۱۰ فناوری نوظهور
در عصر امنیت داده

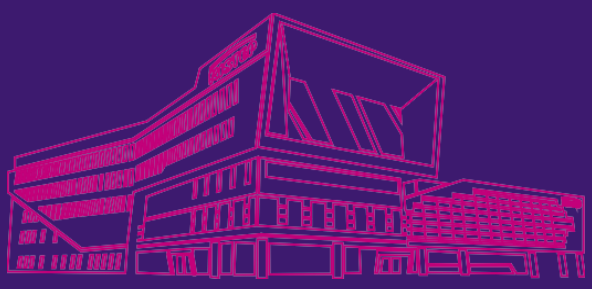
KISTEP 10

EMERGING TECHNOLOGIES

KISTEP 10 Emerging Technologies in the Era of Data Security

گزارش کوتاه

فناوری‌های نوظهور



دبیرخانه برنامه ملی
آینده‌نگاری علم و فناوری ایران

KISTEP Korea Institute of S&T Evaluation and Planning

۱۰ فناوری نوظهور در عصر امنیت داده

تدوین: مؤسسه ارزیابی و برنامه‌ریزی علم و فناوری کره جنوبی (KISTEP)

مترجم: فریدالدین رضائیان

ناشر: دبیرخانه برنامه ملی آینده‌نگاری علم و فناوری ایران

سال نشر: ۱۴۰۲

نشانی: تهران، خیابان ملاصدرا، خیابان شیخ بهایی شمالی، کوچه لادن، پلاک ۲۰

www.iranforesight.isti.ir

10 EMERGING TECHNOLOGIES

فناوری حفاظت از امنیت
کاربر در محیط‌های مجازی
همچون متاورس

فناوری رمزنگاری کوانتومی
برای امنیت کامل داده در
عصر کوانتوم

پیشگیری از جرایم سایبری و
ردیابی سوء استفاده از
فناوری‌های دیجیتال جدید

فناوری امنیت ابر/لبه برای
استفاده از یک محیط
مجازی امن

فناوری تضمین اعتبار
رمزارزها به منظور ارتقاء
امنیت اقتصاد دیجیتال

فناوری امنیت یکپارچه
زیرساخت استفاده از
وسایل نقلیه خودران

فناوری کنترل و پاسخ خودکار
امنیت سایبری هوشمند
مبتنی بر هوش مصنوعی

KISTEP

فناوری امنیت شبکه‌های
5G و 6G

فناوری اتوماسیون تشخیص
آسیب‌پذیری‌های امنیتی زنجیره
تأمین و سیستم تولید

فناوری رمزنگاری عملکردی و
کاربردی مانند رمزنگاری
هومومورفیک در راستای امنیت
داده‌ها و حفظ حریم خصوصی

۱

فناوری امنیت یکپارچه زیرساخت استفاده از وسایل نقلیه خودران

تعریف فناوری امنیت یکپارچه زیرساخت استفاده از وسایل نقلیه خودران، نوعی فناوری امنیت یکپارچه می‌باشد که برای ادغام و عملکرد با سیستم‌های اطلاعات زیرساخت اجتماعی مختلف ضروری است.

دامنه امنیت ابری در محیط وسایل نقلیه خودران، امنیت شبکه ارتباطی وسایل نقلیه خودران بر پایه اترنت، امنیت ارتباطات سیگنال کنترل، امنیت اطلاعات مربوط به تبادل انرژی، امنیت اطلاعات مربوط به تهدیدات ایمنی.

- امنیت ابری در محیط وسایل نقلیه خودران

امنیت ابری در محیط وسایل نقلیه خودران به تدابیر و روش‌هایی اطلاق می‌شود که برای حفاظت از سیستم‌ها و داده‌های مبتنی بر ابر در حوزه وسایل نقلیه خودران مورد استفاده قرار می‌گیرد. این شامل پرداختن به آسیب‌پذیری‌ها، تعریف نیازمندی‌های امنیتی و مورد استفاده‌های مختلف رکوردهای داده‌های رویداد مبتنی بر ابر در یک محیط متحرک می‌باشد.

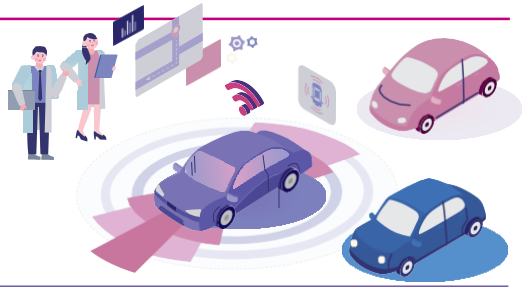
- امنیت شبکه ارتباطی وسایل نقلیه خودران بر پایه اترنت

پروتکل‌های استاندارد تعریف شده که اتصالات مبتنی بر پروتکل آی‌پی را از طریق اترنت فراهم می‌کنند (مانند DoIP یا XCP) برای ارتباط بین محیط‌های خارجی و وسایل نقلیه خودران استفاده می‌شوند.

ضرورت همانطورکه تحول دیجیتال به سرعت رخ می‌دهد، وسایل نقلیه خودران نیز با محیطی از دستگاه‌های اطلاعات مستقل به شکل یک اکوسیستم همکاری و اطلاعاتی در ارتباط هستند که در آن تبادلات فعال اطلاعات انجام می‌شود، بنابراین نیاز به امنیت به طور مداوم در حال افزایش است.

روندهای جهانی به منظور دستیابی به هژمونی زودهنگام در بازار وسایل نقلیه خودران، سیاست‌های گوناگونی توسط کشورهای مختلف اتخاذ می‌شوند و در عین حال مسائل امنیتی مرتبط نیز مورد بحث و بررسی قرار می‌گیرند.

- کره جنوبی: در استراتژی توسعه صنعت خودروهای آینده که در اکتبر ۲۰۱۹ اعلام شد، دولت برنامه‌ریزی می‌کند تا به هژمونی زودهنگام در بازار وسایل نقلیه خودران دست یابد و اولین جاده کاملاً خودکار جهان را تا سال ۲۰۲۷ افتتاح نماید.
- ایالات متحده آمریکا: برنامه «خودروهای خودران نسل ۴» در سال ۲۰۲۰، در زمینه‌های گسترده‌ای مانند تولید پیشرفته، هوش مصنوعی، آموزش علوم، فناوری، مهارت‌های STEM و توسعه منابع انسانی، وظایف همکاری در تحقیقات پایه، زیرساخت‌ها، تنظیمات، مالیات، مالکیت فکری و محیط زیست ارائه شد تا فناوری خودروی خودران را توسعه دهد.
- اروپا: شورای امنیت حمل و نقل اروپا (ETSC) با همکاری شورای مشاوره تحقیقات حمل و نقل جاده ای اروپا (ERTRAC)، به تازگی یک نقشه راه مشترک به نام "نقشه راه خودروهای خودران" به منظور تدوین استانداردهای این حوزه آماده کرده است.



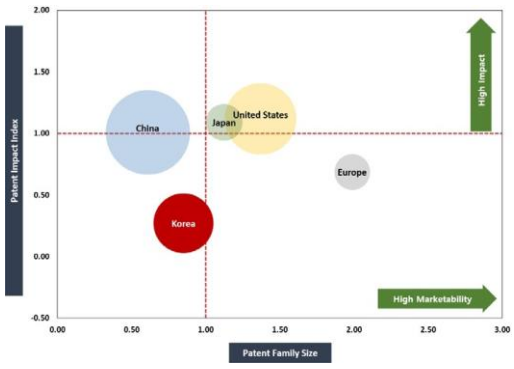
چشم‌انداز آینده در سال ۲۰۳۰ در حال حاضر برنامه‌های بسیار زیادی برای استفاده از پهپادها و وسایل نقلیه خودران در حال توسعه هستند زیرا صنعت در نظر دارد تا سال ۲۰۳۰ به دستاورد خودروهای کاملاً خودران برسد. همچنین، هنگامی که برنامه‌های شهر هوشمند و دیگر برنامه‌ها به مرحله تجاری رسیدند، شبکه‌های اطلاعاتی زیرساخت‌های اجتماعی به وسایل نقلیه خودران متصل می‌شوند.

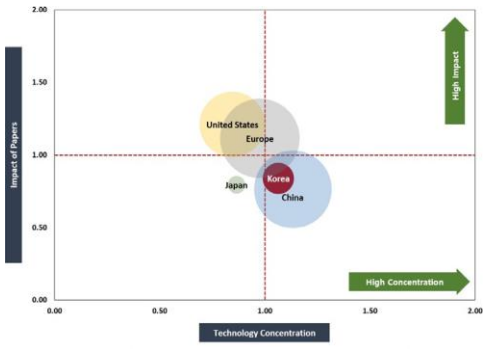
- همانطور که برنامه‌های شهر هوشمند و سایر طرح‌ها به مرحله تجاری رسیده‌اند، شبکه‌های اطلاعاتی زیرساخت‌های اجتماعی به وسایل نقلیه خودران متصل می‌شوند.

