علوم رایانش و فناوری اطلاعات
نشریه علمی انجمن کامپیوتر ایران
مجلد ۱۸، شماره ۱، ۱۳۹۹
صفحات ۵۵- ۴۲
مقاله عادی

ارزیابی اثر خطای انسانی بر اتکاپذیری سامانه‌های ذخیره‌سازی داده

مصطفی کیشانی[۱]، حسین اسدی[۲*]

*نویسنده مسئول، دریافت: ۹۸/۰۸/۰۴، بازنگری: ۹۸/۱۰/۰۱، پذیرش: ۹۹/۰۸/۱۹
[۱] دانش‌آموخته‌ی دکتری، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران
[۲] استاد، دانشکده مهندسی کامپیوتر ، دانشگاه صنعتی شریف، تهران، ایران

چکیده

به‌رغم استفاده از روش‌هایی مانند بازیابی خودکار خرابی، نقش عامل انسانی و متعاقباً خطای انسانی در مراکز داده اجتناب‌ناپذیر است. به این دلیل که مراکز داده از تعداد دیسک بسیار زیادی بهره می‌گیرند، و با توجه به نرخ بالای خرابی دیسک، خطای انسانی در زیرسامانه‌ی دیسک یکی از عوامل اصلی عدم دسترس‌پذیری و فقدان داده است. در این مقاله، اثر جایگزینی دیسک اشتباه را بر دسترس‌پذیری و قابلیت اطمینان سامانه‌های ذخیره‌سازی داده بررسی خواهیم کرد. با این هدف، ابتدا پیامدهای جایگزینی دیسک اشتباه را در آرایه‌ی دیسک بررسی می‌کنیم و سپس با استفاده از شبیه‌سازی‌های مونت‌کارلو عدم دسترس‌پذیری و فقدان داده را ارزیابی می‌کنیم. در چهارچوب پیشنهاد شده الف) پیکربندی‌های مختلف آرایه‌ی دیسک در نظر گرفته می‌شود. ب) معیاری جدید برای عدم دسترس‌پذیری سامانه‌های ذخیره‌سازی داده پیشنهاد می‌شود که مستقل از اندازه‌ی سامانه‌ی مورد آزمایش است و بزرگی عدم دسترس‌پذیری را نیز در خود می‌گنجاند.

کلمات کلیدی: سامانه‌های ذخیره‌سازی داده، دسترس‌پذیری، قابلیت اطمینان، خطای انسانی، آرایه‌ی دیسک، کدهای تشخیص، تصحیح و محوکننده‌ی خطا، تزریق اشکال آماری، شبیه‌سازی مونت‌کارلو.

۱- مقدمه

نیاز فزاینده‌ی امروز به کاربردهای با حجم داده‌ی بالا سامانه‌های ذخیره‌سازی داده[۱] را به عنصری کلیدی در زیرساخت‌های فناوری اطلاعات بدل کرده است. طراحی این سامانه‌ها به‌گونه‌ای است که بتوانند اطلاعات صنایع، سازمان‌ها و شرکت ها را با اتکاپذیری[۲] بالا حفظ کنند. برخلاف کارگزارهای ذخیره‌سازی سنتی، سامانه‌های ذخیره‌سازی داده می‌توانند به چندین درخواست همزمان با حفظ کارایی و اتکاپذیری مورد نیاز کاربردهای تجاری پاسخ دهند.

کارایی و توان عملیاتی بالا و همچنین تأخیر دسترسی پایین سامانه‌های ذخیره‌سازی داده به دلیل استفاده از *حافظه‌ی سراسری*[۳] است. حافظه‌ی سراسری که به‌منظور حفظ داده به پشتیبان باتری مجهز است [۶۲] غالباً از پیمانه‌های[۴] DRAM[۵] ساخته می‌شود و به‌عنوان حافظه‌ی نهان داده‌ی کاربر تأخیر بالای دسترسی به دیسک را تعدیل می‌کند. برای بهبود بهره‌وری حافظه‌ی سراسری، درخواست‌های ارسال شده از سمت کارگزار توسط *منطق پیشین*[۶] دریافت و مدیریت می‌شود. منطق پیشین که از پردازنده‌های با کارایی بالا بهره می‌برد، چندین وظیفه مانند مدیریت حجم، صف‌بندی درخواست‌های خواندن و نوشتن، مدیریت حافظه سراسری و پیش‌واکشی داده را بر عهده دارد. متوسط تأخیر خواندن می‌تواند با پیش واکشی داده از دیسک به حافظه‌ی سراسری با استفاده از *منطق پسین*[۷] بهبود یابد. منطق پسین که وظیفه انتقال داده بین زیرسامانه‌ی دیسک و حافظه‌ی سراسری را بر عهده دارد، عملیاتی همچون زدودن دیسک[۸]، بازیابی خطا و امور مربوط به RAID[۹] را نیز پشتیبانی می‌کند.

یکی از عوامل مهم در خرابی سامانه‌ها *خطای انسانی*[۱۰] است [۱۲][۳۰][۴۹][۳۷][۱۸]. با توجه به هزینه‌ی بالای عدم دسترس‌پذیری (DU[۱۱]) و فقدان داده (DL[۱۲]) و اثرات مخربی که خطای انسانی می‌تواند بر اتکاپذیری سامانه داشته باشد، بررسی اثر خطای انسانی و درجه‌ی آسیب‌های ناشی از آن دارای اهمیت زیادی است. در مراکز داده به‌رغم استفاده از روش‌هایی مانند بازیابی خودکار خرابی، همچنان نقش عامل انسانی در عملیات سرویس و بازیابی پر رنگ است و متعاقباً بروز خطای انسانی اجتناب‌ناپذیر است. در سامانه‌های تجاری غول‌پیکر به دلیل تعداد

بسیار زیاد دیسک‌های مورد استفاده و بالا بودن نرخ خرابی دیسک‌ها عملیات تعمیر و نگهداری با نرخ بسیار زیادی انجام می‌شود. از این رو خطای انسانی در زیر سامانه‌ی دیسک یکی از عوامل مهم عدم دسترس‌پذیری و فقدان داده است، تا جایی که برخی مطالعات میدانی خطای انسانی را عامل اصلی بیش از ۱۹٪ کل خرابی‌های سامانه گزارش می‌کنند [۲۴][۴۹].

در این مقاله اثر خطای انسانی جایگزینی دیسک اشتباه[۱۳] (WDR) را بر فقدان داده و عدم دسترس‌پذیری سامانه‌های ذخیره‌سازی داده بررسی می‌کنیم. برای رسیدن به این هدف ابتدا پیامدهای جایگزینی دیسک اشتباه در آرایه‌ی دیسک تحلیل شده است. پس از آن با شبیه‌سازی مونت‌کارلو[۱۴]، عدم دسترس‌پذیری و فقدان داده در طول مأموریت سامانه ارزیابی شده است. در چهارچوب پیشنهاد شده معیاری جدید برای عدم دسترس‌پذیری سامانه‌های ذخیره‌سازی داده، NOMDU[۱۵]، پیشنهاد می‌شود که مستقل از اندازه‌ی سامانه‌ی مورد آزمایش است و بزرگی عدم دسترس‌پذیری را نیز در خود می‌گنجاند.

پارامترهای مورد استفاده در چهارچوب پیشنهاد شده از داده‌های صنعتی و علمی و داده‌های میدانی یک مرکز با بیش از ۷۰ قفسه[۱۶]ی داده استخراج شده است. نتایج این مطالعه نشان می‌دهد که با چشم‌پوشی از اثر خطای انسانی در مطالعات پیشین، عدم دسترس‌پذیری زیر سامانه‌ی دیسک تا سه درجه بزرگی ناچیز شمرده شده است. همچنین نتایج نشان می‌دهد که با در نظر گرفتن اثر خطای انسانی برتری نسبی پیکربندی‌های RAID آن‌چنان‌که پیش‌ازاین تصور می‌شد نخواهد بود. به‌عنوان‌مثال شرایطی مشاهده شد که پیکربندی RAID1 دسترس‌پذیری کمتری نسب به RAID5 ارائه می‌دهد.

این پژوهش نسبت به [۳۴] نوآوری‌های زیر را داشته است:

- ساختار سامانه‌های ذخیره‌سازی داده به‌دقت مورد بررسی قرار گرفته است.
- مطالعه جامعی بر روی چالش‌های اتکاپذیری سامانه‌های ذخیره‌سازی داده انجام شده است.
- مروری دقیق بر مطالعات پیشین در حوزه خطای انسانی در کاربردهای بحرانی-ایمن و سامانه‌های ذخیره‌سازی داده صورت گرفته است.

این مقاله در پنج بخش تدوین شده است. در بخش دوم و سوم به ترتیب به پیش‌زمینه و کارهای پیشین می‌پردازیم و چالش‌های موجود در سامانه‌های ذخیره سازی داده را مطرح می‌کنیم. بخش چهارم خطای انسانی در آرایه دیسک را مورد تحلیل قرار می‌دهد. در بخش پنجم نتایج شبیه‌سازی‌ها ارائه می‌شود. در آخر در بخش ششم مطالب ارائه شده در این مقاله را جمع‌بندی می‌کنیم.

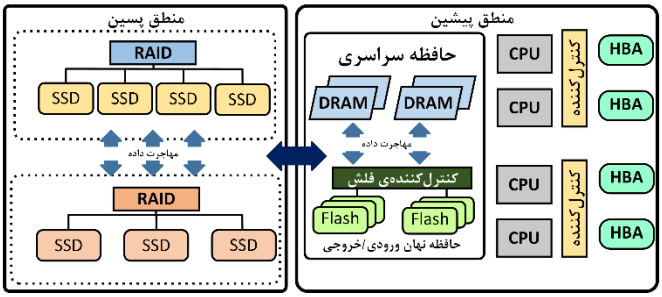
۲- پیش‌زمینه

در این بخش پیش‌زمینه‌ای در مورد ساختار و عملکرد سامانه‌های ذخیره‌سازی داده و چالش‌های اتکاپذیری پیش رو در طراحی سامانه‌ها ارائه می‌شود و در آخر مفاهیم پایه‌ای مانند کدهای محوکننده‌ی خطا و شبیه‌سازی مونت‌کارلو مورد بحث قرار می‌گیرد.

۲-۱- سامانه‌ی ذخیره‌سازی داده

استفاده از سامانه‌های ذخیره‌سازی داده، نیاز زیرساخت‌های فناوری اطلاعات را به عناصر ذخیره‌سازی با کارایی و دسترس‌پذیری بالا پاسخ می‌دهد. این کارایی و دسترس‌پذیری با به‌کارگیری پردازنده‌هایی با کارایی بالا، شبکه‌های پرسرعت و یک حافظه‌ی سراسری حجیم در سامانه، قابل ارائه است. این سامانه‌ها همچنین امکانات ویژه‌ای را همچون الف) نسخه‌برداری آنی[۱۷]: کپی چندین ترابایت داده در زیرسامانه ی دیسک در چند ثانیه؛ ب) آینه‌سازی دوردست[۱۸]: حفظ یک آینه از داده در یک زیرسامانه‌ی دیسک در دوردست به‌منظور محافظت از داده در هنگام خرابی‌های محلی؛ پ) پوشش تعداد واحدهای منطقی[۱۹]: تأمین حفظ و امنیت داده در زمانی که سامانه به‌وسیله‌ی چند کارگزار مورد استفاده قرار می‌گیرد؛ ارائه می‌دهند. ارائه‌ی این امکانات پیشرفته توسط سامانه‌های ذخیره‌سازی داده‌ی نوین، داده‌ی کاربر را نسب به عواملی مانند خرابی‌های محلی، فجایع و حملات ایمن می‌سازد.

اجزای اصلی یک سامانه‌ی ذخیره‌سازی داده می‌تواند بسته به رده‌ی اتکاپذیری، رده‌ی کارایی، و تولید کننده‌ی سامانه متفاوت باشد. اجزای سامانه به‌طور نوعی شامل منطق پیشین، حافظه‌ی سراسری و منطق پسین است (شکل ۱). مسئولیت منطق پیشین ارتباط با کارگزارها و سایر سامانه‌ها و انجام عملیات خواندن، نوشتن و کپی بر روی حافظه‌ی سراسری است. منطق پیشین همچنین وظیفه مدیریت پروتکل‌های ارتباطی (مانند فیبر نوری و اسکازی[۲۰])، نسخه برداری آنی، پیش‌واکشی داده بر اساس تاریخچه‌ی درخواست‌ها، و مدیریت صف خواندن و نوشتن را بر عهده دارد. کنترل‌کننده‌های منطق پیشین و منطق پسین غالباً از پیکربندی *کارکرد دوتایی همزمان*[۲۱] بهره می‌برند. در این پیکربندی هر کنترل‌کننده در حین عملکرد مستقل خود، عملکرد کنترل‌کننده‌ی نظیر خود را نیز زیر نظر دارد. در صورت خرابی یا راه اندازی مجدد یک کنترل‌کننده، کنترل‌کننده‌ی نظیر مسئولیت آن را به عهده می گیرد. بنابراین در این پیکربندی خرابی همزمان هر دو کنترل‌کننده موجب عدم دسترس‌پذیری می‌شود.



شکل ۱: ساختار منطقی یک سامانه‌ی ذخیره‌سازی داده‌ی نوعی

کلیه‌ی ارتباطات میان زیرسامانه‌ی دیسک و منطق پیشین با محوریت حافظه ی سراسری انجام می‌شود. برای غلبه بر تأخیر بسیار زیاد نوشتن بر روی دیسک، همه درخواست‌های *نوشتن* دریافت شده از طرف کارگزار یا سامانه‌ی دیگر بلافاصله پس از کپی داده بر روی حافظه‌ی سراسری پاسخ داده می‌شود. پس از پاسخ به درخواست *نوشتن* و در زمان مقتضی، بلوک‌های داده‌ی در انتظار نوشتن از حافظه سراسری به روی دیسک نوشته خواهد شد. بنابراین پیش از کپی داده‌ی در انتظار نوشتن بر روی زیرسامانه‌ی دیسک، حافظه سراسری تنها دارنده‌ی نسخه‌ی معتبر داده است و خرابی آن موجب فقدان داده می‌شود. در نتیجه در سامانه‌های با اتکاپذیری بالا، محافظت از داده‌ی حافظه سراسری از اهمیت بسیار زیادی برخوردار است. در حافظه‌ی سراسری، داده‌ی در انتظار نوشتن به‌طور معمول بر روی دو حافظه ی آینه‌ای نوشته می‌شود. در صورت خرابی یک آینه، حافظه سراسری همه‌ی داده های در انتظار نوشتن را بی‌درنگ به دیسک‌های پشتیبان انتقال می‌دهد تا احتمال فقدان داده (بر اثر خرابی آینه دوم) به حداقل برسد.

