بسمه‌تعالی

عنوان مستند

امنیت حجیم داده:

بخش ۶ : زیرساخت‌های فیزیکی، تحمل خرابی و حملات

فهرست مطالب

چکیده

در سال‌های اخیر، رشد سریع اینترنت و فراگیر شدن فن‌آوری‌های جدیدی نظیر اینترنت اشیاء، محاسبات ابری و شبکه‌های اجتماعی باعث رشد انفجاری تولید و جمع‌آوری داده‌ها در حوزه‌های مختلف حوزه فن‌آوری اطلاعات شده است. در کنار امکانات جدید سخت‌افزاری و روش‌های کلاسیک علوم داده، دانش یا فن‌آوری جدیدی به نام "حجیم‌داده" پایه‌گذاری شده است که به چالش‌های جدید این حوزه می‌پردازد. اصطلاح حجیم‌داده، یک واژه برای توصیف مجموعه داده‌هایی است که دارای حجم بزرگ، سرعت تولید زیاد و ساختار متنوع و پیچیده نسبت به پایگاه‌داده‌های معمولی هستند. از اینرو، برای ذخیره‌سازی، بازیابی، پردازش، تحلیل و همچنین بصری‌سازی آنها نیازمند ساختارها، الگوریتم‌ها و ابزارهایی متفاوت از گذشته هستیم. با پیشرفت‌های صورت گرفته در این چند سال در حوزه حجیم‌داده، کاربردهای این فن‌آوری روزبه‌روز بیشتر گسترش یافته و میزان داده‌هایی که در بسترهای مبتنی بر حجیم‌داده، ذخیره‌سازی و پردازش می‌شوند افزایش چشم‌گیری داشته است. یکی از چالش‌های اساسی در این زمینه، نحوه تامین امنیت داده در بستر حجیم‌داده است. یک بستر حجیم‌داده کارآمد نباید تنها روی حجم، سرعت یا تنوع داده‌ها تمرکز کند، بلکه با توجه به انبوده داده‌های مهم موجود در آن، باید حفاظت آنرا نیز تضمین نماید. تنوع در ساختار داده‌ها و امکان دسترسی گسترده به آن‌ها توسط کاربران متعدد، موجب شده تا روش‌های سنتی حفاظت در حجیم‌داده کارآمد نباشند و امنیت داده را با چالش-های جدیدی روبرو سازند. از این روی شاهد پیدایش و رشد ابزارها و چارچوب‌های متنوع در بخش‌های مختلف حجیم‌داده در حوزه امنیت هستیم، که مدیران و صاحبان صنایع، کارشناسان حوزه علوم داده و کاربران علاقه‌مند و یا مجبور به رعایت و استفاده از این ابزارها و چارچوب‌ها در راستای حفاظت از داده می‌باشند. در این سلسله مستندات، ما قصد داریم مهمترین چالش‌ها و مباحث را در حوزه امنیت حجیم‌داده تشریح کرده و برای هرکدام از این چالش‌ها، ابزارهای کاربردی را معرفی نماییم. در نهایت، برخی از این ابزارها را که بیشتر مورد استفاده قرار می‌گیرند، مورد بررسی اجمالی قرار خواهیم داد.

در این مستند، موارد امنیتی زیرساخت‌های فیزیکی، مراکز داده، ملزومات و استانداردهای طراحی مراکز داده در سیستم‌های حجیم‌داده و همچنین تحمل خرابی و حملات مهم انجام شده مورد بررسی قرار می‌گیرد.

۱. امنیت زیرساخت‌های فیزیکی

۱-۱ مقدمه

برای ذخیره‌سازی حجیم‌داده به یک زیرساخت ذخیره‌سازی، که به طور خاص برای ذخیره، مدیریت و بازیابی مقادیر گسترده داده‌های بزرگ طراحی شده است، نیاز است. ذخیره‌سازهای حجیم‌داده امکان ذخیره‌سازی و مرتب‌سازی داده‌ها را به گونه‌ای فراهم می‌کنند که به راحتی توسط برنامه‌ها و سرویس‌های کار با حجیم‌داده قابل دسترسی، استفاده و پردازش شوند. همچنین ذخیره‌سازی حجیم‌داده در صورت نیاز، انعطاف‌پذیر است [۱]. ذخیره‌سازهای حجیم‌داده در درجه اول از عملیات ذخیره‌سازی و ورودی / خروجی در ذخیره‌سازی با تعداد بسیار زیاد پرونده ها و اشیاء داده پشتیبانی می کنند.

یک معماری ذخیره‌ساز حجیم‌داده از یک منبع اضافی و مقیاس‌پذیر ذخیره مستقیم متصل (DAS)، یا ذخیره‌سازی متصل به شبکه خوشه‌بندی شده (NAS) یا یک زیرساخت مبتنی بر قالب ذخیره‌سازی شی ساخته شده است. زیرساخت ذخیره‌سازی به گره‌ها یا سرورهای محاسباتی، متصل شده است که پردازش سریع و بازیابی مقادیر زیادی از داده‌ها را قادر می‌سازد. علاوه بر این، بیشتر معماری‌ها و زیرساخت‌های ذخیره‌سازی حجیم‌داده از پشتیبانی بومی برای تحلیلی داده مانند Hadoop، Cassandra و NoSQL برخوردار هستند [۱]. در ادامه روش‌های برقراری امنیت زیرساخت‌های فیزیکی و مراکز داده حجیم‌داده را بررسی می‌کنیم.

۱-۲ امنیت مراکز داده و زیرساخت‌های فیزیکی

یکی از ارکان حجیم‌داده مراکز داده هستند. حداقل مواردی که نیاز است تا مراکز داده بتوانند داده‌ها را به طور امن نگهداری کنند عبارتند از:

الف) کنترل‌های محیطی: کنترل‌های محیطی برای نگهداری از تجهیزات بسیار ضروری هستند، زیرا یک اتاق پر از تجهیزات با قدرت بالا مقدار قابل توجهی حرارت تولید می‌کند. گرمای بیش از حد می‌تواند منجر به خرابی‌های دستگاه و کاهش طول عمر قطعات سرور شود.

ب) منابع برق اضطراری (UPS): در صورت قطع برق، سرورها و سایر تجهیزات باید همچنان در حال اجرا باشند تا اصطلاحا SLA مرکز داده را برآورده سازد. واحدهای UPS و ژنراتورهای پشتیبان می‌توانند سرورها را تا زمانیکه برق مجدداً وصل شود، در حال اجرا نگه دارند.

