New Researches in the Smart City
Vol 3 (Issue 1), 50-70
nrsc.apadana.ac.ir

Apadana Institute of Higher Education

Global Information System for Cyber Threats with Artificial Intelligence and Convolutional Neural Networks

Saemeh Balooch Rooz *
PhD Student, Faculty of Engineering, Department of Computer Engineering, Islamic Azad University, Kerman Branch, Kerman, Iran.

Soodeh Shadravan
Assistant Professor, Faculty of Engineering, Department of Computer Engineering, Islamic Azad University, Bardseer Branch, Kerman, Iran.

Received: 13/September/2024 Accepted: 15/November/2024 eISSN: 3060-6144 ISSN: 2980-8936

Abstract

Global cyberattacks significantly impact the economy, society, organizations, and individuals. Existing research on cyberattacks, particularly in providing AI-based analytical solutions to share information on cyber threats at the national level, is limited. National cybersecurity strategists require AI-based decision support systems to assess the cybersecurity posture or preparedness of a country. This paper proposes an AI-based solution that autonomously collects multidimensional data on cyber-related incidents from social media posts. The proposed system offers crucial analytical capabilities across a spectrum of cyber threats, utilizing sophisticated AI algorithms for anomaly detection, prediction, sentiment analysis, location detection, translation, and more. The system has been operational from April 21, 2021, to May 31, 2023. In 21 days, the system independently collected 30,203 records on cyber threats, covering various aspects of cyber threats. These dimensions included daily records of cyberattacks nationwide, such as ransomware, exploits, web threats, spam, malicious emails, network attacks, local contamination, and demand-based scanning. Additionally, the system obtained and analyzed 3,789 cyber-related tweets from 3,402 users in 37 different languages using AI. It also independently translated 893 non-English tweets. The proposed system is the first solution to employ Convolutional Neural Networks (CNN) for anomaly detection in the global cyber threat spectrum and for the automatic prediction of cyberattacks. The system was demonstrated to provide evidence-based decisions on global cyber threats across multiple platforms, including iOS, Android, and Windows.

Keywords: artificial intelligence, cyber threats, convolutional neural networks

* Corresponding Author: s.baloochrooz@iauk.ac.ir

فصلنامه پژوهش‌های نوین در شهر هوشمند
دوره ۳، شماره ۱، پاییز ۱۴۰۳، ۵۰-۷۰
nrsc.apadana.ac.ir

مؤسسه آموزش عالی آپادانا
غیر دولتی - غیر انتفاعی

تاریخ دریافت: ۱۴۰۳/۰۶/۲۳ تاریخ پذیرش: ۱۴۰۳/۰۸/۲۵ eISSN: 3060-6144 ISSN: 2980-8936

سیستم اطلاعاتی جهانی تهدیدات سایبری با هوش مصنوعی و شبکه عصبی کانولوشنال

ثائمه بلوچ روز * دانشجوی دکتری کامپیوتر، دانشگاه آزاد اسلامی،کرمان، ایران.

سوده شادروان عضو هیئت‌علمی دانشگاه آزاد اسلامی، بردسیر، کرمان، ایران.

چکیده

حملات سایبری جهانی به‌طور قابل‌توجهی بر اقتصاد، جامعه، سازمان‌ها و افراد تأثیر می‌گذارد. تحقیقات موجود در مورد حملات سایبری در ارائه راه‌حل‌های تحلیلی مبتنی بر هوش مصنوعی (AI) جهت در اختیار گذاشتن اطلاعات تهدیدات سایبری در سطح کشور، اندک است. استراتژیست‌های سایبری در سطح ملی برای تصمیم‌گیری در مورد وضعیت یا آمادگی سایبری یک کشور به سیستم‌های پشتیبانی تصمیم مبتنی بر هوش مصنوعی نیاز دارند. این مقاله، یک راه‌حل مبتنی بر هوش مصنوعی را پیشنهاد می‌کند که به‌طور مستقل، داده‌های حملات سایبری چندبعدی در مورد اعتراضات مرتبط با سایبری را در پست‌های رسانه‌های اجتماعی جمع‌آوری می‌کند. سیستم پیشنهادی، قابلیت تحلیلی حیاتی را در طیف تهدیدات سایبری ارائه می‌کند و از الگوریتم‌های پیچیده مبتنی بر هوش مصنوعی برای تشخیص ناهنجاری، پیش‌بینی، تحلیل احساسات، تشخیص مکان، ترجمه و غیره استفاده می‌کند. سیستم پیشنهادی از ۱۱ اردیبهشت ۱۴۰۰ تا ۳۱ اردیبهشت ۱۴۰۲ مستقر شده است. در ۲۱ روز، این سیستم به‌طور مستقل ۳۰۲۰۳ رکورد در مورد تهدیدات سایبری را جمع‌آوری کرد که ابعاد متعددی از تهدیدات سایبری را پوشش می‌داد. این ابعاد شامل سوابق حملات سایبری روزانه در سراسر کشور توسط باج‌افزار، سوءاستفاده‌ها، تهدیدات وب، هرزنامه، نامه‌های مخرب، حملات شبکه، آلودگی‌های محلی و اسکن بر اساس تقاضا بود. علاوه بر این، این سیستم ۳۷۸۹ توییت مرتبط با سایبری را از ۳۴۰۲ کاربر توییت به ۳۷ زبان مختلف بر اساس AI به دست آورده و تجزیه‌وتحلیل کرد. همچنین، این سیستم ۸۹۳ توییت غیر انگلیسی را به‌طور مستقل ترجمه کرد. سیستم پیشنهادی، اولین راه‌حلی است که از تشخیص ناهنجاری مبتنی بر شبکه عصبی کانولوشن (CNN) به‌منظور شناسایی ناهنجاری‌ها در طیف تهدیدات سایبری در سراسر جهان و پیش‌بینی خودکار حملات سایبری استفاده می‌کند. سیستم پیشنهادی برای ارائه تصمیمات مبتنی بر شواهد در مورد تهدیدات سایبری جهانی در پلتفرم‌های متعدد ازجمله iOS، اندروید و ویندوز نشان داده شد.

کلیدواژه‌ها: هوش مصنوعی، تهدیدات سایبری، شبکه عصبی کانولوشن

* نویسندهٔ مسئول: s.baloochrooz@iauk.ac.ir

۱- مقدمه

حملات سایبری در سراسر جهان، تقریباً یک تریلیون دلار برای اقتصاد جهانی در سال ۲۰۲۰ هزینه داشته است (Cremer et al., 2022). هزینه جرائم سایبری تا سال ۲۰۲۵ سالانه ۱۰/۵ تریلیون دلار برآورد شده است (Morgan, 2020). اقتصادهای بزرگ‌تر مانند چین، برزیل، ایالات‌متحده، هند، مکزیک، فرانسه، استرالیا و حتی امارات متحده عربی از میلیاردها دلار ضرر مصرف‌کننده از طریق جرائم سایبری رنج می‌برند (Statista Research Department, 2022). به‌عنوان‌مثال، ضرر مصرف‌کننده چین از طریق جرائم سایبری، ۶۶/۳ میلیارد دلار در سال ۲۰۱۷ بود (Statista Research Department, 2022). حملات سایبری به غیر از ایجاد خسارات اقتصادی، تأثیرات مخربی در سطح اجتماعی و روانی بر زندگی انسان‌ها دارد (Bada & Nurse, 2020). به‌عنوان‌مثال، اخیراً یکی از غول‌های مخابراتی استرالیا، Optus، درنتیجه حملات سایبری در معرض نقض داده‌ها قرار گرفته که باعث ایجاد استرس و خشم عظیم در بین مصرف‌کنندگان شده است (Turnbull, 2022; Australian Securities & Investments Commissions, 2022). به دلیل این حمله سایبری، اطلاعات مشتریان Optus (نام، تاریخ تولد، آدرس ایمیل، گواهینامه رانندگی، کارت مدیکر، شماره پاسپورت و غیره) در معرض دید ۲/۱ میلیون مصرف‌کننده قرار گرفته است (Australian Securities & Investments Commissions, 2022; Merritt, 2022). اخیراً، اطلاعات حساس بیمار شامل تشخیص و روش پزشکی توسط مجرمان سایبری از شماره ۱ بیمه سلامت استرالیا به سرقت رفته است (Kaye, 2022). ازاین‌رو، جرائم سایبری یکی از حیاتی‌ترین دغدغه‌های ملت‌ها، دولت‌ها، سازمان‌ها و افراد مهم به شمار می‌رود. برای کاهش تأثیر جرائم سایبری، دو دستور حیاتی عبارت‌اند از تجمیع داده‌های مرتبط با سایبری و الگوریتم‌های تحلیلی پیچیده برای شناسایی و جلوگیری از تهدیدها. الزامات داده‌های سایبری در کارهای تحقیقاتی اخیر به تصویر کشیده شده است (Cremer et al., 2022; Zibak & Simpson, 2019). از سوی دیگر، نیاز به الگوریتم‌های تحلیلی پیچیده مبتنی بر هوش مصنوعی (AI) در (Guembe et al., 2022; Tetaly & Kulkani, 2022; Xu et al., 2019; Keshk et al., 2021; Abdullahi et al., 2022; Gheyas & Abdullah, 2016; Ten et al., 2011; Yang et al., 2017; Shi et al., 2018; Kotsias et al., 2022) نشان داده شده است. درحالی‌که AI می‌تواند برای انجام حملات سایبری پیچیده استفاده شود (Guembe et al., 2022; Tetaly & Kulkani, 2022)، همچنین می‌تواند در تشخیص حمله سایبری استفاده شود؛ همان‌طور که در (Tetaly & Kulkani, 2022; Xu et al., 2019; Keshk et al., 2021; Abdullahi et al., 2022; Gheyas & Abdullah, 2016; Ten et al., 2011; Yang et al., 2017; Shi et al., 2018; Kotsias et al., 2022) نشان داده شده است. بااین‌حال، هیچ‌یک از ادبیات ذکرشده موجود، آمار سایبری تاریخی در سطح کشور، پیش‌بینی سایبری سطح کشور و تشخیص ناهنجاری‌ها با هوش مصنوعی را ارائه نمی‌دهند؛ بنابراین، داشبورد اطلاعاتی سایبری پیشنهادی به نیازمندی‌های حیاتی (CR) زیر برای استراتژیست‌های سایبری جهت تصمیم‌گیری مبتنی بر شواهد در مورد وضعیت سایبری ملی کمک می‌کند:

CR 1: تجزیه‌وتحلیل طیف تهدید در برابر ابعاد مختلف حملات سایبری برای یک کشور خاص و مقایسه با کشورهای دیگر در جهان

CR 2: تجزیه‌وتحلیل تغییرات طیف تهدید در زمان برای هر کشور (به‌عنوان‌مثال، تغییر روزانه، هفتگی و ماهانه)

CR 3: با تجزیه‌وتحلیل داده‌های حملات سایبری گذشته، حملات سایبری را برای هر کشوری در جهان پیش‌بینی کنید.

