طراحی و تبیین معماری پلتفرم ذخیره‌سازی هیبریدی بومی و هوشمند؛ مبتنی بر امنیت سخت‌افزاری چندلایه و ساختار ماژولار جهت کاربردهای حساس صنعتی

علی لطفی اربط[۱]
۱- گروه مهندسی کامپیوتر ، دانشگاه مهارت ملی تبریز
alilotfyarbat@gmail.com

چکیده

در عصر انقلاب صنعتی چهارم، مدیریت داده‌ها با چالش دوگانه «حریم خصوصی» در سرویس‌های ابری عمومی و «عدم دسترسی‌پذیری هوشمند» در حافظه‌های فیزیکی سنتی مواجه است .این پژوهش جهت رفع این شکاف، پلتفرم ابر امن من (SPC)[۱] را به عنوان معماری ذخیره‌سازی هیبریدی و بومی معرفی می‌کند که پارادایم «حاکمیت دیجیتال» را با امنیت سخت‌افزاری تلفیق کرده است. روش‌شناسی پژوهش بر توسعه سیستم نهفته ماژولار با بهره‌گیری از پردازنده دو هسته‌ای ESP۳۲[۲] برای پردازش در لبه[۳] و یکپارچه‌سازی ماژول امنیت سخت‌افزاری[۴] مدل ATECC۶۰۸A استوار است که مدیریت ایزوله کلیدها و اجرای سخت‌افزاری رمزنگاری AES-۲۵۶[۵] را مستقل از آسیب‌پذیری‌های سیستم‌عامل تضمین می‌کند.

یافته‌های پیاده‌سازی نمونه اولیه نشان می‌دهد که معماری پیشنهادی با ارائه سه سطح دسترسی (مستقیم، شبکه محلی و ابری)، ضمن حذف هزینه‌های ارزی اشتراک، تأخیر شبکه را در کاربردهای بلادرنگ کاهش داده است .همچنین، به‌کارگیری هوش مصنوعی در لبه[۶] امکان پایش سلامت داده‌ها و تشخیص ناهنجاری را بدون نیاز به سرور مرکزی فراهم می‌آورد .این سامانه به عنوان راهکاری مقرون‌به‌صرفه و مقیاس‌پذیر، جایگزینی توانمند برای زیرساخت‌های پرهزینه در صنایع حساس بانکی، فرماندهی نظامی ، اتوماسیون صنعتی ، حتی شخصی و دانشگاهی محسوب می‌شود.

کلمات کلیدی : ذخیره‌سازی هیبریدی، امنیت سخت‌افزار، رایانش در لبه، حاکمیت داده، هوش مصنوعی در لبه

---

۱ Secure Personal Cloud
۲ Espressif Systems
۳ Edge Computing
۴ Hardware Security Module
۵ Advanced Encryption Standard
۶ Edge AI

۱ – مقدمه

در عصر حاضر که از آن به عنوان «عصر داده» یاد می‌شود، اطلاعات به ارزشمندترین دارایی سازمان‌ها و افراد تبدیل شده است. با ظهور انقلاب صنعتی چهارم و گسترش اینترنت اشیاء[۱] ، حجم داده‌های تولید شده به صورت نمایی در حال افزایش است. برای مدیریت این حجم عظیم از اطلاعات، رایانش ابری[۲] به عنوان یک الگوی غالب، انعطاف‌پذیری و مقیاس‌پذیری بی‌نظیری را ارائه کرده است .(Zhang et al., ۲۰۲۰)

با این حال، پذیرش گسترده سرویس‌های ابری عمومی مانند Google Drive چالش‌های امنیتی و حقوقی جدیدی را به وجود آورده است. نگرانی‌های مربوط به حریم خصوصی، نشت داده‌ها، و دسترسی شخص ثالث به اطلاعات حساس، به‌ویژه در صنایع زیرساختی و نظامی، به موانع جدی برای برون‌سپاری ذخیره‌سازی داده‌ها تبدیل شده‌اند.(Ren et al., ۲۰۱۹)

یکی از چالش‌های اصلی در اکوسیستم دیجیتال فعلی، مفهوم حاکمیت داده[۳] است. سازمان‌های حساس مانند بانک‌ها، مراکز نظامی و صنایع استراتژیک نیازمند تضمین این مسئله هستند که داده‌هایشان در محدوده جغرافیایی و تحت قوانین ملی خودشان ذخیره و مدیریت شود. سرویس‌های ابری خارجی به دلیل قرارگیری سرورها در خارج از مرزهای ملی، عملاً کنترل کامل را از دست مالک داده خارج می‌کنند. از سوی دیگر، استفاده از راهکارهای سنتی ذخیره‌سازی آفلاین (مانند هارد دیسک‌های اکسترنال) اگرچه امنیت فیزیکی را تأمین می‌کند، اما فاقد هوشمندی، قابلیت دسترسی از راه دور و امکانات اشتراک‌گذاری مدرن است .(Wang & Li, ۲۰۲۱)

این دوگانگی میان «امنیت ایزوله» و «کارایی ابری»، خلأ بزرگی را در بازار فناوری اطلاعات ایجاد کرده است.

علاوه بر این، در سیستم‌های کنترل صنعتی و محیط‌های عملیاتی حساس، اتصال دائمی به اینترنت جهت استفاده از سرویس‌های ابری، ریسک حملات سایبری را به شدت افزایش می‌دهد. بنابراین، نیاز به معماری‌هایی که بتوانند پردازش را در لبه شبکه انجام دهند و تنها داده‌های ضروری یا رمزنگاری شده را منتقل کنند، بیش از پیش احساس می‌شود. بومی‌سازی زیرساخت‌های ذخیره‌سازی و استفاده از پروتکل‌های رمزنگاری سخت‌افزاری به جای تکیه صرف بر امنیت نرم‌افزاری، راهکاری است که می‌تواند تاب‌آوری زیرساخت‌های ملی را در برابر تهدیدات سایبری تضمین کند.

