجاد میشود، قابلیت اطمینان آن سیستم است. بحث قابلیت اطمینان سیستم نیز مانند هر مبحث دیگری دارای پارامتر ها و مشخصاتی است که با سنجش هرکدام از آن ها میتوان به نتیجه بهتری در مورد قابلیت اطمینان آن سیستم رسید. دسترسی پذیری، مدت زمان دسترسی، گنجایش سرویس ها و موارد این چنینی از جمله ملاک های قابلیت اطمینان هستند. [1]

## معماری شبکه های توزیع محتوا

هدف اصلی سرویس توزیع محتوا، کاهش زمان تاخیر است. با ایجاد فاصله جغرافیایی کم بین سرور میزبان و کاربر، سرعت بارگیری اطلاعات از وبسایت مورد نظر بیشتر میشود. در نتیجه کاربران با ارسال درخواست به وبسایت مورد نظر، از تجربه بهتری برای استفاده از آن سرویس برخوردار میشوند. شبکه های توزیع محتوا متشکل از سه عنصر اصلی هستند: [2]




**شکل 1 – نحوه عملکرد شبکه های توزیع محتوا**

### 1– سرور مبدا (origin server)

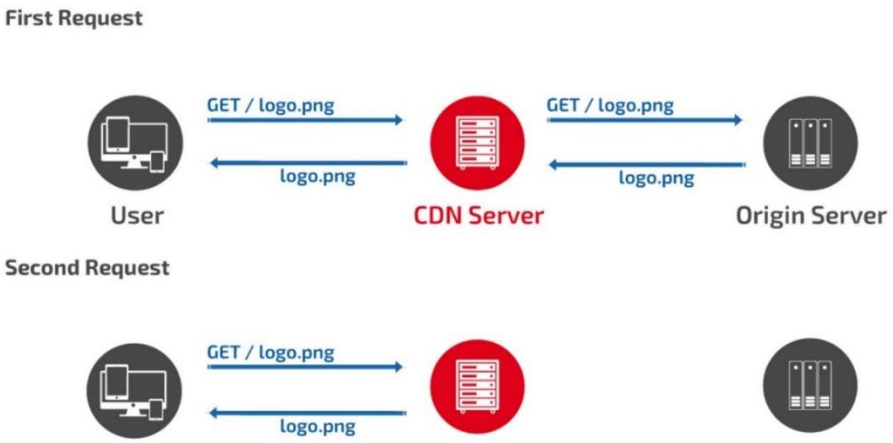
سروری که به عنوان میزبان اصلی وبسایت عمل میکند و تمامی سرور های توزیع شده در سرتاسر جهان که در بستر شبکه توزیع محتوا هستند، اطلاعات را از سرور مبدا یا اصطلاحا سرور اصلی دریافت میکنند و در نهایت تحویل کاربران میدهند. این سرورها وظیفه مدیریت تمامی سرور های دیگر در نقاط مختلف جهان را دارا هستند و به عنوان میزبان اصلی وب یا web host عمل میکنند. پرونده ها و داده های موجود در وبسایت مجهز به شبکه توزیع محتوا ابتدا در این سرورها بطور دائمی ذخیره شده و در ادامه فرایند به سرور های توزیع محتوا یا سرور های لبه ارسال میشوند.

### 2– سرور لبه (edge server)

سرورهای توزیع شده در نقاط مختلف جغرافیایی که وظیفه برقراری ارتباط با کاربر از طرفی و درخواست اطلاعات مد نظر کاربر از سرور مبدا را از طرف دیگر دارند. این سرورها با توجه به مواردی نظیر فاصله جغرافیایی و گنجایش سرور، با کاربر ارتباط برقرار میکنند و در صورتی که حاوی داده های مورد نظر کاربر باشند، آن را به کاربر ارسال میکنند و درغیر این صورت از سرور مبدا ارسال اطلاعات مورد نیاز را درخواست میکنند و آن را در حافظه پنهان خود برای ارائه به کاربران بعدی با درخواست مشابه ذخیره میکنند.