ج) سیستم‌های امنیتی: برای اطمینان از امنیت و حفظ حریم خصوصی مشتریان، مراکز داده طیف گسترده‌ای از اقدامات امنیتی را برای جلوگیری از دسترسی غیرمجاز به کار می‌گیرند. از جمله اقدامات ایجاد دسترسی بیومتریک، قفسه‌های قفل شده برای سرورها، سیستم‌های

نظارتی و موارد استفاده از mantraps می‌باشد. mantraps یک اتاق کوچک است که یک ناحیه ناایمن را به یک مرکز داده ایمن متصل می‌کند [۲].

۳-۱ اقدامات امنیتی مراکز داده و زیرساخت‌های فیزیکی

اگرچه گردآوری یک لیست کامل از اقدامات لازم برای امنیت مراکز داده کار دشواری است ولی در ادامه رایج‌ترین اقدامات امنیتی که می‌تواند هر مرکز داده‌ای را ایمن کند ارائه شده است.

سیستم‌های نظارتی

یکی از مهم‌ترین فاکتورها در هر برنامه امنیتی نظارت کافی است. برای شروع، دوربین‌هایی که در اطراف محیط مرکز داده نصب شده‌اند برای تماشای فعالیت مشکوک مورد استفاده قرار می‌گیرند. در داخل، نظارت‌های ویدئویی برای ضبط در هنگام وقوع یک حادثه امنیتی عمل می‌کند. ردیاب‌های فلزی اطمینان حاصل می‌کنند که سخت افزاری به طور مخفیانه به مرکز وارد یا از آن خارج نمی‌شود.

محافظان امنیتی

در اکثر مراکز داده، محافظانی در داخل تجهیزات استفاده خواهند شد، اما بعضی از آن‌ها مانند گوگل و اپل دارای محافظانی هستند که به طور مرتب در داخل و خارج آنها گشت می زنند. اگرچه بعید است که یک فرد بخواهد به یک مرکز داده حمله کند، برخی از شرکت‌ها محافظان خود را مجهز می‌کنند تا برای این مسئله آماده باشند.

طراحی ساختمان

مراکز داده به طور معمول براساس عملکرد و امنیت موردنیاز به یکی از دو سبک تک منظوره و چند منظوره عمل می‌کنند. مراکز داده چند منظوره امنیت کمتری دارند، زیرا مراکز داده علاوه بر کارکنانی که در محل حضور دارند کارکنان دیگری نیز دارند. مراکز داده چند منظوره ممکن است دارای دفاتر مجاور برای کسب‌وکار موردنظر باشند و معمولاً برای داده‌ها و زیرساخت‌های حساس مورد استفاده قرار نمی‌گیرند. مراکز داده ایمن به طور سخت گیرانه‌ای به منظور قرار گرفتن زیرساخت‌های IT طراحی شده‌اند. به طور معمول، آن‌ها در مسیر قرار نمی‌گیرند بلکه در منطقه‌ای اطراف سایت نگهداری می‌شوند که شامل موانعی برای جلوگیری از سقوط و گشت‌های امنیتی هستند.

اکثر مراکز داده دارای پنجره بیرونی نیستند و اگر داشته باشند این پنجره‌ها معمولاً از شیشه‌های ضدگلوله ساخته می‌شوند. خروجی‌های آتش به بیرون باز می‌شوند و تعداد محدودی از نقاط ورودی، معمولاً یک ورودی جلویی و یک منطقه بارگیری در مراکز دادها وجود دارد. منطقه داخلی به گونه‌ای طراحی شده است که منطقه مرکز داده را از اتاق‌های دیگر مانند اتاق استراحت، لابی ورودی یا سرویس‌های بهداشتی جدا

می‌کند. هرچه شما به قلب مرکز داده نزدیک می‌شوید امنیت افزایش می‌یابد به گونه‌ای که نیاز به چندین شکل شناسایی یا کنترل دسترسی وجود دارد.

کنترل دسترسی

فقط کارکنان مجاز باید اجازه ورود به مناطق امنیتی یعنی جایی که سرورها، روترها و سایر تجهیزات قرار گرفته‌اند، داشته باشند. برای جلوگیری از عدم‌دسترسی افراد غیرمجاز به اطلاعات و داده‌های مشتری و یا نصب سخت‌افزارهای مخرب، یک مجموعه گسترده از کنترل‌های دسترسی در سراسر یک مرکز داده به کار گرفته می‌شود [۲].

برای مثال گوگل از کارت‌های الکترونیکی که به صورت سفارشی طراحی شده است استفاده می‌کند و هنگامی که شما به طبقه مرکز داده نزدیک می‌شوید، پروتکل‌های مجاز پیچیده‌تر می‌شوند. قلب مرکز داده فقط از طریق یک راهرو امنیتی قابل دسترسی است که از کنترل‌های دسترسی چند منظوره با علامت‌ها و بیومتریک‌های مختلف استفاده می‌کند به گونه‌ای که کمتر از یک درصد از کارکنان گوگل تاکنون به داخل مرکز داده قدم گذاشته‌اند.

Mantrapها اغلب برای محدود کردن دسترسی افراد مجاز و جلوگیری از عقب‌نشینی مجرمان به کار گرفته می‌شود. علاوه بر این، افرادی را که از دسترسی غیرمجاز به یک منطقه امنیتی رسیده‌اند، دنبال می‌کند. هر دو درب یک mantrap نیاز به احراز هویت، مانند استفاده از یک قفل بیومتریک یا کلید کارت دارند و تنها یک درب می‌تواند در یک زمان باز شود. این منطقه تحت نظارت قرار می‌گیرد تا نگهبانان بتوانند هر گونه مسئله‌ای را شناسایی کنند یا افراد را از ادامه دادن اقدام خود باز دارند. سنسورهایی استفاده شده‌اند که به وزن افراد حساس هستند و اگر فردی به نسبت وقتی که وارد شده است سنگین‌تر باشد، نشان دهنده این است که آن‌ها ممکن است در حال خارج کردن سخت‌افزار دزدیده شده باشند. اگر مقیاس این تفاوت را تشخیص دهد، در باز نشده و لازم است یک نیروی امنیتی برای تغییر مکانیزم قفل اقدام کرده و در را برای فرد باز کند.

