(رویداد ملی سپر نوآوری)

مرکز رشد واحدهای فناور نوشهر

"فرم معرفی ایده یا طرح خلاقانه"

۱- **عنوان ایده : نام محصول/سرویس:** نام خلاقانه و مرتبط با ایده‌ی هوش مصنوعی شما: (کوتاه و رسا):

سپر هوشمند آریانا

(AI-Driven Cyber & Defense Shield – ARIANA)

توضیح کوتاه:

سامانه‌ی هوش مصنوعی آریانا، یک «سپر دفاعی هوشمند» برای تشخیص، پیش‌بینی و مقابله‌ی خودکار با تهدیدات سایبری و فیزیکی (عامل و غیرعامل) است که با استفاده از یادگیری ماشین، تحلیل رفتار شبکه و داده‌های محیطی، امنیت زیرساخت‌های حیاتی کشور را در شرایط بحران حفظ می‌کند.

۲- معرفی تیم کاری:

نام و نام خانوادگی ارائه دهندگان (کامل)	تاریخ تولد	مقطع و رشته تحصیلی	پست الکترونیکی	تلفن همراه	محل اشتغال	استان
سحر پاسیار	۱۳۶۸	دکترا-فیزیک حالت جامد	Saharpasyar.uni@gmail.com	۰۹۱۴۳۹ ۴۵۸۲۴	شرکت فناوری های پیشرفته پاسیار	آذربایجان شرقی
صبا شاکر	1378	دکترا- مهندسی نفت	shakerrsabaa@gmail.com	091425 92272	دانشگاه صنعتی تبریز	آذربایجان شرقی

۳- تعریف مسئله (Problem Statement)

توضیح مشکل یا چالش خاصی که در حال حاضر وجود دارد و شما قصد دارید با استفاده از هوش مصنوعی آن را حل کنید.

چرا این مسئله اهمیت دارد؟

در شرایط کنونی، زیرساخت‌های حیاتی کشور (از جمله نیروگاه‌ها، پالایشگاه‌ها، مراکز داده و سیستم‌های شهری) به‌صورت فزاینده‌ای به شبکه‌های هوشمند و سامانه‌های دیجیتال وابسته شده‌اند. این وابستگی باعث شده که هرگونه اختلال سایبری یا فیزیکی بتواند زنجیره‌ای از بحران‌ها را ایجاد کند. چالش اصلی این است که سیستم‌های پدافند فعلی عموماً منفعل و واکنشی‌اند؛ یعنی پس از وقوع حمله یا بحران عمل می‌کنند، نه قبل از آن. همچنین، پدافند عامل (اقدامات فنی و امنیتی) و پدافند غیرعامل (زیرساخت، آموزش، تاب‌آوری اجتماعی) معمولاً به‌صورت جداگانه مدیریت می‌شوند و هیچ سامانه هوشمند یکپارچه‌ای برای تحلیل و تصمیم‌گیری همزمان در این دو حوزه وجود ندارد.

نتیجه‌ی این ناهماهنگی، کاهش سرعت واکنش، افزایش خسارت و ضعف در تشخیص تهدیدات ترکیبی است؛ به‌ویژه در شرایطی که حملات سایبری با بحران‌های طبیعی یا انسانی هم‌زمان می‌شوند (مثلاً حمله به شبکه برق در هنگام زلزله یا سیل).

هوش مصنوعی با قابلیت تحلیل آنی، پیش‌بینی الگوهای حمله و تصمیم‌گیری خودکار می‌تواند این چرخه‌ی واکنشی را به مدیریت پیش‌دستانه و هوشمند بحران تبدیل کند.

چرا این مسئله اهمیت دارد؟

- زیرا امنیت سایبری دیگر فقط یک موضوع فناوری نیست، بلکه یک مؤلفه حیاتی از پدافند ملی و امنیت اجتماعی محسوب می‌شود.
- حملات ترکیبی (سایبری + فیزیکی) به زیرساخت‌ها، حتی در کشورهای توسعه‌یافته، خسارات میلیاردی و بحران‌های انسانی ایجاد کرده‌اند.
- با توجه به رشد وابستگی به سیستم‌های هوشمند و اینترنت اشیا در صنایع ایران، نبود یک سامانه‌ی بومی هوش مصنوعی برای دفاع یکپارچه، یک خلأ استراتژیک ملی به‌شمار می‌رود.
- استفاده از هوش مصنوعی در پدافند، توان تاب‌آوری کشور را افزایش می‌دهد و تصمیم‌گیری‌های انسانی را در شرایط بحرانی تسهیل می‌کند.