### 3– حافظه پنهان (caching)

وقتی درخواستی از جانب کاربر به سرور وب مبنی بر ارائه داده هایی خاص ارسال میشود، سرور ابتدا با جستجو در حافظه پنهان خود بررسی میکند که اطلاعات ثابت مورد نظر قبلا در این سرور لبه ذخیره شده است یا خیر. در صورتی که اطلاعات در حافظه پنهان موجود نباشد، درخواست را به سرور مبدا میفرستد و اطلاعات دریافت شده را در حافظه خود کپی میکند تا دفعات بعدی بهینه عمل کند. این عمل به افزایش سرعت بارگیری و بهبود تجربه کاربری کمک بسزایی میکند. شکل 2 نحوه عملکرد حافظه پنهان را نشان میدهد. [3]




**شکل 2 – نحوه عملکرد سرور لبه در صورت ذخیره و عدم ذخیره اطلاعات در حافظه پنهان[4]**

## قابلیت اطمینان در شبکه های توزیع محتوا

قابلیت اطمینان به معنای کارایی بالا و پایایی این شبکه ها برای بکارگیری در زیرساخت های وب است. موارد زیادی میتوانند بر قابلیت اطمینان این بستر موثر باشند. این موارد و ملاک های قابلیت اطمینان از جمله پارامتر های دسترسی پذیری و توان پردازش و گنجایش هستند. مهم ترین پارامترهای سنجش قابلیت اطمینان در شبکه های توزیع محتوا به شرح ذیل است.[5]

### 1- زمان به کار (uptime)

زمان به کار یا آپ تایم یکی از معیارهای ثبات و قابلیت اطمینان در سیستم های کامپیوتری است که در زیرساخت های وب و شبکه های کامپیوتری از اهمیت بسیار بالایی برخوردار است. آپ تایم به معنای زمان فعالیت و در دسترس بودن سیستم بدون قطعی و مشکل است. از آنجایی که شبکه های تحویل محتوا میبایست همیشه در دسترس کاربران قرار گیرند، در دسترس بودن سرور های لبه و زمان به کار بالا یکی از ملاک های مهم برای بررسی قابلیت اطمینان در این زنجیره است.

### 2- افزونگی (Redundancy)

ایجاد شبکه های توزیع محتوا یا هرگونه شبکه کامپیوتری، نیازمند تجهیزات متعددی از جمله تعداد زیادی سرور در نقاط مختلف جغرافیایی است. به دلایل مختلف، امکان از دسترس خارج شدن سرورها وجود دارد، دلایلی مانند مشکلات سخت افزاری، تکمیل شدن ظرفیت، نیاز به بروزرسانی و موارد این چنینی میتوانند از جمله مشکلات سرورها باشند. در صورتی که غیرفعال شدن سروری باعث عدم پاسخگویی به یک منطقه جغرافیایی خاص یا تنزل کیفیت در سرویس شود، قابلیت اطمینان در آن شبکه معنایی ندارد. افزونگی به معنای نصب و راه اندازی تجهیزات جایگزین برای این شرایط است. در این حالت سروری جایگزین با همان کارایی و موقعیت، سریعا به جای سرور در دست تعمیر بکارگرفته میشود و از اسیب دیدن شبکه جلوگیری میشود. افزونگی تجهیزات فقط مختص به سرورها نیست و انواع تجهیزات مانند ماژول ها و منابع تغذیه میتوانند در فهرست افزونگی قرار گیرند.[6]