برای سرورها و تجهیزات حساس، اتاق‌ها و محفظه‌ها یا کابینت‌های جداگانه‌ای به منظور جدا کردن دستگاه‌های حساس از سرورهای غیرحساس استفاده می‌شود. شرکت‌هایی مانند Iron Mountain به مشتریان اجازه می‌دهد در صورت لزوم داخل محفظه‌ها دروبین های CCTV یا نرده‌های حفاظتی و موارد دیگر درخواست کنند.

موارد گفته شده فقط تعداد کمی از اقدامات مختلفی است که توسط مراکز داده به کار می رود. گوگل همچنان به دنبال ساخت سرورهای سفارشی خود و از بین بردن سخت‌افزار یا امکانات غیرضروری برای کاهش سطح حمله است. سایر شرکت‌ها داده ممکن است راه حل‌های مشابه سفارشی را بکار گیرند و سیستم‌های امنیتی یا اقدامات متقابلی را که برای کاهش احتمال خطر به کار می‌گیرند، افشا نکنند [۲].

۱-۴ مروری بر استانداردها

در حال حاضر برای ساخت و بهره برداری از مراکز داده ۲ استاندارد مورد توجه قرار می گیرد: TIA942 **و** ANSI/BICSI 002-201. در ادامه به بررسی این دو استاندارد در موارد مختلف می‌پردازیم [۳].

۱-۴-۱ مساحت و ابعاد

در انتخاب محل مرکز داده باید این نکته مورد توجه قرار بگیرد که محل قرارگرفتن سرورها و رک‌ها و دستگاه‌هایی مثل ژنراتور و تجهیزات برق اظطراری به چه مقدار فضا نیاز دارند زیرا اگر فضا بیش از مقدار نیاز در نظر گرفته شود هزینه‌هایی مثل تجهیزات تهویه و فضاسازی و غیره تحمیل می‌شود و اگر فضا کمتر از حد مورد نیاز باشد متعاقبا هزینه‌های توسعه پیش می‌آید که آن هم اگر غیرممکن نباشد گاهی بالاتر از یک محل جدید خواهد بود [۳].

۱-۴-۲ موقعیت جغرافیایی و محیط

عدم نزدیکی محل مرکز داده به عوامل طبیعی خطر آفرین از جمله رودخانه، معادن، آب‌راه یا خط ساحلی، کانال‌ها، مخازن، سدها، دشت سیلابی و همچنین حداقل ۳ متر ارتفاع از سطح بالای سیل، نکات اولیه انتخاب محل جغرافیایی هستند. توجه به این نکته که محل مورد نظر مثل جزایر ژاپن بسیار زلزله‌خیز است یا نیاز به هزینه کمتری برای پیشگیری از خطرات زلزله دارد، از نکات حائز اهمیت هست. موارد مربوط به مقاومت ساختمان در برابر زلزله با توجه به محل مرکز داده باید به طور کامل رعایت شود. همچنین بررسی سابقه محل مرکز داده در رابطه با ریزش زمین یا نشست خاک قابل توجه است و در صورت نیاز باید خاک محل از این بابت آزمایش شود. بالا بودن بیش از حد دما در مناطق گرم ضمن بالا بردن هزینه‌های تهویه، هزینه نگهداری تجهیزات را بالا برده و عمر تجهیزات را کاهش می‌دهد. همچنین سرمای بیش از حد یا رطوبت بیش از اندازه یا کمتر از مقدار لازم باعث بروز خطا در تجهیزات می‌شوند. رطوبت زیر ۳۰ درصد نیز موجب تخلیه الکترواستاتیکی و رطوبت بالای ۶۰ درصد موجب خرابی مدارهای الکتریکی سرورها می‌شود [۳].

بر اساس استاندارد BICSI، موارد زیر باید برقرار باشد:

- کمترین حد دما ۱۸ درجه
- بالاترین حد دما ۲۷ درجه
- کمترین حد رطوبت ۳۰ درصد
- بالاترین حد رطوبت ۶۰ درصد

۱-۴-۳ فواصل مجاز

فاصله مرکز داده تا فرودگاه:

طبق استاندارد TIA942 فاصله تا فرودگاه کمتر از یک کیلومتر در نظر گرفته شده در حالی که این فاصله در استاندارد BICSI بین ۸ تا ۴۸ کیلومتر در نظر گرفته شده است. در حادثه تلخ سقوط هماپیما در شهرک توحید تهران فاصله تا فرودگاه در حدود ۳ کیلومتر بود.

فاصله تا راه آهن:

استاندارد TIA942 این فاصله را کمتر از یک کیلومتر مشخص کرده ولی در استاندارد BICSI این فاصله ۱.۶ Km مشخص شده با این حال بررسی سوابق موارد خاصی مثل حادثه انفجار قطار باری نیشابور در بهمن ماه ۱۳۸۲ اهمیت این فاصله را بیشتر می‌کند.

فاصله تا مراکز نظامی:

در استاندارد TIA942 این فاصله کمتر از یک کیلومتر تعریف شده و در استاندارد BICSI این فاصله ۱۳ کیلومتر. برای پی‌بردن به اهمیت هر یک از این موارد نمونه‌های بسیاری می‌توان یافت. انفجار سال ۱۳۹۰ یک مرکز نظامی در اطراف کرج یکی از این موارد است.

فاصله تا پمپ‌بنزین:

این فاصله در TIA942 تعریف نشده ولی در BICSI فاصله ۱.۶Km تعریف شده است.

فاصله تا بزرگراه:

در TIA942 این فاصله ۸۰۰ متر و در BICSI فاصله ۱.۶Km است.

فاصله با خطوط فشارقوی:

در TIA942 تعریف نشده ولی در BICSI فاصله ۱.۶Km است.

فاصله تا نیروگاه:

بسته به نوع سوخت نیروگاه متفاوت است. فاصله تا نیروگاه‌های سوخت دیزل یا فسیلی در TIA942 تعریف نشده در BICSI فاصله ۱.۶Km است.

فاصله تا نیروگاه هسته‌ای:

در TIA942 این فاصله ۱.۶ Km و در BICSI فاصله ۸۰Km تعریف شده است. تلخ‌ترین نمونه حوادث نیروگاه‌های هسته‌ای حادثه چرنوویل در

سال ۱۹۸۶ و فوکوشیمای ژاپن در سال ۲۰۱۱ می‌باشند.