ارتباط با سایر فناوری‌های نوظهور این فناوری رابطه‌ای همزمان و تکمیلی با فناوری امنیت ابری و لبه (Edge) و فناوری کنترل امنیت سایبری هوشمند مبتنی بر هوش مصنوعی و فناوری پاسخگویی خودکار دارد.

- فناوری امنیت ابری و لبه (Edge) برای استفاده از محیط مجازی امن، به طور نزدیکی با امنیت ابری در محیط وسایل نقلیه خودران مرتبط است و مسائل امنیت مشترکی را به اشتراک می‌گذارد.
- فناوری کنترل امنیت سایبری هوشمند مبتنی بر هوش مصنوعی و فناوری پاسخگویی خودکار برای نظارت و پاسخگویی در وسایل نقلیه خودران بسیار حائز اهمیت است.

تجزیه و تحلیل جامع مقالات و پتنت‌ها بر اساس یک تجزیه و تحلیل از مقالات و پتنت‌های انتشار یافته در طول ۱۲ سال گذشته در کره جنوبی، ایالات متحده آمریکا، ژاپن، اروپا (۲۸ کشور از جمله انگلستان) و چین، چین بیشترین تمرکز فناوری را دارد، در حالی که اروپا بزرگترین اندازه خانواده پتنت (PFS) را دارد.





۲

فناوری کنترل و پاسخ خودکار امنیت سایبری هوشمند مبتنی بر هوش مصنوعی

تعریف در پی گسترش هوش مصنوعی، فناوری کنترل و پاسخ خودکار امنیت سایبری هوشمند مبتنی بر هوش مصنوعی به منظور محافظت در برابر نفوذ به زیرساخت‌های ملی/اجتماعی و شبکه‌های سازمانی از طریق حملات سایبری دقیق و خودکار توسط هکرهای ماشینی هوش مصنوعی به کار می‌رود.

دامنه دامنه اصلی فناوری کنترل امنیت سایبری هوشمند مبتنی بر هوش مصنوعی و پاسخگویی خودکار به طور کلی در سه حوزه فناوری هماهنگی امنیتی و اتوماسیون امنیت (SOA) فناوری پاسخ به حوادث امنیتی (SIRP) و فناوری اطلاعات تهدید (TIP) دسته‌بندی می‌شود.

- SOA، هماهنگی امنیتی و اتوماسیون

این فناوری با ادغام راه حل های امنیتی ناهمگن در یک پلت فرم واحد و استانداردسازی گردش کار امنیتی برای هر تجهیزات، وظایف امنیتی تکراری را خودکار می کند.

- SIRP، سامانه‌های پاسخ به حوادث امنیتی

این فناوری حادثه‌های امنیتی را دسته‌بندی می‌کند و تصمیم‌گیری خودکار را بر اساس سطوح تهدیدات امنیتی از پیش تعیین شده برای هر نوع حادثه هک در صورت وقوع یک حادثه امنیتی، پشتیبانی می‌کند.

- TIP، پلتفرم‌های اطلاعات تهدید

این فناوری داده‌های تهدید داخلی و خارجی را در زمان واقعی جمع‌آوری و همبسته‌سازی می‌کند تا تجزیه و تحلیل تهدیدات امنیتی در سازمان‌ها را پشتیبانی کند.

ضرورت تکامل به عنوان یک فناوری که وظایف ساده و تکراری کنترل امنیتی متمرکز بر انسان را ساده‌تر می‌کند، رویدادهای امنیتی مختلف را به سرعت و با دقت تجزیه و تحلیل می‌کند و فرآیند پاسخ‌گویی را به صورت خودکار انجام می‌دهد، ضرورت دارد.

روندهای جهانی در حال حاضر پروژه‌های تحقیق و توسعه و سرمایه‌گذاری‌های ملی زیادی به منظور توسعه این فناوری در حال انجام است و در کشورهای بزرگ، دستورات اداری و قابلیت‌های امنیت سایبری در حال تقویت است.

- کره جنوبی: وزارت علوم و فناوری اطلاعات و مؤسسه فناوری اطلاعات و ارتباطات (IITP) یک نقشه راه توسعه فناوری میان‌مدت تا بلندمدت برای اتوماسیون کنترل امنیت هوشمند ایجاد کرده‌اند و در پروژه‌های ملی تحقیق و توسعه به منظور تأمین فناوری‌های مربوطه سرمایه‌گذاری می‌کنند.
- ایالات متحده آمریکا: در سال ۲۰۲۱، دولت بایدن یک «فرمان اجرایی درباره بهبود امنیت سایبری کشور» صادر کرد تا قابلیت پاسخگویی دولت فدرال آمریکا به حملات سایبری را تقویت کند.

- اروپا: در حال حاضر، کمیسیون اروپا در تلاش است تا با ایجاد ساز و کار حفاظت از حقوق دیجیتال، قوانین و استراتژی‌های امنیت سایبری به عنوان یک سیاست تحول دیجیتال برای دهه دیجیتال اروپا قابلیت‌های امنیت سایبری در سطح کلان اتحادیه اروپا را تقویت کند.

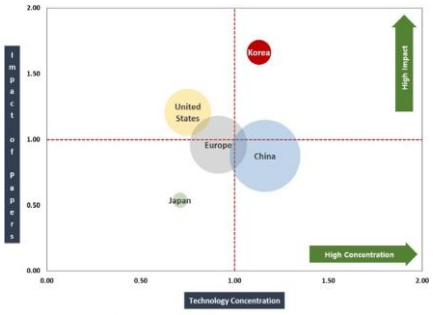
چشم‌انداز آینده در سال ۲۰۳۰ روندهای جدید بازاری مانند رشد سرویس‌های همگانی، ظهور اقتصاد داده و فروشگاه‌های خودکار که فناوری‌های پیشرفته را در بر می‌گیرند، شکل می‌گیرد و بازار فناوری کنترل و پاسخ خودکار امنیت سایبری هوشمند مبتنی بر هوش مصنوعی نیز با میانگین نرخ سالانه ۱۵٫۶ تا ۲۰٫۴ درصد با یک رشد سریع مواجه می‌شود.

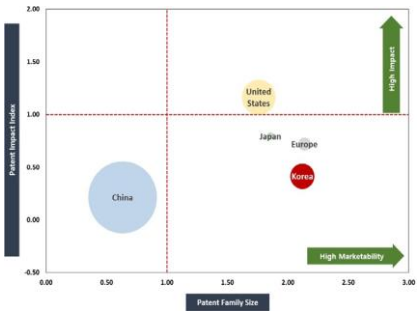
- بازار فناوری پاسخ اتوماتیک و هماهنگی امنیتی در سراسر جهان در انتظار رشد سالانه ۱۵٫۶٪ است، از ۱٫۱۶ میلیارد دلار (۱٫۲ تریلیون وون کره‌ای) در سال ۲۰۲۱ به ۲٫۷۷ میلیارد دلار (۳ تریلیون وون کره‌ای) در سال ۲۰۲۷.

ارتباط با سایر فناوری‌های نوظهور کنترل و پاسخ خودکار امنیت سایبری هوشمند مبتنی بر هوش مصنوعی به عنوان فناوری عناصر امنیتی مرتبط با اتوماسیون و هوشمندی به سایر فناوری‌های نوظهور بسیار مرتبط است.

- فناوری کنترل و پاسخ خودکار امنیت سایبری هوشمند مبتنی بر هوش مصنوعی یک فناوری مرتبط با هوش و اتوماسیون مراکز کنترل امنیتی در سازمان‌ها است و می‌تواند به عنوان یک فناوری عنصری مرتبط با اتوماسیون و هوش در سایر زمینه‌ها استفاده شود.

تجزیه و تحلیل جامع مقالات و پتنت‌ها بر اساس تحلیلی از مقالات و اختراعات در طی ۱۲ سال گذشته در کره جنوبی، ایالات متحده آمریکا، ژاپن، اروپا (۲۸ کشور اروپایی از جمله انگلستان) و چین، چین بیشترین تمرکز فناوری را دارد در حالی که اروپا بزرگترین اندازه خانواده اختراعات (PFS) را دارد.





۳

فناوری امنیت شبکه‌های 5G و 6G

تعریف **فناوری امنیت شبکه 5G/6G یک فناوری برای تجزیه و تحلیل، شناسایی و پاسخ به تهدیدات سایبری است که در بستر شبکه‌های ارتباطی تلفن همراه (5G و 6G) مورد استفاده قرار می‌گیرد. این فناوری شامل مجموعه‌ای از تکنیک‌ها، پروتکل‌ها و ابزارهاست که هدف آن حفاظت از ساختار شبکه، اطلاعات و خدمات در مقابل نفوذهای امنیتی، دسترسی غیرمجاز و فعالیت‌های ناسالم است.**

دامنه **فناوری امنیت شبکه 5G/6G به فناوری تجزیه و تحلیل آسیب پذیری شبکه دسترسی بی سیم، فناوری امنیتی RAN باز، فناوری امنیتی رایانش لبه با دسترسی چندگانه (MEC)، فناوری تجزیه و تحلیل و کنترل تهدیدات امنیتی هوشمند، فناوری ارتباطات رمزنگاری کوانتومی و فناوری امنیتی شبکه تخصصی طبقه‌بندی می شود.**

- **فناوری تجزیه و تحلیل آسیب‌پذیری شبکه دسترسی بی‌سیم**

  این فناوری، آسیب‌پذیری‌های امنیتی ناشی از تنوع فناوری‌های دسترسی مانند ابراتصالی و شبکه‌های غیرزمینی از دستگاه‌های مختلف را، از جمله سنسورها، دستگاه‌های قابل استفاده بر روی بدن، خودروها، پهپادها و ربات‌ها، تجزیه و تحلیل کرده و با برخورداری از پاسخ‌های مناسب به آن‌ها، به این آسیب‌پذیری‌ها پاسخ می‌دهد.