زنجیره‌ی ذخیره‌سازی داده‌ی کاربر با نوشتن داده از حافظه‌ی سراسری به زیرسامانه‌ی دیسک کامل می‌شود. مدیریت انتقال داده از حافظه‌ی سراسری به زیرسامانه‌ی دیسک به عهده‌ی منطق پسین است. منطق پسین همچنین عهده‌دار واکشی (یا پیش‌واکشی) داده از زیرسامانه‌ی دیسک به حافظه‌ی سراسری، اجرای وظایف مربوط به RAID، زدودن دیسک، بازیابی خطا، گرفتن تصویر آنی[۲۲] از داده و مدیریت پروتکل ارتباطی دیسک است.

نهایتاً در زیرسامانه‌ی دیسک داده‌ی کاربر به طور دائمی در رسانه‌های ذخیره سازی داده (مانند دیسک سخت و دیسک حالت جامد) نگهداری می‌شود. بسته به کارایی، اتکاپذیری و هزینه‌ی مطلوب کاربر، زیرسامانه‌ی دیسک از روش‌های متنوعی

از افزونگی مانند انواع پروتکل‌های RAID استفاده می‌کند. پروتکل‌های RAID با توزیع داده میان چندین رسانه‌ی ذخیره‌سازی، کارایی دسترسی به داده را افزایش می‌دهند. این پروتکل‌ها همچنین با نگهداری بیت توازن یا نگهداری آینه‌ای از کل داده در دیسک‌های افزونه، قابلیت اطمینان را افزایش می‌دهند. پروتکل‌های گوناگون RAID سطوح مختلفی از سربار فضای ذخیره‌سازی، کارایی و اتکاپذیری ارائه می‌دهند و انتخاب پروتکل RAID مناسب به کاربر کمک می‌کند که بسته به نیازهای موجود، مصالحه‌ای میان هزینه، اتکاپذیری و کارایی برقرار کند.

شکل ۱ شمایی را از جریان ذخیره‌ی داده در سامانه نشان می‌دهد. درخواست‌ها توسط منطق پیشین دریافت می‌شود و درخواست‌های نوشتن پس از نوشته شدن داده بر روی حافظه‌ی سراسری پاسخ داده می‌شود. بنابراین تأخیر اجرای عملیات نوشتن تنها به اندازه‌ی دسترسی به حافظه DRAM است. درخواست‌های *خواندن* در صورت وجود داده‌ی درخواستی در حافظه‌ی نهان پردازنده‌ی منطق پیشین حتی می‌توانند با تأخیر بسیار کم پاسخ داده شوند. داده‌ی درخواستی درصورتی‌که در حافظه‌ی نهان پردازنده نباشد با تأخیر دسترسی به حافظه‌ی سراسری واکشی می‌شود و در صورت عدم وجود داده در حافظه‌ی سراسری، با دسترسی به دیسک واکشی می‌شود.

۲-۲- شبیه‌سازی مونت‌کارلو

شبیه‌سازی مونت‌کارلو بر نمونه گیری تصادفی پی‌درپی تکیه دارد و در مواقعی که استفاده از سایر روش‌ها، مانند تحلیل‌های ریاضی و جبری، غیر ممکن یا غیر عملی است، بسیار محبوب است. یکی از زیرشاخه‌های شبیه‌سازی مونت‌کارلو، تزریق اشکال آماری[۲۳] است. در تزریق اشکال آماری، از بین N اشکال ممکن، n اشکال به طور تصادفی انتخاب شده، به سامانه تزریق می‌شوند و اثر آن‌ها در عملکرد سامانه ارزیابی می‌شود. یک مسئله‌ی مهم در تزریق اشکال آماری، انتخاب مناسب تعداد نمونه، n، از تعداد کل حالت‌های ممکن، N، است. لواگول[۲۴] و همکارانش [۳۸] **(۱** را برای تعیین n پیشنهاد می‌کنند:

$$n = \frac{N}{1+e^2\times\frac{N-1}{t^2\times p\times(1-p)}} \qquad (۱)$$

در این رابطه N جمعیت اشکال‌ها، p احتمال تبدیل اشکال به خرابی، e حاشیه ی خطا، و t نقطه‌ی برش[۲۵] درجه اطمینان مورد نظر در توزیع نرمال است. با فرض نامتناهی بودن جمعیت اشکال، N، تعداد مناسب نمونه، n، از حد $N \to \infty$ **(۱** به دست می‌آید:

$$n = \frac{t^2\times p\times(1-p)}{e^2} \qquad (۲)$$

در آزمایش‌هایی که در این مقاله انجام شده است، N نامتناهی فرض می‌شود و تعداد مناسب نمونه با در نظر گرفتن حاشیه خطای ۱٪ (e=0.01)، درجه اطمینان ۹۵٪ (t=1.96)، و محافظه‌کارانه‌ترین مقدار برای p (p=0.5) محاسبه می‌شود که نتیجه‌ی آن n=9608 است. در نتیجه در تمامی آزمایش‌ها، برای هر پیکربندی حداقل ۹۶۰۸ عملیات تزریق اشکال انجام شده است.

۳- کارهای پیشین

در این بخش مطالعات انجام شده در حوزه سامانه‌های ذخیره‌سازی داده و چالش های اتکاپذیری پیش رو در طراحی سامانه‌ها مورد بررسی قرار می‌گیرد. مطالعات پیشین در زمینه‌ی اتکاپذیری سامانه‌های ذخیره‌سازی داده به دو دسته‌ی کلی تقسیم می‌شوند. دسته‌ی اول شامل مطالعاتی میدانی است که بر کشف و تحلیل دلایل خرابی سامانه‌ها تمرکز داشته‌اند. این مطالعات عواملی همچون خرابی دیسک، خرابی پردازنده، خطای نرم‌افزار، قطع منبع تغذیه و خطای انسانی را از دلایل خرابی سامانه‌ها برمی‌شمرند. دسته‌ی دوم مطالعاتی هستند که با ارائه‌ی مدل‌های ریاضی و روش‌های مبتنی بر شبیه‌سازی سعی در مدل‌سازی دسترس‌پذیری و قابلیت اطمینان سامانه‌ها دارند.

۳-۱- چالش‌های اتکاپذیری سامانه‌های ذخیره‌سازی داده

دو تهدید جدی برای اتکاپذیری سامانه‌های ذخیره‌سازی داده، فقدان داده (DL) و عدم دسترس‌پذیری است. عدم دسترس‌پذیری به وضعیتی گفته می‌شود که یک درخواست به علت نبود دسترسی به داده‌ی خواسته شده بی‌پاسخ می‌ماند. اما درصورتی‌که بخشی از داده‌ی کاربر به‌طور دائمی از بین برود گفته می‌شود که فقدان داده رخ داده است. از دیگر آسیب‌های محتمل در سامانه‌های ذخیره‌سازی داده آلودگی پنهان داده (SDC) است. در این وضعیت بخشی از داده‌ی کاربر به‌طور غیر قابل تشخیص خراب می‌شود. آلودگی پنهان داده بر اثر عواملی چون رخداد خطای گذرا بر روی اجزای‌های سامانه رخ می‌دهد. فقدان داده، عدم دسترس‌پذیری، و آلودگی پنهان داده می‌تواند عواقبی مانند ازکارافتادگی سامانه تا عواقب جبران ناپذیری مانند ورشکستگی یک شرکت را در پی داشته باشد.

خرابی‌های سامانه‌های ذخیره‌سازی داده می‌تواند ناشی از خرابی محفظه‌ها و دیسک، خرابی اتصالات فیزیکی و زیرساخت‌های مشترک مانند سامانه تهویه هوا و منبع تغذیه، خرابی قرارداد، خطاهای کاربر، خرابی کارایی (عدم توانایی دیسک در انجام درخواست طی زمان مشخص)، و خرابی کنترل‌کننده‌ها باشد.

۳-۲- تحلیل دلایل خرابی سامانه

بخشی از مطالعات میدانی انجام شده بر روی خرابی سامانه‌های ذخیره‌سازی داده بر خرابی دیسک‌های سخت [۳][۱۵][۵۸][۵۶][۵۳][۷۰][۶۶] و [۶۸] دیسک‌های حالت جامد [۶][۲۱][۳۹][۴۳][۵۴][۴][۴۶][۳۱] تمرکز داشته‌اند. خرابی‌های عملیاتی دیسک سخت بر اثر وقوع اشکال در اجزای الکترونیکی یا مکانیکی (مانند صفحه یا دهنه دیسک) اتفاق می‌افتد. این دست از خرابی‌ها موجب تخریب داده یا عدم توانایی دیسک در خواندن داده می‌شود که با به‌کارگیری روش هایی مانند RAID قابل جبران است [۵۲]. علاوه بر خرابی‌های عملیاتی، قرار گرفتن ذرات گردوغبار محیط میان صفحه و دهنه دیسک می‌تواند موجب خطای قطاع شود. این نوع خطا که خطای قطاع نهفته نام دارد می‌تواند به چندین قطاع آسیب بزند و موجب فقدان داده یا خرابی کامل دیسک شود. برای کاهش احتمال آلودگی داده بر اثر خطای قطاع نهفته از روش‌هایی مانند به‌کارگیری کدهای تشخیص و تصحیح خطا، زدودن دیسک، و افزونگی میان دیسکی (مانند RAID) استفاده می‌شود.

برخی مطالعات میدانی بر روی خرابی سامانه‌ها نشان می‌دهد که دیسک‌ها تنها عامل اصلی رخداد DU و DL در سامانه نیستند [۲۷][۴۷][۶۰]. مطالعه انجام شده توسط جیانگ و همکاران بر روی خرابی سامانه‌های ذخیره‌سازی داده، انواع خرابی را به چهار دسته الف) خرابی دیسک، ب) خرابی شبکه میان ارتباطی، پ) خرابی پروتکل و ت) خرابی کارایی تقسیم می‌کند [۲۷]. این مطالعه نشان می‌دهد که علاوه بر خرابی دیسک سایر انواع خرابی نیز تأثیر قابل توجهی بر اتکاپذیری سامانه دارد تا جایی که ۷۵٪ کل زمان ازکارافتادگی سامانه بر اثر عواملی به غیر از خرابی دیسک بوده است. این مطالعه که با تحلیل داده‌های میدانی ۳۹،۰۰۰ سامانه انجام شده است نشان می‌دهد که ۲۰ تا ۲۵ درصد کل خرابی‌ها بر اثر خرابی دیسک، ۲۷ تا ۶۸ درصد خرابی‌ها مرتبط با شبکه میان ارتباطی و ۵ تا ۱۰ درصد خرابی‌ها مرتبط با پشته‌ی پروتکل است.

مطالعات زیادی سعی بر آن داشته‌اند که اتکاپذیری سامانه را با تمرکز بر روش های RAID [۵۶][۶۸][۶۶][۷۰]، گرفتن نقطه وارس ی[۲۶] ، زدودن دیسک [۵۰][۲۵][۴۵][۵۹]، روش‌های آینه‌سازی [۴۰][۴۵]، و فایل‌سیستم [۵۵] بهبود دهند. به‌عنوان‌مثال بایراواسوندارام و همکاران [۲] خرابی‌های ثبت شده‌ی زیرسامانه ی دیسک سامانه‌های ذخیره‌سازی داده (شامل ۱،۵۳ میلیون دیسک) را مورد بررسی

قرار داده‌اند. این مطالعه، مشخصات خطای قطاع نهفته در زیرسامانه‌ی دیسک را به‌دقت مورد بررسی قرار می‌دهد و روش‌های مناسب برای جلوگیری از آلودگی داده را پیشنهاد می‌کند. مطالعه‌ی دیگری توسط لی و همکاران [۴۰] روشی برای بازسازی داده[۲۷] پیشنهاد می‌دهد که از انتشار خطای قطاع نهفته جلوگیری می‌کند. هرچند در حوزه‌ی سامانه‌های ذخیره‌سازی داده، مدل‌سازی اثر خرابی‌های ناشی از خطای نرم بر اتکاپذیری سامانه تاکنون انجام نشده است.

۳-۳- خرابی دیسک سخت

خرابی دیسک که موجب عدم توانایی دیسک در پاسخگویی به درخواست‌های نوشتن یا خواندن می‌شود ناشی از عواملی همچون خرابی قطعات مکانیکی و الکترونیکی است [۱۳][۱۵][۶۹]. مطالعات میدانی نشان می‌دهد که نرخ خرابی دیسک ثابت نیست و از توزیع ویبول[۲۸] پیروی می‌کند [۱۳]. یک خطای محتمل در دیسک، خطای قطاع نهفته[۲۹] (LSE) است. این خطا به طور پنهان در قطاع دیسک اتفاق می‌افتد، منجر به از بین رفتن داده‌ی قطاع می‌شود و تا زمان دسترسی به قطاع قابل تشخیص نیست [۳][۵۸]. در صورت تشخیص این خطا با روش‌هایی مانند زدودن دیسک (خواندن دوره‌ای قطاع‌های دیسک به‌منظور تشخیص خطای قطاع نهفته) می‌توان داده‌ی کاربر را از دیسک‌های سالم آرایه‌ی RAID بازیابی نمود و بدون نیاز به جایگزینی دیسک، داده‌ی قطاع آسیب دیده را به یک قطاع سالم منتقل کرد [۱۵]. مطالعات میدانی الراث[۳۰] و شیندلر[۳۱] [۱۶] نشان می‌دهد که خرابی دیسک و خطای قطاع نهفته‌ی دیسک هر دو به خوبی با توزیع ویبول [۴۸] مطابق رابطه (۳) مدل می‌شوند.

$$f(t) = (\frac{\beta}{\eta})(\frac{t-\gamma}{\eta})^{\beta-1} e^{-(\frac{t-\gamma}{\eta})^{\beta}} \quad (۳)$$

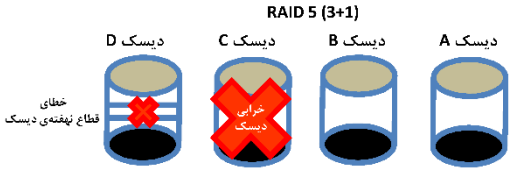
در این رابطه t زمان، η عمر مشخصه۳۲، γ پارامتر موقعیت[۳۳]، و β پارامتر شکل[۳۴] است. جدول ۱ پارامترهای توزیع ویبول خرابی دیسک و خطای قطاع نهفته ی دیسک را برای سه نوع دیسک نشان می‌دهد. این داده‌ها با مطالعه‌ی ۱۰،۰۰۰ سامانه‌ی ذخیره‌سازی داده توسط الراث و شیندلر [۱۶] جمع‌آوری شده است. دیسک‌های A و B با اندازه‌ی یک ترابایت و از نوع SATA[۳۵] رده متوسط هستند و به طور متوسط سه سال در میدان بوده‌اند. دیسک‌های نوع C با اتصال فیبر نوری در رده‌ی بالا جای می‌گیرند، ۲۸۸ گیگابایت ظرفیت دارند و به طور متوسط ۵ سال در میدان بوده‌اند. با توجه به اینکه الراث و شیندلر خرابی دیسک و خطای قطاع نهفته ی دیسک را با توزیع ویبول دو پارامتری توصیف کرده‌اند، در (۳ مقدار γ برابر با صفر خواهد بود.