این پژوهش با درک این چالش‌ها، به طراحی و تبیین معماری یک پلتفرم ذخیره‌سازی هیبریدی بومی با نام (ابر امن من) (SPC) می‌پردازد. هدف اصلی این پلتفرم، پر کردن شکاف میان امنیت سخت‌افزاری و کارایی نرم‌افزاری است. در این طرح، با بهره‌گیری از پردازنده‌های کم‌مصرف و قدرتمند ESP۳۲ و ادغام آن با ماژول‌های امنیت سخت‌افزاری مانند چیپ ATECC۶۰۸A، سیستمی ارائه شده است که امکان ذخیره‌سازی امن، هوشمند و ماژولار را فراهم می‌آورد. این پژوهش نشان می‌دهد که چگونه می‌توان با یک معماری لایه‌بندی شده و استفاده از هوش مصنوعی در لبه، نظارت بر داده‌ها را به صورت محلی انجام داد و در عین حال، دسترسی ایمن را در بسترهای شبکه فراهم نمود.

---

۱ Internet of Things (IoT)
۲ Cloud Computing
۳ Data Sovereignty

۲- مواد و روش‌ها

این پژوهش با رویکرد «توسعه نمونه اولیه کاربردی» (MVP[۱]) و بر اساس متدولوژی چابک[۲] انجام شده است. هدف اصلی، طراحی یک معماری سخت‌افزاری-نرم‌افزاری یکپارچه است که بتواند با کمترین هزینه سخت‌افزاری، بالاترین سطح امنیت و کارایی را در مدیریت داده‌ها ارائه دهد. ساختار کلی سیستم شامل سه لایه اصلی: سخت‌افزار پردازشی امن، میان‌افزار مدیریت داده و رابط کاربری کلاینت است.

۲-۱. معماری سخت‌افزاری و اجزاء هسته مرکزی پردازش

در این پلتفرم، ماژول ESP ۳۲ مدل S۳ (نسخه WROVER) انتخاب گردید. دلیل این انتخاب، معماری دو هسته‌ای[۳] این پردازنده است که امکان تفکیک وظایف حیاتی را فراهم می‌کند؛ به طوری که یک هسته به مدیریت پشته شبکه[۴] و هسته دیگر به مدیریت سیستم فایل و رمزنگاری اختصاص یافته است. همچنین وجود ۸ مگابایت حافظه PSRAM در این ماژول، ایجاد بافرهای بزرگ برای مدیریت جریان داده‌های حجیم[۵] و جلوگیری از سرریز حافظه در هنگام آپلود و دانلود را ممکن می‌سازد.

برای اتصال حافظه‌های جانبی، از رابط سخت‌افزاری USB-OTG استفاده شده است. در نمونه اولیه، یک برد برک‌اوت[۶] مدل USB Type-A جهت اتصال ایمن حافظه‌های فلش به پین‌های GPIO[۷] پردازنده متصل گردید.

جهت تأمین امنیت در سطح لایه فیزیکی و جلوگیری از حملات سخت‌افزاری، از چیپ رمزنگاری اختصاصی مدل ATECC۶۰۸A استفاده شده است .این ماژول وظیفه تولید، ذخیره‌سازی و مدیریت کلیدهای رمزنگاری را در یک محیط ایزوله و مقاوم در برابر دستکاری[۸] بر عهده دارد .منبع تغذیه سیستم نیز یک آداپتور ۵ ولت با جریان پایدار ۲ آمپر است تا توان مصرفی لحظه‌ای حافظه‌های USB پرسرعت را بدون ایجاد نوسان در پردازنده تأمین نماید.

۲-۲. پشته نرم‌افزاری و پروتکل‌ها توسعه فیرمور (Firmware)

دستگاه با استفاده از زبان C++ در محیط توسعه Arduino IDE انجام شده است .این انتخاب به دلیل دسترسی به کتابخانه‌های بهینه شده برای معماری ESP۳۲ و قابلیت توسعه سریع صورت گرفت .سیستم فایل مورد استفاده فرمت FAT۳۲ است که به دلیل سازگاری گسترده با سیستم‌عامل‌های مختلف (Windows, Linux, macOS) به عنوان استاندارد ذخیره‌سازی انتخاب شد.

ساختار نرم‌افزاری بر پایه یک وب‌سرور غیرهمگام[۹] طراحی شده است که درخواست‌های کاربران را از طریق یک API مبتنی بر REST[۱۰] مدیریت می‌کند

---

۱ Minimum Viable Product
۲ Agile
۳ Dual-core
۴ Network Stack
۵ Data Streaming
۶ Breakout Board
۷ General Purpose Input/Output
۸ Tamper-resistant
۹ Async Web Server
۱۰ Representational State Transfer

اندپوینت‌های اصلی پیاده‌سازی شده عبارتند از:

- :api/files[1]/جهت دریافت لیست ساختار درختی فایل‌ها و پوشه‌ها.
- :api/upload/جهت دریافت جریان داده و ذخیره‌سازی امن آن بر روی حافظه.
- :api/download/جهت فراخوانی و ارسال فایل رمزنگاری شده به کلاینت.

۳-۲. مکانیزم‌های امنیتی و شبکه پلتفرم پیشنهادی

از یک رویکرد امنیتی چندلایه بهره می‌برد .در لایه داده، تمام فایل‌ها پیش از ذخیره‌سازی با الگوریتم رمزنگاری متقارنAES ۲۵۶ رمزگذاری می‌شوند .در لایه شبکه، سیستم به صورت هوشمند و هیبریدی عمل می‌کند:

۱. حالت اکسس پوینت :(AP Mode) در صورت عدم وجود شبکه خارجی، دستگاه یک شبکه Wi-Fi مستقل و امن با استاندارد WPA۲ ایجاد می‌کند که برای محیط‌های عملیاتی ایزوله (مانند صنایع دفاعی) مناسب است.

۲. حالت کلاینت :(STA Mode) دستگاه به شبکه داخلی موجود متصل شده و به عنوان یک گره امن در شبکه عمل می‌کند.

فرآیند تست و ارزیابی نمونه اولیه با استفاده از ابزار بردبورد برای اطمینان از صحت عملکرد ماژولار اجزا پیش از طراحی PCB نهایی انجام پذیرفت.

۳- پیاده سازی و جزئیات فنی

در این بخش، مراحل عملیاتی ساخت پلتفرم، ابزارهای به‌کار رفته و معماری دقیق نرم‌افزاری و سخت‌افزاری تشریح می‌گردد. پیاده‌سازی این سامانه با تمرکز بر اصول «ماژولار بودن» و «امنیت در طراحی» صورت گرفته است.