- **فناوری امنیتی RAN باز**

  این فناوری، آسیب‌پذیری‌های امنیتی ناشی از ورود اطلاعات، مجازی‌سازی و باز بودن زیرساخت بی‌سیم 5G/6G را تجزیه و تحلیل کرده و با برخورداری از پاسخ‌های مناسب به آن‌ها، به این آسیب‌پذیری‌ها پاسخ می‌دهد. به عنوان مثال، از این فناوری در استانداردسازی شبکه جلوه‌یابی 5G متن‌باز برای راه‌اندازی شبکه‌های تعریف شده توسط نرم‌افزار و رابط‌های بین دستگاه‌های بی‌سیم و توزیع در ایستگاه‌های پایه استفاده می‌شود.

ضرورت **برای برآورده کردن نیازهای ارتباط فوق‌العاده متصل (mMTC)، تاخیر بسیار پایین (uRLLC) و سرعت بسیار بالا (eMBB) شبکه 5G، ضرورت توسعه فناوری‌های اساسی به منظور تقویت امنیت از مرحله استانداردسازی مشخصات فناوری 6G تا به کارگیری و به‌روزرسانی پایدار خدمات همگرایی مبتنی بر 6G در تمام صنایع وجود دارد.**

روندهای جهانی **فناوری‌های تجاری سازی 5G و 6G در کره جنوبی در حال توسعه هستند و تلاش‌های سیاستی در سراسر جهان برای تأمین فناوری‌ها نیز ادامه دارد.**

- **کره جنوبی: فرآیند استانداردسازی رابط جلوه‌یابی باز 5G مبتنی بر RAN باز توسط ارائه‌دهندگان خدمات ارتباطی داخلی و مؤسسه تحقیقات الکترونیک و ارتباطات (ETRI) حمایت و ترویج می‌شود.**

- ایالات متحده آمریکا: از سال ۲۰۱۷، سازمان پروژه‌های پژوهشی پیشرفته دفاع (DARPA)، یک مؤسسه پژوهشی تحت نظر وزارت دفاع، اقدام به انجام تحقیق و توسعه بلندمدت در حوزه فناوری 6G به منظور تأمین فناوری باند فرکانسی بالا (در حد تراهرتز) نموده است.
- ژاپن: به منظور جبران تأخیر در ساختاردهی شبکه پس از تجاری شدن 5G، ارائه دهنده خدمات ارتباطی سیار نسل چهارم، از ابتدا ترویج استفاده از فناوری RAN باز در شبکه تجاری را ادامه می‌دهد.

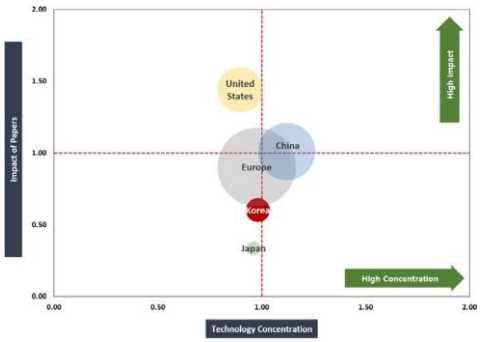
چشم‌انداز آینده در سال ۲۰۳۰ انتظار می‌رود استانداردهای 6G برای 3GPP بین سال‌های ۲۰۲۸ تا ۲۰۳۰ ایجاد شود و به همین ترتیب، تحقیقاتی درباره آسیب‌پذیری‌های امنیتی به صورت فعال انجام شود.

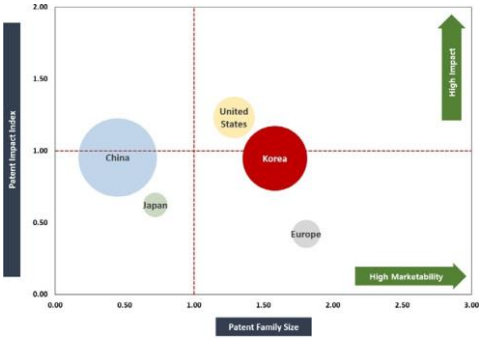
- با ارتقاء ترمینال‌ها، فرایندهای مبتنی بر هوش مصنوعی در تمام حوزه‌ها از ترمینال تا شبکه‌های ارتباطی سیار، توسعه خواهند یافت. همچنین، فناوری‌های همکاری برای حفاظت از داده‌ها و پاسخ به تهدیدات امنیتی نیز فعال خواهند شد.

ارتباط با سایر فناوری‌های نوظهور این فناوری به طور نزدیکی با فناوری کنترل امنیت سایبری هوشمند/پاسخ خودکار، فناوری رمزنگاری کوانتومی برای امنیت داده‌ها و فناوری امنیت ابری/لبه (Cloud/Edge) مرتبط است.

- فناوری امنیت شبکه 5G/6G به طور نزدیکی با فناوری کنترل امنیت سایبری هوشمند/پاسخ خودکار، فناوری رمزنگاری کوانتومی برای امنیت داده‌ها و فناوری امنیت ابری/لبه (Cloud/Edge) مرتبط است و انتظار می‌رود که همکاری‌ها در این حوزه افزایش یابد.

تجزیه و تحلیل جامع مقالات و پتنت‌ها بر اساس تحلیلی از مقالات و اختراعات در طی ۱۲ سال گذشته در کره جنوبی، ایالات متحده آمریکا، ژاپن، اروپا (۲۸ کشور اروپایی از جمله انگلستان) و چین، چین بیشترین تمرکز فناوری را دارد در حالی که اروپا بزرگترین اندازه خانواده اختراعات (PFS) را دارد.





۴

فناوری اتوماسیون تشخیص آسیب‌پذیری‌های امنیتی زنجیره تأمین و سیستم تولید

تعریف فناوری استفاده از هوش مصنوعی برای شناسایی خودکار آسیب‌پذیری‌های امنیتی در سیستم‌های فناوری اطلاعات، از جمله زنجیره‌های تأمین سخت‌افزار و نرم‌افزار (شامل شبکه‌های توزیع) و برنامه‌های شخص ثالث، و پاسخگویی خودکار تهدیدات امنیتی مورد استفاده قرار می‌گیرد.

دامنه فناوری اتوماسیون تشخیص آسیب‌پذیری امنیتی، یک فناوری اصلی در حوزه امنیت است که می‌توان آن را بر اساس نوع تحلیل به دو دسته فناوری تحلیل آسیب‌پذیری نرم‌افزاری و فناوری تحلیل آسیب‌پذیری سخت‌افزاری تقسیم کرد.

- فناوری تجزیه و تحلیل آسیب‌پذیری نرم‌افزاری

  فناوری تجزیه و تحلیل آسیب‌پذیری نرم‌افزاری را می‌توان به دو بخش فناوری تجزیه و تحلیل آسیب‌پذیری کد منبع و فناوری تجزیه و تحلیل آسیب‌پذیری باینری (معکوس کاری) تقسیم کرد.

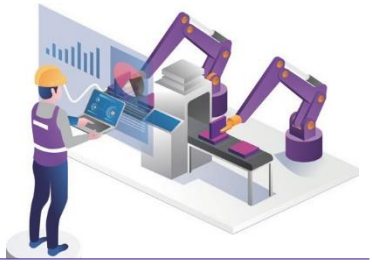
- فناوری تجزیه و تحلیل آسیب‌پذیری سخت‌افزاری

  این فناوری با تحلیل میکروچیپ‌ها (IC chips)، بردهای PCB و فریمور (firmware) که قسمت‌های تشکیل‌دهنده تجهیزات سخت‌افزاری هستند، آسیب‌پذیری‌ها را تجزیه و تحلیل می‌کند.

ضرورت توسعه این فناوری از آنجایی ضروری است که هک کارخانه های هوشمند می تواند به فضای فیزیکی واقعی گسترش یابد و ضربه سنگینی به فروش شرکت ها وارد کند و حتی با ایجاد مشکلات ایمنی در تاسیسات تولیدی منجر به تلفات انسانی شود.

روندهای جهانی در سطح جهانی، سیاست و حمایت مالی برای مدیریت ریسک سخت افزار/نرم افزار زنجیره تامین شتاب می گیرد.