جدول ۱: پارامترهای توزیع ویبول برای خرابی دیسک، بازیابی دیسک، خطا قطاع نهفته‌ی دیسک و زدودن دیسک [۱۶].

مدل دیسک	خرابی دیسک (d_{DF})		بازیابی (d_{Rec})		خطای قطاع نهفته (d_{LSE})		زدودن دیسک (d_{Scrub})	
	η_{DF}	β_{DF}	η_{Rec}	β_{Rec}	η_{LSE}	β_{LSE}	η_{Scrub}	β_{Scrub}
SATA Disk A	302,016	1.13	22.7	1.65	12,325	1	186	1
SATA Disk B	4,833,522	0.576	20.25	1.15	42,857	1	160	0.97
FC/SCSI Disk C	1,058,364	0.721	6.75	1.4	50,254	1	124	2.1

۳-۳-۱- خطای قطاع نهفته در آرایه‌ی دیسک

در یک آرایه‌ی دیسک، مثلاً RAID5، ترکیب خطای قطاع نهفته‌ی دیسک و خرابی دیسک منجر به فقدان داده می‌شود. **شکل ۲** نشان می‌دهد در ترکیب رخداد LSE و خرابی دیسک، سکتورهایی که آلوده به LSE هستند قابل بازیابی نیستند و در نتیجه در این سکتورها فقدان داده رخ می‌دهد. سناریویی را در نظر بگیرید که دیسک A آلوده به LSE است. درصورتی‌که پیش از تشخیص و بازیابی LSE در دیسک A، دیسک B خراب شود، داده‌ی سکتور آلوده به LSE در دیسک A قابل بازیابی نخواهد بود، چرا که آرایه‌ی RAID5 تنها می‌تواند یک خرابی دیسک را تحمل کند.



شکل ۲: مثالی که نشان می‌دهد در ترکیب رخداد LSE و خرابی دیسک، سکتورهایی که آلوده به LSE هستند قابل بازیابی نیستند.

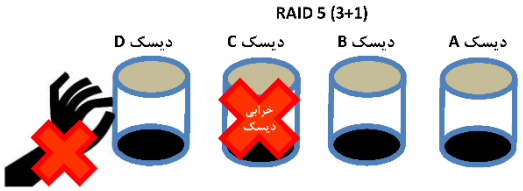
۴-۳- خطای انسانی در سامانه‌های ذخیره‌سازی داده

رخداد خطای انسانی در کاربردهایی که به‌طور کامل خودکار نشده‌اند اجتناب ناپذیر است. در عین حال در بسیاری از کاربردهای بحرانی-ایمن[۳۶] و تجاری در مواقعی که برای تصمیم‌گیری‌های پیچیده به مهارت‌های ذهنی انسان نیاز است خودکار شدن کامل نه تنها ممکن که مطلوب هم نیست. در سامانه‌های کامپیوتری از جمله سامانه‌های ذخیره‌سازی داده، علاوه بر عوامل نرم‌افزاری و سخت‌افزاری، خطای انسانی نیز عاملی برای خرابی است. با وجود همه‌ی تلاش‌های انجام شده برای کاهش نرخ خطای انسانی، رخداد آن در سامانه‌ها و عواقب ناشی از آن غیر قابل اجتناب است. بنابراین از طراحان این انتظار می‌رود که احتمال وقوع خطای انسانی و اثر آن بر اتکاپذیری سامانه را در نظر بگیرند.

به‌عنوان یک مثال از خطای انسانی در سامانه‌های ذخیره‌سازی داده، در زیرسامانه‌ی دیسک رخداد یک خطای انسانی در جایگزینی یک دیسک معیوب می‌تواند منجر به عدم دسترس‌پذیری شود. خطای انسانی همچنین می‌تواند بر روی کنترل‌کننده‌ی ورودی/خروجی، منطق پیشین یا منطق پسین سامانه رخ دهد (که معمولاً در آن‌ها از پیکربندی کارکرد دوتایی همزمان استفاده می‌شود). با خرابی یکی از کنترل‌کننده‌های ورودی/خروجی وظایف کنترل‌کننده‌ی خراب به کنترل‌کننده‌ی نظیر آن محول می‌شود. در این وضعیت عملیات تعمیر یا تعویض مؤلفه‌ی آسیب دیده و پیکربندی مؤلفه‌ی تعمیر یا تعویض شده با اجرای یک فایل دسته‌ای بر عهده ی یک کارشناس فنی است. رخداد هر گونه خطا در فرایند تعمیر/تعویض و پیکربندی می‌تواند موجب عدم موفقیت در فرایند سرویس شود که متعاقباً فقدان داده یا عدم دسترس‌پذیری را در پی خواهد داشت. خطای انسانی همچنین می‌تواند موجب فقدان داده در حافظه‌ی سراسری شود. در صورت خرابی یکی از دو کارت حافظه آینه‌ای، کارت معیوب با یک کارت جدید جایگزین خواهد شد. در این حالت درصورتی‌که سامانه در زمان انجام سرویس در حال کار باشد جایگزینی کارت نادرست (تعویض کارت سالم به جای کارت معیوب) موجب فقدان غیر قابل بازگشت بخشی از داده‌ی کاربر می‌شود.

یکی از اجزای سامانه که احتمال رخداد خطای انسانی در آن بالا است آرایه دیسک می‌باشد. آرایه‌ای با پیکربندی RAID5 و بدون دیسک ذخیره را تصور کنید. در چنین آرایه‌ای درصورتی‌که خرابی دیسک رخ دهد، دیسک خراب باید ابتدا با یک دیسک نو جایگزین شود و پس از آن عملیات بازیابی داده بر روی دیسک جدید آغاز می‌شود. این احتمال وجود دارد که اپراتور به جای جدا کردن دیسک خراب (دیسک B)، یک دیسک سالم (دیسک A) را جدا کند و آن را با دیسک نو جایگزین نماید. این شکل از خطای انسانی، جایگزینی دیسک اشتباه یا WDR نام دارد که بر اثر آن، دو دیسک آرایه از دسترس خارج می‌شود (دیسک خراب B و دیسک سالم A که به اشتباه از آرایه جدا شده است) که در آرایه‌ی RAID5 منجر به عدم دسترس‌پذیری کل آرایه خواهد شد. اگر در گام بعدی خطای انسانی تشخیص داده شود و اپراتور دیسک سالمی که به اشتباه جدا شده بود را به جای اول خود بازگرداند و این بار دیسک خراب را به درستی جدا کند، آرایه‌ی دیسک دوباره در دسترس قرار می‌گیرد.

هرچند، این احتمال وجود دارد که خطای انسانی به موقع تشخیص داده نشود و آرایه‌ی دیسک، پیش از تشخیص خطای انسانی، شروع به بازیابی داده کند که می‌تواند آرایه را به وضعیتی غیر قابل پیش‌بینی، مثلاً فقدان داده ببرد. همچنین این احتمال وجود دارد که پیش از تشخیص خطای انسانی، دیسک جدا شده‌ی سالم آسیب ببیند یا اپراتور، دیسک سالم را (با فرض اینکه خراب است) دور بیندازد که در این صورت، کل داده‌ی آرایه بر اثر خرابی دیسک دوتایی[۳۷] (DDF) از بین خواهد رفت.



شکل ۳: مثالی که نشان می‌دهد چگونه خطای انسان در جایگزینی دیسک خراب می‌تواند کل آرایه را از دسترس خارج کند.

مطالعات زیادی تلاش کرده‌اند تا نقش انسان در پیکربندی و نگهداری سامانه را کاهش دهند [۱۸][۳۷][۲۹][۳۰][۲۴][۴۹]. مطالعه انجام شده توسط اپنهایمر و همکاران [۴۹] علل خرابی در سرویس‌های اینترنت با مقیاس بالا را بررسی کرده است و گزارش می‌کند که خطای اپراتور دست کم عامل ۱۹٪ از کل خرابی سامانه است. این مطالعه در ادامه پیشنهاد می‌کند که خطای انسانی مربوط به اپراتور می تواند با مجهز کردن سامانه به محیط کاربری تصویری کاهش یابد. مطالعات دیگر با پیشنهاد روش‌هایی همچون پشتیبانی معماری برای کاهش تأثیر حوادث [۲۹]، تحلیل بر پایه‌ی مدل ریسک socio-technical [۳۷]، و محاسبات خودمختار[۳۸] [۱۸][۳۰]، سعی در کاهش یا برطرف کردن خطای انسانی داشته‌اند. با وجود همه ی این تلاش‌ها رخداد خطای انسانی در سامانه‌ها و عواقب ناشی از آن غیر قابل اجتناب است [۲۴].

۳-۴-۱- نرخ خطای انسانی در کاربردهای بحرانی-ایمن و تجاری

رخداد خطای انسانی در کاربردهای غیر خودکار اجتناب‌ناپذیر است. در عین حال، در مورد وظایف کلیدی در بسیاری از کاربردهای بحرانی-ایمن و تجاری که نیاز به مهارت‌های شناختی برای تصمیم‌گیری‌های پیچیده دارد، خودکارسازی مطلوب و ممکن نیست. علیرغم وجود روش‌های بسیاری برای کنترل نرخ خطای انسانی، مانند آموزش، استفاده از فهرست، و طراحی Forgiving[۳۹]، وقوع خطای انسانی قابل اجتناب نیست. به‌عنوان‌مثال، بیش از ۷۰٪ سوانح هواپیماهای تجاری بر اثر سقوط هواپیمای تحت کنترل خلبان اتفاق می‌افتد [۸]. از این رو بروز خطا می بایست به‌عنوان بخشی از رفتار طبیعی انسان پذیرفته شود. برای درک بهتر و محاسبه کمی نرخ خطای انسانی در یک سامانه‌ی غیرخوش‌خیم[۴۰]، روش‌های *ارزیابی قابلیت اطمینان انسانی*[۴۱] (HRA) [۶۴] ارائه شده است که تمرکز اصلی آن بر محاسبه کمی *احتمال خطای انسانی*[۴۲] (HEP) می‌باشد. احتمال خطای انسانی به‌سادگی توسط (۴) تعریف می‌شود [۲۰]:

$$HEP = \frac{No.of\ Error\ Cases\ Observed}{No.of\ Opportunities\ for\ Human\ Errors} \quad (۴)$$

برای کاربردهای بحرانی-ایمن و تجاری مقدار HEP به طور عمده بین ۰,۰۰۱ و ۰,۰۱ است (بنابراین، نتایج شبیه‌سازی و مدل‌سازی انجام شده در این بخش از پژوهش با در نظر گرفتن مقدار ۰,۰۱ و ۰,۰۰۱ برای HEP گزارش شده است). به‌عنوان‌مثال مقادیر HEP گزارش شده توسط NASA از این قرار است: $۱,۹\times۱۰^{-۳}$ برای داده‌ی سوییچ پرتاب، $۵,۳\times۱۰^{-۴}$ برای داده‌ی خطای فرمان ISS[۴۳]، و $۱,۰۵\times۱۰^{-۴}$ برای داده‌ی خطای فرمان MER[۴۴] [۷]. مثال‌های دیگری از احتمال خطای انسانی مربوط به خطای قرائت دستورالعمل توسط خلبان می‌باشد که توسط EUROCONTROL گزارش شده است [۲۰]. این نتایج مشابه نتایج گزارش شده توسط ایالات‌متحده و بریتانیا در حوزه‌ی ATM می‌باشد که در جدول ۲ آورده شده است [۲۰]. نتایجی نیز از یک مطالعه‌ی انجام شده توسط NUREG در حوزه‌ی ایمنی راکتور استخراج شده است که خطر حادثه در نیروگاه‌های هسته‌ای ایالات‌متحده را ارزیابی می‌کند [۹][۶۵]. همچنین نتایجی مشابه در [۳۶] گزارش شده است. بخشی از مقادیر HEP گزارش شده توسط NUREG در جدول ۳ آورده شده است.

جدول ۲: احتمال خطای انسانی گزارش شده برای قرائت دستورالعمل توسط خلبان، EUROCONTROL [۲۰]

نوع خطا	En-Route	Tower (Local)	Tower (Ground)	TRACON[۴۵]	Area	ASAS[۴۶] Study
HEP	0.008	0.002	0.004	0.009	0.009	0.005

جدول ۳: احتمال خطای انسانی گزارش شده برای نیروگاه‌های هسته‌ای [۹][۶۵]

فعالیت	احتمال خطای انسانی
احتمال خطای انسانی برای کارهای روزمره‌ی مربوطه	$3\times10^{-3} \sim 1\times10^{-2}$
احتمال غفلت درصورتی‌که آیتم در فرایند گنجانده شده باشد	3×10^{-3}
خطای ساده‌ی ریاضی در هنگام چک کردن	3×10^{-2}
غفلت بازرس از تشخیص خطای اپراتور	10^{-1}
فعالیت‌های همگانی/با استرس بالا/خطرناک	0.2 ~ 0.3
به‌کارگیری نادرست قوانین بازبینی[۴۷]	0.1 ~ 0.9 (0.5 avg.)
احتمال غفلت در صورت استفاده از لیست بازبینی ۱۰ آیتمی	$10^{-4} \sim 5\times10^{-3}$ (1×10^{-3} avg.)
استفاده از سیاست Carry Out Plant/ بدون چک کردن عملکرد اپراتور	$5\times10^{-3} \sim 5\times10^{-2}$ (5×10^{-3} avg.)
انتخاب کنترل نادرست، در زمان استفاده از کنترل‌های مشابه (از نظر ظاهری) و دارای برچسب	$10^{-3} \sim 10^{-2}$ (3×10^{-3} avg.)

۳-۵- مدل‌های اتکاپذیری سامانه

مدل‌های زیادی برای ارزیابی اتکاپذیری سامانه‌های ذخیره‌سازی داده، و البته با تمرکز بر زیرسامانه‌ی دیسک (سخت یا حالت جامد) پیشنهاد شده است که غالباً به تخمین قابلیت اطمینان یا دسترس‌پذیری می‌پردازند. قابلیت اطمینان زیرسامانه‌ی دیسک عبارت است از احتمال اینکه هیچ فقدان داده‌ای در بازه‌ی زمانی ۰ تا t رخ نداده باشد [۱][۲۸]. مقدار این پارامتر به نرخ خرابی دیسک، نرخ تعمیر آن و روش افزونگی به کار گرفته شده در زیرسامانه‌ی دیسک بستگی دارد. در ادبیات سامانه های ذخیره‌سازی داده، علاوه بر قابلیت اطمینان، استفاده از معیارهایی مانند زمان متوسط فقدان داده[۴۸] (MTTDL) [۱۹] ، خرابی دو دیسک[۴۹] (DDF) [۵][۱۴][۱۷]، بزرگی فقدان داده[۵۰] (MDL) [۲۲] و بزرگی نرمال شده‌ی فقدان داده[۵۱] (NOMDL) [۲۲] نیز مرسوم است.

