ارائه نیازهای فناورانه حوزه امنیت فناوری اطلاعات (افتا)

مرکز نوآوری اتاق بازرگانی

عنوان نیاز فناورانه

تشخیص نفوذ با استفاده از روش‌های داده‌کاوی

شرح نیاز فناورانه

سیستم‌های تشخیص نفوذ به شبکه، برنامه‌های کاربردی در زیر ساخت‌های امنیتی شبکه‌ها هستند. رویکردهای تشخیص نفوذ به طور کلی به دو دسته تقسیم می‌شوند:

تشخیص موارد سوء استفاده و تشخیص رفتار غیر عادی.

سیستم‌های تشخیص موارد سوء استفاده تلاش می‌کنند حمله‌ها را با استفاده از کشف الگوهای نفوذ تشخیص داده شده و گزارش شده را شناسایی کنند. رویکرد تشخیص رفتار غیر عادی در واقع توسعه رویکرد قبلی است با این توضیح که در این رویکرد، الگوهایی از رفتار عادی در شبکه از قبل، استخراج شده است و نفوذ می‌تواند مبتنی بر مقداری انحراف از رفتارهای نرمال تعریف شود. در این حال در صورت مشاهده کوچکترین انحراف، هشدار نفوذ در شبکه فعال می‌شود. در سیستم‌های تشخیص نفوذ از روش‌های مختلفی استفاده می‌شود که یکی از این روش‌ها داده کاوی است. ضمن مطالعه الگوریتم‌ها و تکنیک‌های مختلف داده کاوی، با انتخاب مجموعه داده و معیارهای سنجش استاندارد مشترک، بررسی‌های مختلفی انجام گیرد و کارایی هر یک از الگوریتم‌ها به صورت جداگانه مورد بررسی قرارگیرد. سپس مدل پیشنهادی جهت ترکیب الگوریتم‌های منتخب داده کاوی و الگوریتم‌های کاهش بعد ارائه شده و اقدام به پیاده سازی و مقایسه نتایج بدست آمده مطابق مدل پیشنهادی شده است

حوزه فناوری تقاضا

۰۷- فناوری اطلاعات و ارتباطات نرم‌افزارهای رایانه‌ای > ۰۴- امنیت فضای تبادلات > ۰۳- تشخیص > ۰۲- سیستم‌های تحلیل، تشخیص و محافظت در برابر تهدیدها و بدافزارها

حوزه صنعتی تقاضا

۰۷- فناوری اطلاعات و ارتباطات نرم‌افزارهای رایانه‌ای > ۰۴- امنیت فضای تبادلات > ۰۳- تشخیص

پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

تشخیص موارد سوء استفاده و تشخیص رفتار غیر عادی.

تشخیص کوچکترین انحراف.

مدل همکاری مطلوب

انتقال دانش فنی

ارائه نیازهای فناورانه حوزه امنیت فناوری اطلاعات (افتا)

مرکز نوآوری اتاق بازرگانی

عنوان نیاز فناورانه

تشخیص باگ‌های امنیتی توسط تکنیک هوش مصنوعی

شرح نیاز فناورانه

توسعه‌دهندگان نرم‌افزار، هر روز فهرستی طولانی از ویژگی‌ها و باگ‌هایی که باید اصلاح شوند را دریافت می‌کنند. متخصصان امنیتی سعی دارد با استفاده از ابزارهای خودکار به اولویت‌بندی نقص‌ها کمک کنند؛ اما در بیشتر موارد مهندسان روی ایرادات کاذب تمرکز کرده یا آسیب‌پذیری حیاتی طبقه‌بندی نشده موجود را نادیده می‌گیرند. برای رفع این مشکل گروه‌های علوم اطلاعاتی و امنیتی شروع به همکاری با یکدیگر کردند. مشخص شده‌است که با ادغام یادگیری ماشینی و متخصصان امنیتی انسانی می‌توان به طور قابل‌توجهی سطح امنیت سامانه‌ها و طبقه‌بندی باگ‌ها را افزایش داد.

هوش مصنوعی یاد شده ابتدا مشکلات نرم‌افزاری امنیتی و غیرامنیتی را طبقه‌بندی کرد و سپس یاد گرفت بر چست‌هایی مانند مهم یا کم اثر به هر یک از آن‌ها اختصاص دهد. مشخص شده‌است که به منظور پیش‌بینی باگ، از مدلی دو مرحله‌ای بهره گرفت. بخش اول یک رویکرد بازیابی اطلاعات با نام (TF-IDF) است که مشخص می‌کند در یک سند، یک کلمه چند مرتبه تکرار شده است. سپس نوع ارتباط کلمه در مجموعه‌ای از تیترها را بررسی می‌کند. بخش دوم یک مدل رگرسیون لجستیک (logistic regression) است که احتمال وجود کلاس یا عملکردی خاص را در سیستم بررسی می‌کند.

حوزه فناوری تقاضا

۰۷- فناوری اطلاعات و ارتباطات نرم‌افزارهای رایانه‌ای > ۰۴- امنیت فضای تبادلات > ۰۳- تشخیص > ۰۲- سیستم‌های تحلیل، تشخیص و محافظت در برابر تهدیدها و بدافزارها

حوزه صنعتی تقاضا

۰۷- فناوری اطلاعات و ارتباطات نرم‌افزارهای رایانه‌ای > ۰۴- امنیت فضای تبادلات > ۰۳- تشخیص

پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

استفاده از مدلی دو مرحله‌ای برای پیش‌بینی باگ.

تشخیص دادن باگ‌های کوچک کمتر از ۱۰ کلمه.

تشخیص امنیتی بودن باگ و در مرحله‌ی بعد تعیین سطح آن.

ایجاد تفاوت میان باگ‌های امنیتی و غیرامنیتی با دقت ۹۵ درصدی.

تشخیص بحرانی بودن یک باگ با دقت بالای ۹۰ درصد.

فناوری‌ها و راه‌حل‌های نامطلوب

محدود نبودن تشخیص باگ‌ها.