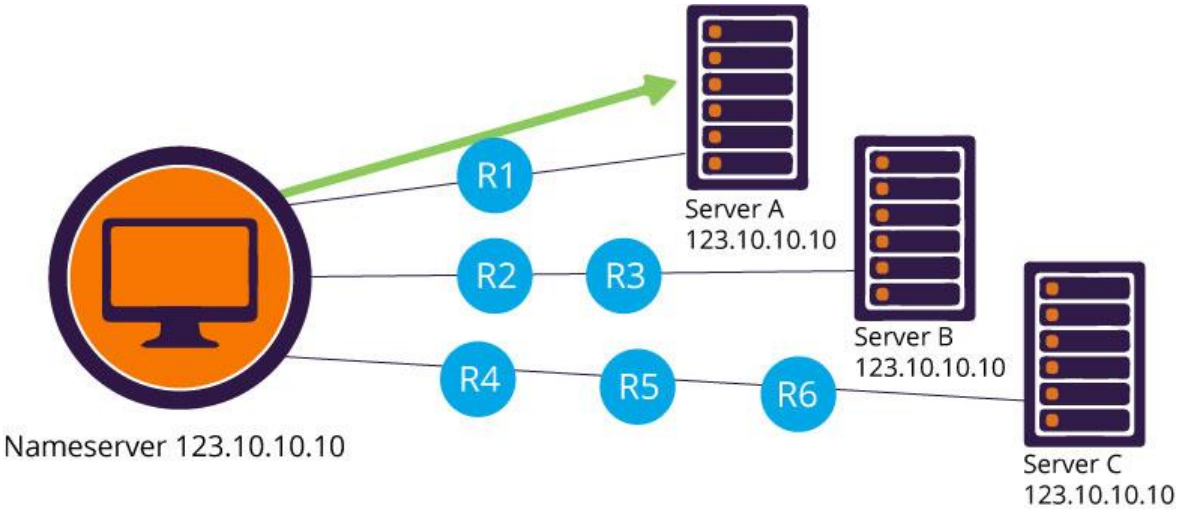
### 3- سرعت بالا و تاخیر پایین

یکی از مهمترین کاربرد های شبکه های توزیع محتوا، بالا بردن سرعت وبسایت ها و کاهش تاخیر بارگیری است. بنابراین سرعت تحویل و پردازش از ملاک های مهم است، زیرا در صورت پایین بودن کارایی و سرعت سرور های لبه، شبکه توزیع میتواند خود به عاملی برای تاخیر و ایجاد پینگ در شبکه تبدیل شود. هرچه حجم داده ها بیشتر باشد، نیاز به زمان انتقال سریع تر نیز بیشتر است. عواملی مانند استفاده از فیبرها و کابل های اترنت در مراکز نصب سرورها، کاهش فاصله جغرافیایی نسبت به مناطق متراکم از لحاظ تقاضا، فشرده سازی و بهینه سازی محتوای تحت وب برای جلوگیری از انتقال

بار بیهوده، استفاده از حافظه پنهان یا caching برای جلوگیری از درخواست های مجدد از سرور مبدا، ایجاد ارتباط بوسیله پروتکل های بروز و پرسرعت مانند HTTP/3، مدیریت بار ترافیک یا و عوامل این چنینی میتواند بر سرعت شبکه تاثیرگذار باشد. [7]

### 4– استفاده از مسیریابی انیکست (anycast)

هرپخشی یا انیکست، یک روش مسیریابی و آدرس دهی در شبکه های کامپیوتری است که روش کار آن، مسیریابی بهترین راه برای اتصال به مقصد است. در شبکه های توزیع محتوا، مسیریابی اصولی میبایست به روش انیکست انجام شود تا کاربر به نزدیک ترین سرور موجود در شبکه منتقل شود. در نگاه کلی، انیکست روشی جهت انتخاب بهترین راه برای اتصال بین چند راه است که هدف شبکه توزیع محتوا را تکمیل میکند. در مسیریابی انیکست، ممکن است سرورهای توزیع محتوا از ادرس IP یکسانی برخوردار باشند اما مسیر بین کاربر و هرکدام از آن سرور ها متفاوت باشد. شکل 3 نشانگر نحوه عملکرد مسیریابی انیکست است.[8]