مطالعه‌ای توسط الراث و همکاران انجام شده است که مدل مارکوف قابلیت اطمینان پیکربندی‌های مرسوم RAID را ارائه می‌دهد. این مطالعه همچنین نشان می‌دهد که نرخ خرابی دیسک سخت در طول عمر آن تغییر می‌کند و توزیع خرابی دیسک سخت بیشتر از آنکه به توزیع نمایی نزدیک باشد، به توزیع ویبول نزدیک است [۱۵]. مطالعات دیگری نشان می‌دهد که خرابی‌های رخ داده در یک محفظه‌ی دیسک سخت، مستقل از هم نیستند و بین این خرابی‌ها همبستگی وجود دارد که این همبستگی می‌تواند ناشی از شرایط محیطی و منابع مشترک دیسک‌ها باشد [۳][۲۷]. مطالعه‌ای توسط بایراواسوندارام و همکاران انجام شده است که از وجود محلیت زمانی[۵۲] و محلیت مکانی[۵۳] در خطای قطاع نهفته دیسک خبر می‌دهد [۳].

با توجه به تغییر نرخ خرابی دیسک سخت در طول عمر آن و از آنجا که مدل های مارکوف تنها با فرض نرخ ثابت خرابی (با توزیع نمایی) معتبر هستند، عده‌ای

از پژوهشگران روش مبتنی بر شبیه‌سازی را به جای مدل مارکوف پیشنهاد می‌کنند. الراث و همکاران با ارائه یک روش مبتنی بر شبیه‌سازی مونت کارلو و با در نظر گرفتن خطای قطاع نهفته‌ی دیسک، قابلیت اطمینان آرایه RAID5 را با فرض پیروی خرابی دیسک از توزیع ویبول تخمین می‌زنند [۱۴]. مدل مشابهی مبتنی بر شبیه سازی ارائه شده است که اثر خطای قطاع نهفته و زدودن دیسک را با هم در نظر می گیرد [۱۵].

مطالعه‌ی انجام شده توسط گرینان و همکاران [۲۲]، نقایص معیارهای مرسوم برای محاسبه قابلیت اطمینان (مانند MTTDL) را برمی‌شمارد. این مطالعه معیار جدیدی با عنوان بزرگی فقدان داده (MDL) را پیشنهاد می‌کند که بیانگر مقدار داده‌ی از بین رفته در هر رخداد فقدان داده است.

۴- تحلیل خطای انسانی در آرایه دیسک

در این بخش، اتکاپذیری آرایه دیسک را با استفاده از شبیه‌سازی مونت‌کارلو ارزیابی می‌کنیم. استفاده از شبیه‌سازی مونت‌کارلو دو مزیت نسب به مدل‌های مارکوف[۵۴] و تحلیل MTTDL دارد. اولین مزیت شبیه‌سازی مونت‌کارلو این است که می‌تواند بی‌نهایت وضعیت خرابی موجود (بی نهایت ترکیب ممکن خرابی سکتور، خرابی دیسک و خطای انسانی) را مدل کند و مزیت دوم این است که می‌تواند نرخ خرابی متغیر با زمان در دیسک را نیز مدل کند. در این بخش ابتدا معیاری جدید، NOMDU، را معرفی خواهیم کرد که برای ارزیابی دسترس‌پذیری سامانه‌های ذخیره سازی داده پیشنهاد می‌شود. سپس چهارچوبی برای ارزیابی اتکاپذیری آرایه‌های RAID با در نظر گرفتن خرابی دیسک، LSE و خطای انسانی پیشنهاد می‌کنیم.

مدل سامانه

جدول ۴ نمادها و پارامترهای مورد استفاده در مدل و توضیحات مربوط به هر یک را نشان می‌دهد.

جدول ۴: نمادها و پارامترهای مورد استفاده در مدل و توضیحات مربوط به هر یک

نماد	توضیحات
LSUD	اندازه منطقی داده خارج از دسترس[۵۵]
UD	مدت زمان عدم دسترس پذیری[۵۶]
TLSS	کل فضای ذخیره سازی منطقی[۵۷]
MT	مدت زمان مأموریت[۵۸]
LSLD	اندازه منطقی فقدان داده[۵۹]
RT	زمان بازیابی[۶۰]

۴-۱- بزرگی نرمال شده‌ی عدم دسترس‌پذیری (NOMDU)

برای محاسبه‌ی عدم دسترس‌پذیری در یک سامانه‌ی ذخیره‌سازی داده به معیاری نیاز است که در سامانه‌های مختلف (با حجم‌ها و معماری‌های گوناگون) قابل محاسبه و قابل مقایسه باشد. معیار سنتی دسترس‌پذیری به دو دلیل برای سامانه‌های ذخیره‌سازی داده مناسب نیست:

الف) دسترس‌پذیری تابعی از حجم سامانه است و زمانی که دو سامانه با معماری دقیقاً یکسان ولی حجم نابرابر با هم مقایسه می‌شوند، سامانه‌ی با حجم بالاتر دسترس‌پذیری کمتری خواهد داشت. بنابراین، معماری سامانه‌هایی با حجم‌های مختلف نمی‌تواند با این معیار مقایسه شود.

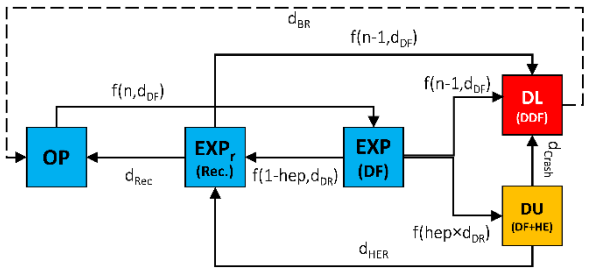
ب) دسترس‌پذیری معیاری است که نمی‌تواند بزرگی داده‌ی خارج از دسترس را نشان دهد. در بسیاری از رخدادهای خرابی، تنها بخشی از داده از دسترس خارج می‌شود، درحالی‌که دسترس‌پذیری سنتی میان عدم دسترس‌پذیری یک بایت داده و عدم دسترس‌پذیری کل داده تفاوتی قائل نیست.

در اینجا معیار NOMDU را پیشنهاد می‌کنیم که مدت زمان عدم دسترس پذیری را در حجم منطقی داده‌ی خارج از دسترس ضرب می‌کند و حاصل را به کل زمان مأموریت و حجم منطقی سامانه نرمال می‌کند (۵). این معیار می‌تواند دسترس پذیری سامانه را مستقل از اندازه و زمان مأموریت آن، گزارش کند.

$$NOMDU = \frac{\sum LSUD \times UD}{TLSS \times MT} \quad (۵)$$

۴-۲- تحلیل RAID5

شکل ۴ نمودار حالت شبیه‌سازی مونت‌کارلو را برای پیکربندی RAID5 با در نظر گرفتن خرابی دیسک و خطای انسانی نشان می‌دهد. در تمامی نمودارهای حالت، برای نام‌گذاری حالت‌ها از قرارداد یکسانی استفاده کرده‌ایم. حالت‌هایی که در آن عدم دسترس‌پذیری رخ داده است با DU و حالت‌هایی که در آن فقدان داده رخ داده است با DL نام‌گذاری شده‌اند. در حالت‌هایی که با EXP[۶۱] نام‌گذاری شده‌اند، با رخداد خرابی بعدی، سامانه به وضعیت DU یا DL می‌رود. در حالت‌هایی که OP[۶۲] نام‌گذاری شده‌اند، رخداد خرابی بعدی منجر به DU/DL نمی‌شود. همچنین فرض می‌کنیم که در ابتدای مأموریت آرایه در وضعیت عملیاتی (OP) قرار دارد.



n: تعداد دیسک
hep: احتمال خطای انسانی
d_{DF}: توزیع زمانی خرابی دیسک
d_{Rec}: توزیع زمانی بازیابی خرابی
d_{HER}: توزیع زمانی بازیابی خطای انسانی
d_{DR}: توزیع زمانی جایگزینی دیسک خراب
d_{BR}: توزیع زمانی بازیابی خرابی با استفاده از پشتیبان
d_{Crash}: توزیع زمان سقوط دیسک پس از خطای انسانی

شکل ۴: نمودار حالت شبیه‌سازی مونت‌کارلو برای پیکربندی RAID5، با در نظر گرفتن خرابی دیسک و خطای انسانی

با رخداد اولین خرابی دیسک، وضعیت آرایه از ***عملیاتی*** (OP) به در معرض *خرابی* یا وضعیت ***هشدار*** (EXP) تغییر می‌کند. در وضعیت هشدار، رخداد دومین خرابی دیسک منجر به DL می‌شود، درحالی‌که وقوع خطای انسانی در جایگزین کردن دیسک خراب منجر به DU می‌شود. در وضعیت هشدار، اگر اپراتور به درستی دیسک خراب را با دیسک نو جایگزین کند، آرایه به وضعیت EXP_r می‌رود که در آن بازیابی داده بر روی دیسک نو آغاز می‌شود. در وضعیت DU، اگر خطای انسانی تشخیص داده شده و برطرف شود، آرایه به وضعیت EXP_r می‌رود که در آن بازیابی داده بر روی دیسک نو آغاز می‌شود. هرچند، اگر دیسک سالمی که به اشتباه از آرایه جدا شده به هر دلیلی آسیب ببیند، DDF رخ می‌دهد و آرایه به وضعیت DL می رود. در اینجا فرض می‌کنیم توزیع زمان آسیب دیدن دیسکی که به اشتباه جدا شده است، *زمان سقوط*، d_{crash} است.

۴-۳- محاسبه‌ی NOMDU در رخداد عدم دسترس‌پذیری

در هر رخداد DU (رخداد i ام)، مقدار NOMDU مطابق (۶ محاسبه شده و به آمار شبیه‌سازی اضافه می‌شود.

$$NOMDU_i = \frac{LSUD_i \times UD_i}{TLSS \times MT} \quad (۶)$$

در نتیجه رابطه (۵) به صورت رابطه (۷) بازنویسی می‌شود:

$$NOMDU = \sum_i NOMDU_i \quad (۷)$$

محاسبه‌ی NOMDL در رخداد فقدان داده در آرایه‌های بی‌پشتیبان

زمانی که آرایه در وضعیت DL قرار دارد کل داده بر اثر DDF از بین رفته است. در آرایه‌های *بی‌پشتیبان*[۶۳]، آرایه‌هایی که هیچ نسخه‌ی پشتیبان یا آینه‌ای از داده ندارند، در وضعیت DL، داده‌ی کاربر به طور دائمی و غیر قابل بازگشت از بین رفته است. بنابراین، بزرگی نرمال شده‌ی فقدان داده[۶۴] (NOMDL) [۲۲] با (۸ محاسبه شده و به آمار شبیه‌سازی اضافه می‌شود.

$$NOMDL_{nonsurvivable_i} = \frac{LSLD_i}{TLSS} \qquad (۸)$$

مقدار NOMDL کل مأموریت آرایه از مجموع NOMDL ناشی از رخدادهای فقدان داده، به دست می‌آید:

$$NOMDL = \sum_i NOMDL_i \qquad (۹)$$

محاسبه‌ی NOMDU در رخداد فقدان داده در آرایه‌های باپشتیبان

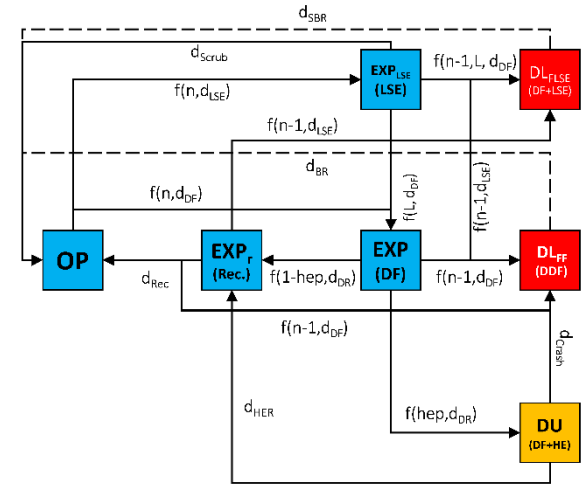
درصورتی‌که DL در آرایه‌ای *باپشتیبان*[۶۵]، آرایه‌ای که حداقل یک نسخه‌ی پشتیبان یا آینه‌ی معتبر از داده‌ی آن وجود دارد، رخ دهد، داده‌ی آرایه می‌تواند از نسخه‌ی پشتیبان بازیابی شود. در این حالت، به اندازه‌ی *زمان بازیابی پشتیبان*، d_{BR}، زمان لازم است تا داده‌ی آرایه از نسخه‌ی پشتیبان بازیابی شود. زمان بازیابی پشتیبان به پارامترهایی مانند اندازه‌ی داده‌ی از بین رفته، گذردهی پشتیبان، گذردهی آرایه، و پهنای باند شبکه بستگی دارد. از دید کاربر نهایی، داده‌ی باپشتیبان از بین نرفته است ولی در طول مدت بازیابی، خارج از دسترس می‌باشد. بنابراین، NOMDUی تحمیل شده توسط فقدان داده‌ی باپشتیبان، از رابطه (۱۰) محاسبه می‌شود:

$$NOMDU_{survivable\_DL_i} = \frac{LSLD_i \times RT_i}{TLSS \times MT} \qquad (۱۰)$$

۴-۴- اتکاپذیری با در نظر گرفتن LSE

در این بخش، نمودار حالت شکل ۴ را توسعه داده‌ایم تا اثر LSE را نیز در کنار خرابی دیسک و خطای انسانی در آرایه‌ی RAID5 در نظر بگیریم. در این آرایه اگر پس از خرابی دیسک، خطای انسانی در جایگزین کردن دیسک رخ دهد، آرایه به وضعیت DU می‌رود. همچنین با رخداد دو خرابی دیسک پشت سر هم آرایه به وضعیت DL_{FF} می‌رود و با ترکیب LSE و خرابی دیسک (در دو دیسک مختلف)، وضعیت DL_{FLSE} پدید می‌آید.

در وضعیت OP تمام دیسک‌ها عملیاتی هستند و هیچ LSE رخ نداده است. با اولین رخداد خرابی دیسک، آرایه به وضعیت EXP می‌رود. درصورتی‌که یک (یا بیشتر) LSE رخ دهد نیز آرایه به وضعیت EXP_{LSE} خواهد رفت. LSE می‌تواند با عملیات زدودن دیسک برطرف شود ولی توزیع زمانی زدودن دیسک، d_{scrub}، به سیاست‌های نگهداری سامانه بستگی دارد (چرا که این عملیات به شدت کارایی را تحت تأثیر خود قرار می‌دهد). حداقل زمان زدودن دیسک نیز تابعی از گذردهی آرایه است. اگر پیش از عملیات زدودن دیسک یک خرابی دیسک رخ دهد، داده‌ی تمام سکتورهایی که آلوده به LSE بوده‌اند غیر قابل بازیابی خواهد بود (DL_{FLSE}). الراث و پچت[۶۶] [۱۵] این ترکیب خرابی را به‌عنوان DDF در نظر می‌گیرند، درحالی‌که بزرگی فقدان داده (و متعاقباً زمان مورد نیاز برای بازیابی داده در آرایه های باپشتیبان) با DDF بسیار متفاوت است که این امر موجب بزرگ انگاری[۶۷] DU و DL می‌شود. سکتورهای باپشتیبان می‌توانند با استفاده از نسخه‌ی پشتیبان بازیابی شوند که توزیع زمان این بازیابی، d_{SBR}، تابعی از تعداد سکتورهای مفقود، گذردهی پشتیبان، گذردهی آرایه، و سرعت شبکه[۶۸] است.



