بررسی حملات کانال جانبی و امنیت در شبکه های روی تراشه و پردازنده های نورومورفیک

در عصر دیجیتال امروز، امنیت پردازنده‌ها یکی از حیاتی‌ترین جنبه‌های فناوری اطلاعات به شمار می‌رود. پردازنده‌ها که به‌عنوان مغز محاسباتی سیستم‌های رایانه‌ای عمل می‌کنند، نقش اساسی در اجرای دستورالعمل‌ها و پردازش داده‌ها دارند. با افزایش پیچیدگی و توانایی‌های این مؤلفه‌ها، مسئله امنیت آنها نیز به یکی از چالش‌های مهم در عرصه فناوری تبدیل شده است. امنیت پردازنده‌ها از اهمیت بالایی برخوردار است؛ زیرا هرگونه آسیب‌پذیری یا نفوذ در این سطح می‌تواند به تهدیدات جدی علیه اطلاعات حساس، امنیت داده‌ها و حریم خصوصی کاربران منجر شود. از جمله ریسک‌ها، حملات سایبری مانند حملات کانال جانبی [1]، ملوارها [2]و اسپایورها [3] هستند که می‌توانند از طریق نقاط ضعف معماری پردازنده‌ها به داده‌های حیاتی دسترسی یابند. شبکه‌های روی تراشه [4] نقش اساسی در طراحی و عملکرد سیستم‌های الکترونیکی پیشرفته امروزی بازی می‌کنند، به خصوص در زمینه‌ی معماری‌های میکروپروسسور و سیستم‌های تعبیه شده. با افزایش تعداد هسته‌ها و ماژول‌های فرآیندی در تراشه‌های سیلیکونی، نیاز به یک سیستم ارتباطی موثر و کارآمد که بتواند این اجزا را به طور کامل به هم متصل کند، ضروری شده است. شبکه‌های روی تراشه به این نیاز پاسخ می‌دهند و امکان انتقال داده‌ها بین اجزا با سرعت بالا، کمینه سازی تاخیر و کاهش مصرف انرژی را فراهم می‌آورند.

حملات کانال جانبی نوعی از تکنیک‌های نفوذ هستند که از طریق جمع‌آوری اطلاعات از فرایندهای فیزیکی و اجرایی سیستم، مانند مصرف انرژی، زمان پردازش و تابش الکترومغناطیسی، به دست می‌آیند. این اطلاعات می‌توانند برای استخراج داده‌های حساس بدون دسترسی مستقیم به داده‌ها یا سیستم استفاده شوند. با پیشرفت‌های اخیر در زمینه پردازش عصبی و توسعه مدل‌های جدیدی مانند شبکه‌های عصبی اسپایکینگ [5]، مسئله امنیت به یک چالش پیچیده‌تر تبدیل شده است. این شبکه‌ها که از الگوهای زمانی برای پردازش اطلاعات بهره می‌برند، قابلیت‌های جدیدی برای پردازش داده‌ها ارائه می‌دهند؛ اما هم‌زمان آسیب‌پذیری‌های جدیدی را نیز به همراه دارند. تحقیقات در زمینه امنیت این پردازنده‌ها و شبکه‌های عصبی اسپایکینگ، به‌ویژه در مواجهه با حملات کانال جانبی، اهمیت ویژه‌ای دارد. این تلاش‌ها شامل شناسایی، تحلیل و رفع

---

[1] Side Channel Attacks

[2] malwar

[3] Spyware

[4] Network-on-chip

[5] Spiking Neural Network

آسیب‌پذیری‌ها به‌منظور تضمین امنیت داده‌ها و حفظ اعتماد به سیستم‌های مبتنی بر این فناوری‌های پیشرفته می‌باشد.

پردازنده‌های نورومورفیک [6] که الهام گرفته از ساختار و کارکرد مغز انسان هستند، به دلیل توانایی‌های منحصربه‌فرد خود در پردازش اطلاعات بیولوژیکی و انجام محاسبات به‌شدت کارآمد و مقرون‌به‌صرفه از نظر انرژی، محبوبیت یافته‌اند. این پردازنده‌ها با استفاده از سیستم‌هایی که از نورون‌ها و سیناپس‌های مصنوعی تشکیل‌شده‌اند، امکان مدل‌سازی دقیق‌تری از فرایندهای عصبی طبیعی را فراهم می‌آورند که این امر به افزایش چشمگیر در کارایی پردازش داده‌های پیچیده می‌انجامد.

در اینجا به چند دلیل کلیدی برای استفاده از پردازنده‌های نورومورفیک و توضیحات مربوط به آنها اشاره می‌کنیم:

- کارایی بالا در مصرف انرژی: پردازنده‌های نورومورفیک با الگوبرداری از کارآمدی انرژی مغز انسان، قادر به اجرای محاسبات پیچیده با مصرف انرژی بسیار کم هستند. این ویژگی آنها را برای استفاده در دستگاه‌های قابل‌حمل و تجهیزاتی که به انرژی محدود دسترسی دارند، ایده‌آل می‌سازد.
- پردازش موازی: این پردازنده‌ها قادر به انجام محاسبات به‌صورت موازی هستند که این امر سرعت پردازش داده‌ها را به طور قابل‌توجهی افزایش می‌دهد. محاسبات موازی به آنها امکان می‌دهد تا وظایف مختلف را هم‌زمان انجام دهند، بدون اینکه بر روی یکدیگر تأثیر منفی بگذارند.
- توانایی یادگیری و تطابق: پردازنده‌های نورومورفیک به طور طبیعی برای یادگیری و تطابق با الگوهای جدید داده‌ها طراحی شده‌اند. این ویژگی آنها را برای کاربردهایی مانند یادگیری ماشینی و هوش مصنوعی بسیار مناسب می‌سازد، جایی که توانایی سریع برای انطباق با داده‌های جدید از اهمیت بالایی برخوردار است.