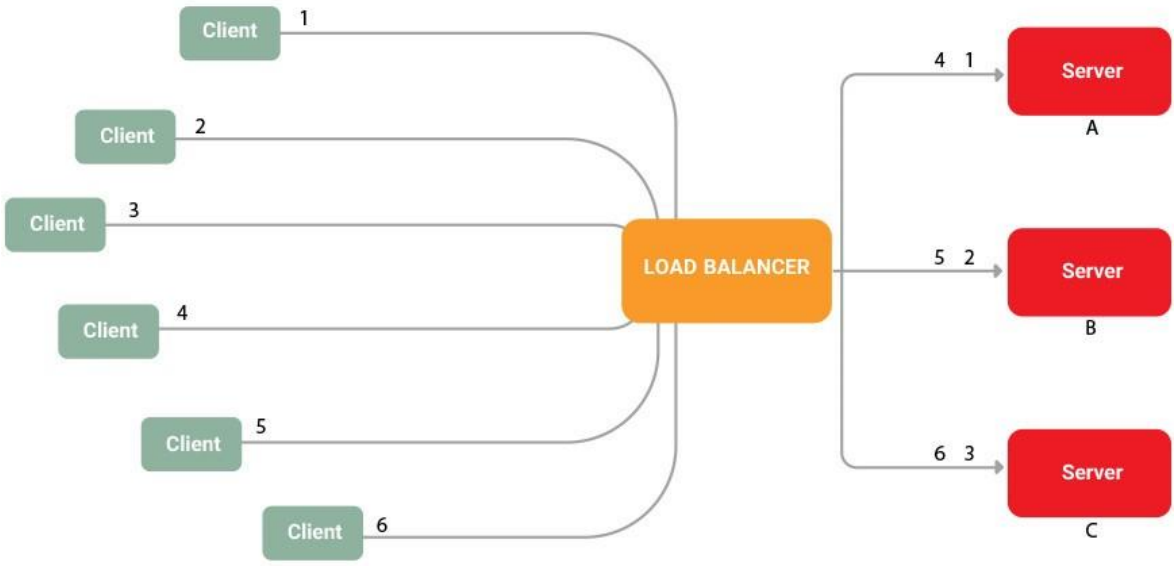



**شکل 3 – در مسیریابی انیکست، کاربر به نزدیک ترین و در دسترس ترین سرور شبکه متصل میشود.**

برای اتصال کاربران به نزدیک ترین سرورهای لبه، انیکست این امکان را میدهد که تعداد زیادی از سرورهای لبه از یک آدرس IP یکسان برخوردار باشند، در این صورت مسیریاب ها سروری که کمترین هاپ ( واسطه های شبکه ای ) را در طی مسیر دارد را برای اتصال انتخاب میکنند. هنگامی که کاربر درخواست اتصال به سرور را دارد، الگوریتم های مسیریابی با محاسبه تعداد واسطه ها و بررسی فاصله، بهترین سرور را برای اتصال انتخاب میکنند.

### 5– متعادل نمودن بار ترافیکی (load balancing)

متعادل نمودن بار ترافیکی یا لود بالانسینگ، به فرایندی برای ایجاد تعادل بار در شبکه گفته میشود که با تقسیم و متعادل کردن بار بین سرورهای شبکه باعث ایجاد ثبات در شبکه و جلوگیری از پر شدن ظرفیت سرورها و در نهایت بازدهی بهتر شبکه میشود. استفاده از الگوریتم های تعادل ترافیک، مزایای امنیتی و بهبود کارایی بالایی را به همراه دارد. هنگامی که کاربران به سرور های وب متصل میشوند، بخشی از گنجایش آن سرور را برای پاسخگویی اشغال میکنند. در صورت نبود ظرفیت کافی برای جواب به کاربران، کارایی سرور پایین خواهد آمد و در نهایت صفر میرسد. استفاده از ابزار های لود بالانسینگ مانند load balancer یا الگوریتم های تعادل ترافیک، میتواند ترافیک اضافه را به سرور های دیگر منتقل کند تا درخواست های تعداد بالا، بصورت همزمان پاسخ داده شوند اما توسط سرور های مختلف. لود بالانسینگ میتواند بار ترافیکی را بین سرور های لبه تقسیم کند تا سرور ها دچار مشکل نشوند.[9] شکل 4 نحوه عملکرد لود بالانسینگ را به نمایش میگذارد.




**شکل 4 – تقسیم کاربران متقاضی در شبکه بین سرورهای میزبان، توسط الگوریتم های لود بالانسینگ انجام میشود**

تقسیم بار بوسیله لود بالانسینگ در شبکه های توزیع محتوا، توسط الگوریتم های لود بالانسینگ داینامیک (dynamic) انجام میشود. لود بالانسینگ داینامیک یا پویا بر خلاف لود بالانسینگ ثابت یا استاتیک (static) که بدون در نظر گرفتن وضعیت و ظرفیت سرورها، درخواست هارا بطور مساوی بین همه سرورها تقسیم میکند، درخواست های وارده را با بررسی وضعیت و گنجایش لحظه ای سرورها تقسیم کرده و با توجه به ظرفیت سرورهای لبه موجود، کاربران را به انها متصل میکند.