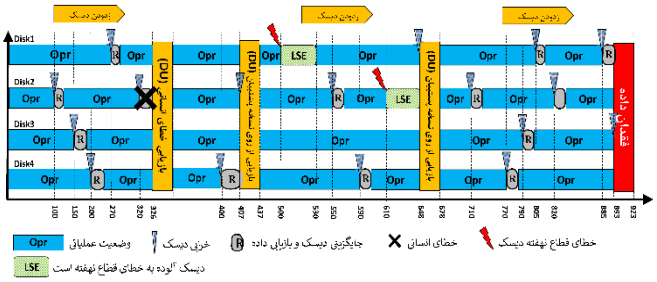
شکل ۵: نمودار حالت شبیه‌سازی مونت‌کارلو برای پیکربندی RAID5، با در نظر گرفتن خرابی دیسک، LSE و خطای انسانی

پارامتر L بیانگر تعداد دیسک آلوده به LSE است. در حالت L=1، زمانی که تنها دیسک آلوده به LSE خراب می‌شود، گذار از وضعیت EXP_{LSE} به EXP رخ می‌دهد. توزیع زمان خرابی دیسک آلوده به LSE با دیسک سالم متفاوت است، چرا که خرابی دیسک آلوده به LSE می‌تواند دلایل دیگری مانند تخصیص افراطی بلوک[۶۹] (EBR) داشته باشد که با مطالعه‌ی داده‌های میدانی قابل اندازه گیری است [۱۵]. هرچند که نرخ آشکاری برای تخصیص افراطی بلوک وجود ندارد و این نرخ به طور ضمنی در d_{DF} گنجانده شده است.

زمانی که یکی از n-1 دیسکی که آلوده به LSE نیستند خراب می‌شود، بر اثر ترکیب LSE و خرابی دیسک، آرایه به وضعیت DL_{FLSE} می‌رود که توزیع زمانی این رخداد تابعی از n-1 و d_{DF} است. لازم به ذکر است که اگر بیش از یک دیسک آلوده به LSE باشد، خرابی هر یک از n دیسک آرایه را به وضعیت DL_{FLSE} می‌برد[۷۰]. بنابراین، گذار از وضعیت EXP_{LSE} به EXP و DL_{FLSE} تابعی از L، تعداد دیسک‌های آلوده به LSE است. در وضعیت‌های EXP و EXP_r، اگر پیش از جایگزینی دیسک یا تکمیل بازیابی خطا، LSE رخ دهد، آرایه به وضعیت DL_{FLSE} می‌رود. هر چند، الراث و پچت [۱۵] احتمال این رخداد را پایین می‌دانند و از آن صرف نظر کرده‌اند. وضعیت های DL_{FF} و DU به ترتیب مشابه وضعیت‌های DL و DU در شکل ۴ است و محاسبات NOMDU و NOMDL مشابه بخش مقدمه انجام می‌شود.

۵-۴- شبیه‌سازی مونت‌کارلو

در شبیه‌سازی مونت‌کارلو، رخدادهای خرابی دیسک و LSE با توزیع دلخواه (در اینجا توزیع ویبول استخراج شده از داده‌های میدانی) ایجاد می‌شوند. پس از رخداد خرابی دیسک، زمان بازیابی خرابی با توزیع استخراج شده از داده‌های میدانی معین می‌شود. شکل ۶ مثالی است که نحوه‌ی شبیه‌سازی مونت‌کارلو برای یک آرایه RAID5(3+1) را نشان می‌دهد. در زمان‌های ۴۰۷ و ۸۹۳، پیش از بازیابی خرابی دیسک اول، خرابی دیسک دوم رخ داده که منجر به فقدان داده شده است. در زمان ۴۰۷، آرایه باپشتیبان بوده است و داده‌ی مفقود با استفاده از نسخه‌ی پشتیبان بازیابی شده است. در زمان ۸۹۳، هرچند، داده بی‌پشتیبان بوده و فقدان داده (DL) به طور غیر قابل بازگشت رخ داده است.



شکل ۶: مثالی از شبیه‌سازی مونت‌کارلوی یک آرایه‌ی RAID5 (3+1)

در زمان ۳۲۶، جایگزینی دیسک خراب با خطای انسانی مواجه شده است و سامانه تا زمان بازیابی خطای انسانی، از دسترس خارج شده است. در زمان ۶۱۰، یک LSE در دیسک ۲ رخ داده است و پیش از برطرف کردن LSE (با عملیات زدودن دیسک)، یک خرابی در دیسک ۱ رخ داده است که منجر به فقدان داده در سکتورهای آلوده به LSE شده است. ولی از آنجا که داده باپشتیبان بوده است، آرایه توانسته است داده‌ی درست را از نسخه‌ی پشتیبان بازیابی کند و داده‌ی کاربر تنها برای مدتی از دسترس خارج شده است.

عملیات زدودن دیسک در بازه‌های زمانی معین انجام می‌شود. با توجه به آدرس فیزیکی داده و مدت زمانی که عملیات زدودن دیسک طول می‌کشد، زمان دقیق تصحیح LSE در هر آدرس محاسبه می‌شود. در اینجا فرض می‌کنیم عملیات زدودن دیسک به تمامی سکتورهای آرایه دسترسی ترتیبی دارد (با شروع از آدرس ۰) و توزیع زمانی دسترسی، یکنواخت[۷۱] است. مثلاً در شکل ۶ در زمان ۵۰۰ یک LSE در دیسک ۱ رخ داده است و در زمان ۵۳۰، با عملیات زدودن دیسک، LSE برطرف شده است.

۴-۶- پارامترهای شبیه‌سازی مونت‌کارلو

همان‌گونه که در بخش مقدمه بحث شد، خرابی دیسک، LSE، بازیابی دیسک، و زدودن دیسک همگی با توزیع ویبول توصیف می‌شوند. جدول ۱ پارامترهای ویبول برای سه دیسک مورد آزمایش را نشان می‌دهد. برای توزیع زمانی عملیات جایگزینی دیسک و بازیابی خطای انسانی نیز توزیع ویبول انتخاب مناسبی است. زمانجایگزینی دیسک، d_{DR}، مقدار کمینه[۷۲] ندارد ($\gamma = 0$)، چرا که اپراتور ممکن است بلافاصله پس از خرابی دیسک، آن را جایگزین کند. ما برای پارامتر شکل، β، مقدار ۲ را در نظر می‌گیریم تا مشابه توزیع بازیابی دیسک، توزیعی متمایل به راست[۷۳] داشته باشیم. برای عمر مشخصه، η، مقدار ۰٫۵ ساعت در نظر گرفته شده است. این مقدار از تاریخچه‌ی سرویس مرکز داده‌ی *دانشگاه صنعتی شریف* ۷۴ استخراج شده است و به‌عنوان زمان مورد انتظار برای جایگزینی دیسک، در شبیه‌سازی‌ها مورد استفاده قرار گرفته است. مرکز داده دانشگاه صنعتی شریف شامل بیش از ۷۰ قفسه پردازشی و ذخیره سازی (با ظرفیتی بیش از ۱۰۰ پتابایت) می‌باشد. این مرکز داده با سامانه‌های ذخیره سازی داده SAB-SE [۷۱] تجهیز شده است که هر گره آن ظرفیت اتصال حداکثر ۷۲ دیسک را دارا می‌باشد و در مجموع ظرفیت نصب ۲۷۰۰۰ دیسک را برای این مرکز داده ایجاد می‌کند.

زمان تشخیص و بازیابی خطای انسانی با d_{HER} نمایش داده می‌شود. از آنجا که خطای انسانی می‌تواند بلافاصله تشخیص داده شده و بازیابی شود، پارامتر موقعیت، γ، را برابر صفر فرض می‌کنیم. برای پارامتر شکل، β، نیز مقدار ۲ را در نظر می‌گیریم تا مشابه توزیع بازیابی دیسک، توزیعی متمایل به راست داشته باشیم. در نهایت، با مشاوره‌ی کارشناس‌های فنی مرکز داده‌ی دانشگاه صنعتی شریف، عمر مشخصه ۱ ساعت ($\eta = 1$) در نظر گرفته شده است. همین‌طور با استفاده از تاریخچه‌ی سرویس مرکز داده، زمان سقوط، d_{crash} را با پارامتر شکل، β، ۱٫۴ و عمر مشخصه، η، ۸۷۶۰ ساعت توصیف می‌کنیم. به این دلیل که دیسکی که به اشتباه از آرایه جدا شده ممکن است بلافاصله دور انداخته شود، پارامتر موقعیت، γ، صفر فرض شده است. جدول ۵ پارامترهای خطای انسانی را نشان می‌دهد.

جدول ۵: پارامترهای خطای انسانی، استخراج شده از داده‌های میدانی و مشاوره با کارشناس‌های فنی مرکز داده

جایگزینی دیسک خراب (d_{DR})		بازیابی خطای انسانی (d_{HER})		سقوط دیسک به اشتباه جدا شده (d_{crash})	
η_{DR}	β_{DR}	η_{HER}	β_{HER}	η_{Crash}	β_{Crash}
0.5	2	1	2	8760	1.4

زمان بازیابی خرابی با استفاده از نسخه‌ی پشتیبان (در رخدادهای DL)، d_{BR}، نیز می‌تواند با توزیع ویبول سه پارامتره توصیف می‌شود. در رخدادهای DDF (یا TDF در RAID6)، داده‌ی دیسک‌های خراب از نسخه‌ی پشتیبان بازیابی می‌شود. روش جایگزینی هم وجود دارد که ابتدا داده‌ی یک دیسک را از نسخه‌ی پشتیبان بازیابی کرده و سپس داده‌ی دیسک دوم را با استفاده از XOR دیسک‌های موجود (n-1 دیسک) تولید می‌کند. با فرض استفاده از یک شبکه‌ی 1Gbps بین سامانه‌ی ذخیره‌سازی داده و نسخه‌ی پشتیبان و استفاده از آرایه‌ای با ۸ دیسک 500GB SATA با سرعت 50MBps، بازیابی دیسک اول از روی نسخه‌ی پشتیبان (با فرض اینکه پشتیبان می‌تواند داده با پهنای باند 1Gbps را تأمین کند) ۱۰ ساعت طول می‌کشد. با فرض اینکه دیسک‌های آرایه با گذرگاه 1.5 Gbps متصل شده‌اند، تولید داده‌ی دیسک n ام با استفاده از XOR دیسک‌های عملیاتی نیز ۱۰٫۴ ساعت طول می‌کشد [۱۵]. این تحلیل نشان می‌دهد که برای بازیابی DDF با استفاده از نسخه ی پشتیبان به حداقل ۲۰ ساعت زمان نیاز است ($\gamma = 20$). در آزمایشات دو برابر این مقدار (۴۰ ساعت) به‌عنوان عمر مشخصه، η، و پارامتر شکل، β، را مقدار ۲ در نظر می‌گیریم.

در مواقعی که بعضی از سکتورهای آرایه بر اثر LSE مفقود شده است، زمان بازیابی فقدان داده، d_{SBR}، تابعی از تعداد سکتورهای مفقود شده و اندازه‌ی سکتور است. از آنجا که هر سکتور معمولاً اندازه‌ی کوچک 4KB دارد، حداقل زمان بازیابی به حداقل زمان پاسخ دیسک و تأخیر شبکه بستگی دارد. ما زمان یک میلی‌ثانیه (1ms) را به‌عنوان کمینه زمان لازم برای بازیابی یک سکتور ($\gamma = 2.7 \times 10^{-7}$)، دو میلی‌ثانیه را برای عمر مشخصه ($\eta = 5.5 \times 10^{-7}$)، و مقدار ۲ را برای پارامتر شکل، β، در نظر می‌گیریم. پارامترهای ویبول d_{BR} و d_{SBR} در **جدول ۶** نشان داده شده است.

جدول ۶: پارامترهای بازیابی فقدان داده، استخراج شده از داده‌های میدانی و مشاوره با کارشناس‌های فنی مرکز داده

بازیابی خرابی دیسک (d_{BR})			بازیابی خرابی سکتور (d_{SBR})		
η_{BR}	β_{BR}	γ_{BR}	η_{SBR}	β_{SBR}	γ_{SBR}
40	2	20	5.5×10^{-7}	2	2.7×10^{-7}

۵- نتایج شبیه‌سازی

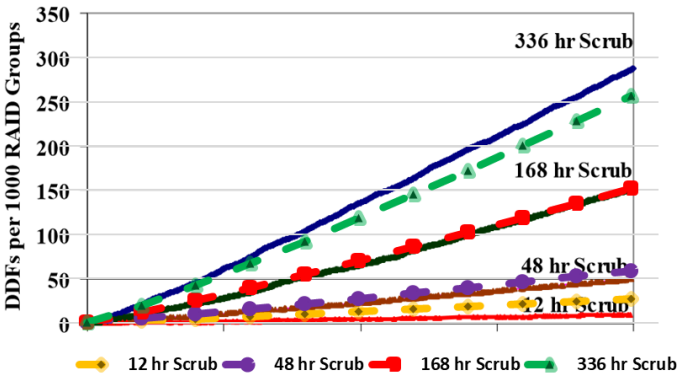
۵-۱- راه‌اندازی محیط آزمایش

برای هر پیکربندی مورد آزمایش، شبیه‌سازی مونت‌کارلو برای ۱۰۰۰ آرایه‌ی دیسک انجام شده است (با پارامترهای ارائه شده در بخش مقدمه). در هر آزمایش ده سال (۸۷۶۰۰ ساعت) مأموریت آرایه شبیه‌سازی می‌شود. محیط شبیه‌سازی مونت‌کارلو به طور کامل در محیط C++ پیاده‌سازی شده است و کد منبع[۷۵] آن در دسترس عموم قرار داده شده است[۷۶]. نتایج این بخش با فرض بی‌پشتیبان بودن سامانه استخراج شده است.

بنابراین، در نتایج فرض شده است که بازیابی فقدان داده امکان‌پذیر نمی‌باشد و NOMDU و NOMDL به ترتیب از (۶ و (۸ استخراج می‌شود.