چندین مثال از پردازنده‌های نورومورفیک که در حال حاضر موردتوجه قرار گرفته‌اند عبارت‌اند از:

- Intel Loihi : پردازنده نورومورفیک Loihi از Intel یک چیپ تحقیقاتی است که برای شبیه‌سازی مغز انسان طراحی شده است. Loihi از معماری خاصی برخوردار است که امکان یادگیری و تعامل با

[6] neuromorphic processors

محیط را در زمان واقعی و با مصرف انرژی بسیار پایین فراهم می‌کند. این پردازنده قادر است برای مدل‌سازی شبکه‌های عصبی اسپایکینگ تا ۱۳۰,۰۰۰ نورون و ۱۳۰ میلیون سیناپس را پشتیبانی کند.

- IBM TrueNorth: یکی دیگر از پردازنده‌های پیشرفته نورومورفیک است که توسط IBM توسعه‌یافته است. با قابلیت پشتیبانی از بیش از یک میلیون نورون و ۲۵۶ میلیون سیناپس، TrueNorth برای اجرای کارآمد الگوریتم‌های یادگیری عمیق با مصرف انرژی بسیار پایین طراحی شده است. این چیپ می‌تواند در برنامه‌های کاربردی مختلف از جمله تجهیزات حسگر، پردازش تصویر و شبکه‌های عصبی مصنوعی استفاده شود.

- SpiNNaker (Spiking Neural Network Architecture): توسعه‌یافته توسط دانشگاه منچستر، SpiNNaker یک پلتفرم محاسباتی است که برای مدل‌سازی مقیاس بزرگ شبکه‌های عصبی اسپایکینگ طراحی شده است. این سیستم قادر است تا یک میلیارد نورون را شبیه‌سازی کند. SpiNNaker برای تحقیقات در زمینه علوم اعصاب و هوش مصنوعی، از جمله مطالعه دینامیک‌های مغز و طراحی الگوریتم‌های مبتنی بر شبکه‌های عصبی اسپایکینگ، مورداستفاده قرار می‌گیرد.

اهمیت پردازنده‌ها در امنیت سیستم‌های کامپیوتری و نقش کلیدی آن‌ها در حفاظت از اطلاعات و داده‌های حساس برجسته شد. باتوجه‌به رشد روزافزون تهدیدات سایبری، از جمله حملات کانال جانبی، فهم دقیق و محافظت از این سطح از معماری سیستم حیاتی است. تأکید بر لزوم تحقیق و توسعه در زمینه‌های امنیت پردازنده‌ها و شبکه‌های عصبی، به‌ویژه پردازنده‌های نورومورفیک، نشان‌دهنده یک گام ضروری در پیشبرد امنیت فناوری‌های آینده است. پردازنده‌های نورومورفیک، با الهام از مکانیزم‌های طبیعی مغز انسان، نه‌تنها قابلیت‌های چشمگیری در کارایی انرژی و پردازش موازی به ارمغان آورده‌اند، بلکه در یادگیری و تطابق با الگوهای جدید نیز برتری نشان داده‌اند. این ویژگی‌ها آن‌ها را برای کاربردهای پیشرفته در یادگیری ماشین و هوش مصنوعی بسیار ارزشمند ساخته است. از Loihi اینتل گرفته تا IBM TrueNorth و SpiNNaker، هر یک از این پلتفرم‌ها به‌نوعی انقلابی در نحوه پردازش و تحلیل داده‌ها به شمار می‌روند، امکان پیشرفت‌های بزرگ در عرصه‌های مختلف را فراهم می‌آورند.

در پروژهٔ ما، مواجه با چالش‌های مربوط به دسترسی و هزینهٔ پردازنده‌های نورومورفیک بودیم. این پردازنده‌ها که برای تحقیقات پیشرفته در زمینهٔ شبکه‌های عصبی و یادگیری ماشینی بسیار کارآمد هستند، به دلیل

محدودیت‌های وارداتی و هزینه‌های بالای خرید در ایران، به‌آسانی در دسترس نبودند. برای مقابله با این مشکل و ادامهٔ تحقیقات خود، ما تصمیم گرفتیم که از FPGA موجود در آزمایشگاه خود استفاده کنیم. با بهره‌گیری از FPGA، ما قادر بودیم تا الگوریتم‌های موردنظر خود را برای پیاده‌سازی و آزمایش حملات ساید چنل بر روی شبکه‌های عصبی اسپایکینگ، بدون نیاز به سخت‌افزار اختصاصی و گران‌قیمت، اجرا کنیم. این تجربه نشان داد که با استفاده خلاقانه از منابع موجود، می‌توان چالش‌های مربوط به دسترسی و هزینه را برطرف ساخت و به پیشبرد اهداف تحقیقاتی ادامه داد.

در نهایت، باتوجه‌به پیشرفت‌های اخیر در فناوری‌های نورومورفیک و چالش‌های امنیتی مرتبط با آنها، تأکید بر اهمیت امنیت در سطح پردازنده و ادامه تحقیقات برای مقابله با تهدیدات احتمالی ضروری است. این رویکرد نه‌تنها به حفظ امنیت داده‌ها کمک می‌کند، بلکه اطمینان از پیشرفت مستمر در فناوری‌هایی که به طور فزاینده‌ای در زندگی روزمره ما نقش دارند را نیز تضمین می‌نماید.