طبقه:

محل مرکز داده اگر هم‌سطح زمین نیست، باید آسانسور امکان حمل بار برای حمل تجهیزات سنگین از جمله باطری‌ها یا ژنراتور رت داشته باشد. همچنین، ابعاد درب‌های ورودی محل به اندازه‌ای طراحی شده باشد که تجهیزات امکان ورود به آن را داشته باشند.

۱-۴-۴ نظارت و حراست فیزیکی

شامل موارد مهمی مثل مانیتورینگ محل توسط دوربین‌های مدار بسته و حفاظ‌های ضد سرقت، روش‌های چند لایه تشخیص خودکار و غیر خودکار افراد و تجهیزات مجاز جهت ورود به مرکز داده است. یکی از نکات مهم، روش‌های دسترسی موجود در محل به پهنای باند است. باید امکان اتصال خطوط فیبر نوری یا سایر تجهیزات انتقال اطلاعات با سرعت بالا و مطمئن وجود داشته باشد، مواردی از جمله موانع جغرافیایی برای ارتباطات بدون سیم یا نزدیکی مراکز مخابراتی.

باید توجه کرد بودجه در نظر گرفته شده با کلاس مرکز داده مورد نظر همخوانی داشته باشد. اگر هزینه و بودجه به هم نزدیک نباشند، ممکن است پروژه ای شروع شود که محکوم به نیمه کاره ماندن است.

۱-۵ منابع انسانی

وجود منابع انسانی متخصص در محدوده قابل سکونت، امکان استخدام و حضور پرسنل متخصص یا تردد آسان پرسنل به محل در تمام شرایط جوی و شب و روز یا حتی شرایط اظطراری از نکات بسیار مهم است که باید به آن‌ها توجه شود.

تعیین منابع انرژی الکتریکی

تعیین منابع انرژی الکتریکی اصلی و اضطراری و تخمین توان مورد نیاز، بررسی امکان تامین برق مورد استفاده از نیروگاه‌های اطراف و بررسی امکان قرار دادن ژنراتور در محل، از مواردی است که توجه به آن‌ها بسیار ضروری است.

روش‌های کنترل دما و تهویه

با توجه به موقعیت جغرافیایی و بودجه باید نوع تجهیزات برای تهویه مرکز داده پیش‌بینی شود.

روش‌های تشخیص و سرکوب آتش

تشخیص و اطفا حریق دو مرحله مجزا و مرتبط هستند. میزان و نوع مواد مورد نیاز برای اطفا حریق و محل قرارگیری آن‌ها باید مشخص شود. گازهای مورد استفاده برای تجهیزات سرکوب آتش در دیتاسنتر معمولا هالون ۱۳۰۱ و CO_2 و برخی گازهای دیگر می‌باشد.

فضاها:

در یک مرکز داده فضاها بر اساس استاندارد تقسیم می‌شوند و می‌توانند شامل موارد زیر باشند:

فضای ورودی، فضای عمومی و اداری، اتاق اصلی سرورها، اتاق کنترل و پشتیبانی، داکت‌ها و محل‌های ورودی و خروجی دیتای مخابراتی در صورت وجود نیاز به دکل، پیش‌بینی ارتفاع و محل آن، اتاق باطری و تجهیزات برق اضطراری، محل تجهیزات تهویه بیرونی و داخلی، محل ژنراتور، مخازن سرکوب آتش، مخزن سوخت ژنراتور (با رعایت فاصله مناسب و نکات ایمنی)، محل بارگیری تجهیزات پارکینگ یا محوطه ورودی کامیون‌های حمل کننده تجهیزات

۲. تحمل خرابی

۲-۱ مقدمه

تحمل خرابی به توانایی سیستم برای کار یا کارکرد حتی در صورت شرایط نامساعد (مانند خرابی قطعات) اشاره دارد. در ادامه، ویژگی تحمل خرابی سیستم حجیم‌داده را با جزئیات بیشتر بیان شده است. این بخش توضیح می‌دهد که چگونه تحمل خرابی در حجیم‌داده تحقق می‌یابد [۴].

۲-۲ مشکلات سیستم‌های موروثی

در سیستم‌های سنتی یا اصطلاحا موروثی مانند پایگاه‌داده‌های رابطه‌ای، کلیه عملیات خواندن و نوشتن توسط کاربر، بر روی یک دستگاه واحد انجام می‌شود. اگر هر یک از شرایط نامطلوب مانند خرابی دستگاه، RAM Crash، خاموش شدن برق، خرابی هارد دیسک و... رخ دهد، کاربران باید منتظر بمانند تا مسئله به صورت دستی اصلاح شود. بنابراین در هنگام خرابی یا از کار افتادن دستگاه، کاربر تا زمانی که مشکلات موجود در دستگاه بهبود نیابد، قادر به دسترسی به داده‌های خود نخواهد بود.

همچنین در سیستم‌های موروثی فقط می‌توان داده‌ها را در محدوده گیگابایت ذخیره کرد. بنابراین برای افزایش ظرفیت ذخیره‌سازی داده-ها، باید یک دستگاه سرور جدید تهیه کرد. از این رو برای ذخیره حجم عظیمی از داده‌ها، باید تعداد زیادی ماشین سرور اضافه کرد که این امر باعث افزایش هزینه می‌شود. سیستم فایل توزیع شده هدوپ یا همان HDFS بر این مشکلات غلبه می‌کند [۴]. در ادامه مقدمه‌ای کوتاه در مورد تحمل خرابی‌های HDFS مشاهده می‌شود.

۲-۳ تحمل خرابی در HDFS

تحمل خرابی در HDFS به قدرت کار یک سیستم در شرایط نامساعد و اینکه چگونه این سیستم می‌تواند چنین وضعیتی را اداره کند، اشاره دارد. HDFS نسبت به خرابی بسیار تحمل‌پذیر است. قبل از Hadoop 3، با استفاده از فرآیند ایجاد نسخه کپی، خرابی‌ها را کنترل می‌کرد.

این فرآیند یک نسخه از داده‌های کاربران را در دستگاه‌های مختلف در خوشه HDFS ایجاد می‌کند. بنابراین هر زمان که هر دستگاهی در خوشه از کار بیفتد، داده‌ها از ماشین‌های دیگر که در آن‌ها همان نسخه از داده‌ها ایجاد شده است، در دسترس قرار می‌گیرند.