۴- راه‌حل(Solution)

- توضیح دهید که چگونه از هوش مصنوعی برای حل این مشکل استفاده می‌کنید.
- روش کار محصول یا سرویس شما چیست؟
- فناوری‌ها یا الگوریتم‌های خاصی که استفاده می‌کنید را توضیح دهید.

سپر هوشمند آریانا (ARIANA) یک سامانه‌ی بومی مبتنی بر هوش مصنوعی ترکیبی (Hybrid AI) است که با تحلیل آنی داده‌های شبکه‌ای، محیطی و انسانی، تهدیدات سایبری و فیزیکی را پیش‌بینی، شناسایی و کنترل می‌کند. این سامانه از چند لایه‌ی اصلی تشکیل شده است:

۱. لایه‌ی پایش هوشمند(Smart Monitoring Layer)
   - داده‌های شبکه، حسگرهای صنعتی(SCADA, IoT) ، تصاویر دوربین‌ها و اطلاعات محیطی را به‌صورت پیوسته جمع‌آوری می‌کند.
   - از الگوریتم‌های یادگیری ماشین (Machine Learning) برای شناسایی الگوهای رفتاری عادی و غیرعادی در شبکه استفاده می‌شود.
۲. لایه‌ی تحلیل و پیش‌بینی(AI Prediction Engine)
   - با استفاده از شبکه‌های عصبی عمیق (Deep Neural Networks) و مدل‌های یادگیری تقویتی (Reinforcement Learning)، رفتار سیستم را تحلیل کرده و وقوع تهدید یا حمله را چند دقیقه تا چند ساعت قبل از وقوع واقعی پیش‌بینی می‌کند.
   - این بخش، داده‌های سایبری را با داده‌های محیطی (مثلاً قطع برق، تغییر دما یا نوسان فشار در تأسیسات) تلفیق می‌کند تا حملات ترکیبی (فیزیکی + سایبری) شناسایی شوند.
۳. لایه‌ی واکنش و خودترمیمی(Self-Healing Defense Layer)
   - در صورت شناسایی تهدید، سامانه به‌صورت خودکار بخش آسیب‌دیده را از شبکه جدا کرده و مسیرهای جایگزین ایمن را فعال می‌کند.
   - از الگوریتم‌های تصمیم‌گیری خودکار (Autonomous Decision Algorithms) برای اجرای واکنش فوری استفاده می‌شود.
۴. لایه‌ی پدافند غیرعامل و تاب‌آوری اجتماعی
   - با تحلیل داده‌های انسانی (رفتار کاربران، اطلاع‌رسانی‌ها، یا الگوهای اشتباه انسانی در شرایط بحرانی)، سامانه به‌صورت هوشمند پیشنهادهایی برای آموزش، هشداردهی یا شبیه‌سازی بحران ارائه می‌دهد.
   - از مدل‌های پردازش زبان طبیعی (NLP) برای تحلیل ارتباطات انسانی و تولید گزارش‌های هشدار استفاده می‌شود.

فناوری‌ها و الگوریتم‌های کلیدی مورد استفاده:

- Machine Learning (ML): برای شناسایی رفتارهای غیرعادی در ترافیک شبکه.
- Deep Neural Networks (DNN): برای پیش‌بینی نوع و شدت تهدید.
- Reinforcement Learning: برای بهینه‌سازی تصمیمات دفاعی خودکار در زمان واقعی.
- Natural Language Processing (NLP): برای تحلیل پیام‌ها، گزارش‌ها و هشدارهای انسانی.
- Edge AI: برای پردازش محلی در محیط‌های صنعتی با تأخیر پایین.
- Federated Learning: جهت آموزش مدل‌های هوش مصنوعی بدون افشای داده‌های حساس ملی.

آریانا با ترکیب هوش مصنوعی، امنیت سایبری و اصول پدافند غیرعامل، یک سپر دفاعی خودکار، بومی و قابل گسترش ایجاد می‌کند که می‌تواند در زیرساخت‌های حیاتی کشور (برق، انرژی، حمل‌ونقل، ارتباطات و مدیریت بحران) به‌کار گرفته شود و زمان واکنش به تهدیدات را تا حد قابل قبولی کاهش دهد.

۵. ارزش پیشنهادی(Value Proposition)

- چه مزیت‌هایی راه‌حل شما نسبت به راه‌حل‌های موجود دارد؟

- چرا مشتریان یا کاربران باید از راه‌حل شما استفاده کنند؟

سپر هوشمند آریانا (ARIANA) با بهره‌گیری از هوش مصنوعی بومی و تحلیل ترکیبی داده‌های سایبری و فیزیکی، راه‌حلی نوآورانه برای دفاع پیش‌دستانه، خودکار و چندلایه در برابر تهدیدات نوین ارائه می‌دهد.