CR 4: با تجزیه‌وتحلیل داده‌های حملات سایبری گذشته، ناهنجاری‌ها را در طیف‌های تهدید سایبری برای هر کشوری در جهان شناسایی کنید.

CR 5: دیدگاه کاربران رسانه‌های اجتماعی را در مورد مسائل مختلف سایبری در طول زمان تجزیه‌وتحلیل کنید.

CR 6: الزامات تحلیلی فوق (CR 1 تا CR 5) را در هر سیستم‌عامل (Windows، Android و iOS) و هر دستگاه (مانند تلفن همراه، تبلت، دسکتاپ) به دست آورید.

در این مقاله، ما یک راه‌حل خلاقانه را پیشنهاد می‌کنیم که با تجمیع داده‌های مربوط به سایبری از منابع متعدد و با استفاده از خدمات و الگوریتم‌های مبتنی بر AI، الزامات تحلیلی برجسته‌شده در CR 1 تا CR 6 را با موفقیت برآورده می‌کند. همان‌طور که از شکل ۱ مشاهده می‌شود، داده‌های حمله سایبری چندبعدی از فروشنده پیشرو نرم‌افزار ضدویروس (به‌عنوان‌مثال، کسپرسکی (۲۰۲۳a)) و داده‌های رسانه‌های اجتماعی مرتبط با سایبر به دست آمده است.

همان‌طور که از شکل ۱ مشاهده می‌شود، آمار حملات سایبری چندبعدی شامل باج افزار (Kaspersky, 2023g)، سوءاستفاده‌ها (Kaspersky, 2023b)، تهدیدات وب (Kaspersky, 2023i)، هرزنامه (Kaspersky, 2023h)، نامه‌های مخرب (Kaspersky, 2023d)، حملات شبکه (Kaspersky, 2023e)، آلودگی‌های محلی (Kaspersky, 2023c; Kaspersky, 2023e) و اسکن درخواستی (Kaspersky, 2023f) برای همه کشورهای جهان بود.

۲- ادبیات پیشینه

ادبیات موجود در اطلاعات تهدید سایبری عمدتاً بر دیدگاه سازمانی متمرکز است، جایی که حمله سایبری بر یک سازمان فردی برای منافع مالی یا سیاسی توسط مجرم تأثیر می‌گذارد (Xu et al., 2019; Keshk et al., 2021; Abdullahi et al., 2022; Gheyas & Abdullah, 2016; Ten et al., 2011; Yang et al., 2017; Shi et al., 2018; Kotsias et al., 2022). درحالی‌که این دیدگاه به دغدغه‌های یک نهاد سازمانی منفرد پاسخ می‌دهد اما نیاز سران سیاسی دولت‌ها را که دیدگاهی کلی‌نگر نسبت به ملت خود دارند، برآورده نمی‌کند. نگرانی در سطح ملی در مورد حمله سایبری مستلزم اطلاعات تهدید سایبری در سطح کشور و شامل طیف حملاتی است که یک کشور جداگانه را همراه با سایر کشورهای جهان برای اهداف معیاری پوشش می‌دهد. استفاده از این دیدگاه جامع از تمام آمار حملات سایبری برای یک کشور در مقایسه با سایر کشورها به تصمیم‌گیرندگان سیاسی اجازه می‌دهد موضع خود را در مورد دفاع سایبری تعیین کنند. به‌عنوان‌مثال، اگر استرالیا در مقایسه با کشورهای دیگری مانند نیوزلند، امارات متحده عربی و مالزی، با تعداد غیرمعمول و بیشتری از حملات سایبری مواجه است، باید موضع دفاع سایبری خود را در سطح بالاتری قرار دهد.

اطلاعات تهدید سایبری در سطح کشور برای آمادگی سایبری یک کشور، حیاتی است. در ضمن، تحقیقات موجود از عدم استفاده تکنیک‌های جمع‌آوری داده‌های کاملاً خودکار مبتنی بر هوش مصنوعی مانند Web Scraping، Entity Detection for Location Intelligence، Sentiment Analysis رنج می‌برد زیرا داده‌های موردنیاز آن‌ها در درجه اول بر روی تشخیص نفوذ در شبکه متمرکز است. درنتیجه، بیشتر مطالعات موجود همان‌طور که در مطالعات مرتبط (Xu et al., 2019; Keshk et al., 2021; Ten et al., 2011; Yang et al., 2017; Dey et al., 2023) نشان داده شد، فقط داده‌های ترافیک شبکه را به دست می‌آوردند. یک مطالعه (Shi et al., 2017) از داده‌های حسگر شبیه‌سازی‌شده در سیستم فیزیکی سایبری استفاده کرد. از سوی دیگر، محقق در یک پژوهش (Khan et al., 2022) از داده‌های نظرسنجی جمع‌آوری‌شده از ۲۹۴ شرکت‌کننده استفاده کرد.

هیچ‌کدام از این تحقیقات موجود، داده‌های تهدید سایبری را از منابع متعددی مانند آمار حملات سایبری برای همه کشورها از فروشندگان نرم‌افزار ضد ویروس یا اعتراضات مربوط به سایبری از پست‌های زنده رسانه‌های اجتماعی به دست نیاوردند. همان‌طور که در مقالات اخیر ما نشان داده شده است، داده‌های رسانه‌های اجتماعی در مورد ارتباط ژئوپلیتیکی، به جمع‌آوری داده‌های مبتنی بر هوش مصنوعی و پیش‌پردازش نیاز دارد. همان‌طور که محتویات رسانه‌های اجتماعی واکشی شدند، روش جدید ما در یک سری مطالعات نشان داده شد (Sufi & Alsulami, 2021a; Sufi, 2022b; Sufi et al., 2023; Sufi, 2022d; Sufi & Alsulami, 2022a; Sufi & Khalil, 2022, Sufi & Alsulami, 2022b; Sufi et al., 2022b). از تشخیص نهاد نام‌گذاری‌شده مبتنی بر هوش مصنوعی (NER) به‌منظور استخراج هوش مکانی، تجزیه‌وتحلیل احساسات برای استخراج ارتباط ذهنی محتوا و ترجمه پویا جهت درک محتوای رسانه‌های اجتماعی به ۱۱۰ زبان مختلف استفاده شد.

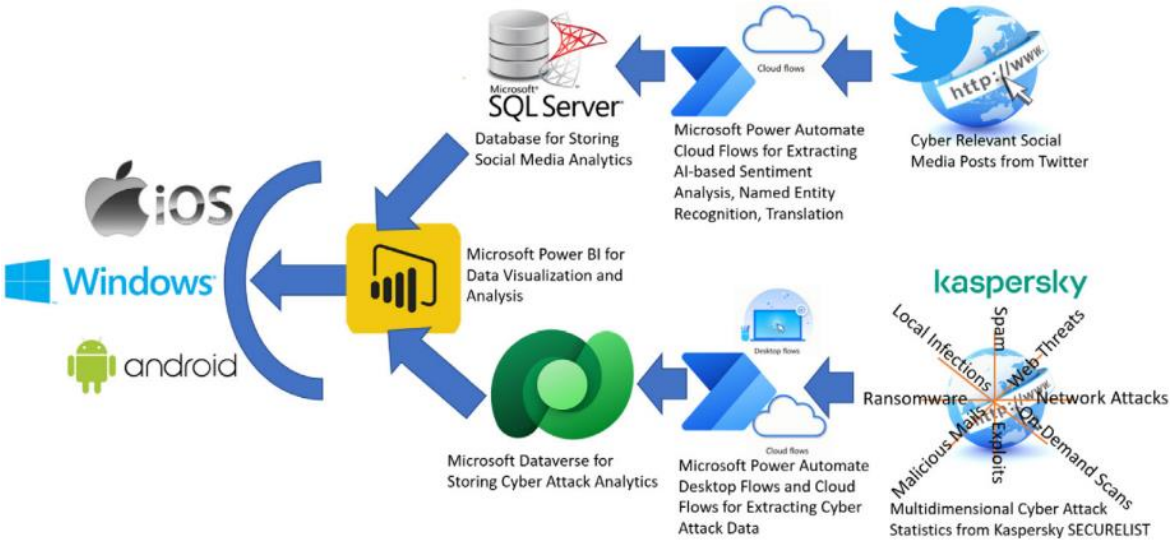
ادبیات موجود نشان می‌دهد که علاقه فزاینده‌ای به استفاده از تشخیص ناهنجاری مبتنی بر هوش مصنوعی و سایر روش‌های یادگیری عمیق برای شناسایی حملات سایبری وجود داشته است (Tetaly & Kulkani, 2022; Xu et al., 2019; Keshk et al., 2021; Abdullahi et al., 2022; Gheyas & Abdullah, 2016; Ten et al., 2011; Yang et al., 2017; Shi et al., 2018; Kotsias et al., 2022). بااین‌حال، در این مطالعات، تشخیص ناهنجاری بر روی داده‌های ترافیک شبکه با هدف تشخیص نفوذ انجام شده و هرگز گزارش نشده است که الگوریتم‌های تشخیص ناهنجاری در آمار حملات سایبری در سراسر کشور مورد استفاده قرار گرفته‌اند.

درنهایت، تقریباً هیچ‌یک از ادبیات موجود در مورد حملات سایبری، داشبوردهای تعاملی را ارائه نکردند که به‌طور خودکار برای ارائه تصمیمات مبتنی بر شواهد در مورد وضعیت سایبری برای رهبران استراتژیک به‌روزرسانی شوند.