۳-۱. محیط توسعه و ابزارها

برای دستیابی به یک معماری پایدار و قابل توسعه، انتخاب ابزارهای مهندسی مناسب در دو لایه نرم‌افزار و سخت‌افزار از اهمیت ویژه‌ای برخوردار است. در این پژوهش، از ابزارهای متن‌باز[2] جهت کاهش هزینه‌های توسعه و افزایش شفافیت امنیتی استفاده شده است.

الف) بستر توسعه نرم‌افزاری[1] توسعه میان‌افزار (Firmware)

دستگاه با استفاده از زبان برنامه‌نویسی C++ در بستر محیط توسعه یکپارچه آردوینو انجام پذیرفت. دلیل انتخاب این محیط، وجود کتابخانه‌های بهینه و پشتیبانی گسترده از هسته پردازشی ۳۲ESP است که فرآیند کدنویسی سطح پایین سخت‌افزار را تسهیل می‌کند. برای مدیریت وظایف موازی (مانند مدیریت همزمان شبکه و رمزنگاری)، از سیستم‌عامل بلادرنگ (FreeRTOS) که به صورت پیش‌فرض در هسته نرم‌افزاری ۳۲ESP تعبیه شده است، بهره‌گیری شد.

[1] Application Programming Interface
[2] Open Source

ب) کتابخانه‌ها و استانداردها

جهت مدیریت فایل‌ها بر روی حافظه جانبی، از استاندارد سیستم فایل ۳۲FAT استفاده شده است تا سازگاری کامل با سیستم‌عامل‌های رایج (ویندوز، لینوکس و مک) تضمین گردد. همچنین برای پیاده‌سازی رابط کاربری تحت وب و مدیریت درخواست‌ها، از کتابخانه‌های «سرور وب غیرهمگام»[۲] استفاده شد تا پردازنده بدون مسدود شدن[۳]، قادر به پاسخگویی به درخواست‌های متعدد باشد.

ج) ابزارهای نمونه‌سازی سخت‌افزاری

در فاز ساخت نمونه اولیه (MVP)، به جای طراحی مدار چاپی نهایی، از روش اتصال موقت بر روی بردبورد استفاده گردید. این روش امکان تغییرات سریع در معماری سخت‌افزار و عیب‌یابی ماژولار را فراهم نمود. برای اتصال ایمن حافظه‌های فلش به پایه‌های ورودی/خروجی (GPIO) پردازنده، از بردهای مبدل[۴] استاندارد درگاه USB نوع A استفاده شده است.

۲-۳ . معماری نرم‌افزار و مدیریت داده‌ها

معماری نرم‌افزاری پلتفرم بر اساس رویکرد رویداد محور (Event-driven) طراحی شده است تا بتواند با کمترین منابع پردازشی، پاسخگوی درخواست‌های همزمان باشد. ساختار اصلی میان‌افزار از سه لایه اصلی تشکیل شده است:

الف) مدیریت هوشمند شبکه[۵]

این ماژول وظیفه تضمین دسترسی پایدار به دستگاه را بر عهده دارد و بر اساس یک الگوریتم اولویت‌بندی عمل می‌کند .در هنگام راه‌اندازی، سیستم ابتدا به جستجوی شبکه‌های بی‌سیم ذخیره شده (مانند شبکه داخلی سازمان) می‌پردازد (حالت کلاینت) .در صورت عدم موفقیت در اتصال یا قرارگیری در محیط‌های عملیاتی فاقد زیرساخت، دستگاه به صورت خودکار به حالت نقطه دسترسی[۶] تغییر وضعیت داده و یک شبکه محلی امن با شناسه مخفی ایجاد می‌کند.

ب) رابط برنامه‌نویسی وب و مدیریت درخواست‌ها

برای تعامل میان کاربران (کلاینت‌ها) و هسته پردازشی، یک وب‌سرور غیرهمگام پیاده‌سازی شده است که درخواست‌ها را از طریق پروتکل انتقال ابرمتن (HTTPS) مدیریت می‌کند .معماری این بخش بر پایه «رابط برنامه‌نویسی کاربردی (API) بنا شده است که اندپوینت‌های[۷] اصلی آن عبارتند از:

- دریافت فهرست :جهت استخراج ساختار فایل‌ها و پوشه‌ها در قالب استاندارد JSON[۸]
- بارگذاری داده :مدیریت جریان داده‌های ورودی و ذخیره‌سازی آن‌ها بر روی حافظه فیزیکی.

---

۱ Software Development Kit
۲ Async Web Server
۳ Non-blocking
۴ Breakout Board
۵ Network Manager
۶ Access Point
۷ Endpoints
۸ javaScript Object Notation

- دریافت فایل :فراخوانی داده‌های رمزنگاری شده و ارسال آن به سمت کاربر.

ج) مدیریت سیستم فایل و امنیت داده

این لایه به عنوان واسط میان نرم‌افزار و سخت‌افزار عمل کرده و وظیفه مدیریت عملیات خواندن و نوشتن بر روی حافظه جانبی را با فرمت FAT۳۲ بر عهده دارد .جهت تضمین امنیت اطلاعات، تمامی داده‌ها پیش از نوشته شدن بر روی دیسک، توسط الگوریتم رمزنگاری پیشرفته (AES-۲۵۶) کدگذاری می‌شوند .این فرآیند تضمین می‌کند که حتی در صورت جداسازی حافظه فیزیکی، دسترسی به محتوای آن بدون کلیدهای سخت‌افزاری امکان‌پذیر نباشد.

۳-۳ . پیاده‌سازی سخت‌افزاری و مکانیزم‌های امنیتی

در این پژوهش، یکپارچه‌سازی اجزای سخت‌افزاری با هدف دستیابی به پایداری عملیاتی و امنیت نفوذناپذیر انجام شده است. معماری فیزیکی سیستم بر پایه تعامل سه بخش اصلی شامل واحد پردازش، واحد ذخیره‌سازی و واحد امنیت استوار است.