مزیت‌های اصلی نسبت به راه‌حل‌های موجود:

۱. هوشمندی پیش‌دستانه(Proactive Defense) :

در حالی‌که بیشتر سامانه‌های فعلی فقط پس از بروز حمله عمل می‌کنند، آریانا با استفاده از یادگیری ماشین، تهدیدات را پیش از وقوع واقعی شناسایی و خنثی می‌کند.

۲. یکپارچگی پدافند عامل و غیرعامل:

آریانا تنها سامانه‌ای است که همزمان داده‌های شبکه‌ای (حملات سایبری) و داده‌های محیطی و انسانی (پدافند غیرعامل) را تحلیل می‌کند و در نتیجه قادر است بحران‌های ترکیبی را تشخیص دهد.

۳. خودترمیمی و استقلال عملیاتی:

با الگوریتم‌های خودترمیمی، آریانا در صورت بروز حمله یا اختلال، به‌صورت خودکار شبکه را ایزوله و مسیر ایمن جایگزین ایجاد می‌کند؛ بدون نیاز فوری به دخالت انسانی.

۴. بومی‌سازی و امنیت داده‌ها:

در حالی که سامانه‌های خارجی به‌دلیل تحریم یا مخاطرات امنیتی قابل استفاده نیستند، آریانا به‌صورت کامل در داخل کشور توسعه یافته و با الگوریتم‌های فدره (Federated Learning) از افشای داده‌های ملی جلوگیری می‌کند.

۵. قابلیت استفاده در حوزه‌های مختلف:

از زیرساخت‌های صنعتی (نیروگاه، پالایشگاه، آب و فاضلاب) تا مراکز داده، بانک‌ها، و حتی مدیریت بحران شهری قابل پیاده‌سازی است.

چرا مشتریان یا کاربران باید از آریانا استفاده کنند؟

- چون آریانا سرعت تشخیص و واکنش به تهدیدات را تا حد زیادی افزایش می‌دهد.
- چون هزینه‌ی نیروی انسانی، آسیب به زیرساخت و زمان بازیابی را به‌طور چشمگیری کاهش می‌دهد.
- چون برخلاف نرم‌افزارهای خارجی، به‌صورت بومی، ایمن و قابل به‌روزرسانی در شرایط بحرانی کشور طراحی شده است.
- چون می‌تواند در کنار سامانه‌های فعلی پدافند، نقش یک لایه‌ی هوش مصنوعی کمکی (AI Co-Defense) را ایفا کند بدون نیاز به حذف زیرساخت‌های موجود.

۶. تحلیل بازار(Market Analysis)

- مخاطبان هدف شما چه کسانی هستند؟
- اندازه بازار چگونه است؟ چقدر پتانسیل رشد وجود دارد؟

مخاطبان هدف(Target Audience) :

۱. سازمان‌ها و نهادهای زیرساختی حیاتی کشور
   - وزارت نیرو، وزارت نفت، شرکت‌های برق منطقه‌ای، پالایشگاه‌ها، پتروشیمی‌ها، نیروگاه‌ها و صنایع مادر.
   - دلیل: بیشترین آسیب‌پذیری در برابر حملات ترکیبی سایبری و فیزیکی را دارند.
۲. نهادهای امنیتی و پدافند غیرعامل
   - سازمان پدافند غیرعامل کشور، مراکز مدیریت بحران، و فرماندهی‌های استانی.
   - دلیل: نیاز به سامانه‌های بومی برای پیش‌بینی و کنترل هوشمند تهدیدات ملی.
۳. مراکز داده و بانک‌ها
   - شرکت‌های فناوری اطلاعات، بانک مرکزی، بانک‌های بزرگ و دیتاسنترهای حساس.

- دلیل: اهمیت حیاتی در حفظ اطلاعات و پایداری خدمات.

۴. صنایع شهری و زیرساخت‌های هوشمند(Smart City Infrastructure)

- شهرداری‌ها، سامانه‌های حمل‌ونقل هوشمند، آب و فاضلاب، و مدیریت انرژی.
- دلیل: رشد سریع شهرهای هوشمند در ایران و نیاز شدید به دفاع دیجیتال و فیزیکی.