اگر به طور ناگهانی یک دستگاه از کار بیفتد، HDFS با ایجاد نسخه کپی از داده‌های سایر دستگاه‌های موجود در خوشه، عامل تکثیر را حفظ می‌کند. Hadoop 3 برای ارائه تحمل خرابی، Erasure Coding را معرفی کرد. کدگذاری Erasure در HDFS باعث افزایش راندمان ذخیره-سازی می‌شود در حالی که همان میزان تحمل خرابی و دوام داده‌ها را نسبت به استقرار سنتی HDFS مبتنی بر تکرار، فراهم می‌کند [۴].

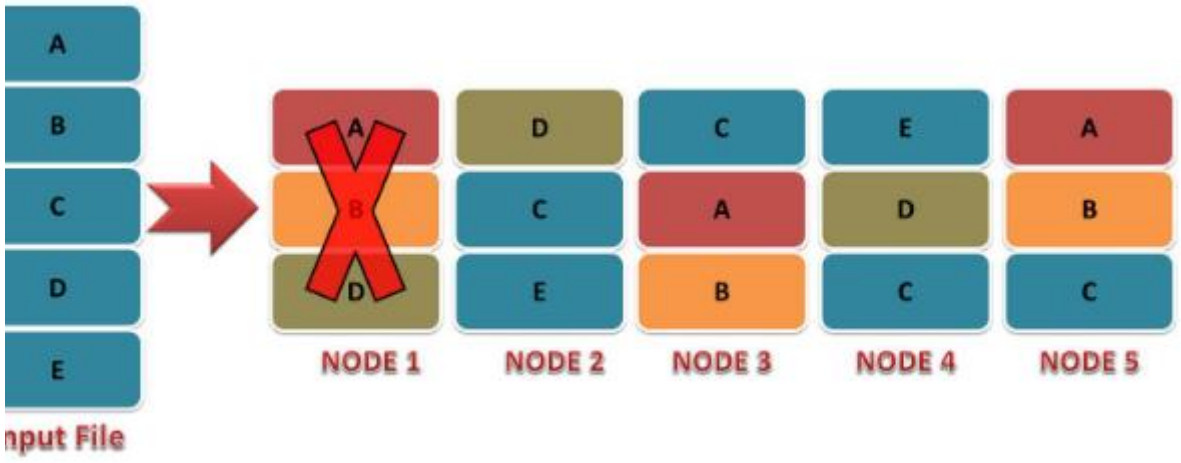
۴-۲ تحمل خرابی در HDFS

قبل از Hadoop 3، سیستم توزیع‌شده Hadoop File از طریق مکانیزم تکثیر به Fault Tolerance دست می‌یافت. Hadoop 3 با Erasure Coding روبرو شد تا تحمل خرابی را با فضای کمتر در اختیار شما قرار دهد. در ادامه هر دو روش برای دستیابی به تحمل خرابی در Hadoop HDFS را مشاهده می‌کنید.

۴-۲-۱ مکانیسم تکثیر

قبل از Hadoop 3، تحمل خرابی در Hadoop HDFS با ایجاد نسخه کپی بدست می‌آمد. HDFS نسخه کپی از بلوک داده را ایجاد می‌کند و آن‌ها را در چندین ماشین (DataNode) ذخیره می‌کند. شکل ۱ نحوه ایجاد نسخه کپی در چند ماشن را نشان می‌دهد. تعداد نسخه‌های ایجاد شده به فاکتور همانندسازی بستگی دارد (به طور پیش فرض ۳).

در صورت عدم‌موفقیت هر یک از دستگاه‌ها، بلوک داده از دستگاه دیگر که دارای همان نسخه از داده‌ها است، قابل دسترس است. از این رو، به دلیل وجود نسخه‌های کپی ذخیره شده در دستگاه‌های مختلف، هیچ‌گونه تلفاتی در داده‌ها وجود ندارد [۴].



شکل ۱. ایجاد چند نسخه از یک داده در ماشین‌های مختلف

۲-۴-۲ Erasure Coding

رمزگذاری Erasure روشی است که برای تحمل خرابی استفاده می‌شود و داده‌ها را با صرفه‌جویی قابل توجهی در فضا نسبت به روش همانندسازی، بطور مدوام ذخیره می‌کند.

RAID (Redundant Array of Independent Disks) از Erasure Coding استفاده می‌کند. Erasure Coding با روش striping فایل‌ها را درون واحدهای کوچک برروی دیسک‌های مختلف ذخیره می‌کند.

برای هر strip از مجموعه داده اصلی، تعداد مشخصی از سلول‌های parity محاسبه و ذخیره می‌شوند. در صورت عدم‌موفقیت هر یک از ماشین‌ها، بلوک را می‌توان از سلول parity بازیابی کرد. Erasure Coding بالای ۵۰٪ فضای ذخیره‌سازی را کاهش می‌دهد [۴].

۳. امنیت غیرفیزیکی حجیم‌داده

به صورت کلی امنیت غیرفیزیکی در سامانه‌های حجیم‌داده از جنبه‌های مختلفی قابل بحث و ملاحظه است، که در قالب دسته‌های زیر بیان می‌شود [۵]:

سامانه توزیع شده: راه‌حل‌های حجیم‌داده، داده‌ها و عملیات را در بسیاری از سامانه‌ها برای پردازش و تجزیه و تحلیل سریع‌تر توزیع می‌کنند. این سامانه‌های توزیع‌شده می‌توانند بار را متعادل کنند و از ایجاد یک نقطه شکست جلوگیری کنند. با این حال، چنین سامانه‌هایی می‌توانند در معرض تهدیدهای امنیتی کاملاً آسیب‌پذیر باشند. نفوذگران برای نفوذ به کل شبکه باید فقط به یک سامانه حمله کنند. از این رو، مجرمان سایبری می‌توانند به راحتی به داده‌های حساس دسترسی پیدا کرده و به سامانه‌های متصل آسیب وارد کنند.