- کره جنوبی: «فناوری اتوماسیون تشخیص آسیب‌پذیری امنیتی زنجیره تأمین و سیستم تولید» در سال ۲۰۲۰ به عنوان یکی از ۱۲ فناوری هدف در «نقشه راه تحقیق و توسعه فناوری ICT سال ۲۰۲۵ » انتخاب شد و توسعه فناوری سازمان‌محور نیز در حال پیشرفت است.
- ایالات متحده آمریکا: سیاست‌های اولویت‌بندی برای مدیریت ریسک سیستم‌های سخت‌افزاری و نرم‌افزاری زنجیره تأمین در حال پیشرفت است و توسعه استانداردها و ابزارهای مرتبط با فرآیند ارزیابی ریسک برای محصولات و خدمات زنجیره تأمین فناوری اطلاعات و ارتباطات در حال ترویج فعال است.
- چین: با اجرای «قانون امنیت شبکه»، «مدیریت امنیت و نظارت بر تأسیسات، عملیات، نگهداری و استفاده از شبکه‌ها در محدوده جمهوری خلق چین، مطابق این قانون خواهد بود» (۲۰۱۹).



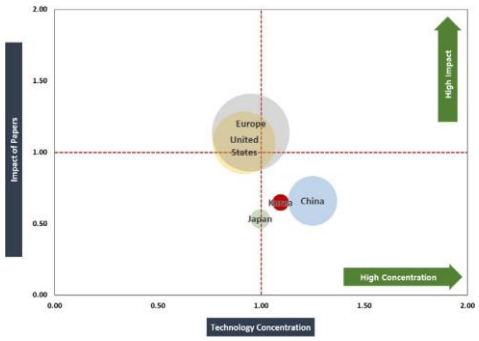
چشم‌انداز آینده در سال ۲۰۳۰ در حالی که وارد دوران جنگ سرد جدید در نتیجه رقابت آمریکا و چین برای هژمونی فناوری، بحران کووید-۱۹ و جنگ اوکراین-روسیه می‌شویم، انتظار می‌رود کشورها قوانین امنیت سایبری را تقویت کنند تا صنایع خود را محافظت کرده و از سرریز فناوری صنعتی جلوگیری کنند که به عنوان یک مانع تجاری جدید در تجارت جهانی تلقی خواهد شد.

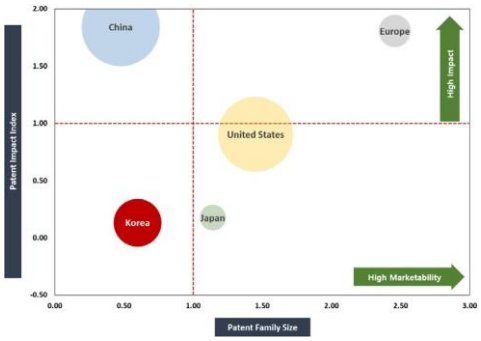
- **داشتن فناوری‌های خودکار می‌تواند غربالگری تهدیدات امنیتی سایبری و آسیب‌پذیری‌های امنیتی از قبل یا در زمان واقعی هنگام ورود فناوری‌های خارجی و صادرات فناوری‌های داخلی را بهبود بخشیده و امنیت را با خیال راحت کنترل کند.**

ارتباط با سایر فناوری‌های نوظهور فناوری اتوماسیون تشخیص آسیب‌پذیری امنیتی می‌تواند به فناوری امنیت یکپارچه زیرساخت استفاده از وسایل نقلیه خودران و فناوری پیگیری جرم سایبری کمک کند.

- **فناوری اتوماسیون تشخیص آسیب‌پذیری امنیتی سیستم، یک فناوری کلیدی است که با تجزیه و تحلیل خودکار آسیب‌پذیری‌ها در طول طراحی، ساخت و عملیات فناوری امنیت یکپارچه زیرساخت استفاده از وسایل نقلیه خودران، به پیشگیری از وقوع حوادث امنیتی کمک می‌کند.**
- **فناوری اتوماسیون تشخیص آسیب‌پذیری امنیتی سیستم، در درون خود فناوری تجزیه و تحلیل آسیب‌پذیری نرم‌افزاری را نیز در بر دارد که می‌تواند به عنوان پایه‌ای برای فناوری پیگیری جرم سایبری با تجزیه و تحلیل سوابق دیجیتالی جنایتکاران عمل کند.**

تجزیه و تحلیل جامع مقالات و پتنت‌ها بر اساس تحلیلی از مقالات و اختراعات در طی ۱۲ سال گذشته در کره جنوبی، ایالات متحده آمریکا، ژاپن، اروپا (۲۸ کشور اروپایی از جمله انگلستان) و چین، چین بیشترین تمرکز فناوری را دارد در حالی که اروپا بزرگترین اندازه خانواده اختراعات (PFS) را دارد.





۵

فناوری رمزنگاری عملکردی و کاربردی مانند رمزنگاری هomomورفیک در راستای امنیت داده‌ها و حفظ حریم خصوصی

تعریف فناوری رمزنگاری عملکردی و کاربردی برای افزایش بهره‌وری داده‌ها در حفظ اطلاعات حیاتی ، تقویت حریم خصوصی در طول چرخه استفاده از داده‌ها و پشتیبانی از استفاده ایمن از آنها، مورد بهره‌برداری قرار می‌گیرد.

دامنه این فناوری شامل حفاظت از حریم خصوصی تفاضلی، رمزنگاری مانند رمزنگاری هomomورفیک و تولید داده مصنوعی که به صورت مصنوعی داده‌ها را برای یادگیری هوش مصنوعی تولید می‌کند تا یک محیط داده‌ی ایمن را در برابر تهدیدات نفوذ داده ایجاد کند، می‌شود.

- حفاظت از حریم خصوصی تفاضلی

  این فناوری با افزودن نویز به داده‌ها، ویژگی‌های آماری را حفظ کرده و در عین حال اطلاعات خصوصی موجود در داده‌ها را محافظت می‌کند.

- رمزنگاری هomomورفیک

  برخلاف روش‌های رمزنگاری سنتی، این فناوری امکان تجزیه و تحلیل داده‌ها و عملیات بر روی آن‌ها را در حالت رمزنگاری فراهم می‌کند. این فناوری سبب ارتقاء چشمگیر امنیت شده، اما سرعت پردازش داده‌ها نسبت به متن ساده به دلیل افزایش حجم داده پس از رمزنگاری کاهش می‌یابد.

- تولید داده مصنوعی

  این فناوری با حذف اطلاعات شخصی حساس و در عین حفظ حریم خصوصی، داده‌های مصنوعی را برای یادگیری مدل هوش مصنوعی ایجاد می‌کند.

ضرورت با افزایش خدمات مختلفی که از اطلاعات شخصی استفاده می‌کنند به دلیل به اشتراک گذاری داده‌ها، نیاز به یک پلتفرم اشتراک گذاری کلان‌داده‌ها، سفارشی شده برای هدف تجزیه و تحلیل داده‌ها برای افزایش بهره‌وری از داده‌های به اشتراک گذاشته شده و در عین حال جلوگیری از وقوع حوادث مربوط به سرریز داده‌ها، لازم است.

روندهای جهانی در حال حاضر در سرتاسر دنیا توسعه فناوری رمزنگاری و تصویب قوانین مرتبط برای حفاظت ایمن از اطلاعات شخصی در حال پیشرفت می‌باشد.

- کره جنوبی: در محیط اقتصاد داده، فناوری‌های رمزنگاری در حال توسعه و پیشرفت هستند تا به منظور جلوگیری از سرریز و سوءاستفاده از اطلاعات، اطلاعات مهم را به صورت ایمن محافظت کنند. این فناوری‌ها شامل پوشش اطلاعات حساس در داده‌ها، جلوگیری از استخراج و شناسایی مجدد داده‌های بدون شناسه می‌شوند.

- ایالات متحده آمریکا: اگرچه استفاده از داده‌ها به طور کلی مهم‌تر از حفاظت از حریم خصوصی در نظر گرفته می‌شود، اما در سال‌های اخیر حفظ حریم خصوصی توجهات فراوانی را به خود جلب نموده و قوانین متعددی در ایالات مختلف برای دستیابی به این مهم در حال تدوین است.
- اروپا: قانون کلی حفاظت اطلاعات شخصی (۲۰۱۸) شامل تعریف اطلاعات شخصی، اعمال خارج از کشور، اجازه برای پردازش نام مستعارها، شفاف‌سازی حقوق اشخاص و افزایش تعهدات پردازشگران اطلاعات شخصی است.

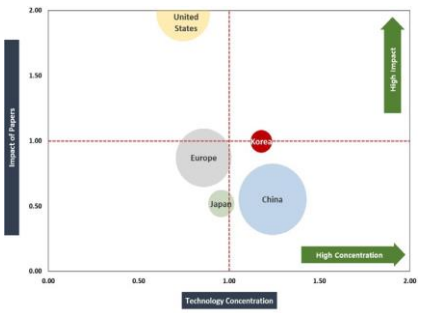
چشم انداز آینده در سال ۲۰۳۰ انتظار می رود امنیت داده مبتنی بر توزیع بیش از پیش مورد توجه قرار گیرد و فناوری هایی مانند حفظ حریم خصوصی تفاضلی و رمزنگاری هومومورفیک تکامل یابند.

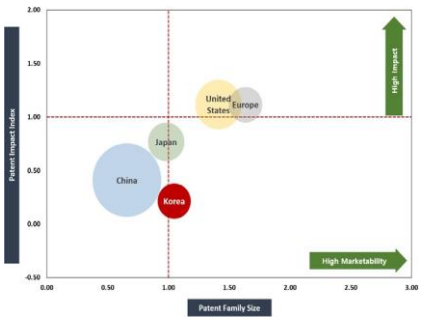
- تقاضا برای فناوری «شناسایی همه‌منظوره» افزایش می‌یابد و انتظار می‌رود امنیت داده‌های توزیع‌محور به جای امنیت داده‌های ذخیره‌محور مورد توجه قرار گیرد.
- تعیین سطح مناسب نویز برای اعمال در روش‌های حفظ حریم خصوصی تفاضلی برای حفظ ارزش داده‌ها (در عین ناشناس بودن آنها) مهم است.

ارتباط با سایر فناوری‌های نوظهور فناوری رمزنگاری هومومورفیک می‌تواند در زمینه‌های گوناگون نیازمند امنیت (مانند مراقبت‌های پزشکی، مالی، خدمات عمومی و دفاع ملی) مورد استفاده قرار گیرد.

- شتاب‌دهنده سخت‌افزاری رمزنگاری هومومورفیک، می‌تواند در یادگیری هوش مصنوعی مورد استفاده قرار گرفته و همزمان حریم خصوصی را نیز تضمین کند. با استفاده مستقیم از داده‌های رمزنگاری شده، خدمات سفارشی شده متنوعی بر اساس اطلاعات مختلف در بخش‌های پزشکی، مالی، عمومی و دفاع ملی ارائه می‌شود.

تجزیه و تحلیل جامع مقالات و پتنت‌ها بر اساس تحلیلی از مقالات و اختراعات در طی ۱۲ سال گذشته در کره جنوبی، ایالات متحده آمریکا، ژاپن، اروپا (۲۸ کشور اروپایی از جمله انگلستان) و چین، چین بیشترین تمرکز فناوری را دارد در حالی که اروپا بزرگترین اندازه خانواده اختراعات (PFS) را دارد.





۶

فناوری حفاظت از امنیت کاربر در محیط‌های مجازی همچون متاورس

تعریف فناوری حفاظت از امنیت کاربران، زیرساخت‌ها و خدمات در فضای متاورس، یک «جهان (پلتفرم) است که در آن افراد و اشیاء در یک فضای مجازی و واقعی تعامل داشته و ارزش‌های اقتصادی/اجتماعی/فرهنگی ایجاد می‌کنند».

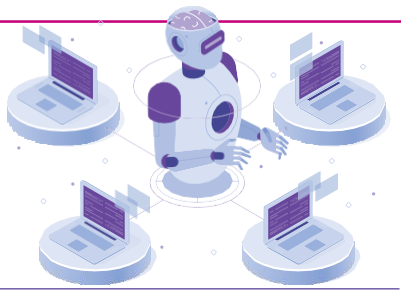
دامنه در حال حاضر، هیچ توافق علمی درباره ترکیب فناوری‌های اجرایی اصلی و فناوری‌های امنیتی و همچنین تعریف دقیقی از متاورس وجود ندارد، اما دیدگاه‌ها و تفسیرهای متنوعی در حال ظهور هستند.

- فناوری احراز هویت در فضای متاورس
- فناوری حفاظت از حریم خصوصی در فضای متاورس
- فناوری اعتماد مجازی در فضای متاورس

ضرورت از آنجایی که متاورس دارای برخی ویژگی های کلیدی نظیر تعامل بین افراد و اشیاء در ترکیبی از فضای مجازی و واقعی است، تهدید هک می تواند مستقیماً بر امنیت و زندگی کاربر تأثیر بگذارد، بنابراین توسعه فناوری‌های امنیتی برای محافظت از کاربران در این فضا بسیار مهم است.

روندهای جهانی برنامه‌های تحقیق و توسعه میان‌مدت و بلندمدت متاورس در کره جنوبی در حال آماده‌سازی است و قوانین و استانداردهای مرتبط و همچنین تحقیقات پروتکل امنیتی در سطح بین‌الملل نیز در حال انجام می‌باشد.

- کره جنوبی: کره جنوبی در حمایت از توسعه پنج فناوری اصلی (فضای فرامنطقه‌ای متا، انسان دیجیتال، رسانه بسیار واقع‌گرا، رابط کاربری/تجربه کاربری به زمان واقعی و پلتفرم توزیع شده و باز) برای تحقق خدمات متاورس در آینده، اقداماتی را انجام می‌دهد و در حال آماده‌سازی برنامه راهبردی تحقیق و توسعه متاورس در میان‌مدت و بلند مدت است.
- ایالات متحده آمریکا: سازمان غیرانتفاعی بین‌المللی XRSI (XR Safety Initiative) که به مسائل حریم خصوصی، امنیت و اخلاقیات در فناوری واقعیت ترکیبی (XR) می‌پردازد، یک چارچوب حریم خصوصی و امنیت ایجاد کرده که از ۴ حوزه (دسترسی، مدیریت، اطلاعات و پیشگیری) تشکیل شده و تدابیر حفاظتی گوناگونی متناسب با هریک از حوزه‌ها تعریف نموده است (۲۰۲۰).
- چین: چین موضوع تقویت امنیت فضای UGC (محتوای تولید شده توسط کاربران)، افزایش قابلیت‌های مدیریت مالکیت فکری، تقویت قابلیت‌های حفاظت اطلاعات شخصی، گسترش دسترسی عمومی و استانداردها و پروتکل‌های برنامه‌های کاربردی متاورس به منظور توسعه بیشتر متاورس را مورد توجه قرار داده است.



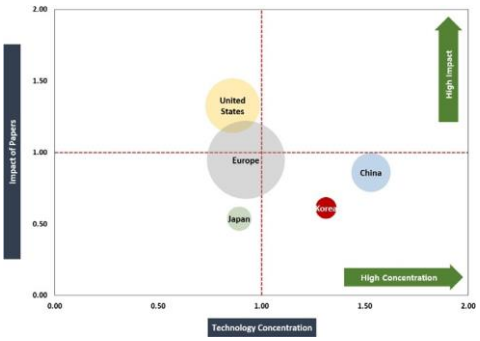
چشم انداز آینده در سال ۲۰۳۰ **پیش‌بینی می شود که اطلاعات کاربران می تواند با امنیت و سهولت کامل در یک محیط چندجهانی متاورس به اشتراک گذاشته شود.**

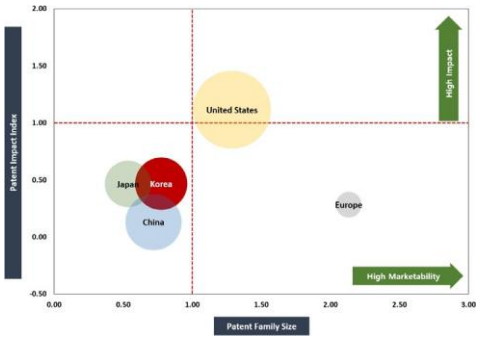
- فرا رسیدن دوران چندجهانی (Multiverse) جایی که تمام داده‌ها و عملکردهای متاورس توزیع و پردازش می‌شوند و پلتفرم‌ها به صورت متقابل به هم پیوند می‌خورند تا در عین تکامل با همزیستی همکاری کنند.
- توسعه استفاده از فضاهای اعتماد مجازی شخصی‌سازی شده، که بر اساس ویژگی‌های سرویس قادر به ایجاد و مدیریت امن و قابل اعتماد فضاهای اعتماد مجازی هستند.

ارتباط با سایر فناوری های نوظهور **این فناوری ارتباط نزدیکی با فناوری رمزنگاری عملکردی و کاربردی مانند رمزنگاری هومومورفیک در راستای امنیت داده‌ها و حفظ حریم خصوصی دارد.**

- فناوری‌های امنیت داده برای خدمات شبکه تلفن همراه نسل بعد (5G و 6G) و فناوری‌های رمزنگاری عملکردی و کاربردی مانند رمزنگاری هومومورفیک جهت حفاظت از حریم خصوصی و امنیت داده می‌توانند در محیط‌های مجازی مورد استفاده قرار گیرند.

تجزیه و تحلیل جامع مقالات و پتنت‌ها **بر اساس تحلیلی از مقالات و اختراعات در طی ۱۲ سال گذشته در کره جنوبی، ایالات متحده آمریکا، ژاپن، اروپا (۲۸ کشور اروپایی از جمله انگلستان) و چین، چین بیشترین تمرکز فناوری را دارد در حالی که اروپا بزرگترین اندازه خانواده اختراعات (PFS) را دارد.**





۷

فناوری رمزنگاری کوانتومی برای امنیت کامل داده در عصر کوانتوم

تعریف این فناوری عبارت است از رمزنگاری با استفاده از اصل عدم قطعیت کوانتومی و اصل عدم تکرارپذیری، که می تواند ایمنی مطلق را تضمین کند.