ازآنجایی‌که یک تصمیم‌گیرنده استراتژیک نیاز به تصمیم‌گیری فوری دارد، در تصمیم‌گیری‌ها، داشبوردها باید در طیف گسترده‌ای از پلتفرم‌ها شامل موبایل، تبلت و یا دسکتاپ های سنتی، در دسترس باشند. کار تحقیقاتی موجود در مورد حمله سایبری که در (Tetaly & Kulkani, 2022; Xu et al., 2019; Keshk et al., 2021; Abdullahi et al., 2022; Gheyas & Abdullah, 2016; Ten et al., 2011; Yang et al., 2017; Shi et al., 2018; Kotsias et al., 2022) به تصویر کشیده شده است، در طیف گسترده‌ای از پلتفرم‌ها مانند ویندوز، iOS یا اندروید در دسترس نبود. لازم به ذکر است که الزام تصمیم‌گیرندگان استراتژیک برای تصمیم‌گیری فوری در طیف گسترده‌ای از پلتفرم‌ها مانند تلفن همراه دارای iOS یا Android در (Sufi & Alsulami, 2021a; Sufi, 2022b; Sufi et al., 2023; Sufi, 2022d; Sufi & Alsulami, 2022a; Sufi & Khalil, 2022; Sufi & Alsulami, 2022b, Sufi & Alsulami, 2021b; Sufi, 2021; Sufi et al., 2022a; Sufi, 2022a; Sufi, 2023c) نشان داده شده است. جدول ۱، تنگنای مطالعات موجود را به‌وضوح نشان داده که چگونه راه‌حل ارائه‌شده در این مقاله با هدف رسیدگی به این کاستی‌ها مطرح شده است.

جدول ۱. بررسی ادبیات مطالعات موجود در تحلیل تهدید سایبری با ویژگی‌های پشتیبانی‌شده

ارجاع	۱. اطلاعات تهدید سایبری در سطح کشور	۲. اکتساب خودکار داده مبتنی بر هوش مصنوعی	۳. استفاده از داده‌های چند منبعی	۴. یادگیری عمیق/ تشخیص ناهنجاری/ پیش‌بینی مبتنی بر هوش مصنوعی	۵. داشبورد، خود به‌روز می‌شود.	۶. داشبورد تعاملی برای تصمیم‌گیری	۷. در دسترس بودن داشبورد در چندین پلتفرم
Xu et al. (2019)	خیر	خیر	خیر	بله	خیر		
Keshk et al. (2021)	خیر	خیر	خیر	بله	خیر		
Dey et al. (2023)	خیر	خیر	خیر	بله	خیر		
Ten et al. (2011)	خیر	خیر	خیر	بله	بله		
Yang et al. (2018)	خیر	خیر	خیر	بله			
Shi et al. (2017)	خیر	خیر	خیر	بله			
Kotsias et al. (2022)	خیر	خیر	خیر	بله			
Khan et al. (2022)	خیر	خیر	خیر	خیر			



شکل ۱. معماری دستیابی به داده‌های حمله سایبری چندبعدی و داده‌های مربوط به رسانه‌های اجتماعی مربوط به سایبری برای تجسم داده‌های غنی و تجزیه‌وتحلیل

همان‌طور که از جدول ۱ مشاهده می‌شود، رویکرد پیشنهادی ارائه‌شده در این مقاله، داده‌های چندبعدی در مورد پوشش حملات سایبری را به‌طور خودکار به دست می‌آورد؛ ابعادی مانند هرزنامه، باج‌افزار، تهدیدات وب، حملات شبکه، ایمیل‌های مخرب، آلودگی‌های محلی، سوءاستفاده‌ها و اسکن‌های درخواستی. علاوه بر این، رویکرد ارائه‌شده، پست‌های مرتبط با سایبری را برای داشتن درک جامعی از تهدیدات سایبری که کاربران رسانه‌های اجتماعی درباره آن صحبت می‌کنند، از رسانه‌های اجتماعی زنده همچون توییتر به دست می‌آورد. در ضمن، این مقاله تکنیک‌های یادگیری عمیق مبتنی بر هوش مصنوعی (به‌عنوان‌مثال، تشخیص ناهنجاری) را بر روی داده‌های حمله سراسری در سراسر کشور اعمال می‌کند تا به‌طور خودکار سطوح بالا یا پایین غیرعادی حملات به یک کشور را شناسایی کند. درنهایت، راه‌حل ارائه‌شده در چندین سیستم‌عامل مانند دسکتاپ، تبلت و موبایل در طیف گسترده‌ای از محیط‌ها مانند

iOS، Android و Windows مستقر شده است. ازاین‌رو، تصمیم‌گیرندگان استراتژیک می‌توانند تصمیمات فوری مبتنی بر شواهد را از دستگاه انتخابی خود اتخاذ کنند. به‌روزرسانی‌های داشبورد، به‌روزترین اطلاعات را به شکل کاملاً تعاملی (خود را تازه می‌کند) ارائه می‌کند و از پشتیبانی تصمیم‌گیری مبتنی بر داده‌های موردنیاز رهبران استراتژیک امروزی پشتیبانی می‌کند (Ainslie et al., 2023).

۳- مواد و روش‌ها

داده‌های حمله سایبری جهانی چندبعدی با استفاده از ترکیبی از دسکتاپ فلو و جریان ابری در Power Automate به دست می‌آید (Microsoft Documentation, 2021). جریان دسکتاپ از جریان کنترل‌نشده Power Automate Desktop برای خودکار کردن یک سری کارها استفاده می‌کند. این اتوماسیون مرورگر را باز می‌کند، به هشت پیوند مختلف می‌رود (Kaspersky, 2023b, 2023c, 2023d, 2023e, 2023f, 2023g, 2023h, 2023i)، هشت فایل آمار حمله مختلف را دانلود می‌کند و این فایل‌ها را (به‌عنوان Microsoft Excel .xlsx) در پوشه اختصاصی One Drive برای کسب‌وکار ذخیره می‌کند. با هر فایل جدیدی که ایجاد می‌شود، یک ماشه، یک جریان ابری جداگانه Microsoft Power Automate را آغاز می‌کند که این آمار حملات را پردازش کرده و آن‌ها را در Microsoft Dataverse ذخیره می‌کند (Microsoft, 2022a).

بنابراین، با استفاده از Desktop flow و Cloud Flow، سیستم ارائه‌شده به‌طور خودکار و ناشناس خود را در یک برنامه روزانه با آمار سایبری روزانه ارائه‌شده توسط کسپرسکی به‌روز می‌کند. لازم به ذکر است که سایت‌های کسپرسکی در (Kaspersky, 2023b, 2023c, 2023d, 2023e, 2023f, 2023g, 2023h, 2023i) دسترسی به داده‌های تاریخی را فراهم نمی‌کند. هر روز، آمار روزانه سایبری با آمارهای به‌روز جایگزین می‌شود.

ازاین‌رو، سیستم ارائه‌شده آمار سایبری تاریخی را به‌صورت روزانه (نه در زمان واقعی) ایجاد می‌کند. بااین‌حال، سیستم ارائه‌شده از به‌روزرسانی‌های بی‌درنگ (با استفاده از پشته فناوری Microsoft Power Automate)، زمانی که آمار حملات سایبری در زمان واقعی (توسط منابع داده) ارائه می‌شود، پشتیبانی می‌کند. از سوی دیگر، پست‌های رسانه‌های اجتماعی از توییتر با استفاده از جریان Microsoft Power Automate استخراج می‌شوند. در طول این استخراج، تجزیه‌وتحلیل احساسات مبتنی بر هوش مصنوعی، NER، ترجمه همان‌طور که در جدیدترین تحقیق ما نشان داده شده است، انجام می‌شود. درنهایت، این رکوردها در پایگاه داده مایکروسافت SQL Server ذخیره می‌شوند.

Microsoft Power BI (۲۰۲۲b)، هر دو این منابع داده را به دست می‌آورد (داده‌های تهدید سایبری چندبعدی کسپرسکی و پست‌های رسانه‌های اجتماعی مرتبط با سایبری از توییتر) تا تجزیه‌وتحلیل داده‌ها و تجسم داده‌ها را برای تصمیم‌گیرندگان استراتژیک در پلتفرم‌های iOS، ویندوز و اندروید ارائه دهد. شکل ۲، این فرآیند کلی را نشان می‌دهد. علاوه بر این، جدول ۲ جزئیات مربوط به اجزاء مختلف فناوری مورد استفاده در سیستم پیشنهادی را همراه با توجیهات ارائه می‌دهد. جدول ۲ به ویژگی‌های فردی که در جدول ۱ ارائه شده است، اشاره داشته و آن ویژگی‌ها را به اجزاء فناوری ترسیم می‌کند.

همان‌طور که از شکل ۲ و جدول ۱ پیداست، تشخیص ناهنجاری مبتنی بر هوش مصنوعی، فناوری کلیدی است که به تجزیه‌وتحلیل تصمیم‌گیری قدرت می‌بخشد. تشخیص ناهنجاری با شناسایی خودکار ناهنجاری‌ها در داده‌های سری زمانی، ویژگی‌های اضافی را به نمودارهای خطی اضافه می‌کند. همچنین، توضیحاتی بر اساس (Microsoft Documentation, 2020) پردازش زبان طبیعی (NLP) برای ناهنجاری‌هایی که تجزیه‌وتحلیل علت ریشه‌ای را تسهیل می‌کنند، ارائه می‌کند. در جدیدترین مطالعه خود، از تشخیص ناهنجاری مبتنی بر هوش مصنوعی برای شناسایی

موارد غیرعادی زمین‌لغزش همراه با علل ریشه‌ای (Sufi & Alsulami, 2021b; Sufi, 2021)، ناهنجاری‌های رویدادهای فاجعه از پست‌های رسانه‌های اجتماعی (Sufi & Khalil, 2022; Sufi, 2022c)، ناهنجاری‌ها در رویدادهای جهانی توسط نظارت بر ۲۳۹۷ منبع خبری جهانی (Sufi & Alsulami, 2021a; Sufi, 2022b) و حتی برای آگاهی موقعیتی COVID-19 (Sufi, 2023c) استفاده نمودیم. قبل از پرداختن به جزئیات تشخیص ناهنجاری، ما تعریف مسئله را ارائه می‌کنیم.

مسئله ۱. با توجه به دنباله‌ای از مقادیر واقعی $x = x1$، $x2$، $x3$، ...، xn، وظیفه تشخیص ناهنجاری سری‌های زمانی این است که یک دنباله خروجی $y = y1$، $y2$، y،...، yU تولید کنند. آیا $i \{ ۰$ یک نقطه ناهنجار است؟

راه‌حل پیاده‌سازی‌شده، باقیمانده طیفی (SR) را از حوزه تشخیص برجستگی بصری قرض گرفت و سپس، یک شبکه عصبی کانولوشنال (CNN) را به نتایج تولیدشده توسط مدل SR اعمال کرد (Ren et al., 2019).