دسترسی داده: سامانه‌های حجیم‌داده برای محدود کردن دسترسی به داده‌های حساس به کنترل دسترسی نیاز دارند. در صورت عدم انجام این کار، هر کاربر می‌تواند به داده‌های محرمانه دسترسی پیدا کند و برخی ممکن است از آنها برای اهداف مخرب استفاده کنند. همچنین، مجرمان سایبری می‌توانند به سامانه‌های متصل به سامانه‌های حجیم‌داده برای سرقت داده‌های حساس دسترسی پیدا کنند. از این رو، شرکت‌هایی که از حجیم‌داده استفاده می‌کنند، باید هویت هر کاربر را بررسی و تأیید کنند. درصورتی که یک شرکت از روش‌های تأیید هویت ناکافی استفاده کند، آنها می‌توانند به کاربران یا نفوذگران غیرمجاز اجازه دسترسی ناخواسته بدهند. چنین دسترسی غیرقانونی می‌تواند داده‌های حساس را به خطر بیاندازد. این داده‌ها می‌توانند به صورت آنلاین فاش شوند یا به اشخاص ثالث فروخته شوند.

داده نادرست: مجرمان سایبری با دست‌کاری داده‌های ذخیره‌شده می‌توانند روی دقت سامانه‌های حجیم‌داده تأثیر بگذارند. بدین منظور، مجرمان سایبری می‌توانند داده‌های نادرستی ایجاد کرده و چنین داده‌هایی را به سامانه‌های حجیم‌داده منتقل کنند. به عنوان مثال، موسسات بهداشت و درمان می‌توانند از سامانه‌های حجیم‌داده برای مطالعه سوابق پزشکی بیماران خود استفاده کنند. نفوذگران می‌توانند برای تولید نتایج نادرست، این داده‌ها را تغییر دهند. چنین نتایج نادرست و ناقص را نمی‌توان به راحتی تشخیص داد و شرکت‌ها ممکن است به استفاده از داده-

های نادرست ادامه دهند. حملات سایبری مانند این‌ها به طور جدی بر جامعیت و تمامیت داده‌ها و عملکرد سامانه‌های حجیم‌داده تأثیر می‌گذارد.

۳-۱ نقض حریم خصوصی

سامانه‌های حجیم‌داده اغلب حاوی داده‌های محرمانه هستند، که مورد توجه بسیاری از افراد است. این گونه تهدیدات بزرگ حریم خصوصی داده‌ها توسط متخصصان در سراسر جهان مورد بحث قرار گرفته است. علاوه بر این، مجرمان سایبری اغلب به سامانه‌های حجیم‌داده حمله می‌کنند تا داده‌های حساس را با نقض داده به خطر بیاندازند. چنین نقض داده‌ها عناوین را ایجاد کرده است و داده‌های حساس میلیون‌ها نفر از مردم دزدیده شده‌اند. این اطلاعات محرمانه همچنین می‌تواند به صورت آنلاین فاش شود. به عنوان مثال، اطلاعات ثبتی و هویتی و سایر اطلاعات محرمانه نزدیک به ۸۰ میلیون نفر اخیراً به صورت آنلاین فاش شدند. این مسائل امنیتی می‌تواند حریم‌خصوصی افراد را تهدید کند.

۳-۲ امنیت نامناسب فضای ابری

داده‌های جمع‌آوری شده توسط سامانه‌های حجیم‌داده معمولاً در سامانه‌های ابری ذخیره می‌شوند. این می‌تواند یک تهدید امنیتی بالقوه باشد. مجرمان سایبری داده‌های ابر بسیاری از شرکت‌های معتبر را نقض کرده‌اند. اگر داده‌های ذخیره شده رمزگذاری نشده باشند و امنیت مناسب داده‌ها در دست نباشد، این موارد ممکن است رخ دهد. بدون اینها نفوذگران به راحتی می‌توانند به داده‌های حساس دسترسی پیدا کنند. شرکت‌ها باید قبل از استفاده داده‌ها، به این مشکلات امنیتی بزرگ داده بپردازند و برای غلبه بر آنها تمرکز کنند. برای رفع چنین موارد امنیتی، شرکت‌ها می‌توانند کلیه داده‌های حساس را رمزگذاری کرده و از سامانه‌های پیشگیری از نفوذ برای شناسایی مزاحمان شبکه استفاده کنند. در کنار اینها، شرکت‌ها می‌توانند از تأیید هویت چند عاملی برای تأیید اعتبار کاربران با داده‌های بیومتریک و همچنین گذرواژه‌ها استفاده کنند. چنین مکانیسم‌های تأیید هویت می‌تواند در محافظت از داده‌های حساس از نفوذگران کمک کند. علاوه بر این، شرکت‌ها همچنین می‌توانند ممیزی امنیتی منظم را برای یافتن آسیب‌پذیری‌ها و نقاط ضعف در رویکرد امنیتی موجود انجام دهند.

۳-۳ دسته‌بندی حملات در سیستم‌های حجیم‌داده و توزیع‌شده:

حملات از نظر تاثیر بر روی سامانه‌های حجیم‌داده به دو دسته زیر تقسیم‌بندی می‌شوند:

۱. **حمله غیرفعال:** یک حمله غیرفعال معمولاً بر ترافیک بدون رمزگذاری نظارت می‌کند و به دنبال رمزهای عبور آسان و اطلاعات حساس است که می‌تواند در انواع دیگر حملات استفاده شود. حملات غیرفعال شامل تحلیل ترافیک، نظارت بر ارتباطات محافظت نشده، رمزگشایی ترافیک رمزگذاری شده ضعیف و گرفتن اطلاعات احراز هویت مانند گذرواژه‌ها است. رهگیری منفعل از عملیات شبکه، متخلفان را قادر می‌سازد عملیات آینده را مشاهده کنند.

۲. **حمله فعال:** در یک حمله فعال، مهاجم تلاش می‌کند تا سیستم‌های امن را دور بزند یا مکانیزم امنیتی و کارکردی آنها را دچار اختلال کرده و باعث ناکارآمدی آنها شود. این کار را می‌توان از طریق خفا، ویروس‌ها، کرم‌ها یا اسب‌های تروجان انجام داد. حملات فعال شامل تلاش برای دور زدن یا شکستن ویژگی‌های محافظت، معرفی کد مخرب و سرقت یا تغییر اطلاعات است. این حملات بر روی ستون فقرات شبکه اجرا می‌شوند، از اطلاعات در هنگام انتقال سوء استفاده می‌کنند، حملات فعال منجر به افشای یا انتشار پرونده‌های داده یا تغییر داده‌ها می‌شود [۶].