### 6– جلوگیری از حملات منع سرویس (DDOS protection)

حمله محروم سازی سرویس یا denial of service attack نوعی از حملات تخریبگرانه بر روی سرور های وب با هدف تکمیل ظرفیت یک سرور به منظور خارج کردن سرور مورد نظر از دسترسی است. عوامل این نوع حملات، تعداد بالایی از پیغام ها و درخواست های متعدد را به قصد ایجاد اختلال در وبسایت قربانی بر روی وب سرور او ارسال میکنند و در صورت تکمیل گنجایش سرور مورد نظر، وبسایت قادر به پاسخگویی به کاربران عادی نیست و مهاجم، کاربران را از وبسایت محروم میکند. این حملات میتواند از نوع درخواست های ICMP یا هرنوع درخواست دیگری باشد. از آنجایی که شبکه های توزیع محتوا باید مجهز به الگوریتم های تعادل بار و لود بالانسینگ باشند، درخواست های مهاجم بین سرور های لبه تقسیم شده و در نهایت علاوه بر سرور مبدا، ظرفیت سرور های لبه هم همچنان توانایی پاسخگویی به کاربران وبسایت را دارد. جلوگیری از حملات منع سرویس یکی از کاربرد های محبوب شبکه توزیع محتوا است و بسیاری از مدیران وب، برای حفظ امنیت وبگاه خود از آن استفاده میکنند.

### نتیجه گیری

در جمع بندی کلی، بهره وری از شبکه های توزیع محتوا میتواند باعث بهینه سازی خدمات و افزایش کیفیت در رابطه کاربری شود. این شبکه ها با پوشش جغرافیایی بالا و قدرت ایجاد ثبات و یکپارچگی در زیرساخت های وب به فناوری مورد نیاز در زیرساخت وبگاه های بزرگ و پربازدید تبدیل شده اند. بررسی و ارزیابی هر یک از پارامتر های قابلیت اطمینان در مبحث شبکه های کامپیوتری از اهمیت بالایی برخوردار است و شبکه های توزیع محتوا نیز از این مسئله مستثنی نیستند. ایجاد اختلال و مشکلات فنی مرتبط با شبکه های توزیع محتوا میتوانند باعث کاهش کیفیت در عرضه خدمات و ارتباطات بین کاربران و وبسایت ها شوند. استفاده از این شبکه ها همواره به منظور یک هدف خاص نیست و مدیران وبسایت ها بسته به خدمات وبسایت خود از شبکه توزیع محتوا استفاده میکنند. اما همواره پارامتر های قابلیت اطمینان در این زنجیره پرقدرت وابسته به یکدیگر هستند و نباید از آنها چشم پوشی کرد.

### مراجع

توسعه ارتباط هوشمند تبیان (1402) ، شبکه توزیع محتوا چیست و چه مزایایی دارد[1]

[2] noormohamadpour . M ; et al (2017) DCCast: Efficient Point to Multipoint Transfers Across Datacenters

[3] NCZOnline. 29 November (2011) How content delivery networks (CDNs) work, from the original on 1 December 2011. Retrieved 22 September 2015.

[4] Evi, Nemeth (2018). "Chapter 19, Web hosting, Content delivery networks". UNIX and Linux system administration handbook (Fifth ed.). Boston: Pearson Education. p. 690

[5] American Society for Quality. 24 July 2024.

[6] R. Jayapal (2003-12-04) , Analog Voting Circuit Is More Flexible Than Its Digital Version

[7] Zhong, Liang; Zheng, Xueqian; Liu, Yong; Wang, Mengting; Cao, Yang (February 2020)

[8] Woodcock, Bill (June 1996) Best Practices in Anycast Routing. https://www.pch.net/resources/Tutorials/anycast/Anycast-v06.pdf

[9] Alakeel, Ali (November 2009). A Guide to Dynamic Load Balancing in Distributed Computer Systems