دامنه فناوری رمزنگاری کوانتومی فناوری است که می تواند کارکردهای رمزنگاری مدرن را پیاده سازی کند و امنیت آن را بر اساس مکانیک کوانتومی تحقق بخشد و به توزیع کلید رمزنگاری کوانتومی، احراز هویت کوانتومی و امضای الکترونیکی و انتقال امنیت کوانتومی طبقه بندی می شود.

- فناوری توزیع کلید رمزنگاری کوانتومی

این فناوری برای توزیع کلیدهای رمزنگاری مورد استفاده برای رمزگذاری با ارسال و دریافت اطلاعات رمزگذاری شده/رمزگشایی شده با استفاده از ویژگی‌های یک موج کوانتومی است و می‌تواند با استفاده از اصول مکانیک کوانتومی امنیت در برابر استراق سمع را تضمین کند.

- احراز هویت کوانتومی و فناوری امضای الکترونیکی

این فناوری برای معرفی مکانیک کوانتومی به فرآیند اصلی احراز هویت طرف دیگر با استفاده از اصل فناوری توزیع کلید رمزنگاری کوانتومی و ایجاد امضای الکترونیکی برای داده‌ها با استفاده از مکانیک کوانتومی استفاده می‌شود.

- فناوری انتقال امن کوانتومی

این فناوری برای انتقال اطلاعات به صورت امن با استفاده از مکانیک کوانتومی استفاده می‌شود و برای تضمین امنیت، نیاز به ترکیب آن با فرایند احراز هویت دارد.

ضرورت فناوری توزیع کلید رمزنگاری کوانتومی که در سال ۱۹۸۴ بر اساس اصول مکانیک کوانتومی مانند عدم قطعیت کوانتومی و عدم تکرارپذیری پیشنهاد شد، فناوری‌ای است که برخلاف رمزنگاری مدرن، بدون توجه به توسعه روش‌های محاسباتی و رمزگشایی، امنیت مطلق را فراهم می‌کند.

روندهای جهانی این فناوری به عنوان یک فناوری استراتژیک ملی در کره جنوبی انتخاب شده است، در حالی که در سراسر جهان، کشورهای مختلف در حال توسعه قوانین و تجاری سازی برای ارتقاء امنیت آن هستند.

- کره جنوبی: کره جنوبی فناوری کوانتوم را به عنوان یکی از ۱۲ فناوری استراتژیک ملی انتخاب کرده و از آن عمیقا پشتیبانی می کند و فناوری رمزنگاری کوانتومی در حوزه فناوری اطلاعات و ارتباطات مورد استفاده قرار گرفته است.
- ایالات متحده آمریکا: ایالات متحده قانون NQI را برای پشتیبانی مستمر از فناوری کوانتوم وضع کرده و بر ایجاد یک سیستم ارتباطی کوانتومی تمرکز داشته و آن را به عنوان مهم‌ترین وظیفه فنی در آینده تلقی می‌کند.

- اروپا: اروپا آغاز تحقیقات در مورد توزیع کلید رمزنگاری کوانتومی و تولید کننده اعداد تصادفی کوانتومی را رهبری کرده و پروژه‌های مختلفی برای ارتقاء امنیت و تجاری‌سازی فناوری‌های برتر در حال انجام است.

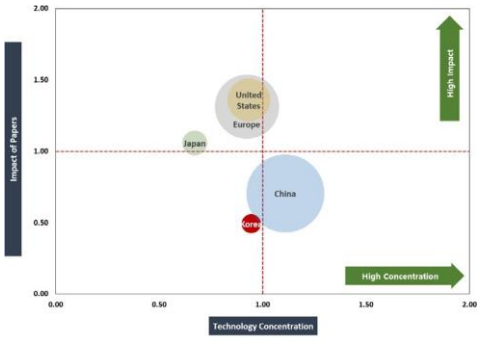
چشم انداز آینده در سال ۲۰۳۰ با ظهور رایانه های کوانتومی و هوش مصنوعی و توسعه فناوری های حمله سایبری، انتظار می رود تهدید سرقت / تغییر / رمزگشایی داده ها به طور قابل توجهی افزایش یابد و انتظار می‌رود معرفی فناوری رمزنگاری کوانتومی که ایمنی مطلق را فراهم می کند، در بخش های عمده کشور و جامعه افزایش یابد.

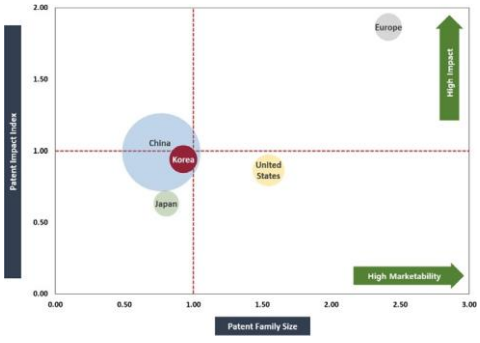
- انتظار می‌رود توزیع کلید رمزنگاری کوانتومی برای دستگاه‌های کوچک مانند دستگاه‌های تلفن همراه به دلیل کوچک‌سازی و قیمت پایین قطعات مورد نیاز برای فناوری کوانتومی اعمال شود.

ارتباط با سایر فناوری‌های نوظهور فناوری رمزنگاری کوانتومی با امنیت وسایل نقلیه خودران و حفاظت از امنیت کاربر در محیط‌های مجازی رابطه مکمل دارد.

- فناوری توزیع کلید رمزنگاری کوانتومی و فناوری احراز هویت کوانتومی به طور مکمل با فناوری توزیع کلید رمزنگاری و تأیید اعتبار در امنیت سایبری موجود مطابق با محیط شبکه ترکیب می‌شوند و امنیت وسایل نقلیه خودران و حفاظت از کاربر در محیط مجازی را تامین می‌کنند.
- فناوری رمزنگاری کوانتومی یک فناوری پایه است که می‌تواند امنیت سایبری را بر روی اینترنت کوانتومی تامین کند، شبکه‌ای که در آینده توجه‌ها را به خود جلب می‌کند و انتظار می‌رود سنگ بنای تمامی فناوری‌ها و خدمات امنیتی مختلف باشد.

تجزیه و تحلیل جامع مقالات و پتنت‌ها بر اساس تحلیلی از مقالات و اختراعات در طی ۱۲ سال گذشته در کره جنوبی، ایالات متحده آمریکا، ژاپن، اروپا (۲۸ کشور اروپایی از جمله انگلستان) و چین، چین بیشترین تمرکز فناوری را دارد در حالی که اروپا بزرگترین اندازه خانواده اختراعات (PFS) را دارد.





۸

پیشگیری از جرایم سایبری و ردیابی سوء استفاده از فناوری‌های دیجیتال جدید

تعریف فناوری اطلاعات تهدید سایبری، به منظور مقابله با جرایم سایبری پیشرفته و هوشمند در محیط تحول دیجیتال استفاده می‌شود. این فناوری شامل مجموعه‌ای از ابزارها، روش‌ها و فرآیندهایی است که برای شناسایی، جمع‌آوری، تحلیل و درک تهدیدات سایبری پیشرفته، به سازمان‌ها کمک می‌کند.

دامنه این فناوری به عنوان یک فناوری حفاظت از ریسک دیجیتال دسته‌بندی می‌شود که از طریق تحلیل فرآیند حملات مبتنی بر زنجیره حملات سایبری (Cyber Kill Chain) جرایم سایبری را ردیابی و پیش‌بینی می‌کند و همچنین فناوری شکار تهدید سایبری (Cyber Threat Hunting) را برای پاسخ فعال به حملات فراهم می‌کند.

- فناوری حفاظت از ریسک دیجیتال

این فناوری برای نظارت و پیگیری فعالیت‌های جمع‌آوری اطلاعات و پیش‌بینی حملات در مرحله پیش از حمله سایبری (مراحل زنجیره حمله سایبری، از مرحله ۱ تا ۲) استفاده می‌شود که شامل مرحله شناسایی (reconnaissance) و مرحله تسلیح (weaponization) است.

- شکار تهدید سایبری

این فناوری به منظور پیشگیری فعال و از بین بردن آسیب‌پذیری‌های هدف‌های تهدید در مراحل فرآیند حمله سایبری (مراحل زنجیره حمله سایبری، از مرحله ۳ تا ۶) استفاده می‌شود که شامل مراحل تحویل (delivery)، استخراج (exploitation)، نصب (installation) و کنترل و دستور (command and control) است.

ضرورت اگرچه مقیاس آسیب به دلیل ظهور جرایم سایبری جدید و گسترش تهدیدات سایبری هوشمند ارتقا یافته رو به افزایش است، اما فناوری‌های واکنش غیرفعال موجود (شبکه‌گرایانه هشدار، پس‌پاسخ و غیره) دارای محدودیت‌ها و بازداشت هستند. نرخ نیز ناکافی است.

روندهای جهانی کره استراتژی امنیت سایبری ملی خود را اعلام کرد، در حالی که کشورهای سراسر جهان از طریق دستورات و توافقات اداری به تهدیدات امنیتی پاسخ می دهند.