الف) رابط سخت‌افزاری ذخیره‌سازی

جهت برقراری ارتباط میان هسته پردازشی و حافظه‌های جانبی مانند فلش مموری یاSSD ، از پروتکل گذرگاه سریال عمومی (USB) در حالت میزبان (Host Mode) استفاده شده است .در مدار طراحی شده، پایه‌های ورودی/خروجی شماره ۱۹ و ۲۰ (GPIO ۱۹/۲۰) در پردازنده ESP۳۲ به عنوان خطوط داده به ماژول رابط USB متصل گردیدند .این پیکربندی امکان تبادل داده با سرعت بالا را بدون نیاز به درایورهای پیچیده فراهم می‌آورد.

ب) زیرساخت تغذیه و پایداری

یکی از چالش‌های اصلی در سیستم‌های ذخیره‌سازی مبتنی بر پردازنده‌های نهفته، نوسانات جریان در هنگام عملیات نوشتن بر روی حافظه است . برای رفع این چالش، مدار تغذیه با استفاده از یک رگولاتور ولتاژ تثبیت‌کننده و منبع تغذیه ۵ ولت با جریان‌دهی مداوم ۲ آمپر طراحی شد .این ظرفیت جریان، مانع از افت ولتاژ و بازنشانی ناخواسته (Reset) سیستم در زمان اتصال هاردهای اکسترنال پرمصرف می‌گردد.

ج) امنیت لایه فیزیکی

متمایزترین ویژگی این معماری، استفاده از «ماژول امنیت سخت‌افزاری (HSM) مدل ATECC۶۰۸A است .این تراشه از طریق پروتکل ارتباطی I۲C به پردازنده اصلی متصل شده و وظیفه «مدیریت چرخه حیات کلیدها» را بر عهده دارد .در این معماری، کلیدهای رمزنگاری هرگز از داخل این تراشه ایمن خارج نمی‌شوند و عملیات رمزنگاری درون خود تراشه یا با نظارت مستقیم آن انجام می‌پذیرد. این طراحی موجب می‌شود که حتی در صورت سرقت فیزیکی دستگاه و مهندسی معکوس مدار، استخراج کلیدهای خصوصی غیرممکن باشد.

د) پردازش هوشمند در لبه علاوه بر امنیت فیزیکی، یک لایه نظارتی مبتنی بر هوش مصنوعی بر روی سخت‌افزار پیاده‌سازی شده است .این واحد با پایش مداوم الگوی مصرف جریان و ترافیک داده‌ها، رفتارهای ناهنجار مانند تلاش برای کپی‌برداری انبوه یا حملات brute-force را شناسایی کرده و در صورت لزوم، ارتباط پورت‌ها را به صورت فیزیکی قطع می‌کند.

۳-۴. تحلیل هزینه و توجیه اقتصادی

یکی از شاخص‌های کلیدی در ارزیابی موفقیت پلتفرم‌های زیرساختی، نسبت هزینه به کارایی[۱] است. در این پژوهش، هزینه تمام‌شده ساخت نمونه اولیه بر اساس قیمت قطعات در بازار داخلی محاسبه گردید .مجموع هزینه‌های سخت‌افزاری شامل برد توسعه، ماژول امنیتی، رابط‌ها و قطعات جانبی معادل ۳۰دلار برآورد شده است.

مقایسه این رقم با راهکارهای جایگزین موجود در بازار، مزیت رقابتی قابل توجهی را نشان می‌دهد:

- در مقایسه با سرویس‌های ابری خارجی :اشتراک سالیانه یک سرویس ابری تجاری با فضای ۲ ترابایت مانند Google Driveیا Dropbox ، هزینه‌ای ارزی و تکرار شونده دارد که با نوسانات نرخ ارز، ریسک مالی بالایی را به سازمان‌ها تحمیل می‌کند .در حالی که پلتفرم پیشنهادی، هزینه‌ای یک‌بار پرداخت[۲] داشته و فاقد هزینه‌های پنهان ماهیانه است.

- در مقایسه با سرورهای ذخیره‌سازی سازمانی :(NAS) تجهیزات ذخیره‌سازی تحت شبکه برندهای خارجی مانند QNAP یا Synology با قابلیت‌های امنیتی مشابه، قیمتی بالغ بر ۱۰ تا ۳۵ برابر هزینه تمام‌شده این طرح دارند.

علاوه بر صرفه اقتصادی مستقیم، معماری ماژولار این سیستم باعث کاهش هزینه‌های نگهداری[۳] می‌شود؛ زیرا در صورت خرابی حافظه یا نیاز به ارتقای ظرفیت، کاربر می‌تواند بدون نیاز به تعویض کل دستگاه و تنها با جایگزینی حافظهUSB ، سیستم را بازیابی یا ارتقا دهد .این ویژگی برای صنایع حساس که تداوم کسب‌وکار[۴] در آن‌ها حیاتی است، یک مزیت استراتژیک محسوب می‌شود.

۴ - نتایج و یافته ها

در این فصل، نتایج حاصل از پیاده‌سازی نمونه اولیه (MVP) پلتفرم ابر امن من (SPC) مورد ارزیابی و تحلیل قرار می‌گیرد. عملکرد سیستم از سه منظر «کارایی عملیاتی»، «امنیت» و «توجیه اقتصادی» بررسی شده و در نهایت، مزیت‌های رقابتی آن نسبت به نمونه‌های مشابه خارجی در قالب جداول تطبیقی ارائه می‌گردد.

۱-۴ . ارزیابی عملکرد عملیاتی

آزمایش‌های انجام شده بر روی سخت‌افزار توسعه‌یافته نشان داد که معماری دو هسته‌ای پردازنده (ESP۳۲) با موفقیت توانسته است سربار پردازشی ناشی از مدیریت شبکه و رمزنگاری همزمان را مدیریت کند .سیستم در سه حالت عملکردی زیر مورد تست قرار گرفت و نتایج پایداری را ثبت نمود:

---

۱ Cost-benefit Analysis
۲ One-time Cost
۳ Maintenance
۴ Business Continuity

۱. **حالت مستقیم :(AP)** در این حالت، دستگاه با ایجاد یک شبکه مستقل، امکان انتقال داده‌ها را با تأخیر کمتر از ۱۰ میلی‌ثانیه برای تکنسین‌ها در محیط‌های ایزوله فراهم کرد.