۳-۴ حملات از نظر اهداف

حملات از نظر اهداف و مقاصد افراد بر روی سامانه‌های حجیم‌داده به دو دسته زیر تقسیم‌بندی می‌شوند:

۱. حملات تصادفی: حملات تصادفی مواردی است که بدون قصد از پیش تعیین شده رخ می‌دهد. چنین حملاتی در نتیجه نقص سیستم، اشتباهات عملیاتی، اشکالات نرم‌افزاری و اشتباهات کاربر اتفاق می‌افتد. بعضا مشاهده می‌شود افراد سازمان به دلیل نداشتن دانش کافی به طور ناخواسته اقدام به افشای اطلاعات به افراد غیرمجاز می‌شود.

۲. حملات عمدی: حملات عمدی مواردی هستند که با قصد از پیش تعیین شده اتفاق می‌افتند و ممکن است از داده‌های گاه‌به‌گاه و بررسی سیستم با استفاده از ابزارهای نظارتی آسان در دسترس تا حملات پیشرفته با استفاده از دانش سیستم ویژه متغیر باشد [۶].

۳-۵ حمله منع خدمات

یک حمله انکار خدمات توزیع شده (DdoS) تلاش می‌کند تا ظرفیت منابع مورد نظر را مصرف کند تا نتواند خدمات ارائه دهد. یکی از راه‌های طبقه بندی حملات DDoS از نظر نوع منبع مصرفی است. به طور کلی، منبع مصرف‌شده یا یک منبع داخلی در سیستم موردنظر یا ظرفیت انتقال داده در شبکه محلی است که به آن حمله می‌شود. یک مثال ساده از این نوع حملات به منابع داخلی حمله سیل‌آسا است. در ادامه این نوع حملات به طور مفصل‌تر شرح داده می‌شود [۷].

در زیر به ۱۲ نوع از مهم‌ترین حملات انکار خدمات اشاره شده است که از خطرناک‌ترین و مضرترین حملات هستند و دانستن در مورد آنها به تیم‌های امنیتی کمک می‌کند تا با داشتن برنامه‌های مناسب برای دفاع و مقابله با آنها، از خود محافظت نمایند:

۱ – **DNS Amplification**: این حمله یک نوع "انعکاس" حمله است که در آن یک عامل مرتکب شده اقدام به نوشتن پرس‌وجوهایی می‌کند که از آدرس IP تقلبی قربانی مورد نظر استفاده می‌کنند. استفاده از آسیب پذیری‌ها در سرورهای نام دامنه (DNS)، پاسخ‌ها را به بسته‌های UDP بسیار بزرگتر کرده و سرورهای هدف، دچار مشکل می‌شوند.

۲ – **UDP Flood:** در این حمله، مهاجم از بسته‌های IP حاوی دیتاگرام UDP برای قرار دادن پورت‌های تصادفی در یک شبکه هدف استفاده می‌کند. سامانه قربانیان تلاش می‌کند تا هر یک از استراتژی‌های دیتاگرام را با یک برنامه مطابقت دهد، اما نمی‌تواند و دائم تلاش می‌کند که جلوی پاسخ بسته‌ی UDP را بگیرد که این تلاش، بزودی سامانه هدف را خسته کرده و از پا درخواهد آورد.

۳ – **DNS Flood:** شبیه به حمله UDP Flood است، این حمله شامل عواملی است که با استفاده از مقادیر جمعی از بسته‌های UDP برای از بین بردن منابع سرور تلاش می‌کنند. با این حال، در اینجا، هدف این است که سرورهای DNS و مکانیسم‌های حافظه پنهان خود را با هدف جلوگیری از تغییر مسیر درخواست‌های قانونی ورودی به منابع منطقه DNS، فلج نمایند.

۴ – **HTTP Flood:** این حمله به منظور هدف قرار دادن یک برنامه یا وب سرور با استفاده از تعداد زیادی از درخواست HTTP GET یا POST، ظاهرا قانونی انجام می‌گردد. این درخواست‌ها اغلب برای جلوگیری از تشخیص مجرمان با به دست آوردن اطلاعات مفید در مورد هدف، قبل از حمله ساخته شده است.

۵ – **IP Fragmentation Attack:** این حمله از استفاده نمودن MTU جهت سرزیر نمودن سرور هدف است. این حمله را می‌توان با ارسال بسته‌های ICMP و UDP جعلی که بیش از MTU شبکه است به مقصد ارسال نمود تا منابع سرور به سرعت مصرف شوند تا سامانه نتواند بسته‌ها را بازسازی نماید و از دسترس خارج شود. مجرمان همچنین می‌توانند یک حمله Teardrop یا گاز اشک آور را اجرا کنند که با جلوگیری از بازسازی بسته‌های TCP / IP کار می‌کند. این حمله نیز شامل ارسال بسته‌های IP است که با هم تداخل دارند یا بسته‌هایی با سایز بزرگ یا بسته‌هایی با ترتیب نامناسب می‌باشند. این حمله می‌تواند سامانه عامل‌های مختلف را به علت اشکالی که در کد بازسازی مجدد بخش‌های TCP/IP دارند را دچار اشکال کند.

۶ – **NTP Amplification:** دستگاه‌های متصل به اینترنت از پروتکل‌های زمان شبکه (NTP) برای هماهنگ‌سازی ساعت استفاده می‌کنند. همانند حمله متمرکز DNS، در اینجا نیز حمله کنندگان از تعداد زیادی از سرورهای NTP استفاده می‌کنند تا توسط آنها بسته‌های UDP زیادی را به سمت مقصد ارسال کنند تا مقصد از دسترس خارج شود.

۷ – **Ping Flood:** یکی دیگر از حملات سیلاب معمولی که از پخش شدن تعداد زیادی از درخواست‌های ICMP استفاده می‌کند. برای هر پینگ فرستاده شده، باید یک پاسخ متقاطع که حاوی همان تعداد بسته است بازگشت شود، لذا سامانه هدف تلاش می‌کند تا به درخواست‌های بی‌شماری پاسخ دهد، در نهایت پهنای‌باند شبکه خود را مسدود می‌کند. همچنین ping of death که نوع دیگری از این حمله است نیز به ارسال‌هایی از بسته‌های ping با فرمت و شکل نامناسب به سمت قربانی گفته می‌شود که باعث اختلال کارایی سامانه عامل می‌گردد.