اندازه بازار و پتانسیل رشد(Market Size & Growth Potential) :

- طبق برآوردهای جهانی، بازار امنیت سایبری و پدافند دیجیتال تا سال ۲۰۳۰ بیش از ۲۵۰ میلیارد دلار رشد خواهد داشت.
- در ایران نیز بر اساس داده‌های وزارت ارتباطات و سازمان پدافند غیرعامل، حجم سرمایه‌گذاری سالانه در حوزه امنیت سایبری و زیرساختی حدود ۸ تا ۱۰ هزار میلیارد تومان برآورد می‌شود که هر سال در حال افزایش است.
- با توجه به سیاست‌های جدید کشور در زمینه هوشمندسازی زیرساخت‌ها و صنایع ۴.۰، نیاز به سامانه‌های بومی هوش مصنوعی برای دفاع سایبری در پنج سال آینده حداقل سه برابر خواهد شد.
- سپر هوشمند آریانا می‌تواند با پوشش ٪۵ از بازار داخلی پدافند هوشمند، به ارزش تقریبی ۵۰۰ میلیارد تومان در افق سه‌ساله، جایگاه پیشرو در حوزه دفاع هوشمند ملی پیدا کند.

مزیت بازار بومی:

در حال حاضر هیچ سامانه‌ی هوشمند بومی که بتواند تحلیل ترکیبی پدافند عامل و غیرعامل انجام دهد در کشور وجود ندارد. بنابراین آریانا می‌تواند نخستین پلتفرم ملی هوش مصنوعی برای پدافند سایبری و فیزیکی باشد و از حمایت سازمان‌های راهبردی نیز برخوردار شود.

۷. مزیت رقابتی(Competitive Advantage)

- چه عواملی شما را از رقبا متمایز می‌کند؟
- ویژگی‌های منحصربه‌فرد محصول یا خدمات شما چیست؟

سپر هوشمند آریانا (ARIANA) به‌عنوان یک سامانه‌ی بومی و ترکیبی در حوزه‌ی پدافند عامل و غیرعامل، مجموعه‌ای از ویژگی‌های فناورانه و استراتژیک دارد که آن را از محصولات مشابه داخلی و خارجی متمایز می‌سازد.

۱ .دفاع ترکیبی و چندلایه(Hybrid & Multilayer Defense) :

در حالی‌که اغلب سامانه‌های امنیتی صرفاً بر تهدیدات سایبری تمرکز دارند، آریانا هم‌زمان داده‌های سایبری، محیطی و انسانی را پردازش می‌کند و می‌تواند حملات ترکیبی (Hybrid Threats) را شناسایی کند — قابلیتی که در راهکارهای خارجی نیز به‌ندرت وجود دارد.

۲ .هوش مصنوعی خودآموز و خودترمیمی(Self-Learning & Self-Healing AI) :

آریانا از الگوریتم‌های یادگیری تقویتی و شبکه‌های عصبی پویا استفاده می‌کند تا با هر حمله، تجربه کسب کند و خود را تقویت نماید. در صورت نفوذ، سیستم به‌صورت خودکار بخش آلوده را ایزوله کرده و مسیرهای سالم را فعال می‌کند —بدون دخالت نیروی انسانی.

۳ .بومی‌سازی امنیت داده‌ها(National Data Sovereignty) :

برخلاف نرم‌افزارهای خارجی که داده‌ها را به سرورهای بین‌المللی ارسال می‌کنند، آریانا از معماری Federated Learningاستفاده می‌کند که امکان آموزش مدل‌ها بدون خروج داده‌های حساس از شبکه‌های داخلی را فراهم می‌کند. این ویژگی، اطمینان کامل از امنیت ملی اطلاعات را به همراه دارد.

۴ .سازگاری با زیرساخت‌های صنعتی ایران:

آریانا به‌صورت اختصاصی برای ساختار شبکه‌های صنعتی کشور (از جمله سیستم‌های SCADA، ICS، و شبکه‌های برق منطقه‌ای (طراحی شده و با تجهیزات داخلی و پروتکل‌های بومی کاملاً سازگار است.

۵ .قابلیت یکپارچه‌سازی با سامانه‌های موجود:

بدون نیاز به تغییر زیرساخت یا جایگزینی تجهیزات فعلی، آریانا می‌تواند به‌صورت Plug & Playدر شبکه‌های موجود نصب شود و نقش یک لایه‌ی هوش مصنوعی مکمل پدافند را ایفا کند.

۶ .حمایت از تصمیم‌گیری انسانی در بحران:
سامانه علاوه بر تحلیل فنی، با استفاده از ماژول NLPو تحلیل رفتار انسانی، گزارش‌ها و پیشنهادهای تصمیم‌محور تولید می‌کند تا مدیران بحران و کارشناسان امنیت بتوانند سریع‌تر و دقیق‌تر تصمیم بگیرند.