۲. **حالت شبکه محلی :(STA)** سرعت انتقال داده در شبکه داخلی برای فایل‌های حجیم (مانند ویدیوهای دوربین‌های مداربسته) به دلیل استفاده از بافرهایPSRAM ، بدون افت کیفیت یا قطعی ارتباط انجام شد.

۳. **حالت ابری :(Cloud)** دسترسی از راه دور با موفقیت برقرار شد، هرچند وابستگی به پهنای باند اینترنت در این بخش عامل تعیین‌کننده بود.

۴-۲ .تحلیل مقایسه‌ای با نمونه‌های خارجی

برای تبیین جایگاه این پلتفرم، یک مقایسه تطبیقی میان ابر امن من ، سرویس‌های ابری عمومی خارجی مانند Google Drive و راهکارهای ذخیره‌سازی فیزیکی (هارد اکسترنال) انجام شده است. جدول شماره (۱) خلاصه این مقایسه را نشان می‌دهد.

جدول شماره (۱): مقایسه ویژگی‌های فنی و امنیتی پلتفرم پیشنهادی با راهکارهای متداول

معیار مقایسه	سرویس ابری خارجی مانند Google Drive	ذخیره‌سازی فیزیکی هارد اکسترنال	پلتفرم پیشنهادی (SPC)
حاکمیت داده (Data Sovereignty)	خیر (در اختیار شرکت ثالث)	بله (نزد کاربر)	بله (کنترل مطلق)
امنیت سخت‌افزاری	نامشخص (سمت سرور)	خیر (معمولاً نرم‌افزاری)	بله (چیپ A۶۰۸ATECC)
دسترسی از راه دور	دارد	ندارد	دارد (امن و خصوصی)
هزینه اشتراک	دارد (ماهیانه/سالیانه)	ندارد	ندارد (یک‌بار پرداخت)
کارکرد آفلاین	خیر	بله	بله (هیبریدی)
هوش مصنوعی	دارد (سمت سرور)	ندارد	دارد (در لبه/Edge)

همان‌طور که در جدول (۱) مشاهده می‌شود، پلتفرم پیشنهادی تنها گزینه‌ای است که مزایای هر دو روش سنتی و مدرن (امنیت فیزیکی و دسترسی ابری) را به صورت همزمان ارائه می‌دهد.

۴-۳. ارزیابی امنیت چندلایه

تحلیل امنیتی معماری پیشنهادی نشان‌دهنده برتری محسوس آن نسبت به روش‌های رمزنگاری نرم‌افزاری رایج است .استفاده از چیپ امنیتی سخت‌افزاری باعث شده است که کلیدهای رمزنگاری حتی در صورت نفوذ به سیستم‌عامل دستگاه، قابل استخراج نباشند .این ویژگی برای کاربردهای بانکی و نظامی که در معرض حملات پیشرفته قرار دارند، حیاتی است .همچنین، پیاده‌سازی رمزنگاری استاندارد AES-۲۵۶ بر روی تمامی فایل‌ها، تضمین می‌کند که در صورت سرقت فیزیکی حافظه، داده‌ها برای سارق غیرقابل استفاده باشند.

۴-۴ . تحلیل هزینه و توجیه اقتصادی

یکی از یافته‌های کلیدی این پژوهش، کاهش چشمگیر هزینه‌های عملیاتی است .برآورد هزینه ساخت نمونه اولیه (MVP) شامل تمامی ماژول‌های پردازشی، امنیتی و جانبی، رقمی معادل ۳۰ دلار را نشان می‌دهد .جدول شماره (۲) مقایسه هزینه ۵ ساله استفاده از این پلتفرم را در برابر سرویس‌های خارجی نشان می‌دهد.

جدول شماره (۲): مقایسه هزینه انباشته در یک دوره ۵ ساله (ارقام به دلار است)

نوع سرویس	هزینه اولیه (راه‌اندازی)	هزینه اشتراک سالیانه	مجموع هزینه ۵ ساله	ریسک ارزی
سرویس ابری خارجی (TB۲)	۰	۲۰۰دلار	۲۵۰ دلار	بسیار بالا
سرور ذخیره‌سازی (NAS)	۲۰دلار	۱۵۰دلار	۲۰۰ دلار	متوسط
پلتفرم ابر امن من (SPC)	۳ دلار	۱۰	**۳۰ دلار**	**ندارد**

نکته: ارقام مربوط به سرویس‌های خارجی بر اساس نرخ میانگین اشتراک دلاری و نرخ ارز فعلی تخمین زده شده‌اند
یافته‌های جدول (۲) اثبات می‌کند که استفاده از پلتفرم بومی SPC، هزینه‌های ذخیره‌سازی داده را در بلندمدت تا ۹۰ درصد نسبت به سرویس‌های ابری خارجی کاهش می‌دهد. این صرفه‌جویی اقتصادی در کنار حذف ریسک قطع دسترسی ناشی از تحریم‌ها، توجیه پذیری بالای این طرح را برای پیاده‌سازی در مقیاس صنعتی اثبات می‌کند.

۴-۵ . تحلیل قابلیت‌های توسعه و مقیاس‌پذیری

یکی از یافته‌های مهم در طراحی معماری پلتفرمSPC ، سطح بالای توسعه‌پذیری آن است. برخلاف سخت‌افزارهای بسته تجاری، معماری ماژولار این سیستم اجازه می‌دهد تا قابلیت‌های سخت‌افزاری و نرم‌افزاری بدون نیاز به تغییر هسته اصلی پردازنده، ارتقا یابند. تحلیل فنی نشان می‌دهد که پلتفرم طراحی شده در سه محور اصلی قابلیت توسعه دارد:

۱. **توسعه سخت‌افزاری :**وجود رابط‌های استاندارد مانند UART, I۲C, SPI بر روی بردESP۳۲ ، امکان افزودن ماژول‌های جانبی نظیر مودم ۴ G/LTE برای اتصال مستقل اینترنتی، نمایشگر OLED برای نمایش وضعیت سیستم و «ماژول مدیریت باتری (BMS) «برای عملکرد پرتابل را فراهم کرده است.

۲. **توسعه نرم‌افزاری (اکوسیستم باز) :**با پیاده‌سازیAPI های استاندارد RESTful ، توسعه‌دهندگان شخص ثالث می‌توانند اپلیکیشن‌های اختصاصی برای صنایع خاص (مانند اپلیکیشن پاتولوژی برای بیمارستان‌ها) بر روی این بستر ایجاد کنند.

۳. **یکپارچه‌سازی با اینترنت اشیاء :**نتایج تست‌ها نشان داد که این دستگاه می‌تواند فراتر از یک حافظه عمل کرده و به عنوان یک هاب مرکزی (IoT Hub) وظیفه جمع‌آوری داده‌های سنسورهای محیطی و صدور فرمان‌های کنترلی را در محیط‌های صنعتی بر عهده بگیرد.

۶-۴ . ارزیابی امکانات و نسخه‌های تخصصی

انعطاف‌پذیری معماری پیشنهادی این امکان را فراهم می‌آورد که بر اساس هسته مشترک طراحی شده، نسخه‌های متفاوتی برای صنایع گوناگون با ویژگی‌های منحصربه‌فرد تولید گردد. در این بخش، امکان‌سنجی تولید نسخه‌های تخصصی (بانکی، نظامی، سازمانی) بررسی و ویژگی‌های فنی هر یک در مقایسه با نسخه پایه استخراج شده است.

جدول شماره (۳): دسته‌بندی امکانات و ویژگی‌های فنی نسخه‌های تخصصی پلتفرمSPC

نسخه محصول (Series)	کاربرد و مخاطب هدف	امکانات ویژه و توسعه‌یافته (Features)	سطح امنیت
SPC Core (پایه)	کاربران خانگی، دانشجویان	- همگام‌سازی خودکار گالری - پشتیبان‌گیری با یک کلیک - مدیریت فایل تحت وب	استاندارد (-AES ۲۵۶)
SPC Military (نظامی)	میدان نبرد، مراکز دفاعی	- بدنه مقاوم در برابر ضربه و نویز (EMP) - قابلیت انهدام اطلاعات اضطراری - ارتباط رادیویی آفلاین (LoRa)	نظامی (Military Grade)
SPC Bank (بانکی)	شعب بانک، موسسات مالی	- احراز هویت چندعاملی (بیومتریک/NFC) - لاگ‌برداری غیرقابل تغییر (Blockchain-ready) - پشتیبانی از RAID برای افزونگی داده	سازمانی (Enterprise)
SPC Industrial (صنعتی)	کارخانجات، پتروشیمی	- تحمل دمای بالا و محیط‌های خشن - پروتکل‌های صنعتی (Modbus/MQTT)- پایش سلامت سنسورها	صنعتی (Industrial)

نسخه محصول (Series)	کاربرد و مخاطب هدف	امکانات ویژه و توسعه‌یافته (Features)	سطح امنیت
SPC Media (رسانه)	عکاسان، خبرگزاری‌ها	- درگاه کارت حافظه پرسرعت (SD Express) - مودم G۵ داخلی برای ارسال سریع - نمایشگر لمسی جهت پیش‌نمایش	استاندارد پیشرفته

همان‌طور که در جدول (۳) مشاهده می‌شود، هسته پردازشی و امنیتی در تمامی نسخه‌ها یکسان است + ESP۳۲ ATECC۶۰۸A، اما با افزودن ماژول‌های جانبی مانند ماژول LoRa برای نسخه نظامی یا ماژول NFC برای نسخه بانکی، کاربری دستگاه کاملاً تغییر می‌کند. این ویژگی تطبیق‌پذیری باعث می‌شود که هزینه تحقیق و توسعه (R&D) برای تولید محصولات جدید به شدت کاهش یابد، چرا که شالوده اصلی ثابت است.

این معماری ماژولار، پلتفرم SPC را از یک «گجت ذخیره‌سازی» صرف، به یک «زیرساخت استراتژیک» تبدیل می‌کند که قادر است نیازهای متنوع اکوسیستم دیجیتال کشور را با تکیه بر دانش بومی پوشش دهد.

۵ - نتیجه‌گیری

در این پژوهش، چالش‌های امنیتی و عملیاتی مرتبط با ذخیره‌سازی داده‌ها در صنایع حساس و کاربردهای شخصی مورد بررسی قرار گرفت و پلتفرم ابر امن من (SPC) به عنوان یک راهکار بومی و هیبریدی معرفی گردید .نتایج حاصل از طراحی و پیاده‌سازی نمونه اولیه نشان می‌دهد که معماری پیشنهادی با موفقیت توانسته است پارادایم حاکمیت داده را محقق سازد.

برخلاف سرویس‌های ابری عمومی که کاربر را ملزم به پذیرش ریسک‌های حریم خصوصی و هزینه‌های جاری می‌کنند، پلتفرم SPC با تلفیق «امنیت سخت‌افزاری» و «انعطاف‌پذیری نرم‌افزاری»، مدلی را ارائه داده است که در آن مالکیت داده‌ها به طور مطلق در اختیار کاربر باقی می‌ماند . استفاده از چیپ رمزنگاری ATECC۶۰۸A در کنار پردازشگرESP۳۲ ، سطحی از امنیت را فراهم کرده است که پیش از این تنها در تجهیزات گران‌قیمت سازمانی در دسترس بود، اما اکنون با هزینه‌ای مقرون‌به‌صرفه برای طیف وسیعی از کاربران (از دانشجویان تا سازمان‌های نظامی) قابل پیاده‌سازی است.

یافته‌های این تحقیق ثابت می‌کند که رویکرد «ذخیره‌سازی هیبریدی» (ترکیب دسترسی آفلاین و آنلاین)، بهترین پاسخ به نیازهای امنیتی عصر حاضر است .این معماری ماژولار نه تنها وابستگی به زیرساخت‌های خارجی را قطع می‌کند، بلکه با قابلیت توسعه‌پذیری بالا، پتانسیل تبدیل شدن به استاندارد ملی ذخیره‌سازی امن در زیرساخت‌های بانکی و صنعتی کشور را داراست . در نهایت، می‌توان گفت که این پروژه گامی مؤثر در جهت تحقق استقلال دیجیتال و ارتقای تاب‌آوری سایبری در برابر تهدیدات نوین می‌باشد.