- کره جنوبی: در پاسخ به افزایش تهدیدات سایبری مانند هک و سرقت اطلاعات، استراتژی امنیت سایبری ملی که حاوی دستورالعمل‌های سیاستی در حوزه امنیت سایبری است (۲۰۱۹) اعلام شد.
- ایالات متحده آمریکا: بایدن فرمان اجرایی بهبود امنیت سایبری برای حفاظت از زیرساخت ها و شبکه‌های فدرال را امضا کرد (۲۰۲۱).
- اروپا: اتحادیه اروپا که مرجع سیستم حقوقی هر کشور در واکنش به جرایم سایبری است، ایجاد کنوانسیون جرایم سایبری را برای تسریع همکاری بین کشورها در تحقیقات تصویب کرد.

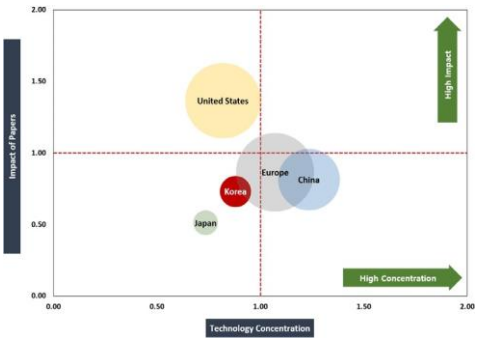
چشم انداز آینده در سال ۲۰۳۰ انتظار می رود جرایم سایبری که افراد، شرکت‌ها و کشورها را هدف قرار می‌دهند، افزایش یافته و تقابل بین کشورها تشدید شود.

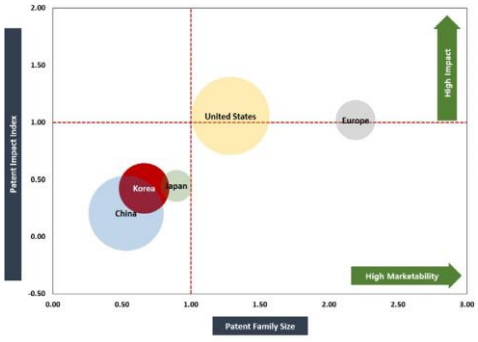
- جرایم سایبری در سال ۲۰۳۰ هوشمندتر و خودآموزتر خواهد شد و دفاع و حمله بین کشورها با استفاده از هوش مصنوعی امکان پذیر خواهد بود.
- با گسترش زیرساخت‌های دیجیتال جدید مانند فناوری 5G، ابر (Cloud) و هوش مصنوعی (AI) و توسعه خدمات فوق‌العاده متصل (Hyper-connected) انتظار می‌رود که هدف و تنوع حملات سایبری افزایش یابد.

ارتباط با سایر فناوری‌های نوظهور این فناوری می‌تواند به همراه فناوری کنترل و پاسخ خودکار امنیت سایبری مبتنی بر هوش مصنوعی (AI) و اتوماسیون تشخیص آسیب‌پذیری امنیتی زنجیره تأمین و سیستم تولید استفاده شود.

- فناوری شکار تهدید سایبری با کنترل امنیت سایبری هوشمند مبتنی بر هوش مصنوعی و فناوری پاسخ خودکار به جرایم سایبری هم‌افزایی دارد.
- فناوری شکار تهدید سایبری می‌تواند برای ارتقاء امنیت زنجیره تامین و اتوماسیون تشخیص آسیب‌پذیری امنیتی سیستم تولید مورد استفاده قرار گیرد.

تجزیه و تحلیل جامع مقالات و پتنت‌ها بر اساس تحلیلی از مقالات و اختراعات در طی ۱۲ سال گذشته در کره جنوبی، ایالات متحده آمریکا، ژاپن، اروپا (۲۸ کشور اروپایی از جمله انگلستان) و چین، چین بیشترین تمرکز فناوری را دارد در حالی که اروپا بزرگترین اندازه خانواده اختراعات (PFS) را دارد.





۹

فناوری امنیت ابر/لبه برای استفاده از یک محیط مجازی امن

تعریف این فناوری امنیتی مبتنی بر فناوری ابر/ لبه است که از ابزار رایانش و داده ها به عنوان یک شبکه در پاسخ به افزایش تهدیدات سایبری مرتبط با گسترش نقاط تماس حمله به طور موثر استفاده می کند.

دامنه این فناوری به سه حوزه اصلی فناورانه مرتبط با امنیت و حفاظت اطلاعات اختصاص دارد: فناوری پاسخ چند تهدیدی برای مقابله با گسترش نقاط تماس حملات، فناوری مدیریت امنیت داده برای حفاظت و پردازش اطلاعات امن و فناوری مدیریت امنیت بدون اعتماد که مدیریت اختیارات را بر اساس عدم اعتماد انجام می‌دهد.

- فناوری پاسخ چند تهدیدی

یک فناوری امنیتی چندپاسخی که شامل پاسخ‌های پیشگیرانه برای مسدود کردن دسترسی غیرمجاز، پاسخ‌های حسگری برای شناسایی تغییرات غیرمجاز، پاسخ‌های خودکار برای پاسخ دادن فوری و مدیریت امنیت برای مدیریت سیاست‌ها و رویه‌های امنیتی است.

- فناوری امنیت بدون اعتماد

این فناوری امنیتی، بر اساس این فرضیه که هیچ کس قابل اعتماد نیست، به هیچ فرد یا دستگاه داخلی یا خارجی دسترسی و اختیار نمی‌دهد مگر آنکه به عنوان کاربر عادی شناخته و به طور مداوم تأیید شود.

ضرورت از زمان شیوع بیماری کووید-۱۹، به دلیل رواج دورکاری و افزایش حملات به داده‌های ذخیره شده در ابر، وابستگی به فضای ذخیره ابری افزایش یافته است.

روندهای جهانی کره جنوبی در حال معرفی یک سیستم گواهی‌نامه امنیت ابر است، ایالات متحده و چین نیز برای اصلاح قوانین، مقررات و سیستم‌ها جهت گسترش خدمات ابر تلاش می‌کنند.

- کره جنوبی: کره جنوبی یک سیستم گواهی‌نامه امنیت ابر را معرفی کرده است که در آن سازمان‌های گواهی‌دهنده، تطابق با استانداردهای حفاظت اطلاعاتی برای خدمات ارائه شده توسط ارائه‌دهندگان خدمات ابر را ارزیابی و گواهی می‌کنند.
- ایالات متحده آمریکا: ایالات متحده سیاست «ابتدا ابر» را به سیاست «هوشمند ابر» تغییر داده و در حال بهبود مقررات خود برای گسترش خدمات ابری است.
- چین: چین از طریق قانون اطلاعات ملی و قانون حفاظت از اطلاعات شخصی، فضایی را برای دولت برای اعمال نفوذ بر شرکت های خدمات ابری ایجاد کرده است.

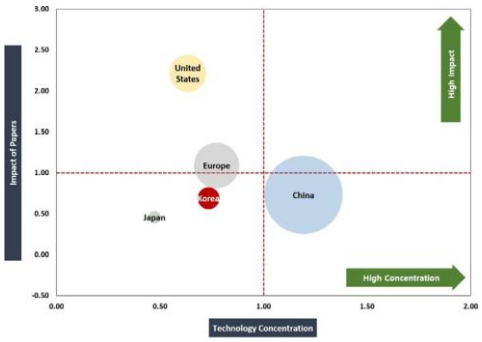
چشم انداز آینده در سال ۲۰۳۰ **پیش بینی می شود که بهره برداری از خدمات رایانش ابری و داده ای شتاب گرفته و به دلیل عدم محدودیت نسبت به قوانین و کارآمدی هزینه های مرتبط با استفاده از ابر در هر کشور، سهم کم شرکت‌های جهانی خدمات ابری رشد خواهد یافت.**

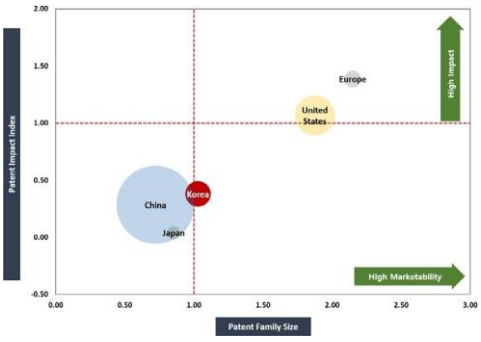
- انتظار می رود توسعه و استفاده از فناوری هایی مانند رایانش محرمانه سرعت بیشتری بگیرد تا استانداردهای نظارتی هر کشور به راحتی توسط شرکت های جهانی مورد پذیرش قرار گیرد.

ارتباط با سایر فناوری‌های نوظهور **فناوری تضمین قابلیت اطمینان رمزارزها برای استفاده در اقتصاد دیجیتال به عنوان یک فناوری مبتنی بر ابر عمل می‌کند.**

- فناوری رمزارز مبتنی بر فضای ابری است و قابلیت اطمینان آن نه تنها به قابلیت اطمینان پروتکل بلکه به قابلیت اطمینان کلی زیرساخت ابری وابسته است.