الگوریتم SR از سه مرحله اصلی تشکیل شده است:

۱. تبدیل فوریه را برای به دست آوردن طیف دامنه log انجام دهید.

۲. SR را محاسبه کنید.

۳. تبدیل فوریه معکوس را انجام دهید که دنباله را به حوزه فضایی برمی‌گرداند.

$$A(f) = Amplitude(f(x))$$
$$P(f) = Phrase(f(x))$$
$$L(f) = log(A(f))$$
$$AL(f) = h_q(f).L(f)$$
$$R(f) = L(f) - AL(f)$$
$$S(x) = \left\| f^{-1}(\exp(R(f) + iP(f))) \right\|$$

جدول ۲. اجزاء فناوری مورد استفاده برای اتوماسیون

مؤلفه تکنولوژی	هدف	ویژگی مورد حمایت از جدول ۱
Microsoft Power Automate	گرفتن توییت‌های مرتبط با سایبری ترجمه مبتنی بر هوش مصنوعی تجزیه‌وتحلیل احساسات مبتنی بر هوش مصنوعی تشخیص نهاد نام‌گذاری‌شده مبتنی بر هوش مصنوعی	ویژگی ۱ (در سطح کشور) ویژگی ۲ (اکتساب داده) ویژگی ۳ (داده‌های چند منبعی)
Microsoft Desktop Automate	اتوماسیون برای دستیابی به حمله سایبری دریافت داده‌ها از ۸ منبع مختلف و ذخیره آن‌ها به‌عنوان فایل‌های xlsx در مایکروسافت یک درایو	ویژگی ۱ (در سطح کشور) ویژگی ۲ (اکتساب داده) ویژگی ۳ (داده‌های چند منبعی)
Microsoft Power BI	تشخیص ناهنجاری مبتنی بر هوش مصنوعی پیش‌بینی هموارسازی نمایی داشبورد برای ویندوز برنامه iOS برنامه اندروید	ویژگی ۴ (استفاده از AI/CNN) ویژگی ۵ (داشبورد) ویژگی ۶ (داشبورد) ویژگی ۷ (چند پلتفرم)
Microsoft Dataverse	ذخیره آمار حملات سایبری روزانه	ویژگی ۱ (در سراسر کشور) ویژگی ۲ (اکتساب داده)
Microsoft SQL Server	ذخیره‌سازی و مدیریت توییت‌ها	ویژگی ۱ (در سراسر کشور) ویژگی ۲ (اکتساب داده)

حوزه فضایی با استفاده از تبدیل فوریه معکوس. دنباله حاصل S(x) به‌عنوان نقشه برجسته نامیده می‌شود (Zhao et al., 2015). مقادیر نقاط ناهنجاری به‌صورت زیر محاسبه می‌شود:

$$x = (\text{میانگین} + x) + r.x1+(\text{میانگین} + \text{var}) \quad (۸)$$

که در آن، x میانگین محلی نقاط قبلی است، میانگین و var میانگین و واریانس تمام نقاط در پنجره کشویی فعلی هستند و r~N (۰، ۱) به‌طور تصادفی نمونه‌برداری می‌شود. در این فرآیند، CNN به‌جای استفاده از ورودی خام، بر روی نقشه برجسته اعمال می‌شود؛ بنابراین، کارایی فرآیند کلی تشخیص ناهنجاری افزایش می‌یابد (Ren et al., 2019; Zhao et al., 2015). درواقع، ما تشخیص ناهنجاری را با استفاده از تجسم نمودار خطی Microsoft Power BI در سه مرحله پیاده‌سازی می‌کنیم:

• همه ناهنجاری‌ها را در سری‌های زمانی (به‌عنوان‌مثال، هر مقداری که خارج از محدوده آستانه قرار دارد) شناسایی کنید. برای فرآیند تشخیص ناهنجاری، از تمام آمار حملات خاص کشور (داده‌های سری زمانی) استفاده شد. تجسم نمودار خطی Microsoft Power BI از CNN (شامل تبدیل فوریه، SR و تبدیل فوریه معکوس) برای انجام تشخیص ناهنجاری در آمار حملات خاص کشور استفاده می‌کند.

محرک‌های اصلی این ناهنجاری‌ها را شناسایی کنید. برای به دست آوردن محرک‌های اصلی از داده‌های رسانه‌های اجتماعی و آمار حملات سایبری از کسپرسکی (۲۰۲۳a) استفاده شد.

• نتایج را به زبان طبیعی (توضیح علت اصلی) با استفاده از NLP توضیح دهید (Microsoft Documentation, 2020).

لازم به ذکر است که فرآیند بالا برای تشخیص ناهنجاری مبتنی بر CNN با اجرای Microsoft BI تقریباً آنی است (Microsoft Documentation, 2023). همان‌طور که از جدول ۲ مشاهده می‌شود، سیستم ارائه‌شده از یک الگوریتم هموارسازی نمایی برای پیش‌بینی حملات سایبری در سطح کشور استفاده می‌کند. هموارسازی نمایی، یک تکنیک پیش‌بینی سری زمانی برجسته و ماهرانه است که به طرز ماهرانه‌ای با حوزه پیش‌بینی حملات سایبری سازگار شده است (Ravinder & Kulkani, 2023; Sufi, 2023a). این الگوریتم از طریق تعامل هنرمندانه میانگین‌های وزنی، روندها و الگوهای پنهان موجود در داده‌های حمله سایبری تاریخی را شناسایی می‌کند. با محاسبه مجدد پیش‌بینی‌ها و تعدیل ماهرانه پارامتر هموارسازی، الگوریتم به‌خوبی ظرفیت پیش‌بینی خود را برای تطبیق با اولویت زمانی تنظیم می‌کند و درعین‌حال، تأثیر داده‌های تاریخی را کاهش می‌دهد (Altintasi, 2023). با توجه به کیفیت و کمیت داده‌ها و استواری الگوهای حملات سایبری، کارآمدی این روش (هموارسازی تصاعدی) در ارائه دقیق و روشن چشم‌انداز تهدیدات سایبری است.

۴- نتایج

روش پیشنهادی با استفاده از مؤلفه‌های مختلف Microsoft Power Platform (Microsoft Documentation, 2021; Microsoft, 2022a, 2022b)، همان‌طور که در بخش قبلی از ۱۱ اکتبر ۲۰۲۲ تا ۳۱ اکتبر ۲۰۲۲ شرح داده شد، پیاده‌سازی و اجرا شد. آلودگی محلی، نامه‌های مخرب، حمله شبکه، اسکن درخواستی، باج‌افزار، هرزنامه و تهدید وب به‌طور خودکار با استفاده از Microsoft Power Automate و Microsoft Dataverse ضبط شدند. جدول ۳، آمار دقیق این ۳۰ هزار رکورد را ارائه می‌دهد. هر یک از ستون‌های جدول ۳، از آمارهای روزانه بهره‌برداری تا تهدید وب به‌طور خودکار توسط سیستم ارائه‌شده از URL آمار تهدیدات کسپرسکی (https://statistics.securelist.com) برای هشت نوع مختلف از تهدیدات سایبری واکشی شده است.

به‌عنوان‌مثال، بهره‌برداری، آلودگی محلی، ایمیل مخرب، حمله شبکه، اسکن درخواستی، باج‌افزار، گستره و تهدید وب. تجمیع روزانه این هشت نوع تهدید در ستون "آمار تعداد حملات" جدول ۳ ارائه شده است.

علاوه بر این، پیاده‌سازی ما با Microsoft Power Automate و Microsoft SQL Server، به‌طور خودکار ۳۷۸۹ توییت را از ۳۴۰۲ کاربر مجزای توییت جمع‌آوری کرد. همان‌طور که از جدول ۴ مشاهده می‌شود، این توییت‌ها به‌طور خودکار با الگوریتم‌های مبتنی بر هوش مصنوعی برای درک توییت ها در ۳۷ زبان مجزا پردازش شدند. ۸۹۳ توییت غیر انگلیسی نیز به‌صورت پویا ترجمه شدند. ستون «تعداد ترجمه‌ها» نشان می‌دهد که هر روز چند توییت غیر انگلیسی با ترجمه بعدی ثبت می‌شود.