ترکیب سه عامل زیر، مزیت رقابتی اصلی آریانا را تشکیل می‌دهد:

۱. بومی بودن و امنیت داده‌ها
۲. دفاع چندلایه و پیش‌دستانه با هوش مصنوعی خودآموز
۳. قابلیت اجرا بر روی زیرساخت‌های فعلی بدون تغییر گسترده

به همین دلیل، «سپر هوشمند آریانا» نه‌تنها یک محصول فناورانه، بلکه یک زیرساخت ملی هوشمند برای آینده‌ی پدافند کشور به شمار می‌آید.

۸. مدل کسب و کار(Business Model)

- چگونه قصد دارید از محصول یا خدمات خود درآمدزایی کنید؟
- آیا مدل کسب و کار شما مبتنی بر اشتراک، فروش، تبلیغات یا مدل‌های دیگر است؟

سپر هوشمند آریانا (ARIANA) به‌عنوان یک محصول نرم‌افزاری-تحلیلی(AI-Powered Defense Platform) ، با مدل درآمدی چندلایه طراحی شده است تا قابلیت اجرا در مقیاس ملی و صنعتی را داشته باشد.

۱ .مدل اصلی درآمدزایی: فروش اشتراکی(Subscription-Based Model)

- سازمان‌ها و نهادهای زیرساختی، بر اساس سطح استفاده(Basic, Advanced, Enterprise) ، اشتراک سالانه دریافت می‌کنند.
- خدمات شامل:
  - به‌روزرسانی مداوم الگوریتم‌های هوش مصنوعی،
  - پشتیبانی فنی هفت روز هفته و ۲۴ ساعت،
  - پایش تهدیدات در زمان واقعی،
  - و ارائه گزارش‌های تحلیلی امنیتی است.
- این مدل باعث درآمد پایدار و قابل پیش‌بینی می‌شود و امکان توسعه نرم‌افزار در طول زمان را فراهم می‌کند.

۲ .فروش ماژولار(Modular Licensing) :

- آریانا شامل چند ماژول جداگانه است (مانند: تشخیص تهدید، خودترمیمی، تحلیل رفتاری، مدیریت بحران).
- مشتریان می‌توانند تنها ماژول‌های مورد نیاز خود را خریداری کنند.
- این مدل مناسب صنایع مختلف است و انعطاف بالایی در قیمت‌گذاری ایجاد می‌کند.

۳ .پروژه‌های سفارشی(Custom Deployment for Strategic Clients) :

- برای سازمان‌های حساس (مثلاً نیروگاه‌ها، پالایشگاه‌ها یا وزارتخانه‌ها)، نسخه‌ی اختصاصی و نصب‌شده در محل (On-Premise) ارائه می‌شود.
- درآمد از طریق قراردادهای توسعه، استقرار و آموزش نیروهای داخلی تأمین می‌گردد.

۴ .خدمات هوش دفاعی ابری(AI Defense Cloud Service) :

- در مرحله توسعه آتی، نسخه‌ی ابری آریانا به‌صورت سرویس SaaS قابل ارائه خواهد بود تا نهادهای کوچک‌تر نیز بدون زیرساخت سنگین بتوانند از آن استفاده کنند.
- این نسخه از طریق اشتراک ماهانه و بسته‌های تحلیلی امنیتی درآمدزایی می‌کند.

۵ .مدل همکاری و هم‌افزایی(Partnership & Integration Model) :

- آریانا می‌تواند با شرکت‌های داخلی فعال در حوزه امنیت شبکه و نرم‌افزار همکاری کند و سهم درآمدی از ادغام در محصولات آنها دریافت نماید.
- این رویکرد مسیر رشد بازار و صادرات منطقه‌ای را هموار می‌کند.

مدل ترکیبی آریانا بر پایه‌ی اشتراک + ماژولار + پروژه‌های سفارشی طراحی شده تا:

- درآمد پایدار و قابل گسترش ایجاد کند،
- هزینه اولیه مشتریان را کاهش دهد،
- و امکان گسترش ملی و صادرات فناوری بومی پدافند هوشمند را فراهم آورد.

۹. نقشه راه(Roadmap)

- مراحل توسعه محصول از حال حاضر تا زمان عرضه به بازار
- چشم‌انداز آینده برای گسترش و بهبود محصول چیست؟

مرحله ۱: تحقیق و طراحی مفهومی (۳ تا ۶ ماه)

- تحلیل تهدیدات سایبری و فیزیکی در صنایع زیرساختی کشور.
- طراحی معماری سامانه و انتخاب الگوریتم‌های هوش مصنوعی مناسب (ML، NLP، Reinforcement Learning).
- ایجاد نمونه مفهومی (Prototype) در محیط شبیه‌سازی برای آزمایش الگوریتم تشخیص تهدید.

خروجی :مدل مفهومی سامانه و تست اولیه دقت تشخیص.

مرحله ۲: توسعه نسخه آزمایشی (۶ تا ۱۲ ماه)

- توسعه ماژول‌های اصلی:
  ۱. پایش بلادرنگ(Monitoring)
  ۲. پیش‌بینی تهدید(AI Prediction Engine)
  ۳. واکنش خودکار و خودترمیمی
- اتصال به داده‌های واقعی از شبکه‌های صنعتی یا مراکز داده آزمایشی.
- انجام آزمون‌های امنیتی و ارزیابی عملکرد در شرایط شبه‌بحران.

خروجی : نسخه آزمایشی قابل اجرا (Pilot Version) برای تست در یکی از مراکز داده یا زیرساخت‌های منتخب.

مرحله ۳: اجرای پایلوت صنعتی و اعتبارسنجی ملی (سال دوم)

- استقرار سامانه در یک سازمان زیرساختی (مثلاً شرکت برق منطقه‌ای یا مرکز داده دولتی).
- جمع‌آوری بازخورد، بهینه‌سازی مدل‌های یادگیری، و افزایش دقت سیستم.
- ثبت مالکیت فکری و اخذ تأییدیه از سازمان پدافند غیرعامل کشور.

خروجی :نسخه پایدار و قابل استقرار در سطح ملی.

مرحله ۴: تجاری‌سازی و توسعه بازار (سال سوم)

- عرضه نسخه‌ی رسمی به نهادهای دولتی و صنعتی.

- عقد قراردادهای اشتراکی با سازمان‌های حساس.
- ایجاد تیم‌های فنی برای پشتیبانی و آموزش کاربران.
- آماده‌سازی نسخه ابری (Cloud-Based Defense Platform) برای نهادهای کوچک‌تر.

خروجی :سامانه در مرحله بهره‌برداری تجاری قرار می‌گیرد.

چشم‌انداز آینده(Vision 2030) :

۱. توسعه نسخه آریانا ۲.۰ با قابلیت تحلیل خودکار تصاویر (AI Vision) برای تشخیص تهدیدات فیزیکی از طریق دوربین‌ها.
۲. اتصال سامانه به شبکه ملی هشدار بحران و سامانه‌های هوش اجتماعی جهت افزایش تاب‌آوری شهری و صنعتی.
۳. توسعه همکاری‌های بین‌المللی در قالب صادرات فناوری پدافند هوشمند به کشورهای منطقه.
۴. تشکیل مرکز ملی داده‌های تهدید (National Threat Intelligence Hub) با محوریت آریانا.

نقشه راه آریانا ترکیبی از پژوهش، توسعه، آزمایش میدانی و تجاری‌سازی مرحله‌به‌مرحله است تا محصول در بازه‌ی سه‌ساله از سطح ایده به زیرساخت ملی دفاع هوشمند ارتقاء یابد.

۱۰. چالش‌ها و ریسک‌ها

- چالش‌های فنی، عملیاتی یا بازاریابی که ممکن است با آن مواجه شوید.
- برنامه شما برای غلبه بر این چالش‌ها چیست؟

۱ .چالش فنی(Technical Challenges) :

- پیچیدگی ترکیب داده‌های ناهمگون (سایبری، محیطی و انسانی) و نیاز به الگوریتم‌های دقیق برای تحلیل بلادرنگ.
- نبود دیتاست‌های ملی استاندارد برای آموزش مدل‌های هوش مصنوعی دفاعی.
- ریسک حمله به خود سامانه‌ی دفاعی (Adversarial Attacks) که می‌تواند عملکرد الگوریتم‌ها را مختل کند.

راهکار:

- ایجاد پایگاه داده بومی تهدیدات با همکاری نهادهای امنیتی و صنعتی.
- استفاده از یادگیری فدره (Federated Learning) برای حفظ امنیت داده‌ها در حین آموزش.
- طراحی لایه‌ی ایمن‌سازی مدل با روش‌های Adversarial Trainingجهت افزایش مقاومت سامانه در برابر نفوذ.

۲ .چالش عملیاتی(Operational Challenges) :

- مقاومت اولیه سازمان‌ها در برابر استقرار فناوری‌های جدید به‌ویژه در حوزه‌های حساس.
- نیاز به هماهنگی بین چند نهاد مختلف (پدافند غیرعامل، وزارتخانه‌ها، صنایع و مراکز داده).
- کمبود نیروی انسانی متخصص در حوزه هوش مصنوعی دفاعی.

راهکار:

- اجرای پروژه‌ی پایلوت مشترک با یکی از سازمان‌های زیرساختی جهت اثبات کارایی سامانه.
- برگزاری دوره‌های آموزشی برای مدیران فناوری و امنیت سازمان‌ها.
- ایجاد تیم مشترک بین دانشگاه و صنعت برای توسعه و بومی‌سازی دانش تخصصی پدافند هوشمند.

۳ .چالش اقتصادی و بازاریابی(Economic & Market Risks) :

- محدودیت بودجه در نهادهای دولتی برای سرمایه‌گذاری در فناوری‌های نو.
- طولانی بودن فرآیند تأییدیه‌های امنیتی و مجوزهای رسمی.
- رقابت با راهکارهای خارجی یا نرم‌افزارهای سنتی که ممکن است قیمت پایین‌تری داشته باشند.

راهکار:

- طراحی مدل کسب‌وکار اشتراکی برای کاهش هزینه اولیه سازمان‌ها.
- همکاری با سازمان پدافند غیرعامل برای دریافت تأییدیه ملی امنیتی.(National Security Certification)
- تمرکز بر بومی بودن و امنیت داده‌ها به‌عنوان مزیت کلیدی در برابر محصولات خارجی.

۴ .چالش مقیاس‌پذیری و توسعه آینده(Scalability & Growth Challenges) :

- افزایش حجم داده‌ها و نیاز به پردازش سریع در محیط‌های بزرگ صنعتی.
- هماهنگی میان نسخه‌های محلی (On-Premise) و نسخه ابری.(Cloud Defense)

راهکار:

- استفاده از فناوری‌های Edge AI برای پردازش محلی و کاهش فشار بر سرور مرکزی.
- طراحی معماری مقیاس‌پذیر مبتنی بر Microservices برای گسترش آسان سامانه در سطح ملی.

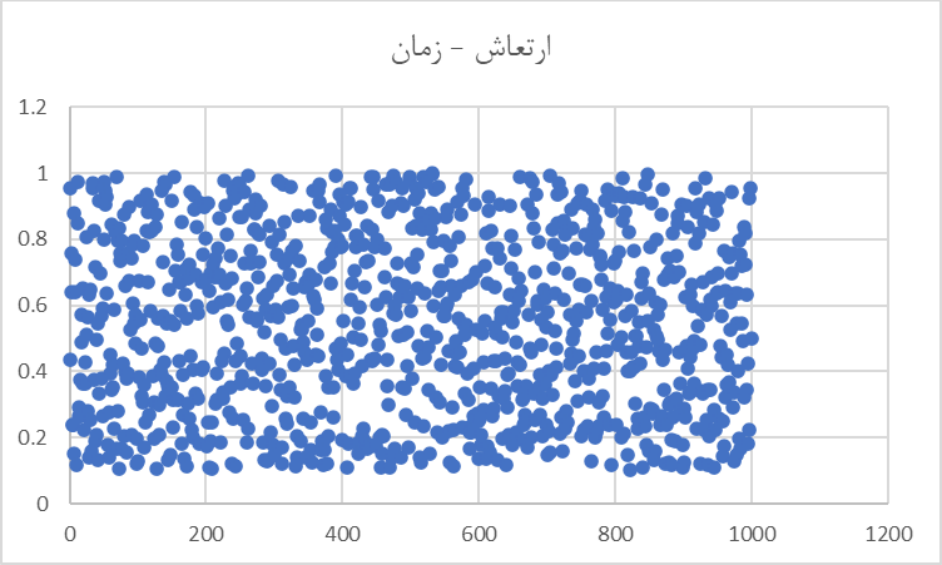
با وجود چالش‌های فنی، اجرایی و بازاری، سپر هوشمند آریانا با تکیه بر طراحی بومی، همکاری بین‌نهادی، و رویکرد تدریجی توسعه (از پایلوت تا تجاری‌سازی)، قادر است بر موانع موجود غلبه کرده و به‌عنوان نخستین پلتفرم ملی دفاع هوشمند ایران تثبیت شود.

۱۱. ARIANA-داشبورد هوشمند دفاع فیزیکی برای شناسایی ناهنجاری‌های صنعتی

در این طرح، داشبوردی هوشمند با نام *آریانا (ARIANA)* بصورت ساده از داده‌های موجود در پایگاه‌های داده، طراحی و توسعه داده شد که با تحلیل هم‌زمان داده‌های دما، فشار و ارتعاش تجهیزات صنعتی، وضعیت عملکرد سیستم را در گذر زمان ارزیابی کرده و به‌صورت خودکار ناهنجاری‌ها را شناسایی می‌کند. این سامانه با استفاده از روش آماری خودسازگار (بدون نیاز به آستانه‌های دستی) شاخصی به نام »امتیاز ناهنجاری Anomaly) « (Scoreرا محاسبه می‌نماید و بر اساس آن، وضعیت تجهیزات را در سه سطح ایمن(SAFE) ، هشدار (ALERT) و بحرانی (CRITICAL) طبقه‌بندی می‌کند.