تجزیه و تحلیل جامع مقالات و پتنت‌ها **بر اساس تحلیلی از مقالات و اختراعات در طی ۱۲ سال گذشته در کره جنوبی، ایالات متحده آمریکا، ژاپن، اروپا (۲۸ کشور اروپایی از جمله انگلستان) و چین، چین بیشترین تمرکز فناوری را دارد در حالی که اروپا بزرگترین اندازه خانواده اختراعات (PFS) را دارد.**





۱۰

فناوری تضمین اعتبار رمزارزها به منظور ارتقاء امنیت اقتصاد دیجیتال

تعریف این فناوری می تواند قابلیت اطمینان صدور یا تراکنش ارز دیجیتال یا دارایی را تضمین کند، مانند فناوری بلاک چین و فناوری دفترکل توزیع شده.

دامنه این فناوری به دو دسته فناوری دفترکل توزیع شده و فناوری ارز دیجیتال مربوط می شود.

- دفترکل توزیع شده

یک فناوری است که به وسیله آن دفترچه‌هایی که اطلاعات تراکنش را ثبت می‌کنند را کپی کرده و این اطلاعات را به چندین گره (شرکت‌کننده) توزیع کرده و در آنها ذخیره می‌کند.

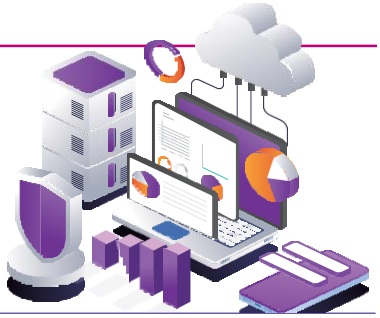
- فناوری رمزارز

فناوری رمزارز شامل الگوریتم توافق، رمزنگاری، فناوری بهبود حفاظت اطلاعات شخصی، مدیریت امنیت و امضای دیجیتال است.

ضرورت داشتن هارد فورک به دلیل هک انبوه بلاک چین و اتریوم و توسعه فناوری هایی برای جلوگیری از سرقت ارزهای دیجیتال از طریق هک و سرعت پایین تراکنش و مقیاس پذیری ضروری است.

روندهای جهانی حمایت از صنعت بلاک چین و توسعه فناوری به رهبری دولت ها در حال انجام است، اما مسائل نظارتی نیز در این بین حائز اهمیت می‌باشد.

- کره جنوبی: در سال ۲۰۲۰، وزارت علوم و فناوری اطلاعات و ارتباطات، راهبردی را برای گسترش فناوری بلاک چین اعلام کرد و از استفاده از BaaS (بلاک چین به عنوان یک سرویس) برای توسعه خدمات کاربردی بلاک چین و اجرای ایده‌ها حمایت کرد.
- ایالات متحده آمریکا: ایالات متحده در حال حاضر بالاترین سطح فناوری را از نظر فناوری کلی بلاک‌چین دارد و در حال انجام طیف وسیعی از تحقیقات، از جمله در زمینه شبکه توزیع شده بلاک چین و فناوری تأیید حساب بلاک چین است.
- چین: چین صنعت بلاک‌چین تحت رهبری ملی را حمایت و ترویج کرده و ۲۲ مجتمع صنعتی بزرگ بلاک‌چین ایجاد کرده است.
- اروپا: اتحادیه اروپا قابلیت استفاده از اطلاعات ناشناس را برای داده های بلاک‌چین به رسمیت می‌شناسد و مقرراتی برای آن تدوین نموده است.



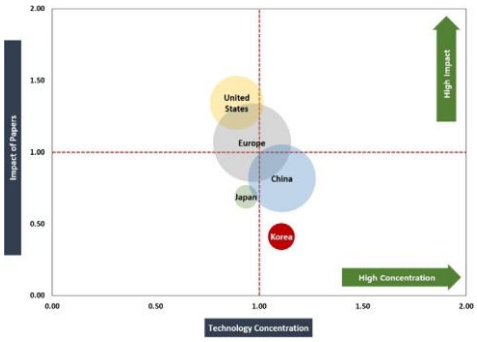
چشم انداز آینده در سال ۲۰۳۰ انتظار می‌رود که معرفی خدمات مالی عمومی قابل اعتماد مبتنی بر فناوری بلاک‌چین، رقابت را در میان ارائه‌دهندگان خدمات پرداخت خصوصی ارتقا دهد و در عین حال به افزایش کارایی سیستم پرداخت کمک کند.

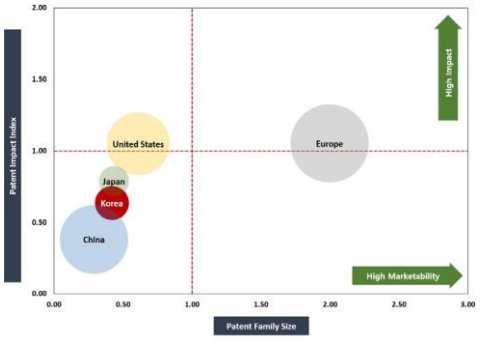
- توسعه مداوم فناوری برای غلبه بر محدودیت‌های بلاک‌چین و دفترکل توزیع شده و حل نوسانات بالا، قابلیت اطمینان داده ها و مسائل مربوط به حریم خصوصی در ارزهای دیجیتال ضروری است.
- با توسعه رایانه‌های کوانتومی، حمله به سیستم دفترکل توزیع شده فعلی آسان تر می شود و احتمال ناتوانی در بلاک‌چین افزایش می‌یابد، بنابراین راهی برای دفاع از رمزنگاری کوانتومی در بلاک‌چین مورد نیاز است.

ارتباط با سایر فناوری‌های نوظهور فناوری تضمین قابلیت اطمینان رمزارز برای استفاده در اقتصاد دیجیتال به عنوان یک فناوری مبتنی بر ابر عمل می‌کند.

- فناوری رمزارز مبتنی بر فضای ابری است و قابلیت اطمینان آن نه تنها به قابلیت اطمینان پروتکل بلکه به قابلیت اطمینان کلی زیرساخت ابری وابسته است.

تجزیه و تحلیل جامع مقالات و پتنت‌ها بر اساس تحلیلی از مقالات و اختراعات در طی ۱۲ سال گذشته در کره جنوبی، ایالات متحده آمریکا، ژاپن، اروپا (۲۸ کشور اروپایی از جمله انگلستان) و چین، چین بیشترین تمرکز فناوری را دارد در حالی که اروپا بزرگترین اندازه خانواده اختراعات (PFS) را دارد.





منابع و مآخذ

- NIC, Global Trends 2040 (2021)
- NISTEP, The 11th Science and Technology Foresight (2019)
- Intelligent Transport Systems (ITS); Communications Architecture, European Standard (Telecommunications series)
- Security guidelines for vehicle–to–everything (V2X) communication, TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU
- ARISTA NETWORK, The 5 Levels of Autonomous Security, 2022 ECSO, Input to the horizon programme for cyber security (2021–2027)
- Deutsche Telekom, 5G Technology in Industry Campus Networks, (2022)
- Singh et al., Quantum Internet– Applications, Functionalities, Enabling Technologies, Challenges, and Research Directions (2021)
- Ministry of Science and ICT, Innovate Korea 2045 (2020) Changhyun Park et al., A Study on the 6th S&T foresight (2021)
- KISTEP, A Study on the Selection of KISTEP 10 Emerging Technologies in 2019, (2019) KISTEP, A Study on the Selection of KISTEP 10 Emerging Technologies in 2020, (2020) KISTEP, A Study on the Selection of KISTEP 10 Emerging Technologies in 2021, (2021) KISTEP, A Study on the Selection of KISTEP 10 Emerging Technologies in 2022, (2022)
- KISTI, Technology commercialization analysis report, In the era of the Next Normal, looking for new business opportunities (2020)
- KRIBB, 2022 Emerging Biotechnology (2022)
- NIA, Data–based post–COVID–19 issue analysis and 10 megatrends (2021)
- Korean government, 5G+ Strategy to Realize Innovative Growth, (2019.4.8.)
- Ministry of Science and ICT, Future telecommunication R&D promotion strategy to lead the 6G era, (2020.8.6.)
- ETRI, Trends in Supply–Chain Security Technologies (2020)
- IITP Weekly ICT Trends, Fully Homomorphic Encryption technology and standards trends, (2021.09)
- IITP, Metaverse R&D Roadmap (2021)
- KISA, 2020 4th Quarter Cyber Threat Trends Report
- Dongyoung Koo, Cloud Computing Security Technology Trends, Review of KIISC Volume 30, Issue 6, 2020
- Bank of Korea, Current status of central bank digital currency (CBDC) response in major countries
- https://www.gartner.com/en/information–technology/insights/top–technology–trends

- https://www.technologyreview.com/2021/02/24/1014369/10-breakthrough-technologies-2021/
- https://www.weforum.org/press/2021/11/top-10-emerging-technologies-to-watch-in-2021/
- https://www2.deloitte.com/us/en/insights/focus/tech-trends.html
- https://www.wef.org