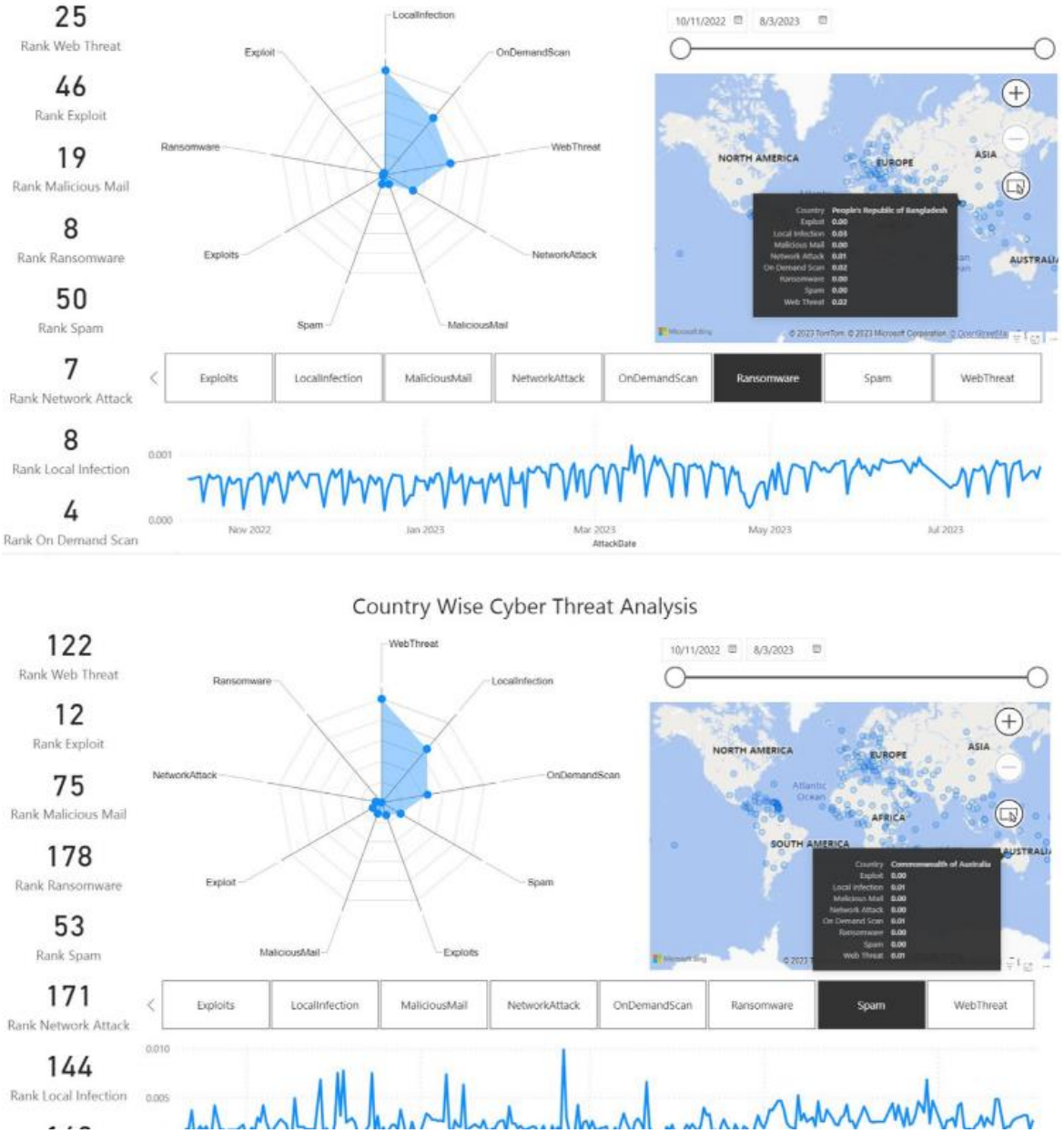
این ستون (تعداد ترجمه) نشان‌دهنده توانایی و ظرفیت سیستم ارائه‌شده در درک توییت‌های چندزبانه برای آگاهی موقعیتی جامع‌تر است. تجزیه‌وتحلیل دقیق احساسات نشان داد که بیشترین احساسات منفی (با میانگین احساسات منفی ۰/۴۴) در ۲۴ اکتبر ۲۰۲۲ مشاهده شد، زمانی که بسیاری از مردم از حملات سایبری اخیر به ارائه‌دهندگان مخابرات و بیمه درمانی استرالیا ناراحت بودند.

درحالی‌که جدول ۳، آمار مربوط به داده‌های حملات سایبری را نشان می‌دهد، جدول ۴ آماری را در مورد داده‌های رسانه‌های اجتماعی تحلیل‌شده نشان می‌دهد. سیستم ارائه‌شده شروع به دریافت داده‌های رسانه‌های اجتماعی از ۱۳ اکتبر ۲۰۲۲ در مقابل ۱۱ اکتبر ۲۰۲۲ کرد؛ بنابراین، تاریخ شروع جدول ۳ و جدول ۴ ۲ روز متفاوت است. لازم به ذکر است که اطلاعات مربوط به سایبری (اعم از داده‌های حمله واقعی یا داده‌های به‌دست‌آمده از طریق رسانه‌های اجتماعی) بسته به پویایی‌های ژئوپلیتیک، اجتماعی، نظامی و دیپلماتیک روزانه تغییر می‌کند. این پویایی در حال تغییر داده‌های مرتبط با سایبری، بینش‌های کاملاً متفاوت مبتنی بر هوش مصنوعی را همان‌طور که در مقالات اخیر گزارش شده است، ارائه می‌کند (Yadav et al., 2023; Dale et al., 2023; Dempsey, 2023; Maathuis & Godschalk, 2023).

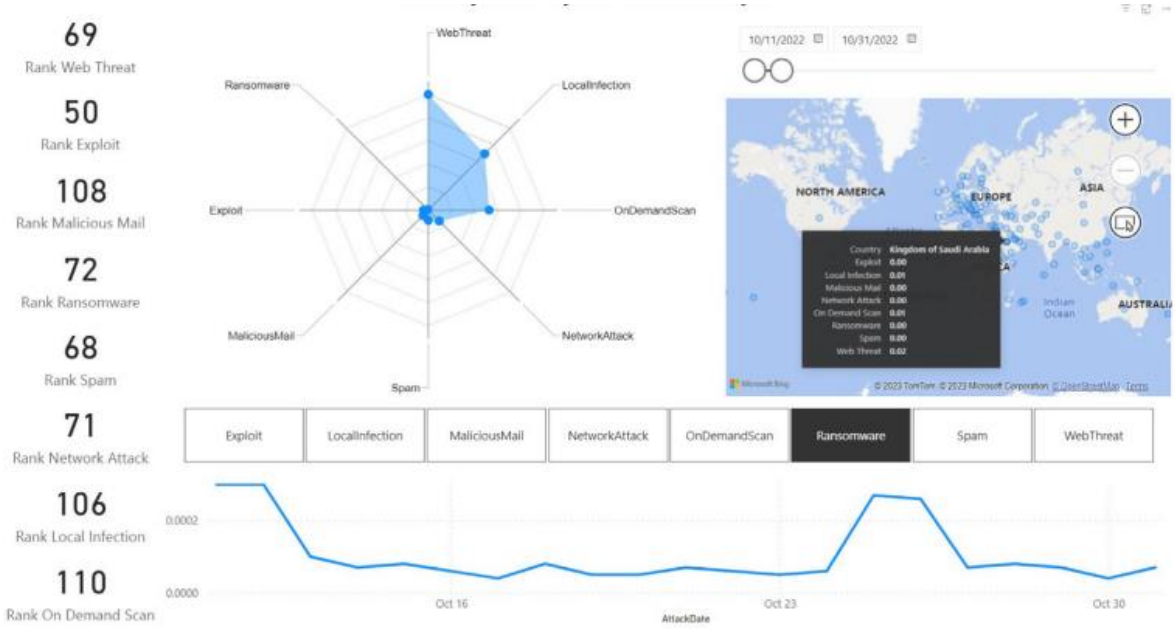
اولین نیاز همان‌طور که در CR 1 شناسایی شده است، تجزیه‌وتحلیل طیف تهدید در برابر ابعاد مختلف حملات سایبری برای یک کشور خاص و مقایسه با سایر کشورهای جهان است. در شکل ۱(a)، همان‌طور که بنگلادش مشخص شده است، تصمیم‌گیرنده استراتژیک می‌تواند به‌راحتی رتبه‌بندی در مورد تهدیدات سایبری مختلف را مشاهده کند (سمت چپ). برای بنگلادش، در دوره نظارت‌شده، رتبه تهدید وب ۲۵، رتبه Exploit 46، رتبه ایمیل‌های مخرب ۱۹، رتبه باج‌افزار ۸، رتبه هرزنامه ۵۰، رتبه حمله شبکه ۷، رتبه آلودگی محلی ۸ و درنهایت، On بود (رتبه اسکن تقاضا در مقیاس جهانی ۴ بود). همچنین، نمودار رادار در مرکز شکل ۳ (الف) نشان می‌دهد که در بنگلادش، درصد آلودگی مکان بالاتر است و به دنبال آن، اسکن بر اساس تقاضا، تهدید وب، حمله شبکه و سپس، ابعاد دیگر قرار دارند. شکل ۳(b)، طیف تهدید سایبری استرالیا را نشان می‌دهد که در همان دوره زمانی کاملاً متفاوت است. در استرالیا (به‌عنوان‌مثال، شکل ۳ (ب))، درصد تهدیدات وب بالاترین است و پس از آن، آلودگی‌های مکان، اسکن بر اساس تقاضا، Span، Exploit و سپس موارد دیگر قرار دارند. شکل ۳، نمونه‌ای از اینکه چگونه یک تصمیم‌گیرنده استراتژیک می‌تواند تفاوت در طیف‌های تهدید سایبری را در بین تعدادی از کشورها تجزیه‌وتحلیل کند، ارائه می‌دهد.

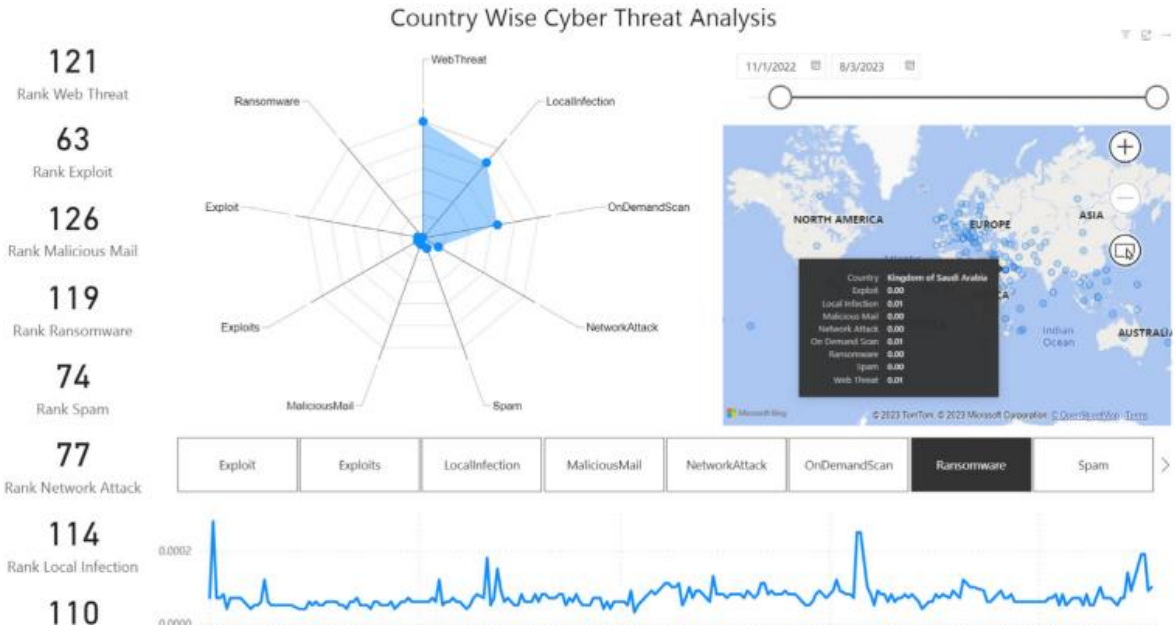
سپس، CR 2 تجزیه‌وتحلیل تغییر طیف تهدید را بر حسب زمان برای هر کشوری الزامی می‌کند. شکل ۴، طیف تهدید سایبری برای عربستان سعودی را بین دو بازه زمانی مختلف نشان می‌دهد. همان‌طور که از شکل ۴ (الف) مشاهده می‌شود، رتبه عربستان سعودی در مورد تهدید وب، سوءاستفاده، پست‌های مخرب، باج‌افزار، هرزنامه، حمله شبکه، آلودگی محلی و اسکن درخواستی، از ۱۱ اکتبر ۲۰۲۲ تا ۳۱ اکتبر ۲۰۲۲، به ترتیب ۶۹، ۵۰، ۱۰۸، ۷۲، ۶۸، ۷۱، ۱۰۶ و