۸ – **SNMP Reflection:** پروتکل SNMP به مدیران سامانه کمک می‌کند که اطلاعات مهمی‌را از سرورهای داخل شبکه کسب نموده و یا دستورات ساده‌ای را برای این سرورها ارسال نمایند. در این نوع حمله با استفاده از یک آدرس IP جعلی قربانی، یک حمله کننده می‌تواند

بسیاری از درخواست‌های SNMP را بصورت انفجاری به دستگاه‌ها بفرستد، که در ازای هر درخواست، انتظار می‌رود که به طور صریح پاسخ داده شود. تعداد دستگاه‌های متصل شده می‌تواند به طور مصنوعی بیشتر بشود، به طوری که سرعت و کیفیت شبکه در نهایت توسط مقدار پاسخ‌های SNMP کاهش می‌یابد.

۹ – **SYN Flood**: هر جلسه TCP نیاز به برقراری ارتباط سه جانبه بین دو سامانه دارد. با استفاده از یک سیل SYN، مهاجم به سرعت به هدف با درخواست‌های اتصال بسیاری می‌پردازد که نمی‌تواند آن را حفظ کند و منجر به اشباع شبکه شود. در واقع زمانی اتفاق می‌افتد که میزبانی از بسته‌های سیل آسای TCP/SYN استفاده کند که آدرس فرستنده آنها جعلی است. هر کدام از این بسته‌ها همانند یک درخواست اتصال بوده و باعث می‌شود سرور درگیر اتصالات متعدد نیمه باز بماند و با فرستادن یا برگرداندن بسته‌های TCP/SYN ACK، منتظر بسته‌های پاسخ از آدرس فرستنده بماند ولی چون آدرس فرستنده جعلی است هیچ پاسخی برگردانده نمی‌شود. این اتصالات نیمه باز تعداد اتصالات در دسترس سرور را اشباع می‌کنند و آن را از پاسخ‌گویی به درخواست‌های مجاز تا پایان حمله باز می‌دارد. بنابراین منابع سرور به اتصال‌های‌های نیمه‌باز اختصاص خواهد یافت و امکان پاسخ‌گویی به درخواست‌ها از سرور منع می‌شود.

۱۰ – **Smurf Attack**: این نوع حمله به پیکربندی نامناسب تجهیزات شبکه که اجازه ارسال بسته‌ها به همه کامپیوترهای میزبان روی یک شبکه خاص با آدرس‌های همه پخشی را می‌دهد، متکی است. در چنین حمله‌ای مهاجمان با یک IP جعلی یک تقاضای ping به یک یا چندین سرور همه پخشی ارسال کرده و آدرس IP ماشین هدف (قربانی) را بازنشانی می‌کنند. سرور همه پخشی این تقاضا را برای تمام شبکه ارسال می‌کند. تمام ماشین‌های شبکه پاسخ را به سرور، ارسال همه پخشی می‌کنند. سرور همه پخشی پاسخ‌های دریافتی را به ماشین هدف هدایت یا ارسال می‌کند. بدین صورت زمانی که ماشین حمله‌کننده تقاضایی را به چندین سرور روی شبکه‌های متفاوت همه پخشی می‌نماید، مجموعه پاسخ‌های تمامی‌کامپیوترهای شبکه‌های گوناگون به ماشین هدف ارسال می‌گردند و آن را از کار می‌اندازند. بنابراین پهنای‌باند شبکه به سرعت استفاده می‌شود و از انتقال بسته‌های مجاز به مقصدشان جلوگیری به عمل خواهد آمد. برای مبارزه با حمله منع سرویس در اینترنت سرویس‌هایی مانند Smurf Amplifier Registry توانایی تشخیص پیکربندی‌های نامناسب شبکه وانجام عملیات مناسب مثل فیلترینگ را می-دهند.

۱۱ – **Ping of Death**: یک شیوه است که نفوذگران بسته‌های غیرعادی یا بادکنکی (به وسیله pinging) ارسال می‌کنند تا حافظه سرور سرریز کرده و از سرویس خارج شود. سرریز حافظه زمانی اتفاق می‌افتد که در تلاش برای بازسازی بسته‌های حجیم‌داده باشد. مهاجمان می‌توانند از هر نوعی از IP datagram، از جمله ICMP echo، UDP، IDX و TCP برای حمله استفاده کنند.

۱۲ – **Fork Bomb**: این حمله منع سرویس از داخل یک سرور هدف آغاز می‌شود. در یک محیط مبتنی بر یونیکس، یک Fork، یک کپی از والد خود را برای فرزند فراخوانی می‌کند. هر دو فرآیند می‌توانند وظایف همزمان را در هسته سامانه مستقل از یکدیگر انجام دهند. با استفاده

از یک بمب انفجاری داده، یک حمله کننده مرتکب بسیاری از Forkهای بازگشتی می‌شود که سامانه هدف به طور داخلی غرق شده و از دسترس خارج می‌گردد.

حملات منع خدمات توزیع‌شده بسیار قدرتمند هستند و می‌توانند باعث آسیب مالی و کارکردی زیادی به سازمان‌ها شوند. با این حال، در حالی که اهداف و انگیزه‌های مهاجمین این حملات همیشه ثابت هستند، اما روش‌هایی که استفاده می‌کنند، به طور مداوم در حال پیشرفت هستند. لذا مدیران شبکه‌های حتما باید اطلاعات کامل و جامعی از این نوع از حملات داشته باشند تا بتوانند پیشگیری مناسبی را داشته باشند.

مراجع

[1] https://www.techopedia.com/definition/29473/big-data-storage
[2] http://lavancom.com/portal/magazine/rm-magazine/data-center/1356-2018-07-24-06-41-15
[3] https://www.bicsi.org/docs/default-source/publications/002-2019-preview.pdf
[4] https://data-flair.training/blogs/learn-hadoop-hdfs-fault-tolerance/
[5] “The Big Data Security Gap:Protecting the Hadoop Cluster”,A White Paper, Zettaset Company, California, USA, 2013
[6] I.Shadmanov , K.Shadmanova., Summarization of Various Security Aspects and Attacks in Distributed Systems: AReview , ACSIJ Advances in Computer Science: an International Journal, Vol. 5, Issue 1,No.19,January2016 ISSN : 2322-5157
[7] J.Mirkovic, J.Martin , P.Reiher, A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms