(رویداد ملی سپر نوآوری)

"فرم معرفی ایده یا طرح خلاقانه"

نکته مهم: لطفا فایل تکمیل شده را در دو قالب Word و PDF در آدرس وبسایت www.separnoavari.ir بارگذاری فرمائید.

۱- عنوان ایده : نام محصول/سرویس: نام خلاقانه و مرتبط با ایده‌ی محورهای رویداد سپر نوآوری طرح یا ایده ی شما: (کوتاه و رسا):

شبیه‌ساز جنگ سایبری مبتنی بر دوقلوهای دیجیتال

۲- معرفی تیم کاری:

نام و نام خانوادگی ارائه دهندگان (کامل)	تاریخ تولد	مقطع و رشته تحصیلی	پست الکترونیکی	تلفن همراه	محل اشتغال	استان
حسن صدیق	۱۳۶۴/۱۰/۸	کارشناسی ارشد مهندسی کنترل	hasan.sedigh@shahroodut.ac.ir	۰۹۰۲۵۹۶۳۳۸۰	شاهرود	سمنان
سیده فهیمه دلپاک	۱۳۶۵/۱/۱۶	کارشناسی ارشد هوش مصنوعی	etajco@gmail.com	۰۹۱۵۶۹۶۲۸۶۸	مشهد	خراسان
محمد مهدی احمدی	۱۳۸۱/۴/۲۷	کارشناسی مهندسی الکترونیک	Ahmadi٦١@gmail.com	۰۹۰۳۳۸۸۵۳۵۲	مشهد	خراسان

۳- تعریف مسئله (Problem Statement)

در شرایط کنونی، زیرساخت‌های حیاتی کشورها (نظیر شبکه برق، مخابرات، سامانه‌های نظامی، مالی و حمل‌ونقل) بیش از هر زمان دیگری در معرض حملات سایبری پیچیده قرار دارند.

یکی از چالش‌های اساسی در پدافند سایبری، نبود محیط‌های تمرینی واقعی، امن و پویا برای آموزش نیروهای دفاعی و آزمون سناریوهای حمله و دفاع است.

محیط‌های شبیه‌سازی موجود معمولاً:

ایستا و غیرواقعی‌اند؛

رفتار دینامیک شبکه‌های واقعی را بازتاب نمی‌دهند؛

نمی‌توانند تأثیر حملات را در مقیاس بزرگ پیش‌بینی کنند.

برای حل این مشکل، می‌توان از دوقلوی دیجیتال زیرساخت‌های سایبری استفاده کرد — مدلی زنده و پویا از سامانه‌های واقعی که رفتار آن‌ها را در زمان واقعی یا نزدیک به آن بازسازی می‌کند. با ترکیب این فناوری با هوش مصنوعی و یادگیری ماشین، می‌توان یک شبیه‌ساز جنگ سایبری طراحی کرد که در آن هم مدافع و هم مهاجم در محیطی واقع‌گرایانه تعامل دارند.

۴- محور ایده

نوآوری در حوزه توان سایبری و پدافند

دبیرخانه مسابقات : استان مازندران – نوشهر – خیابان رازی- خیابان ۲۲ بهمن – کوچه مسجد- ساختمان مرکز رشد و نوآوری نوشهر

تلفن و نمابر دبیرخانه : ۵۲۱۴۱۱۷۳–۰۱۱ کسب اطلاعات بیشتر از طریق پیام رسان های ایتا یا واتس آپ به شماره ۰۹۰۵۵۷۸۴۹۷۹ پیام نموده

یا با دبیرخانه رویداد (مهندس ترابی با شماره ۰۹۱۱۳۹۵۱۹۷۹) تماس حاصل نمایید.

لطفا فایل تکمیل شده در در دو قالب Word و PDF در آدرس وبسایت www.separnoavari.ir بارگذاری نمایید.

۵- راه‌حل(Solution)

مشکل: نبود محیط تمرینی واقعی و امن برای آموزش نیروهای دفاع سایبری و آزمایش سناریوهای حمله و دفاع.

راه حل نوآورانه ما:

دوقلوی دیجیتال زیرساخت‌های حیاتی: با شبیه‌سازی دقیق شبکه‌ها، سرورها، پروتکل‌ها و نقاط آسیب‌پذیر، یک بازتاب زنده از سامانه‌های واقعی ایجاد می‌کنیم.

هوش مصنوعی برای مهاجم و مدافع: الگوریتم‌های هوش مصنوعی رفتار مهاجم و مدافع را شبیه‌سازی می‌کنند تا سناریوهای حمله و دفاع پویا و واقع‌گرایانه باشند.

محیط امن و قابل تکرار: امکان تمرین و تحلیل واکنش‌ها بدون خطر برای زیرساخت واقعی فراهم می‌شود.

یادگیری و بهینه‌سازی: داده‌های شبیه‌سازی‌شده برای بهبود تاکتیک‌های دفاعی و خودکارسازی تصمیم‌گیری استفاده می‌شوند.

با ترکیب این دو فناوری، مشکل نبود محیط آموزشی و آزمایش واقعی برای پدافند سایبری به صورت مؤثر حل می‌شود.

روش کار محصول به صورت مرحله‌ای:

ایجاد دوقلوی دیجیتال (Digital Twin)

شناسایی عناصر حیاتی شبکه: سرورها، پایگاه داده، تجهیزات شبکه، پروتکل‌ها.

ایجاد مدل دیجیتال که رفتار واقعی شبکه را بازتولید کند.

شبیه‌سازی حمله و دفاع

استفاده از هوش مصنوعی برای شبیه‌سازی مهاجم: تولید حملات با سناریوهای واقعی، شامل بدافزارها، نفوذ شبکه، حملات DDoS و فیشینگ.

شبیه‌سازی رفتار مدافع: واکنش نیروها و سامانه‌های دفاعی در مقابل حملات.

تحلیل و تصمیم‌گیری

جمع‌آوری داده‌ها از شبیه‌ساز (میزان موفقیت حمله، واکنش مدافع، نقاط ضعف).

استفاده از الگوریتم‌های یادگیری ماشین و تقویتی برای پیشنهاد بهینه‌ترین واکنش‌ها.

بازخورد و بهینه‌سازی

به‌روزرسانی دوقلوی دیجیتال و الگوریتم‌ها بر اساس داده‌های جدید.

امکان تمرین مداوم و یادگیری مستمر برای تیم‌های دفاع سایبری.

۶- ارزش پیشنهادی(Value Proposition)

ارزش اصلی این محصول، ترکیب آموزش، تحلیل و بهینه‌سازی تاکتیک‌ها در یک محیط شبیه‌سازی واقع‌گرایانه و امن است که هیچ سیستم سنتی تمرینی یا شبیه‌سازی ساده‌ای نمی‌تواند ارائه دهد.

۷- تحلیل بازار(Market Analysis)

بازار «شبیه‌سازی بحران سایبری (Cyber Crisis Simulator)» در سال ۲۰۲۴ حدود ۱.۱۵۸ میلیارد دلار بوده است.

این بازار پیش‌بینی می‌شود تا سال ۲۰۳۵ به حدود ۳.۵ میلیارد دلار برسد، با نرخ رشد مرکب حدود ۱۰.۶٪ در بازه ۲۰۲۵-۲۰۳۵.

بازار «میدان نبرد دیجیتال (Digital Battlefield)» — که شامل شبیه‌سازی‌ها، فناوری‌های دیجیتال نظامی، دوقلوهای دیجیتال و غیره است — طبق گزارش‌های مختلف، در سال ۲۰۲۵ حدود ۷۰.۴ میلیارد دلار بوده و تا سال ۲۰۳۰ به حدود ۱۵۷ میلیارد دلار می‌رسد، با CAGR حدود ۱۷.۴٪.

بازار «شبیه‌سازی و تمرین نظامی (Military Simulation & Virtual Training)» در سال ۲۰۲۴ حدود ۱۴.۳۷ میلیارد دلار بوده و پیش‌بینی می‌شود تا سال ۲۰۳۵ به حدود ۲۵ میلیارد دلار برسد، با CAGR حدود ۵.۱۵٪.

بازار «دوقلوهای دیجیتال برای امنیت سایبری (Digital Twin Cybersecurity)» نیز نرخ رشد قوی دارد: پیش‌بینی شده که بازار از حدود ۲.۵ میلیارد دلار در سال ۲۰۲۵ رشد کند و تا سال ۲۰۳۳ به حدود ۸.۷ میلیارد دلار برسد، با CAGR حدود ۲۲.۴٪.

۸- مزیت رقابتی(Competitive Advantage)

- ترکیب دوقلوی دیجیتال و هوش مصنوعی
- شبیه‌سازی سناریوهای پیچیده و یادگیری خودکار
- محیط امن و قابل اعتماد برای زیرساخت‌های حیاتی
- قابلیت مقیاس‌پذیری و انعطاف‌پذیری
- تحلیل و داشبورد هوشمند
- تمرکز بر نیازهای واقعی و کاربرد عملیاتی

۹ - مدل کسب و کار(Business Model)

۱-مشتریان هدف (Customer Segments)

سازمان‌های دفاعی و نظامی: وزارت دفاع، نیروهای مسلح، مراکز فرماندهی و کنترل.

زیرساخت‌های حیاتی: نیروگاه‌ها، شبکه‌های برق، آب، گاز، صنایع حساس.

سازمان‌های بزرگ فناوری و مالی: بانک‌ها، مراکز داده بزرگ، شرکت‌های فناوری اطلاعات.

مراکز آموزشی و تحقیقاتی: دانشگاه‌ها، موسسات پژوهشی و مدارس تخصصی امنیت سایبری.

۲-ارزش پیشنهادی (Value Proposition)

محیط امن و واقع‌گرایانه برای تمرین و شبیه‌سازی حملات سایبری.

بهینه‌سازی تاکتیک‌ها و تصمیم‌گیری دفاعی با کمک هوش مصنوعی و دوقلوی دیجیتال.

کاهش هزینه و زمان تمرین و تست واکنش در زیرساخت واقعی.

گزارش‌ها و داشبوردهای هوشمند برای تحلیل عملکرد و نقاط ضعف شبکه.

۳-کانال‌های توزیع (Channels)

فروش مستقیم به سازمان‌های دولتی و نظامی (G۲B).

قرارداد با شرکت‌های فناوری و زیرساخت برای ارائه سرویس شبیه‌ساز (B۲B).

ارائه به مراکز آموزشی و دانشگاه‌ها به شکل سرویس ابری یا نرم‌افزار محلی.

نمایشگاه‌ها و کنفرانس‌های تخصصی دفاع و امنیت سایبری برای معرفی و جذب مشتری.

۴-روابط با مشتری (Customer Relationships)

پشتیبانی حرفه‌ای ۷/۲۴: برای سازمان‌های حیاتی و نظامی.

آموزش و راه‌اندازی: جلسات آموزشی و راهنمایی برای کار با شبیه‌ساز.

به‌روزرسانی مداوم سناریوها و الگوریتم‌ها: به شکل اشتراک یا قرارداد سالانه.

همکاری در توسعه سناریوهای جدید: مشتریان می‌توانند نیازهای خاص خود را بهبود دهند و سفارشی کنند.

۵-منابع درآمد (Revenue Streams)

فروش نرم‌افزار / لایسنس: پرداخت یک‌باره برای نصب و استفاده.

مدل اشتراک (Subscription): دسترسی به سناریوهای جدید، به‌روزرسانی‌ها و الگوریتم‌های هوش مصنوعی.

شبیه‌سازی به‌عنوان سرویس (Simulation-as-a-Service): ارائه محیط تمرین ابری و پویا برای مشتریان.

خدمات مشاوره و سفارشی‌سازی: طراحی سناریوهای خاص، تحلیل داده‌ها و آموزش نیروهای سازمان.

۶-فعالیت‌های کلیدی (Key Activities)

توسعه دوقلوی دیجیتال زیرساخت‌ها و شبکه‌ها.

طراحی الگوریتم‌های هوش مصنوعی برای شبیه‌سازی حمله و دفاع.

ایجاد سناریوهای متنوع و قابل تکرار برای آموزش و تمرین.

ارائه داشبوردهای تحلیلی و گزارش‌های دقیق عملکرد.

پشتیبانی و به‌روزرسانی مداوم محصول.

۷-منابع کلیدی (Key Resources)

تیم توسعه نرم‌افزار و هوش مصنوعی.

متخصصان امنیت سایبری و مهندسی شبکه.

زیرساخت سخت‌افزاری برای شبیه‌سازی و پردازش داده‌ها.

داده‌های واقعی شبکه و زیرساخت برای آموزش دوقلوهای دیجیتال و AI.

۸- شرکای کلیدی (Key Partners)

شرکت‌های فناوری و امنیت سایبری برای همکاری فنی و داده‌ای.

مراکز تحقیقاتی و دانشگاه‌ها برای توسعه الگوریتم‌ها و سناریوهای جدید

سازمان‌های دولتی برای دسترسی به داده‌های عملیاتی و تایید امنیتی.

تامین‌کنندگان سخت‌افزار برای سرورها و شبکه‌های شبیه‌سازی.

۹-ساختار هزینه (Cost Structure)

توسعه و نگهداری نرم‌افزار و الگوریتم‌ها.

هزینه سخت‌افزار و زیرساخت پردازشی.

حقوق تیم متخصصان امنیت سایبری و توسعه نرم‌افزار.

هزینه‌های تحقیق و توسعه سناریوهای جدید.

هزینه‌های فروش، بازاریابی و آموزش مشتری.

۱۰ - نقشه راه(Roadmap)

فاز ۱: تحقیق و توسعه (۰–۱۲ ماه)

هدف: ایجاد پایه فنی و الگوریتمی محصول

تحلیل دقیق نیازهای مشتریان (سازمان‌های دفاعی، زیرساخت‌های حیاتی و دانشگاه‌ها)

جمع‌آوری داده‌های واقعی و شبیه‌سازی زیرساخت‌های حیاتی

طراحی و توسعه دوقلوی دیجیتال شبکه‌ها و زیرساخت‌ها

طراحی الگوریتم‌های هوش مصنوعی برای شبیه‌سازی مهاجم و مدافع

توسعه اولیه داشبورد تحلیل و گزارش عملکرد

تعریف سناریوهای پایه آموزشی و دفاعی

ارزیابی امنیت و اعتمادپذیری محصول

نقطه عطف: نسخه اولیه MVP آماده و قابل نمایش به مشتریان بالقوه

فاز ۲: آزمایش و اعتبارسنجی (۱۲–۲۴ ماه)

هدف: تست واقعی و بهبود محصول بر اساس بازخورد

آزمایش MVP با مشتریان منتخب یا مراکز آموزشی و تحقیقاتی

جمع‌آوری داده‌های عملکرد و بازخورد برای بهبود الگوریتم‌ها و سناریوها

توسعه سناریوهای پیچیده حمله چندمرحله‌ای و هوش مصنوعی تطبیقی

ارتقای دقت دوقلوی دیجیتال و تعامل با تجهیزات واقعی (Integration)

طراحی مدل شبیه‌سازی به‌عنوان سرویس (Simulation-as-a-Service)

تهیه مستندات و بسته‌های آموزشی برای مشتریان

اطمینان از تطابق با استانداردها و مقررات امنیتی

نقطه عطف: آزمایش موفق MVP با حداقل یک سازمان دفاعی یا زیرساخت حیاتی

فاز ۳: تجاری‌سازی و گسترش بازار (۲۴–۴۸ ماه)

هدف: ورود به بازار و ایجاد جریان درآمد پایدار

معرفی رسمی محصول به بازار داخلی و بین‌المللی

عقد قراردادهای G۲B و B۲B با سازمان‌های دفاعی و زیرساخت‌ها

ارائه مدل اشتراک سالانه و شبیه‌سازی به‌عنوان سرویس

گسترش سناریوها و محیط‌ها برای صنایع مختل

بازاریابی از طریق نمایشگاه‌ها، کنفرانس‌های تخصصی و همکاری با دانشگاه‌ها

بهبود مستمر الگوریتم‌های هوش مصنوعی با داده‌های جدید

تحقیق و توسعه برای افزودن قابلیت‌های جدید (مانند واقعیت افزوده یا شبیه‌سازی بلادرنگ شبکه‌های گسترده)