۶ - پیشنهاد برای مطالعات آتی

بر اساس معماری ماژولار و یافته‌های حاصل از این پژوهش، مسیر توسعه پلتفرم SPC به سمت تخصصی‌سازی برای صنایع مختلف و ارتقای توان پردازشی ترسیم شده است. پیشنهادهای زیر جهت تکمیل اکوسیستم و پوشش نیازهای بازارهای هدف در فازهای بعدی ارائه می‌گردد.

۶-۱ . ارتقای معماری سخت‌افزاری

اگرچه پردازنده ESP۳۲ برای کاربردهای عمومی و اینترنت اشیاء عملکرد مطلوبی دارد، اما برای پردازش‌های سنگین‌تر و کاربردهای حرفه‌ای، ارتقای سخت‌افزار ضروری است:

۱. **طراحی برد مدار چاپی (PCB) اختصاصی :**جایگزینی ماژول‌های توسعه فعلی با یک برد یکپارچه صنعتی جهت کاهش ابعاد، حذف سیم‌کشی‌های اضافی و افزایش پایداری در برابر نویزهای محیطی.

۲. **استفاده از پردازنده‌های قدرتمندتر (SBC) :** برای نسخه‌های حرفه‌ای(Pro) ، پیشنهاد می‌شود از رایانه‌های تک‌بردی نظیر Raspberry Pi five یا ماژول‌های CM٤ استفاده شود .این ارتقا امکان پیاده‌سازی RAID نرم‌افزاری برای جلوگیری از از دست رفتن داده‌ها و اجرای مدل‌های هوش مصنوعی پیشرفته (مانند تشخیص چهره در تصاویر) را فراهم می‌کند.

۳. **افزودن منبع تغذیه اضطراری UPS داخلی :**تجهیز دستگاه به باتری‌های لیتیومی و مدار مدیریت شارژ (BMS) برای جلوگیری از آسیب دیدن فایل‌ها در صورت قطع ناگهانی برق، به‌ویژه در محیط‌های اداری و آزمایشگاهی.

۶-۲ . توسعه نسخه‌های تخصصی (Vertical Editions)

با توجه به انعطاف‌پذیری نرم‌افزاری پلتفرم، پیشنهاد می‌شود نسخه‌های زیر با امکانات متناسب با هر قشر طراحی و عرضه گردند.

جدول شماره (۴): معرفی نسخه‌های پیشنهادی آینده برای صنایع و گروه‌های کاربری خاص

نام نسخه (Edition)	گروه هدف (Target)	ویژگی‌های سخت‌افزاری و نرم‌افزاری پیشنهادی
SPC Lab (آزمایشگاهی)	مراکز تحقیقاتی و پزشکی	- **سخت‌افزار:** مقاوم در برابر مواد شیمیایی، پورت‌های ایزوله شده. - **نرم‌افزار:** اتصال خودکار به دستگاه‌های آنالیزور، رمزنگاری مطابق استاندارد HIPAA برای پرونده بیماران.
Studio SPC (هنری)	عکاسان، فیلم‌برداران	- **سخت‌افزار:** درگاه کارت حافظه SD Express پرسرعت، بدنه ضدضربه. - **نرم‌افزار:** پشتیبان‌گیری خودکار از دوربین به محض اتصال، پیش‌نمایش فایل‌های RAW روی موبایل.
SPC Enterprise (اداری)	ادارات، حسابداری، شرکت‌ها	- **سخت‌افزار:** استفاده از **Raspberry Pi** برای پردازش بالا، پورت شبکه گیگابیتی. - **نرم‌افزار:** تعریف سطوح دسترسی کارمندان، لاگ‌برداری دقیق از تغییرات فایل‌های مالی، قابلیت اتصال به نرم‌افزارهای حسابداری.

نام نسخه (Edition)	گروه هدف (Target)	ویژگی‌های سخت‌افزاری و نرم‌افزاری پیشنهادی
SPC Kids/Edu (کودکان)	مدارس، خانواده‌ها	- **سخت‌افزار:** طراحی رنگارنگ و مقاوم، فاقد قطعات ریز جدا شونده. - **نرم‌افزار:** قفل کودک (Parental Control)، فیلترینگ محتوای نامناسب، محیط کاربری ساده شده و آموزشی.
SPC Nomad (سیار)	خبرنگاران، طبیعت‌گردان	- **سخت‌افزار:** باتری داخلی با عمر طولانی، ماژول GPS برای ثبت موقعیت فایل‌ها، مودم G/LTE۴ داخلی. - **نرم‌افزار:** آپلود آنی خبرها به محض اتصال به شبکه، دکمه امحای اضطراری داده‌ها. [۶]

۳-۶. توسعه هوش مصنوعی و امنیت

برای فازهای آتی، پیشنهاد می‌شود تمرکز تحقیق و توسعه بر روی موارد زیر معطوف گردد:

- **تشخیص هوشمند محتوا :**پیاده‌سازی الگوریتم‌های یادگیری عمیق[۱] جهت دسته‌بندی خودکار اسناد حسابداری، تشخیص بیماری در تصاویر آزمایشگاهی در نسخه Lab و شناسایی چهره در عکس‌های خانوادگی.
- **امنیت بیومتریک :**افزودن ماژول اثر انگشت خازنی روی بدنه دستگاه برای احراز هویت سخت‌افزاری و حذف نیاز به کلمه عبور در نسخه‌های مخصوص کودکان و سالمندان جهت سهولت استفاده.
- **معماری همتا-به-همتا (P۲P):** توسعه پروتکلی که به چندین دستگاه (مثلاً در یک اداره) اجازه دهد بدون نیاز به سرور مرکزی، نسخه‌های پشتیبان را روی یکدیگر ذخیره کنند تا افزونگی داده‌ها تضمین شود.

تشکر و قدردانی

اکنون که این پژوهش به سرانجام رسیده است، بر خود فرض می‌دانم مراتب سپاس و امتنان عمیق قلبی خویش را تقدیم اساتید گرانقدر و اعضای محترم هیئت علمی **گروه مهندسی کامپیوتر دانشگاه مهارت ملی تبریز** نمایم.