۵-۲- اعتبار سنجی پیاده‌سازی مونت‌کارلو

برای اعتبارسنجی پیاده‌سازی مونت‌کارلو، DDF به دست آمده با صرف نظر از خطای انسانی را با DDF گزارش شده توسط الراث و پچت [۱۵][۱۷] مقایسه می کنیم (لازم به یادآوری است که هیچ‌یک از مطالعات پیشین اثر خطای انسانی را در نظر نگرفته‌اند). برای این مقایسه، آزمایش‌هایی با پیکربندی مشابه [۱۵][۱۷] راه اندازی شده است که در آن ۱۰۰۰ آرایه‌ی RAID5(7+1) شرکت دارند و رخدادهای ترکیبی DF+LSE و DF+DF همگی به‌عنوان DDF تلقی می‌شوند (این فرضی است اشتباه که [۱۵][۱۷] در شبیه‌سازی‌های خود داشته است). نتایج [۱۵][۱۷] با خطوط نقطه‌چین نشان داده شده است. همان‌طور که شکل ۷ نشان می‌دهد، خروجی پیاده‌سازی مونت‌کارلوی این مقاله برای η_{scrub} ۱۲، ۴۸ و ۱۶۸ ساعت کمی بزرگ‌تر از نتایج [۱۵][۱۷] است (به ترتیب ۵۶٪، ۱۳٪ و ۱,۳٪). این در حالی است که برای η_{scrub} برابر ۳۳۶ ساعت [۱۵][۱۷] نتایج ۹٪ بزرگ‌تری تولید می‌کند. لازم به ذکر است که مقایسه خروجی مدل پیشنهادی با داده‌های میدانی در بخش مقدمه ارائه شده است.



شکل ۷: نتایج شبیه‌سازی مونت‌کارلو برای ده سال مأموریت ۱۰۰۰ آرایه‌ی RAID5(7+1) و مقایسه با [۱۵][۱۷] (خطوط نقطه‌چین مربوط به نتایج [۱۵][۱۷] است).

۵-۳- اثر خطای انسانی در آرایه‌های بی‌پشتیبان

شکل ۸ NOMDU و NOMDL را برای ۱۰۰۰ آرایه RAID5 (با استفاده از ماشین حالت ارائه شده در بخش مقدمه) نمایش می‌دهد. در این شکل مقادیر NOMDL ناشی از DDF و DF+LSE تفکیک شده و به ترتیب در زیرشکل‌های ب و پ نمایش داده شده است. شکل الف نشان می‌دهد که با افزایش احتمال خطای انسانی، HEP، با یک مرتبه بزرگی[۲۷]، NOMDU نیز تقریباً با یک مرتبه بزرگی افزایش می‌یابد. در عین حال، HEP اثر کوچک‌تری بر NOMDL ناشی از DDF (شکل ب) و اثری جزئی بر NOMDL ناشی از DF+LSE دارد. در مجموع می‌توان گفت زمانی که برای مقادیر HEP کوچک‌تر از ۰,۰۰۱، خطای انسانی تقریباً تأثیر بر NOMDL ندارد (صرف‌نظر از نوع دیسک مورد آزمایش). هرچند، برای مقادیر HEP ۰,۰۱ و فراتر از آن، اثر خطای انسانی بر NOMDL بسیار چشمگیر است. مثلاً در دیسک A، افزایش HEP از ۰ به ۰,۰۱ و ۰,۱، NOMDL ناشی از DDF را به ترتیب ۴,۷ برابر و ۳۸ برابر می‌کند.

مشاهده‌ی مهم دیگر این است که NOMDL ناشی از LSE، پنج مرتبه بزرگی از NOMDL ناشی از DDF کوچک‌تر است. این در حالی است که نتایج شبیه‌سازی نشان می‌دهد LSE مسبب بیش از ۹۰٪ رخدادهای DL است. این مشاهده با تفاوت بزرگی فقدان داده در DDF و DF+LSE توضیح داده می‌شود. درحالی‌که رخداد DDF منجر به فقدان داده‌ی کل آرایه می‌شود، DF+LSE تنها یک یا چند نوار داده را مفقود می‌کند. این مشاهده نشان می‌دهد که شیوه‌ی الراث و پچت [۱۵][۱۷] که رخدادهای DF و DF+LSE را یکی فرض می‌کند (هر دو رخداد را به‌عنوان DDF در نظر می‌گیرد)، مقدار DL را به شدت دست بالا می‌گیرد.

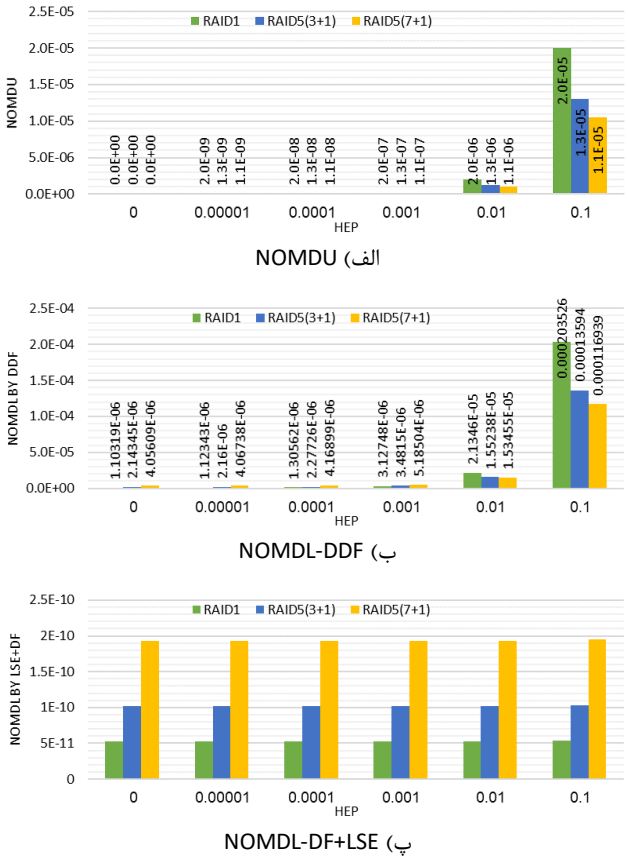
شکل ۸: NOMDU و NOMDL برای سه دیسک مختلف و مقادیر گوناگون خطای انسانی برای ۱۰۰۰ آرایه RAID5(7+1).

۵-۴- مقایسه‌ی پیکربندی‌های گوناگون RAID با حجم منطقی مساوی

در این بخش قصد داریم به این سؤال پاسخ دهیم که آیا خطای انسانی می‌تواند مفروضات قبلی ما در مورد اتکاپذیری پیکربندی‌های گوناگون RAID تغییر دهد. با این هدف، NOMDU و NOMDL سه پیکربندی RAID5(3+1)، RAID5(7+1) و RAID1(1+1) را با فرض اینکه هر سه آرایه حجم منطقی[۲۸] یکسانی دارند، مقایسه می‌کنیم.

۵-۴-۱- به‌کارگیری مدل اتکاپذیری RAID5 برای RAID1

آرایه‌ی RAID1 با آینه‌سازی داده‌ی دیسک بر روی یک دیسک افزونه، پیاده می‌شود. بنابراین، این آرایه می‌تواند مانند یک سیستم با تحمل‌پذیری یک خرابی مدل شود. مشابه آرایه RAID5، رخداد DDF و DF+LSE منجر به فقدان داده می شود و رخداد خطای انسانی در جایگزینی دیسک خراب، آرایه را از دسترس خارج می‌کند. بنابراین از دیدگاه اتکاپذیری، می‌توان RAID1 را مانند یک آرایه‌ی RAID5 با دو دیسک (یک دیسک داده و یک دیسک افزونه) در نظر گرفت.



الف) NOMDU

ب) NOMDL-DDF

پ) NOMDL-DF+LSE

شکل ۹: NOMDU و NOMDL برای آرایه‌های RAID مختلف با در نظر گرفتن حجم منطقی مساوی. آزمایش برای ۲۱۰۰۰ آرایه RAID1، ۷۰۰۰ آرایه‌ی RAID5(3+1) و ۳۰۰۰ آرایه‌ی RAID5(7+1) انجام شده است.

شکل ۹ مقادیر NOMDU و NOMDL را برای سه پیکربندی با اندازه‌ی منطقی ۲۱۰۰۰ دیسک نشان می‌دهد. با مقایسه‌ی نتایج با در نظر گرفتن خطای انسانی صفر (صرف‌نظر از خطای انسانی) درمی‌یابیم که RAID1 کمترین NOMDL را دارد و NOMDL آرایه RAID5(7+1) از RAID5(3+1) بالاتر است. این نتیجه، مفروضات قبلی در مورد آرایه‌های RAID که افزونگی بیشتر به معنای اتکاپذیری بیشتر است را تائید می‌کند. هرچند، با در نظر گرفتن اثر خطای انسانی، مشاهده می شود که NOMDU آرایه RAID1 از RAID5 بیشتر است و آرایه‌ی RAID5 (7+1) کمترین NOMDU را دارد. این مشاهده با مقدار بالاتر ERF[۷۹] آرایه‌ی RAID1 (ERF=2) نسبت به آرایه RAID5(3+1) (ERF=1.33) و آرایه RAID5(7+1) (ERF=1.14) توضیح داده می‌شود. زمانی که یک آرایه ERF بالاتری دارد، برای رسیدن به یک حجم منطقی مشخص، باید از تعداد بیشتری دیسک استفاده کند که این امر احتمال خرابی دیسک و متعاقباً خطای انسانی را بالا می‌برد. مشاهده‌ی دیگر این است که با افزایش HEP به ۰,۰۱ و فراتر از آن، NOMDL ناشی از DDF در آرایه RAID1 از RAID5(7+1) و RAID5(3+1) بیشتر می‌شود. این مشاهده به این معناست که در محیط‌هایی با احتمال رخداد خطای انسانی بالا، آرایه RAID1 نه تنها دسترس‌پذیری کمتر از RAID5 دارد، بلکه قابلیت اطمینان آن نیز کمتر است.

۵-۵- مقایسه با مدل‌های قبلی و داده‌های میدانی

در این بخش، نتایج مدل پیشنهادی را با مدل‌های قبلی (برای آرایه‌ی RAID5) مقایسه می‌کنیم. مدل‌های قبلی مورد مقایسه شامل *MTTDL* سنتی ارائه شده توسط گیبسون[۸۰] [۱۹]، *NOMDL* ارائه شده توسط گرینان[۸۱] [۲۲]، و *DDF* ارائه شده توسط الراث و پچت [۱۷] است، که هیچ‌یک اثر خطای انسانی را در نظر نمی گیرند. جدول ۷ مدل‌های قبل را با مدل پیشنهادی برای ۱۰۰۰ آرایه‌ی RAID5 (7+1) و ۱۰ سال مأموریت سامانه مقایسه می‌کند. در این مقایسه فرض شده است که آرایه بی‌پشتیبان بوده و دیسک ذخیره‌ای ندارد احتمال خطای انسانی ۰,۰۰۱ است.

جدول ۷: مقایسه‌ی مدل‌های قبلی قابلیت اطمینان آرایه‌ی دیسک با مدل پیشنهادی برای ۱۰۰۰ آرایه‌ی RAID5(7+1) و ۱۰ سال مأموریت سامانه. برای خطای انسانی مقدار نوعی HEP=0.001 در نظر گرفته شده است فرض شده است که آرایه، دیسک ذخیره ندارد. مابقی پارامترهای مورد استفاده در شبیه‌سازی در جدول ۱، جدول ۵ و جدول ۶ آورده شده است.

مدل قابلیت اطمینان آرایه دیسک	عدم دسترس پذیری			فقدان داده		
	DISK C	DISK B	DISK A	DISK C	DISK B	DISK A
NOMDL/NOMDU (Proposed) 10-years	بایت خارج از دسترس در هر ساعت به ازای هر ترابایت			بایت مفقود شده در هر ترابایت		
	118	79	113	5276	20871	5567
NOMDL (Greenan [22]) 10-years	در نظر گرفته نشده			بایت مفقود شده در هر ترابایت		
	-	-	-	4031	19374	4355
DDF (Elerath [17],[15]) 10-years	در نظر گرفته نشده			تعداد رخداد DDF		
	-	-	-	1	35	169
MTTDL (Gibson [19]) 10-years	در نظر گرفته نشده			MTTDL بر حسب سال		
	-	-	-	17	18	8

همان‌طور که جدول ۷ نشان می‌دهد، تنها مدل پیشنهادی اثر خطای انسانی و DU ناشی از آن را در نظر می‌گیرد. به‌عنوان‌مثال، مدل پیشنهادی نشان می‌دهد که برای آرایه RAID5(7+1) دیسک A، ۵۵۶۷ بایت فقدان داده به ازای هر ترابایت داده در یک مأموریت ۱۰ ساله مورد انتظار است. نتایج همچنین نشان می‌دهد که برای آرایه‌ی RAID5(7+1) دیسک A، در هر ساعت ۱۱۳ بایت از ۱ ترابایت داده از دسترس خارج خواهد بود. NOMDL گزارش شده توسط گرینان [۲۲] اندکی از مدل پیشنهادی پایین‌تر است، چرا که گرینان اثر DL ناشی از خطای انسانی را در نظر نمی‌گیرد. DDF گزارش شده توسط الراث [۱۷] نشان می‌دهد که در ۱۰۰۰ آرایه‌ی RAID5(7+1) از دیسک A، ۱۶۹ رخداد DDF در یک مأموریت ۱۰ ساله مورد انتظار است. هر چند، DDF گزارش شده توسط الراث هیچ اطلاعاتی در مورد اینکه چه تعداد از این DDF ناشی از DF+DF (که منجر به فقدان کل داده‌ی آرایه می‌شود) و چه تعداد ناشی از DF+LSE (که منجر به فقدان یک یا چند نوار داده می‌شود) بوده است، ندارد. علاوه بر این، DDF تابعی است از تعداد آرایه‌های مورد آزمایش (در اینجا ۱۰۰۰) درحالی‌که NOMDL و NOMDU کاملاً مستقل از تعداد آرایه است. در آخر، MTTDL گزارش شده توسط گیبسون [۱۹]، MTTDL برابر ۸ سال را برای ۱۰۰۰ آرایه‌ی RAID5(7+1) گزارش می‌کند. این معیار هیچ اطلاعاتی در مورد تعداد خرابی مورد انتظار، بزرگی فقدان داده، و اثر خطای انسانی ندارد.

در نهایت، به‌منظور بهتر نشان دادن کاستی‌های مدل‌های پیشین نسبت به مدل پیشنهادی در نادیده گرفتن اثر خطای انسانی، نتایج مدل پیشنهادی و مطالعات پیشین را با داده‌های میدانی استخراج شده از سامانه‌های رده-بالای یک شرکت پیشرو (که در اینجا آن را CorpX می‌نامیم) مقایسه می‌کنیم (جدول ۸). مطالعات میدانی بر روی خرابی چهار نسل از سامانه‌های CorpX نشان می‌دهد که ۱۵٪ از کل فقدان داده و عدم دسترس‌پذیری ناشی از خطای انسانی است.