۱۱۰ بوده است. بااین‌حال، از ۱ نوامبر ۲۰۲۲ تا ۳ آگوست ۲۰۲۳، رتبه جهانی عربستان سعودی از نظر تهدید وب، سوءاستفاده، ایمیل مخرب، باج‌افزار، هرزنامه، حمله شبکه، آلودگی موضعی و اسکن درخواستی، به ترتیب ۱۲۱، ۶۳، ۱۲۶، ۱۱۹، ۷۴، ۷۷، ۱۱۴ و ۱۱۰ بود (همان‌طور که در شکل ۴ (ب) مشاهده می‌شود). ازاین‌رو، شکل ۴ به‌وضوح تغییر طیف تهدید را بر حسب زمان برای عربستان سعودی که از CR 2 حمایت می‌کند، نشان می‌دهد.

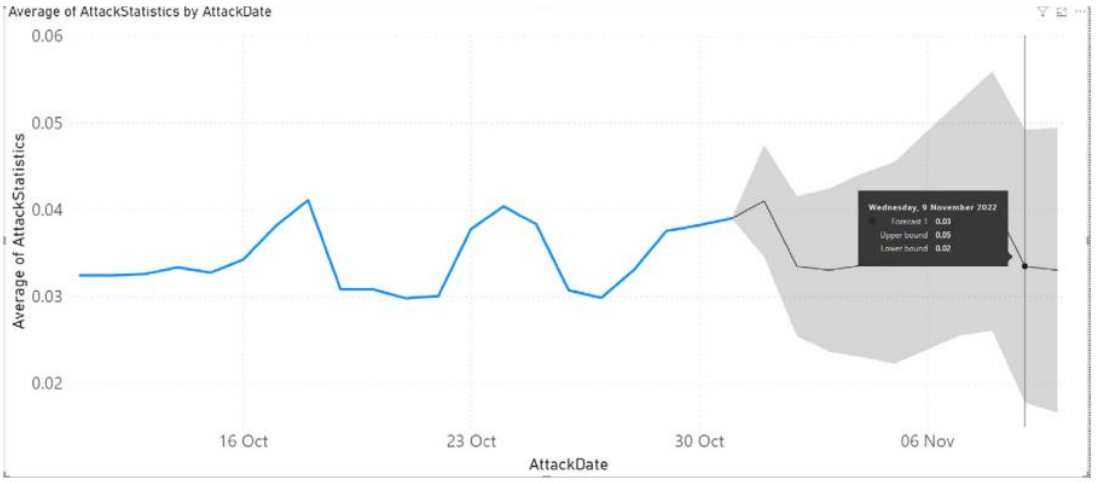


شکل ۲. تجزیه‌وتحلیل طیف تهدید سایبری در برابر ابعاد متعدد حملات سایبری بین بنگلادش و استرالیا که CR 1 را برآورده می‌کند.

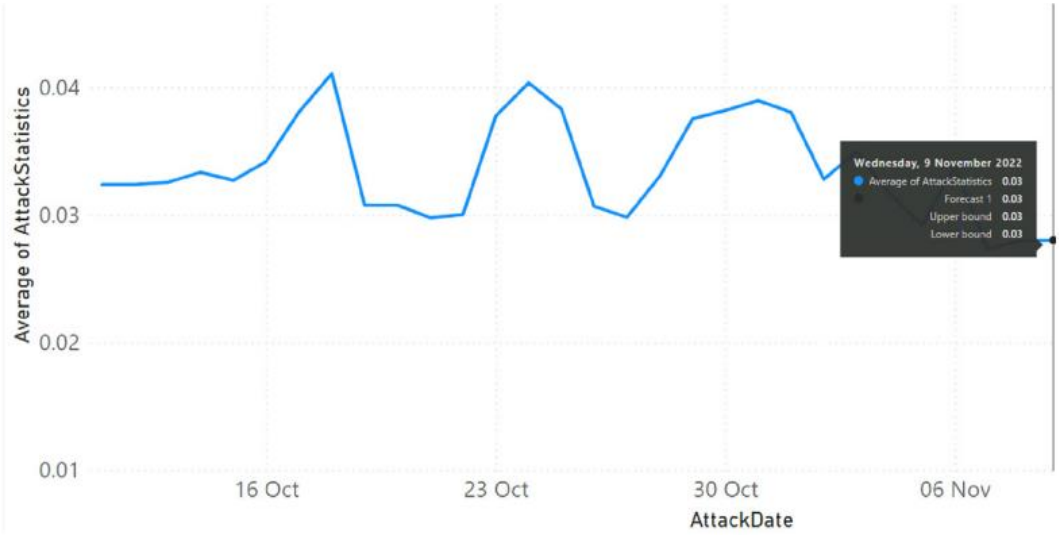




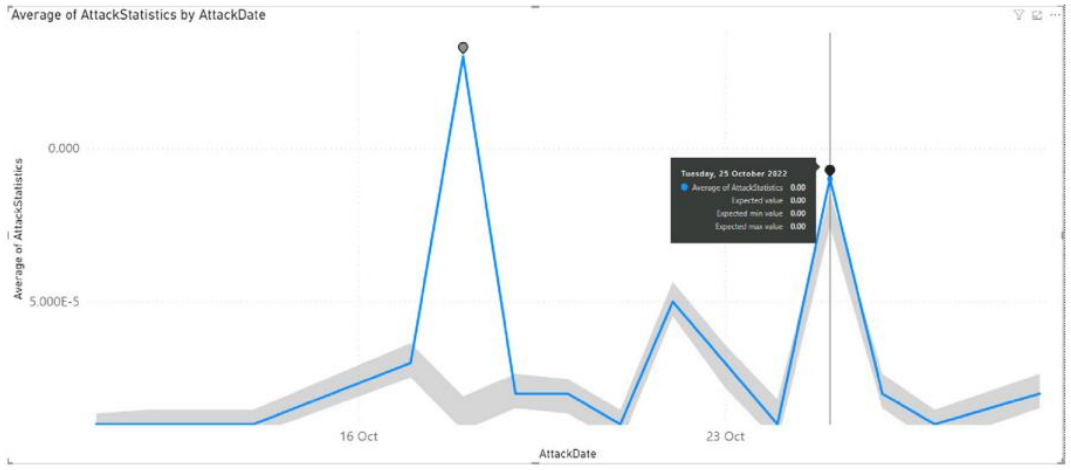
شکل ۳. تجزیه‌وتحلیل طیف تهدید سایبری در برابر ابعاد متعدد حملات سایبری بین دو بازه زمانی مختلف برای عربستان سعودی که CR 2 را برآورده می‌کند.



شکل ۴. با تجزیه‌وتحلیل داده‌های حملات سایبری گذشته که CR 3 را انجام می‌دهند، حملات سایبری را برای هر کشوری در جهان پیش‌بینی کنید.



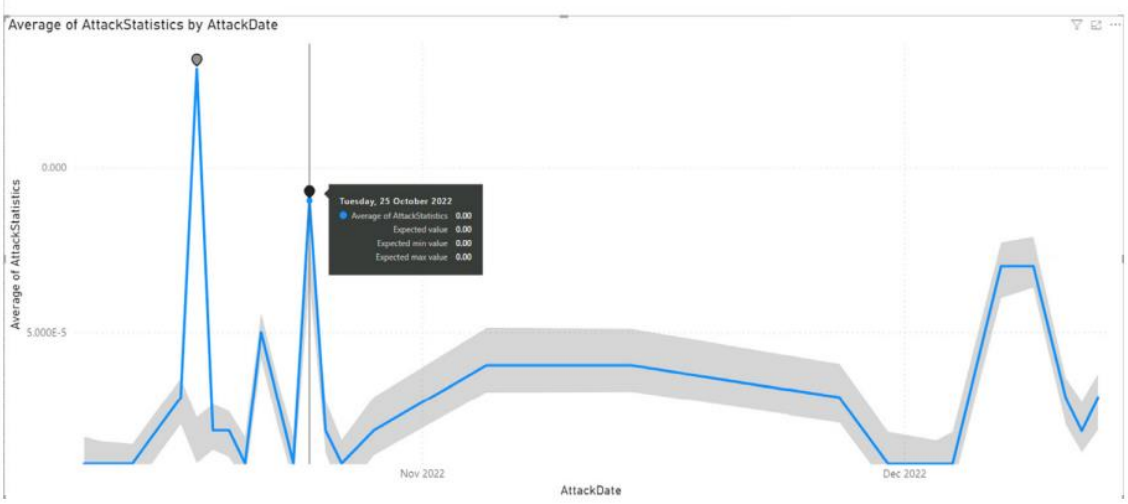
شکل ۵. اعتبارسنجی حمله سایبری پیش‌بینی‌شده شکل ۵ با داده‌های واقعی حمله سایبری در ۹ نوامبر ۲۰۲۲ برای چین (اعتبارسنجی CR 3).