بی‌شک، به ثمر نشستن این تلاش علمی بدون بهره‌مندی از دانش وافر، بینش علمی ژرف و رهنمودهای داهیانه ایشان میسر نمی‌گردید. مشاوره‌های تخصصی و نقدهای سازنده این بزرگواران، چه در تبیین مبانی نظری و تدوین چارچوب پژوهش و چه در هدایت مسیر فنی جهت عبور از چالش‌های پیچیده پیاده‌سازی، چراغ راه من بوده است.

به‌ویژه، از حمایت‌های بی‌دریغ این گروه آموزشی و مساعدت مسئولین محترم در تخصیص منابع و فراهم‌سازی **زیرساخت‌های پردازشی و تجهیزات سخت‌افزاری پیشرفته** که بستر عملیاتی لازم را برای پیاده‌سازی کارآمد مدل‌های پیشنهادی و انجام ارزیابی‌های عملکردی دقیق سامانه در شرایط واقعی مهیا ساخت صمیمانه سپاسگزارم. استخراج نتایج قابل‌اتکا و اعتبارسنجی نهایی یافته‌های این پژوهش، مرهون این پشتیبانی‌های همه‌جانبه علمی و عملی است.

[۱] Deep Learning

مراجع

١. badi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., ... & Zheng, X. (٢٠١٦). TensorFlow: A system for large-scale machine learning. In *12th USENIX symposium on operating systems design and implementation (OSDI 16)* (pp. ٢٦٥-٢٨٣).

٢. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (٢٠١٥). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, ١٧(٤), ٢٣٤٧-٢٣٧٦.

٣. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (٢٠١٠). A view of cloud computing. *Communications of the ACM*, ٥٣(٤), ٥٠-٥٨.

٤. Barry, R. (٢٠١٦). *Mastering the FreeRTOS Real Time Kernel: A Hands-On Tutorial Guide*. Real Time Engineers Ltd.

٥. Buyya, R., Yeo, C. S., & Choo, S. S. (٢٠٠٩). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the ٥th utility. *Future Generation Computer Systems*, ٢٥(٦), ٥٩٩-٦١٦.

٦. Daeman, J., & Rijmen, V. (٢٠٠٢). *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer-Verlag.

٧. Espressif Systems. (٢٠٢٣). *ESP32 Technical Reference Manual (Version 5.1)*. Shanghai: Espressif Systems. Retrieved from https://www.espressif.com

٨. Fielding, R. T. (٢٠٠٠). *Architectural styles and the design of network-based software architectures* (Doctoral dissertation). University of California, Irvine. [Seminal paper on REST API].

٩. Mell, P., & Grance, T. (٢٠١١). *The NIST Definition of Cloud Computing* (NIST Special Publication ٨٠٠-١٤٥). Gaithersburg, MD: National Institute of Standards and Technology.

١٠. Microchip Technology. (٢٠٢٠). *ATECC608A CryptoAuthentication™ Device Summary Datasheet*. Chandler: Microchip Technology Inc.

١١. Ren, W., Wan, X., Gan, P., & Qui, X. (٢٠١٩). Edge computing security: A survey. *Digital Communications and Networks*, ٥(٤), ٤٣٣-٤٤٥.

١٢. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (٢٠١٦). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, ٣(٥), ٦٣٧-٦٤٦.

١٣. Stallings, W. (٢٠١٧). *Cryptography and Network Security: Principles and Practice* (٧th ed.). London: Pearson Education.

١٤. Vue.js. (٢٠٢٤). *The Progressive JavaScript Framework Documentation*. Retrieved from https://vuejs.org/guide/introduction.html

١٥. Wang, Y., & Li, Z. (٢٠٢١). Data sovereignty in the cloud: Challenges and solutions. *Journal of Cloud Computing*, ١٠(١), ١-١٥.

١٦. Zhang, J., & Tao, D. (٢٠٢٠). Empowering things with intelligence: A survey of the progress, challenges, and opportunities in artificial intelligence of things. *IEEE Internet of Things Journal*, ٨(١٠), ٧٧٨٩-٧٨١٧.

۱۷. استالینگز، ویلیام .(۱۳۹۸) .*مبانی امنیت شبکه و رمزنگاری* .(ترجمه عین‌الله جعفرنژاد قمی). بابل: انتشارات علوم رایانه.

۱۸. پرسمن، راجر اس .(۱۴۰۰) .*مهندسی نرم‌افزار: رویکردی عملی (با تاکید بر مهندسی وب)* .(ترجمه سالار و همکاران). تهران: انتشارات نیاز دانش .*مرتبط با توسعه رابط کاربری و پنل وب*

۱۹. تپسکات، دان و تپسکات، الکس .(۱۳۹۷) .*انقلاب بلاک‌چین: چگونه فناوری زیربنای بیت‌کوین پول، کسب‌وکار و جهان را تغییر می‌دهد* .ترجمه مازیار میر). تهران: انتشارات دنیای اقتصاد) .*مرتبط با پیشنهاد توسعه نسخه بانکی و لاگ‌های تغییرناپذیر*

۲۰. جلالی، علی‌اکبر .(۱۳۹۵) .*اینترنت اشیاء: مفاهیم، کاربردها و چالش‌ها* .تهران: انتشارات دانشگاه علم و صنعت ایران.

۲۱. راسل، استوارت و نورویگ، پیتر .(۱۴۰۱) .*هوش مصنوعی: رهیافتی نوین* .(ترجمه رامین رمضانی). تهران: انتشارات نص . *مرتبط با پیشنهاد توسعه هوش مصنوعی در لبه و تشخیص محتوا*

۲۲. شیرین‌کام، دانیال و محمدی، سارا .(۱۳۹۹) .*طراحی رابط کاربری و تجربه کاربری (UI/UX) در سیستم‌های هوشمند* .تهران: انتشارات دیباگران .*مرتبط با طراحی تجربه کاربری برای نسخه‌های کودکان و سالمندان*

۲۳. ملکیان، احسان .(۱۳۹۹) .*رایانش ابری: معماری، پلتفرم‌ها و کاربردها* .تهران: انتشارات نص.

۲۴. وزارت ارتباطات و فناوری اطلاعات .(۱۴۰۱) .*سند تبیین الزامات شبکه ملی اطلاعات و بومی‌سازی زیرساخت‌های داده* .تهران: سازمان فناوری اطلاعات ایران.