نقطه عطف: کسب سهم بازار و تثبیت محصول به عنوان ابزار استاندارد شبیه‌سازی سایبری

۱۱- چالش‌ها و ریسک‌ها

- پیچیدگی دوقلوی دیجیتال: ایجاد نسخه دقیق و لحظه‌ای از زیرساخت‌ها و شبکه‌های واقعی بسیار دشوار است و نیاز به داده‌های کامل و دقیق دارد.
- شبیه‌سازی حملات پیچیده: طراحی الگوریتم‌های هوش مصنوعی که رفتار مهاجم و دفاع‌کننده را واقع‌گرایانه شبیه‌سازی کنند، چالش بزرگی است.
- ادغام با سیستم‌های واقعی: اتصال دوقلوی دیجیتال به تجهیزات و شبکه‌های واقعی بدون خطر برای عملیات زنده دشوار است.
- مقیاس‌پذیری: افزایش اندازه شبکه‌ها یا زیرساخت‌های شبیه‌سازی شده، نیاز به منابع سخت‌افزاری و پردازشی بسیار بالایی دارد.
- ورود به بازار دفاعی: فروش به سازمان‌های نظامی و زیرساخت حیاتی معمولاً نیازمند تاییدیه‌ها و مجوزهای امنیتی است
- رقابت با شرکت‌های بزرگ: رقبا ممکن است محصول مشابه یا پیشرفته‌تری داشته باشند، مخصوصاً شرکت‌های جهانی دفاعی و شبیه‌سازی.
- پذیرش فناوری جدید: سازمان‌ها ممکن است در ابتدا نسبت به اعتماد به شبیه‌سازی دیجیتال و AI مقاومت داشته باشند.
- نیاز به تیم‌های متخصص: مهندسان دوقلوی دیجیتال، هوش مصنوعی و امنیت سایبری باید به‌صورت هماهنگ کار کنند.
- آموزش و پذیرش کاربر: کاربران باید با محیط شبیه‌ساز و داشبوردهای پیچیده آشنا شوند تا بیشترین بهره را ببرند.

این پروژه با چالش‌های فنی و امنیتی بالا و ریسک‌های بازار و قانونی قابل توجه همراه است، اما با برنامه‌ریزی دقیق، فازبندی توسعه، همکاری با مشتریان کلیدی و رعایت استانداردهای امنیتی، می‌توان این ریسک‌ها را به حداقل رساند.

۱۲- نتیجه‌گیری و درخواست(Closing and Ask)

- شبیه‌ساز جنگ سایبری مبتنی بر دوقلوهای دیجیتال و هوش مصنوعی با هدف ایجاد یک محیط شبیه‌سازی واقع‌گرایانه برای تمرین، تست و تحلیل دفاع سایبری در شبکه‌ها و زیرساخت‌های حیاتی، با استفاده از ترکیب دوقلوی دیجیتال و هوش مصنوعی.

در صورت حمایت قابلیت های بسیار کاربردی این طرح به توان دفاعی کشور و نیروهای مسلح مان کمک شایانی خواهد نمود.

در صورتی که ایده یا طرح شما ماهیت نظامی / امنیتی یا دفاعی دارد ضمن عنوان کلیات و ثبت ایده در وبسایت جهت ارسال پروپوزال بهمراه جزییات ایده و به جهت راهنمایی بیشتر به شماره ۰۹۰۵۵۷۸۴۹۷۹ پیام تا با شما تماس حاصل شده و راهنمایی لازم صورت پذیرد.

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 ☐

* لطفا فرم تکمیل شده را حداکثر تا تاریخ ۱۴۰۴/۰۸/۲۴ در آدرس وبسایت www.separnoavari.ir بارگذاری نمایید.

دبیرخانه مسابقات : استان مازندران – نوشهر – خیابان رازی- خیابان ۲۲ بهمن – کوچه مسجد- ساختمان مرکز رشد و نوآوری نوشهر
تلفن و نمابر دبیرخانه : ۵۲۱۴۱۱۷۳–۰۱۱ کسب اطلاعات بیشتر از طریق پیام رسان های ایتا یا واتس آپ به شماره ۰۹۰۵۵۷۸۴۹۷۹ پیام نموده
یا با دبیرخانه رویداد (مهندس ترابی با شماره ۰۹۱۱۳۹۵۱۹۷۹) تماس حاصل نمایید.

لطفا فایل تکمیل شده در در دو قالب Word و PDF در آدرس وبسایت www.separnoavari.ir بارگذاری نمایید.