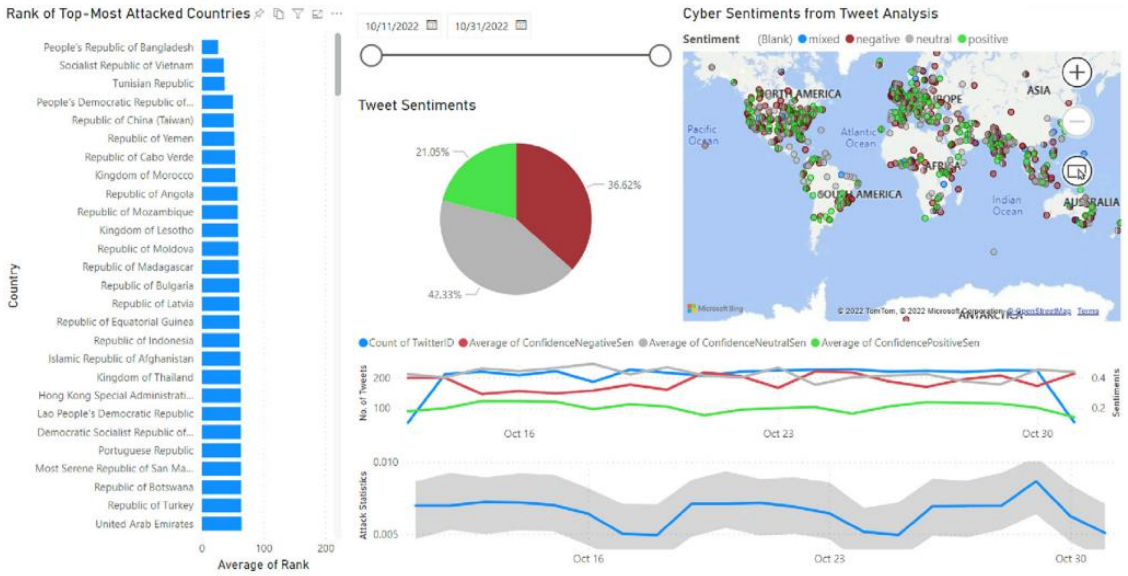
شکل ۶. دو ناهنجاری در طیف‌های تهدید سایبری برای جمهوری پالائو با تجزیه‌وتحلیل داده‌های حملات سایبری گذشته که CR 4 را برآورده می‌کردند، شناسایی شد.

الزام در CR 3 مشخص می‌کند که سیستم پیشنهادی باید بتواند با تجزیه‌وتحلیل داده‌های حملات سایبری گذشته، حملات سایبری را برای هر کشوری در جهان پیش‌بینی کند. شکل ۵ نشان می‌دهد که حمله سایبری برای چین در ۹ نوامبر ۲۰۲۲ با استفاده از داده‌های حمله سایبری تاریخی از ۱۱ اکتبر ۲۰۲۲ تا ۳۱ اکتبر ۲۰۲۲ پیش‌بینی شده است. سیستم ارائه‌شده در این مقاله به تصمیم‌گیرندگان استراتژیک اجازه می‌دهد تا هر کشوری را در جهان با استفاده از آن انتخاب کنند. لیست کشویی و بلافاصله تهدید سایبری با تجزیه‌وتحلیل سوابق حملات سایبری گذشته با رعایت الزامات مشخص‌شده در CR 3، پیش‌بینی می‌شود. آمار واقعی تهدید برای همان روز (۹ نوامبر ۲۰۲۳) به دست آمد. شکل ۶ نشان می‌دهد که تهدید واقعی برای چین در ۹ نوامبر ۲۰۲۳ برابر با ۰/۰۳ بوده؛ همان چیزی است که در شکل ۵ پیش‌بینی شده بود. در تجزیه‌وتحلیل داده‌های حملات سایبری گذشته، همان‌طور که در شکل ۷ مشاهده می‌شود، جمهوری پالائو از لیست کشویی بالا انتخاب شده است و دو ناهنجاری (یکی در ۱۸ اکتبر ۲۰۲۲ و دیگری در ۲۵ اکتبر ۲۰۲۲) با استفاده از یادگیری عمیق مبتنی بر CNN شناسایی شده است. برای تأیید تداوم این دو ناهنجاری، تشخیص ناهنجاری تا پایان سال ۲۰۲۲ (دسامبر ۲۰۲۲) در همان کشور انجام شد. همان‌طور که از شکل ۷ مشاهده می‌شود، این دو ناهنجاری شکل ۶ تا دسامبر ۲۰۲۲ ادامه داشت.

شکل ۸، یکی دیگر از ویژگی‌های سیستم پیشنهادی را نشان می‌دهد؛ جایی که یک تحلیلگر سایبری در حال تجزیه‌وتحلیل احساسات سراسر جهان در مورد موضوعات مرتبط با سایبری با تجزیه‌وتحلیل رسانه‌های اجتماعی مبتنی بر هوش مصنوعی است. کاربر سیستم می‌تواند هر بازه زمانی را با استفاده از جدول زمانی انتخاب کند و بلافاصله احساسات جهانی در طول مدت‌زمان مشخص‌شده ارائه می‌شود. احساسات منفی، مثبت و خنثی با رنگ‌های قرمز، سبز و خاکستری نشان داده می‌شود. همان‌طور که از نمودار دایره‌ای در شکل ۸ مشاهده می‌شود، میانگین احساسات کاربران رسانه‌های اجتماعی بین ۱۱ اکتبر ۲۰۲۲ و ۳۱ اکتبر ۲۰۲۲، ۳۶/۶۲ درصد منفی، ۲۱/۰۵ درصد مثبت و ۴۲/۳۳ درصد بوده است. نمودار خطی، درست زیر نمودار دایره‌ای، پویایی تغییر احساسات کاربران را در طول زمان بین ۱۱ اکتبر ۲۰۲۲ و ۳۰ اکتبر ۲۰۲۲ نشان می‌دهد. CR 5، تجزیه‌وتحلیل دیدگاه کاربران رسانه‌های اجتماعی را در مورد مسائل مختلف سایبری در طول زمان الزامی می‌کند. همان‌طور که در شکل ۷ مشاهده می‌شود، پیام رسانه‌های اجتماعی مرتبط با سایبر به هر زبانی به دست می‌آید و به دنبال آن، ترجمه خودکار به زبان انگلیسی (برای پست‌های غیر انگلیسی) و تجزیه‌وتحلیل احساسات انجام می‌شود. این فرآیند تجزیه‌وتحلیل احساسات، دیدگاه کاربران را به احساسات چندگانه (به‌عنوان‌مثال، مثبت، منفی، مختلط) تبدیل می‌کند، همان‌طور که در شکل ۸ نشان داده شده است. باید توجه داشت که در چارچوب CR 5، دیدگاه کاربران رسانه‌های اجتماعی، عمومی است (به‌عنوان‌مثال، هر چیزی که مربوط به کلمه کلیدی "سایبر" یا "هک" است، همان‌طور که قبلاً در شکل ۱ نشان داده شده است). تجزیه‌وتحلیل موضوع در این مطالعه اعمال نشده بود؛ بنابراین، شکل ۸ نشان می‌دهد که چگونه سیستم پیشنهادی به دستورات CR 5 عمل می‌کند.



شکل ۷. اعتبارسنجی ناهنجاری‌های مشخص‌شده در طول زمان (اعتبارسنجی CR 4).



شکل ۸. تجزیه‌وتحلیل دیدگاه کاربران رسانه‌های اجتماعی در مورد مسائل مختلف سایبری بین ۱۱ اکتبر ۲۰۲۲ و ۳۱ اکتبر ۲۰۲۲ با حمایت از CR 5

درنهایت، CR 6 به کاربران استراتژیک نیاز دارد که الزامات تحلیلی را از CR 1 تا CR 5 در هر دستگاهی (چه موبایل، تبلت یا رایانه رومیزی) انجام دهند. درحالی‌که انجیر ۳ تا ۹ سیستم پیشنهادی در حال اجرا بر روی محیط دسکتاپ مبتنی بر ویندوز را نشان می‌دهد، شکل ۱۰ نشان می‌دهد که تهدید سایبری در سراسر جهان در یک تبلت (Apple iPad) دارای iOS تجزیه‌وتحلیل می‌شود. در برنامه iOS مستقرشده، تصمیم‌گیرنده می‌تواند به‌وضوح ببیند که بنگلادش با ترکیب چندین ابعاد تهدیدات سایبری در طول دوره نظارت‌شده، بالاترین تهدید کشور است. پس از بنگلادش، پنج کشور در معرض خطر سایبری، ویتنام، تونس، الجزایر، چین و یمن بودند. این رتبه‌بندی با گذشت زمان تغییر می‌کند. با استفاده از اطلاعات ارائه‌شده توسط راه‌حل پیشنهادی ما، استراتژیست‌های ملی سایبری می‌توانند تصمیمات آگاهانه‌ای در مورد وضعیت سایبری یک کشور در هر زمان اتخاذ کنند.

درنهایت، شکل ۱۱ برنامه اندروید مستقرشده را نشان می‌دهد که راه‌حل ارائه‌شده را در تلفن همراه (Samsung

Ultra Galaxy S23) اجرا می‌کند. همان‌طور که از شکل ۱۱ پیداست، یک تحلیلگر در حال انجام تجزیه‌وتحلیل دقیق تهدیدات سایبری برای هند است. در طول دوره نظارت، هند بیشتر تحت تأثیر هرزنامه، تهدید وب، آلودگی محلی و سایر ابعاد تهدیدات سایبری قرار گرفت. همچنین، شکل ۱۱ نشان داد که در دوره نظارت‌شده، رتبه هرزنامه هند نهمین در جهان بود. رتبه تهدیدات وب، سوءاستفاده‌ها، ایمیل‌های مخرب، باج‌افزارها، هرزنامه‌ها و حملات شبکه، به ترتیب ۱۱۰، ۸۱، ۱۵۲، ۱۰۸، ۹ و ۳۴ بود.

هر دو انجیر ۱۰ و ۱۱ نشان دادند که چگونه الزامات مشخص‌شده در CR 6 توسط راه‌حل پیشنهادی برآورده شده است. در ابتدای این مقاله، شش نیاز تحلیلی شناسایی شد. این الزامات حیاتی توسط مطالعات موجود در (Tetaly & Kulkani, 2022; Xu et al., 2019; Keshk et al., 2021; Abdullahi et al., 2022; Gheyas & Abdullah, 2016; Ten et al., 2011; Yang et al., 2017; Shi et al., 2018; Kotsias et al., 2022) مورد توجه قرار نگرفته است. همان‌طور که از جدول ۳ مشاهده می‌شود، این ۶ نیاز حیاتی به‌طور کامل راه‌حل پیشنهادی را برآورده می‌کنند.