در بخش تحلیل داده‌ها، نمودار دما بر حسب زمان روند حرارتی سیستم را نشان می‌دهد که افزایش پیوسته یا جهشی آن بیانگر افزایش اصطکاک، ضعف در خنک‌کنندگی یا شروع خرابی حرارتی است. نمودار فشار بر حسب زمان تغییرات فشار فرآیندی را در طول بهره‌برداری نمایش می‌دهد؛ ثبات نسبی فشار نشان‌دهنده‌ی عملکرد پایدار بوده و نوسانات ناگهانی آن می‌تواند نشانه‌ی نشت، انسداد یا کاویتاسیون باشد. نمودار ارتعاش بر حسب زمان نیز شاخص سلامت مکانیکی تجهیزات را بازتاب می‌دهد؛ افزایش دامنه ارتعاش معمولاً با بروز عدم‌تعادل، خرابی بلبرینگ یا سایش قطعات متحرک همراه است.

در نسخه‌ی نهایی داشبورد آریانا، این سه متغیر به‌صورت تلفیقی تحلیل شده‌اند و نتایج آن در قالب نمودارهای خطی، ستونی، پراکندگی و دایره‌ای در محیط Excel و قابل اجرا در محیط پایتون با کد نویسی به نمایش درآمده‌اند. برای نمونه در شکل ۱ تغییرات ارتعاش بر حسب زمان آورده شده است. این داشبورد علاوه بر پایش وضعیت عملیاتی، توانایی ارائه‌ی هشدارهای زودهنگام را دارد و می‌تواند به‌عنوان یک ابزار تصمیم‌یار در حوزه‌ی نگهداشت پیشگیرانه و مدیریت ریسک صنعتی به کار رود.



شکل ۱ ارتعاش بر حسب زمان

۱۲. نتیجه‌گیری و درخواست(Closing and Ask)

- خلاصه‌ای از ایده و اهمیت آن.
- درخواست مشخص (مثلاً جذب سرمایه، همکاری‌های استراتژیک، مشاوره یا منابع خاص)

سپر هوشمند آریانا یک سامانه‌ی بومی مبتنی بر هوش مصنوعی است که با هدف افزایش تاب‌آوری سایبری و دفاع غیرعامل در زیرساخت‌های حیاتی کشور طراحی شده است.
این سامانه با بهره‌گیری از تحلیل بلادرنگ داده‌ها، یادگیری ماشین، و پیش‌بینی هوشمند تهدیدات، می‌تواند ضمن کاهش زمان واکنش در بحران‌ها، از بروز خسارات گسترده‌ی سایبری و فیزیکی جلوگیری کند.
در شرایطی که تهدیدات نوین، ترکیبی از حملات دیجیتال و اختلالات زیرساختی هستند، آریانا می‌تواند نقش سپر هوشمند ملی را ایفا کند؛ سامانه‌ای که بین انسان، ماشین و داده پیوندی هوشمند برقرار می‌سازد و به تصمیم‌گیران امکان می‌دهد در لحظه‌ی بحران، به‌جای واکنش، پیش‌بینی و پیشگیری کنند.
به منظور توسعه و استقرار «سپر هوشمند آریانا»، نیازمند همکاری در محورهای زیر هستیم:

۱. حمایت مالی و تسهیلات تحقیقاتی برای توسعه نسخه پایلوت در یکی از سازمان‌های زیرساختی کشور (به‌ویژه حوزه انرژی یا ارتباطات).
۲. همکاری استراتژیک با سازمان پدافند غیرعامل، وزارت ارتباطات و مراکز داده ملی برای به‌اشتراک‌گذاری داده‌ها و دریافت مجوزهای امنیتی.
۳. دسترسی به متخصصان حوزه امنیت سایبری و هوش مصنوعی جهت تکمیل تیم فنی و ارتقای سامانه.

با حمایت از این طرح، می‌توان گام مؤثری در بومی‌سازی فناوری‌های دفاع هوشمند، ارتقاء تاب‌آوری ملی، و ایجاد اشتغال در حوزه امنیت سایبری پیشرفته برداشت.
سپر هوشمند آریانا، نه‌تنها یک محصول فناورانه، بلکه پایه‌ای برای نسل آینده‌ی سامانه‌های دفاعی کشور است.

آیا نمونه اولیه ایده یا طرح خود را ساخته اید؟ بلی ☐ خیر ■

آیا آمادگی ارائه نمونه اولیه محصول یا خدمت خود را جهت بررسی داوران دارید؟ بلی ■ خیر ☐