همان‌طور که جدول ۸ نشان می‌دهد، پیش‌بینی گرینان [۲۲] و الراث [۱۵][۱۷] از فقدان داده پایین‌تر از مدل پیشنهادی است، چرا که این مطالعات اثر DL ناشی از خطای انسانی را در نظر نمی‌گیرند. اما کاستی بسیار مهم‌تر مطالعات پیشین در صرف‌نظر از عدم دسترس‌پذیری ناشی از خطای انسانی است. درحالی‌که داده‌های میدانی گزارش می‌کند که ۱۵٪ از کل عدم دسترس‌پذیری سامانه ناشی از خطای انسانی است، مطالعات پیشین اثر خطای انسانی بر عدم دسترس‌پذیری را به هیچ عنوان در نظر نگرفته‌اند. مقایسه‌ی نتایج مدل پیشنهادی با نتایج میدانی نشان می دهد زمانی که HEP=0.001 و $\eta_{crash} = 10h$ در نظر گرفته می‌شود، خروجی مدل به نتایج میدانی نزدیک است. این نتیجه رضایت‌بخش است، چرا که CorpX هم متوسط احتمال خطای انسانی را در همین بازه گزارش کرده است (۰٫۰۲٪ تا ۰٫۱٪). این نتایج میدانی برای RAID5(7+1) گزارش شده است و نتایج سایر پیکربندی‌ها در دسترس نیست.

آمار میدانی DeepSpar [۶۳] نیز فقدان داده را به تفکیک ریشه‌های آن گزارش می‌کند و نشان می‌دهد که ۱۲٪ فقدان داده در زیر سامانه‌ی دیسک بر اثر خطای انسانی رخ داده است. این آمار نیز به پیش‌بینی مدل پیشنهادی بسیار نزدیک است. با در نظر گرفتن HEP=0.001، مدل پیشنهادی ۱۲٫۸٪ از کل فقدان داده را ناشی از خطای انسانی گزارش می‌کند. نتیجه‌ی مقایسه‌ی مدل پیشنهادی با هر دو نتایج میدانی CorpX و DeepSpar نشان می‌دهد که دقیق‌ترین خروجی مدل، با در نظر گرفتن HEP=0.001 تولید می‌شود. این مشاهده همچنین با ارزیابی قبلی ما از احتمال خطای انسانی به دست آمده از مرکز داده‌ی دانشگاه صنعتی شریف و گزارش‌های میدانی پیشین، مطابقت دارد.

جدول ۸: مقایسه‌ی پیش‌بینی مدل پیشنهادی و مدل‌های قبلی با داده‌های میدانی CorpX

مدل	NOMDL	NOMDU
داده‌های میدانی	**0.00164**	15% of total DU
مدل پیشنهادی (HEP = 0.001)	**0.00158**	1.61E-08
مدل پیشنهادی (HEP = 0.0001)	0.00141	9.96E-10
مدل پیشنهادی (HEP = 0.01)	0.00316	1.58E-07
مدل پیشنهادی (HEP = 0.1)	0.0166	1.82E-06
مدل گرینان و الراث با در نظر گرفتن خرابی دیسک و خطای قطاع نهفته با توزیع ویبول (HEP = 0.0)	0.00140	0
روش سنتی با در نظر گرفتن خرابی دیسک با توزیع نمایی	0.00145	0

۶- نتیجه‌گیری

در این مقاله قابلیت اطمینان و دسترس‌پذیری زیرسامانه‌ی دیسک با در نظر گرفتن خطای انسانی ارزیابی شد. در این پژوهش تلاش کردیم تا به جای مدل‌های تقریبی و شبیه‌سازها، از پیاده‌سازی سامانه‌ی واقعی استفاده کنیم. ارزیابی عدم دسترس پذیری و فقدان داده تماماً با استفاده از تزریق اشکال آماری انجام شد که دقتی به مراتب بیشتر از مدل‌های مارکوف و تحلیل‌های احتمالی دارد. در این مقاله معیار جدیدی برای ارزیابی دسترس‌پذیری سامانه‌های ذخیره‌سازی داده نیز ارائه شده است. از نوآوری‌های این مقاله همچنین می‌توان به مطالعه‌ی اثر خطای انسانی اشاره کرد. در بخشی از این مقاله تلاش کردیم تا اثر خطای انسانی در زیرسامانه‌ی دیسک سخت را بر عدم دسترس‌پذیری و فقدان داده ارزیابی کنیم. این مطالعه نشان داد که صرف‌نظر از اثر خطای انسانی می‌تواند تا چند درجه بزرگی منجر به ناچیزشماری عدم دسترس‌پذیری و فقدان داده شود. این مطالعه همچنین نشان داد که با در نظر گرفتن خطای انسانی، انتخاب بهترین پیکربندی سامانه از دیدگاه اتکاپذیری نیاز به بازنگری دارد.

۷- مراجع

[1] A. Avizienis, J. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing." *IEEE transactions on dependable and secure computing,* vol. 1, pp. 11-33, 2004.

[2] L. N. Bairavasundaram, A. C. Arpaci-Dusseau, R. H. Arpaci-Dusseau, G. R. Goodson, and B. Schroeder, "An analysis of data corruption in the storage stack." *ACM Transactions on Storage (TOS),* vol. 4, pp. 8:1--8:28, 2008.

[3] L. N. Bairavasundaram, G. R. Goodson, S. Pasupathy, and J. Schindler, "An analysis of latent sector errors in disk drives." *ACM SIGMETRICS international conference on Measurement and modeling of computer systems*, vol. 35, pp. 289-300, 2007.

[4] M. Balakrishnan, A. Kadav, V. Prabhakaran, and D. Malkhi, "Differential raid: Rethinking raid for ssd reliability." *ACM Transactions on Storage (TOS),* vol. 6, no. 4, pp. 1-10, 2010.

[5] M. Blaum, J. Brady, J. Bruck, and J. Menon, "EVENODD: An efficient scheme for tolerating double disk failures in RAID architectures." *IEEE Transactions on computers*, vol. 44, pp. 192-202, 1995.

[6] M. Blaum, J. L. Hafner, and S. Hetzler, "Partial-MDS Codes and Their Application to RAID Type of Architectures." *IEEE Transactions on Information Theory*, vol. 59, pp. 4510-4519, 2013.

[7] F. Chandler, I. Heard, M. Presley, A. Burg, E. Midden, and P. Mongan, NASA Human Error Analysis. Retrieved from www.hq.nasa.gov/office/codeq/rm/docs/hra.pdfâ€Ž, Sep 2010

[8] P. L. Clemens, Human Factors and Operator Errors. *Jacobs Sverdrup,* 2002.

[9] U. S. Commission, Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants. *International Nuclear Information System (INIS),* vol 2, 1975.

[10] B. S. Dhillon, "System reliability evaluation models with human error." *IEEE Transactions on Reliability,* vol 32, pp. 47-59, 1983.

[11] A. Dholakia, E. Eleftheriou, X. Y. Hu, I. Iliadis, J. Menon, and K. K. Rao, "A New Intra-disk Redundancy Scheme for High-reliability RAID Storage Systems in the Presence of Unrecoverable Eerrors." *ACM Transactions on Storage (TOS),* vol 4, pp. 1-42, 2008.

[12] B. Dufrasne, and R. Eriksson, *IBM XIV Storage System Architecture, Implementation, and Usage.* Tech. rep., IBM. Retrieved from http://www.redbooks.ibm.com/abstracts/sg247659.html, 2011

[13] J. Elerath, "*Reliability Model and Assessment of Redundant Arrays of Inexpensive Disks (RAID) Incorporating Latent Defects and Non-Homogeneous Poisson Process Events."* Ph.D. dissertation, 2007.

[14] J. Elerath, "A simple equation for estimating reliability of an N+1 redundant array of independent disks (RAID)." *Dependable Systems and Networks (DSN), International Conference on*, pp. 484-493, 2009.

[15] J. Elerath, and M. Pecht, "Enhanced reliability modeling of raid storage systems." *Dependable Systems and Networks (DSN), International Conference on*,, pp. 175-184, 2007.

[16] J. Elerath, and J. Schindler, "Beyond MTTDL: A closed-form RAID 6 reliability equation." *ACM Transactions on Storage (TOS), vol 10*, no 7, pp. 256-279, 2014.

[17] J. Elerath, and M. Pecht, "A highly accurate method for assessing reliability of redundant arrays of inexpensive disks (RAID)." *IEEE Transactions on Computers, vol 58*, pp. 289-299, 2009.

[18] S. Forrest, S. Hofmeyr, A. Somayaji, and T. A. Longstaff, "A Sense of Self" Unix Processes. *Security and Privacy, IEEE Symposium on*, pp. 120-128. 1996.

[19] G. A. Gibson, "*Redundant Disk Arrays: Reliable, Parallel Secondary Storage."* Ph.D. dissertation, Univeristy of California, Berkeley, 1990.

[20] W. H. Gibson, B. Hickling, and B. Kirwan, *Feasibility Study Into the Collection of Human Error Probability Data.* EUROCONTROL. Retrieved from https://www.eurocontrol.int/feasibility-study-collection-human-error-probability-data, 2006

[21] K. M. Greenan, D. D. Long, E. L. Miller, and A. Wildani, "Building flexible, fault-tolerant flash-based storage systems." *Proceedings of the 5th Workshop on Hot Topics in System Dependability (HotDep).* Yokohama, 2009.

[22] K. M. Greenan, J. S. Plank, and J. J. Wylie, "Mean Time to Meaningless: MTTDL, Markov Models, and Storage System Reliability." *USENIX conference on Hot topics in storage and file systems (HotStorage)*, pp. 1-5, 2010.

[23] S. K. Hari, S. V. Adve, and H. Naeimi, "Low-Cost Program-Level Detectors for Reducing Silent Data Corruptions." *Dependable Systems and Networks (DSN), Annual IEEE/IFIP International Conference on*, pp. 1-12. 2012.

[24] E. Haubert, "Threats of Human Error in a High-Performance Storage System: Problem Statement and Case Study," *CoRR, abs/cs/0412074*, 1-13. Retrieved from http://arxiv.org/abs/cs/0412074, 2004

[25] I. Iliadis, R. Haas, X.-Y. Hu, and E. Eleftheriou, "Disk scrubbing versus intra-disk redundancy for high-reliability raid storage systems." *ACM SIGMETRICS Performance Evaluation Review*, *36*, pp. 241-252. 2008.

[26] G. Jacques-Silva, Z. Kalbarczyk, B. Gedik, H. Andrade, K.-L. Wu, and R. K. Iyer, "Modeling Stream Processing Applications for Dependability Evaluation." *Dependable Systems and Networks (DSN), Annual IEEE/IFIP International Conference on*, pp. 430-441, 2011.

[27] W. Jiang, C. Hu, Y. Zhou, and A. Kanevsky, "Are disks the dominant contributor for storage failures?: A comprehensive study of storage subsystem failure characteristics." *ACM Transactions on Storage (TOS),* vol 4, pp. 1-25, 2008.

[28] K. Keeton, and A. Merchant, "A framework for evaluating storage system dependability." *Dependable Systems and Networks (DSN), International Conference on*, pp. 877-886. 2004.

[29] K. Keeton, C. A. Santos, D. Beyer, J. S. Chase, and J. Wilkes, "Designing for Disasters." *USENIX Conference on File and Storage Technologies (FAST)*, vol *4*, pp. 59-62, 2004.

[30] J. O. Kephart, and D. M. Chess, "The Vision of Autonomic Computing." *Computer,* vol 36, pp. 41-50, 2003.

[31] J. Kim, J. Lee, J. Choi, D. Lee, and S. H Noh, "Improving SSD reliability with RAID via elastic striping and anywhere parity." *Dependable Systems and Networks (DSN)*, pp. 1-12. Budapest, 2013.

[32] S. Kim, "Area-efficient error protection for caches." *Design, Automation and Test in Europe. DATE'06. Proceedings*, *1*, pp. 1-6, 2006.

[33] S. Kim, and A. K. Somani, "Area efficient architectures for information integrity in cache memories." *ACM SIGARCH Computer Architecture News,* vol 27, pp. 246-255, 1999.

[34] M. Kishani, and H. Asadi, "Modeling Impact of Human Errors on the Data Unavailability and Data Loss of Storage Systems." *IEEE Transactions on Reliability (TR),* vol. 67, no. 3, pp. 1111-1127, 2018.

[35] M. Kishani, R. Eftekhari, and H. Asadi, "Evaluating Impact of Human Errors on the Availability of Data Storage Systems." *Design, Automation and Test in Europe Conference (DATE)*, pp. 314-317. 2017.

[36] F. Lees, "*Lees' Loss prevention in the process industries: Hazard identification, assessment and control."* Butterworth-Heinemann, 2017.

[37] N. G. Leveson, "Model-based analysis of socio-technical risk", 2004.

[38] R. Leveugle, A. Calvez, P. Maistri, and P. Vanhauwaert, "Statistical Fault Injection: Quantified Error and Confidence." *Conference on Design, Automation and Test in Europe (DATE)*, pp. 502-506, 2009.

[39] M. Li, and P. P. Lee, "Stair codes: A general family of erasure codes for tolerating device and sector failures." *ACM Transactions on Storage (TOS),* vol. 10, no. 14, pp. 719-740, 2014.

[40] M. Li, and J. Shu, "Preventing silent data corruptions from propagating during data reconstruction." *IEEE Transactions on Computers,* vol. 59, pp. 1611-1624, 2010.

[41] M. Li, J. Shu, and W. Zheng, "GRID codes: Strip-based erasure codes with high fault tolerance for storage systems." *ACM Transactions on Storage (TOS),* vol 4, pp. 15:1-15:22, 2009.

[42] X. Li, M. Lillibridge, and M. Uysal, "Reliability analysis of deduplicated and erasure-coded storage." *ACM SIGMETRICS Performance Evaluation Review, 38*, 4-9, 2011.

[43] Y. Li, P. P. Lee, and J. C. Lui, "Analysis of Reliability Dynamics of SSD RAID." *IEEE Transactions on Computers,* vol. 65, pp. 1131-1144, 2016.

[44] D. Meister, "The nature of human error." *Global Telecommunications Conference and Exhibition'Communications Technology for the 1990s and Beyond'(GLOBECOM)*, pp. 783-786, 1989.

[45] N. Mi, A. Riska, E. Smirni, and E. Riedel, "Enhancing data availability in disk drives through background activities. *Dependable Systems and Networks (DSN), International Conference on*, pp. 492-501, 2008.

[46] S. Moon, and A. L. Reddy, "Does RAID Improve Lifetime of SSD Arrays?" *ACM Transactions on Storage (TOS),* vol. 12, no. 11, pp. 1217-1241, 2016.

[47] B. Mullins, H. Asadi, M. B. Tahoori, D. Kaeli, K. Granlund, R. Bauer, and S. Romano, "Case Study: Soft Error Rate Analysis in Storage Systems." *VLSI Test Symposium*, pp. 256-264, 2007.

[48] W. B. Nelson, *Applied life data analysis*, vol. 577. John Wiley and Sons, 2005.

[49] D. Oppenheimer, "The Importance of Understanding Distributed System Configuration." *Human Factors in Computer Systems workshop*, pp. 1-3, 2003.

[50] A. Oprea, and A. Juels, "A clean-slate look at disk scrubbing." *USENIX conference on File and storage technologies (FAST)*, pp. 57-70, 2010.

[51] D. A. Patterson, "A Simple Way to Estimate the Cost of Downtime." *USENIX System Administration Conference (LISA)*, *2*, pp. 185-188. 2002.

[52] D. A. Patterson, G. Gibson, and R. H. Katz, "A case for redundant arrays of inexpensive disks (RAID)." *SIGMOD international conference on Management of data. 17*, pp. 109-116. Chicago: ACM, 1988.

[53] E. Pinheiro, and L. A. Barroso, "Failure Trends in a Large Disk Drive Population." *USENIX Conference on File and Storage Technologies (FAST)*, pp. 17-28, 2007.

[54] J. S. Plank, and M. Blaum, "Sector-Disk (SD) Erasure Codes for Mixed Failure Modes in RAID Systems." *ACM Transactions on Storage (TOS),* vol. 10, no. 4, pp. 660-689, 2014.

[55] V. Prabhakaran, L. N. Bairavasundaram, N. Agrawal, H. S. Gunawi, A. C. Arpaci-Dusseau, and R. H. Arpaci-Dusseau, "*IRON File Systems"*, vol. 39, 2005.

[56] E. W. Rozier, W. Belluomini, V. Deenadhayalan, J. Hafner, K. K. Rao, and P. Zhou, "Evaluating the impact of undetected disk errors in raid systems." *Dependable Systems and Networks (DSN), International Conference on*, pp. 83-92, 2009.

[57] L. Rui, L. Chuan, Z. Yingzhi, and Z. Dong, "The preliminary study on the human-factor evaluation system for maintainability design." *Intelligent Human-Machine Systems and Cybernetics (IHMSC), International Conference on*, vol *2*, pp. 107-112, 2009.

[58] B. Schroeder, S. Damouras, and P. Gill, "Understanding Latent Sector Errors and How to Protect Against Them." *ACM Transaction on Storage (TOS),* vol. 6, no. 3, pp. 9:1-9:23, 2010.

[59] T. J. Schwarz, Q. Xin, E. L. Miller, D. D. Long, A. Hospodor, and S. Ng, "Disk scrubbing in large archival storage systems." *Modeling,*

Analysis, and Simulation of Computer and Telecommunications Systems (MASCOTS), pp. 409-418, 2004.

[60] S. Z. Shazli, M. Abdul-Aziz, M. B. Tahoori, and D. R. Kaeli, "A field analysis of system-level effects of soft errors occurring in microprocessors used in information systems." *International Test Conference (ITC)*, pp. 1-10. 2008.

[61] I. Sideris, and K. Pekmestzi, "Cost Effective Protection Techniques for TCAM Memory Arrays." *IEEE Transactions on Computers*, vol 61, pp. 1778-1788, 2012.

[62] C. W. Slayman, "Cache and Memory Error Detection, Correction, and Reduction Techniques for Terrestrial Servers and Workstations." *IEEE Transactions on Device and Materials Reliability,* vol. 5, pp. 397-404, 2005.

[63] D. M. Smith, and M. L. Williams, *Data Loss and Hard Drive Failure: Understanding the Causes and Costs*, 2017.

[64] A. D. Swain, "Human Reliability Analysis: Need, Status, Trends and Limitations." *Reliability Engineering and System Safety,* vol. 29, 301-313, 1990.

[65] A. D. Swain, and H. E. Guttmann, "*Handbook of Human-Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report."* Tech. rep., Sandia National Labs., Albuquerque, NM (USA), 1983.

[66] T. Tsai, N. Theera-Ampornpunt, and S. Bagchi, "A Study of Soft Error Consequences in Hard Disk Drives." *Dependable Systems and Networks (DSN), Annual IEEE/IFIP International Conference on*, pp. 1-8. 2012.

[67] K. V. Vishwanath, and N. Nagappan, "Characterizing Cloud Computing Hardware Reliability." *ACM Symposium on Cloud Computing*, pp. 193-204, 2010.

[68] S. Xu, R. Li, P. Lee, Y. Zhu, L. Xiang, Y. Xu, and J. Lui, "Single Disk Failure Recovery for X-code-based Parallel Storage Systems." *IEEE Transactions on Computers,* vol. 63, no. 4, pp. 995-1007, 2013.

[69] J. Yang, and F. Sun, "A comprehensive review of hard-disk drive reliability." *Reliability and Maintainability Symposium, 1999. Proceedings. Annual*, pp. 403-409, 1999.

[70] Y. Zhu, P. P. Lee, L. Xiang, Y. Xu, and L. Gao, "A Cost-based Heterogeneous Recovery Scheme for Distributed Storage Systems with RAID-6 Codes." *Dependable Systems and Networks (DSN), Annual IEEE/IFIP International Conference on*, pp. 1-12, 2012.

[71] SAB-SE Data Storage Systems. http://hpdss.com/En/SAB-SE.html, 2020

[72] HPDS Corporation. http://hpdss.com/En/index.html, 2020

مصطفی کیشانی کارشناسی خود را در سال ۱۳۸۷ در رشته مهندسی کامپیوتر از دانشگاه فردوسی مشهد، کارشناسی ارشد را در سال ۱۳۸۹ در رشته مهندسی کامپیوتر از دانشگاه صنعتی امیرکبیر، و دکتری را در سال ۱۳۹۷ در رشته مهندسی کامپیوتر از دانشگاه صنعتی شریف اخذ نمودند. ایشان در حال حاضر پژوهشگر فوق دکتری در آزمایشگاه پژوهشی «ذخیره‌سازی، پردازش و شبکه‌های داده (DSN)» در دانشگاه صنعتی شریف است. ایشان از سال ۱۳۸۹ تا ۱۳۹۱ به‌عنوان مهندس سخت‌افزار در پژوهشکده سامانه‌های ماهواره سازمان فضایی ایران مشغول به کار بودند. ایشان همچنین در سال ۱۳۸۹ در تیم Memocode پژوهشگاه دانش‌های بنیادی (IPM) عضویت داشتند. در سال ۱۳۹۵ ایشان به‌عنوان دستیار پژوهشی در Chinese University of Hong Kong (CUHK) مشغول به فعالیت بودند. همچنین در سال ۱۳۹۶ ایشان به‌عنوان دانشیار پژوهشی در Hong Kong Polytechnic University (PolyU)فعالیت داشتند .

آدرس پست الکترونیکی ایشان عبارت است:

mostafa.kishani@sharif.edu

حسین اسدی استادتمام دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف است. ایشان از سال ۱۳۸۸ تا سال ۱۳۹۳ به‌عنوان استادیار و در ادامه تا دی‌ماه ۱۳۹۸ به‌عنوان دانشیار و از آن تاریخ تاکنون به‌عنوان استادتمام در دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف مشغول به فعالیت می‌باشد. ایشان مدیر و مؤسس آزمایشگاه پژوهشی «ذخیره‌سازی، پردازش و شبکه‌های داده» (DSN) بوده و در طی یک دهه‌ی اخیر بیش از ۶۰ دانشجوی کارشناسی، کارشناسی ارشد و دکترا پایان‌نامه خود را در این آزمایشگاه انجام داده است. در حال حاضر نیز بیش از ۱۵ دانشجوی کارشناسی، کارشناسی ارشد و دکترا در این آزمایشگاه در حال انجام پروژه خود می‌باشند. در سال ۱۳۸۹ به‌عنوان استاد نمونه دانشکده مهندسی کامپیوتر برگزیده شد. قبل از شروع همکاری در این دانشگاه در شرکت EMC2 به‌عنوان محقق و مهندس ارشد در ایالت ماساچوست آمریکا به مدت سه سال مشغول به کار بود. همچنین، ایشان حدود ۱۰۰ مقاله در مجلات و کنفرانس‌های معتبر بین‌المللی داشته و چندین سال داور مجلات معتبر انجمن IEEE می‌باشد. در سال ۲۰۱۴ نیز به‌عنوان دبیر مهمان مجله IEEE Transactions on Computers خدمت نموده است. در سال ۲۰۱۵ به‌عنوان دبیر علمی کنفرانس بین‌المللی CADS انتخاب شده و همچنین در تحریریه چندین مجله داخلی و خارجی از جمله Microelectronics Reliability فعالیت نموده است. در سال ۲۰۱۵ نیز اولین شرکت دانش‌بنیان تولیدکننده سامانه‌های ذخیره‌سازی داده (شرکت پردازش و ذخیره‌سازی سریع داده) را در ایران و غرب آسیا تأسیس نمود. این شرکت در حال حاضر با بیش از ۵۰ نیروی حرفه‌ای تمام‌وقت، بیش از چهار رده محصول تولید و به بازار ارائه نموده است. از سال ۲۰۱۵ تاکنون از میان بیش از ۴۵۰ عضو هیئت‌علمی دانشگاه صنعتی شریف، ایشان به‌صورت پیوسته جزو ۱۰ نفر اول اعضای هیئت‌علمی در رتبه‌بندی معاونت پژوهش و فناوری دانشگاه قرار داشته است. در چهار سال اخیر نیز، جوایز مختلفی ازجمله جایزه «پژوهشگر برتر»، «فناور برتر»، «موسسه پژوهشی برتر» و «آزمایشگاه پژوهشی برتر» را در سطح دانشکده و دانشگاه و همچنین جایزه بهترین مقاله کنفرانس بین‌المللی DATE2019 را کسب نموده است. زمینه تخصصی ایشان سامانه‌های ذخیره‌سازی داده، سامانه‌های اتکاپذیر، پردازش قابل بازپیکربندی، دیسک‌های حالت جامد و سیستم‌های عامل بوده و عضو ارشد (Senior Member) انجمن IEEE نیز می‌باشد.

آدرس پست الکترونیکی ایشان عبارت است:

asadi@sharif.edu

---

۱ Data Storage System (DSS)

۲ Dependability

۳ Global Memory (GM)

۴ Module

۵ Dynamic Random Access Memory

۶ Front-End (FE) Logic

۷ Back-End (BE) Logic

۸ Disk Scrubbing

۹ Redundant Array of Independent Disks

۱۰ Human Error

۱۱ Data Unavailability

۱۲ Data Loss

[۱۳] Wrong Disk Replacement
[۱۴] Monte Carlo
[۱۵] NOrmalized Magnitude of Data Unavailability (NOMDU)
[۱۶] Rack
[۱۷] Instant Copy
[۱۸] Remote Mirroring
[۱۹] Logical Unit Number (LUN) Masking
[۲۰] SCSI
[۲۱] Dual Initiator
[۲۲] Snapshot
[۲۳] Statistical Fault Injection
[۲۴] Leveugle
[۲۵] Cut-Off Point
[۲۶] Check Pointing
[۲۷] Data Reconstruction
[۲۸] Weibull
[۲۹] Latent Sector Error
[۳۰] Elerath
[۳۱] Schindler
[۳۲] Characteristic Life
[۳۳] Location Parameter
[۳۴] Shape Parameter
[۳۵] Serial AT Attachment
[۳۶] Safety-Critical
[۳۷] Double Disk Failure
[۳۸] Autonomic Computing
[۳۹] Forgiving Design
[۴۰] Non-benign
[۴۱] Human Reliability Assessment (HRA)
[۴۲] Human Error Probability (hep)
[۴۳] Internal Error Station
[۴۴] Mars Exploration Rover
[۴۵] Terminal Radar Approach Control
[۴۶] Airbone Separation Assistance System
[۴۷] Checkoff
[۴۸] Mean Time to Data Loss
[۴۹] Double Disk Failure
[۵۰] Magnitude of Data Loss
[۵۱] Normalized Magnitude of Data Loss
[۵۲] Temporal Locality
[۵۳] Spatial Locality
[۵۴] Markov Models
[۵۵] Logical Size of Unavailable Data
[۵۶] Unavailability Duration
[۵۷] Total Logical Storage Size
[۵۸] Mission Time
[۵۹] Logical Size of Lost Data
[۶۰] Recovery Time
[۶۱] Exposed
[۶۲] Operational
[۶۳] Non-Survivable
[۶۴] NOrmalized Magnitude of Data Loss
[۶۵] Survivable
[۶۶] Pecht
[۶۷] Overestimation
[۶۸] در اینجا می‌توانیم یک محدودیت مدل مارکوف نسبت به شبیه‌سازی مونت‌کارلو را بازگو کنیم: مدل‌های مارکوف، به دلیل بی‌حافظه بودن، نمی‌توانند تعداد رخداد LSE را نگه دارند، و در نتیجه نمی‌توانند تخمین دقیقی از زمان بازیابی خرابی یا بزرگی فقدان داده داشته باشند. این محدودیت مدل مارکوف ما را مجبور می‌کند که مفروضاتی غیر واقعی در مدل اعمال کنیم. مثلاً فرض کنیم تنها یک سکتور به LSE آلوده شده است.
[۶۹] Exessive Block Reallocation
[۷۰] این مورد نیز نمی‌تواند به درستی توسط مدل مارکوف ارزیابی شود. چرا که در مدل مارکوف به دلیل بی‌حافظه بودن نمی‌توان فهمید چه تعداد از دیسک‌ها آلوده به LSE است.
[۷۱] Uniform
[۷۲] Minimum
[۷۳] Right-Skewed
[۷۴] Sharif University of Technology
[۷۵] Source Code
[۷۶] http://dsn.ce.sharif.edu/
[۷۷] Order of Magnitude
[۷۸] Logical (Usable) Capacity
[۷۹] Effective Replication Factor
[۸۰] Gibson
[۸۱] Greenan

The CSI Journal on Computing Science and Information Technology

The CSI Journal on
Computing Science and
Information Technology
Vol. 18, No.1, 2020

Investigation of Human-Error Impact on Dependability of Data Storage Systems

Mostafa Kishani[1], Hossein Asadi[2]

[1, 2] Department of Computer Engineering, Sharif University of Technology, Tehran, Iran

Abstract

Despite using automatic failure recovery mechanisms, human error in service and maintenance of datacenters is inevitable. Human error in disk subsystem is one of the most common causes of data unavailability and data loss, due to the large population of disk drives in datacenters. In this paper, we investigate the impact of wrong disk replacement on data unavailability and data loss in storage systems. To this end, we first analyze the consequences of wrong disk replacement in the disk array. Afterwards, we conduct Monte-Carlo simulations to evaluate data unavailability and data loss. In this framework A) different array configurations are investigated, and B) a new metric for data unavailability of storage systems is proposed. This new metric is independent of storage size and can project the extent of data unavailability.

Keywords: Data Storage System; Availability; Reliability; Human Error; Disk Array; Erasure Codes; Error Detection and Correction Codes; Statistical Fault Injection; Monte-Carlo Simulation