نسخه آزمایشی سیستم ارائه‌شده در

https://app.powerbi.com/view?r=eyJrIjoiYWJjOGY5YTUŁZDBINY00MTg1LWFkMTMtM2RmYzYzODQ1NzE1IiwidCI6IjBkMWI4YmRILWJjOGY5YTUŁZDBINY00MTg1LWFkMTMtM2RmYzYzODQ1NzE1IiwidCI6IjBkMWI4YmRILWJjOGY5YTUŁZDBINY00MTg1LWFkMjYmEwNSJ9&pageName=ReportSection در دسترس است. همان‌طور که از جدول ۳ مشاهده می‌شود، این مقاله علمی یک راه‌حل هوشمند سایبری پیچیده را ارائه می‌دهد که شامل شش معیار تصمیم‌گیری حیاتی جهت تصمیم‌گیری استراتژیک مبتنی بر شواهد در امنیت سایبری است. در مرحله اول، این راه‌حل مستلزم تجزیه‌وتحلیل عمیق تهدیدات سایبری، با در نظر گرفتن ابعاد مختلف حملات برای کشورهای خاص و مقایسه آن‌ها در سطح جهانی است (به‌عنوان‌مثال، CR 1 از جدول ۳). این تجزیه‌وتحلیل، بینش‌های ارزشمندی را در مورد پیچیدگی تهدیدات سایبری ارائه می‌کند و سهامداران را قادر می‌سازد تا اقدامات امنیت سایبری خود را در برابر همتایان بین‌المللی، ارزیابی و همکاری در مبارزه جهانی علیه جرائم سایبری را تسهیل کنند. ثانیاً، این راه‌حل شامل نظارت در زمان واقعی نوسانات تهدید در طول زمان است و تصمیم‌گیرندگان را قادر می‌سازد تا به‌سرعت به تهدیدات نوظهور پاسخ دهند و منابع را به‌طور مؤثر تخصیص دهند (CR 2 از جدول ۳). با درک الگوهای زمانی در حملات سایبری، تیم‌های امنیتی می‌توانند اقدامات دفاعی پیشگیرانه را اجرا نموده و بودجه‌های امنیت سایبری را بر اساس روند تهدید بهینه سازند.

جدول ۳. ارضای CR 1 تا CR 6 توسط راه‌حل پیشنهادی

الزامات بحرانی (CR) راه‌حل پیشنهادی مطابق با CR
CR 1: تجزیه‌وتحلیل طیف تهدید در برابر ابعاد مختلف حملات سایبری برای یک کشور خاص و مقایسه با سایر کشورهای جهان، شکل ۳
CR 2: تجزیه‌وتحلیل تغییر طیف تهدید بر اساس زمان برای هر کشور، شکل ۴
CR 3: پیش‌بینی حملات سایبری برای هر کشوری در جهان با تجزیه‌وتحلیل داده‌های حملات سایبری گذشته، شکل ۵ و شکل ۶
CR 4: با تجزیه‌وتحلیل داده‌های حملات سایبری گذشته، ناهنجاری‌ها را در طیف‌های تهدید سایبری برای هر کشوری در جهان شناسایی کنید؛ شکل ۷ و شکل ۸
CR 5: تجزیه‌وتحلیل دیدگاه کاربران رسانه‌های اجتماعی در مورد مسائل مختلف سایبری در طول زمان، شکل ۸
CR 6: الزامات تحلیلی فوق را در هر پلتفرم روی هر دستگاهی به دست آورید؛ شکل ۳، شکل ۴، شکل ۵، شکل ۶، شکل ۷، شکل ۸، شکل. ۹، شکل ۱۰ و شکل ۱۱.

ثالثاً، این راه‌حل از تجزیه‌وتحلیل پیش‌بینی‌کننده داده‌های حمله سایبری گذشته برای پیش‌بینی تهدیدات آینده استفاده می‌کند (به‌عنوان‌مثال، CR 3 از جدول ۳). این قابلیت پیش‌بینی، سازمان‌ها و دولت‌ها را برای اتخاذ تدابیر پیشگیرانه، افزایش انعطاف‌پذیری و کاهش تأثیر حملات سایبری بالقوه توانمند می‌سازد. توانایی پیش‌بینی و آماده‌سازی برای تهدیدات سایبری در حفاظت از زیرساخت‌های حیاتی و داده‌های حساس مهم است.

چهارم، راه‌حل اطلاعات سایبری مجهز به قابلیت‌های تشخیص ناهنجاری است که امکان شناسایی الگوهای غیرعادی و کمپین‌های هدفمند را فراهم می‌کند (به‌عنوان‌مثال، CR 4 از جدول ۵). با شناسایی اکسپلویت‌های روز صفر و حملات پیچیده، تحلیلگران امنیتی می‌توانند استراتژی‌های واکنش به حادثه را افزایش دهند و درنتیجه، آسیب‌های احتمالی را به حداقل برسانند. پنجم، راه‌حل‌های شامل تجزیه‌وتحلیل احساسات نظرات کاربران رسانه‌های اجتماعی در مورد مسائل سایبری، ارائه بینش‌های ارزشمند در مورد آگاهی عمومی و نگرانی‌های مربوط به امنیت سایبری است (به‌عنوان‌مثال، CR 5 از جدول ۳). دولت‌ها و سازمان‌های امنیت سایبری می‌توانند از این تحلیل برای تطبیق برنامه‌های آگاهی و ابتکارات مشارکت عمومی به‌طور مؤثر استفاده کنند.

درنهایت، دسترسی راه‌حل در چندین پلتفرم و دستگاه، قابلیت استفاده گسترده را تضمین می‌کند و به متخصصان امنیت سایبری و تصمیم‌گیرندگان این امکان را می‌دهد تا در هر زمان و هر مکان، به اطلاعات حیاتی تهدید دسترسی داشته باشند و بدون توجه به موقعیت مکانی یا دستگاه موردنظرشان (به‌عنوان‌مثال، CR 6)، آگاهانه تصمیم بگیرند (از جدول ۳). این مقیاس‌پذیری به یک چشم‌انداز سایبری ایمن‌تر در سطح جهانی کمک می‌کند.

۵- نتیجه‌گیری

داشبوردهای اطلاعاتی سایبری غالب، همان‌طور که در منابع معتبر (Tetaly & Kulkani, 2022; Xu et al., 2019; Keshk et al., 2021; Abdullahi et al., 2022; Gheyas & Abdullah, 2016; Ten et al., 2011; Yang et al., 2017; Shi et al., 2018; Kotsias et al., 2022) مستند شده است، دچار نارسایی‌های متعددی هستند. چنین محدودیت‌هایی شامل کمبود آمار حملات سایبری تاریخی در سطح کشور، ناتوانی در پیش‌بینی تهدیدات سایبری خاص کشور و ناتوانی در استفاده از روش‌های تشخیص ناهنجاری مبتنی بر CNN در طیف‌های سایبری در سطح کشور است. با توجه به این کمبودها، کار علمی ارائه‌شده، راه‌حلی پیشرو و مبتکرانه را معرفی می‌کند که تمام کاستی‌های ذکرشده در سیستم‌های اطلاعات سایبری موجود را به شکلی مؤثر اصلاح می‌کند. راه‌حل پیشنهادی، درک همه‌جانبه‌ای از تهدیدات سایبری در سراسر جهان ارائه می‌دهد. با استفاده از مجموعه‌ای از داشبوردهای موجود در همه پلتفرم‌ها (iOS، Android و Windows)، یک تصمیم‌گیرنده استراتژیک می‌تواند موارد زیر را انجام دهد:

- تجزیه‌وتحلیل و مقایسه تهدیدات سایبری در میان هر تعداد از کشورهای جهان
- تجزیه‌وتحلیل و مقایسه تهدید سایبری یک کشور بر اساس زمان
- ناهنجاری‌های موجود در طیف تهدید سایبری را برای هر کشور شناسایی یا تشخیص دهید.
- تهدیدات سایبری را برای هر کشوری پیش‌بینی کنید.
- نظرات کاربران رسانه‌های اجتماعی در مورد مسائل مربوط به سایبری را به‌طور انتقادی تجزیه‌وتحلیل کنید.

با استفاده از سیستم ارائه‌شده، یک تحلیلگر سایبری استراتژیک می‌تواند تهدیدات سایبری چندبعدی را برای هر کشوری تجزیه‌وتحلیل نموده و بر این اساس، وضعیت سایبری مناسب را توصیه کند. خطای پیش‌بینی کلی با استفاده از داده‌های واقعی تا ۳ آگوست ۲۰۲۳، کمتر از انحراف میانگین مربعات ریشه 0.19 (RMSE) با استفاده از معادله

اندازه‌گیری شد (Zibak & Simpson, 2019). این سطح نسبتاً بالاتری از دقت پیش‌بینی را در مقایسه با سیستم‌های موجود پیش‌بینی تهدیدات سایبری نشان می‌دهد (Sufi, 2023a; Yadav et al., 2023).

سپ – ۲۰۱۱۲

$$\sqrt{\frac{\sum_{i=1}^{N} ||y(i) - \hat{y}(i)||^2}{N}} = RMSE$$

تحقیقات اخیر در تجزیه‌وتحلیل گفتمان توییتر مبتنی بر هوش مصنوعی نشان داده است که تجزیه‌وتحلیل رسانه‌های اجتماعی با چالش‌های مختلفی ازجمله موضوعات مربوط به کیفیت داده‌ها، اطلاعات نادرست، حساب کاربری جعلی و نگرانی‌های اخلاقی روبه‌رو است (Sufi, 2023b, 2023d). در این مطالعه، فرض بر این بود که تمام ۳۰۲۰۳ توییت از حساب‌های کاربران واقعی توییتر منشأ گرفته‌اند. بااین‌حال، توجه به این نکته مهم است که در زمان واقعی، توییت‌ها می‌توانند توسط کاربران جعلی تولید شوند (Gurajala et al., 2016) و ممکن است حاوی اطلاعات گمراه‌کننده باشند (Ajao et al., 2018).

علاوه بر این، هنگام بررسی محدودیت‌های تجزیه‌وتحلیل رسانه‌های اجتماعی با تمرکز خاص بر توییتر، این مطالعه به‌شدت به استفاده از API توییت در زمان واقعی، پلتفرم برق مایکروسافت و مایکروسافت Azure متکی بود. هر یک از این پلتفرم‌ها نیازمند سرمایه‌گذاری مالی مداوم هستند و معمولاً از طریق تراکنش‌های کارت اعتباری تسهیل می‌شوند. به‌عنوان‌مثال، یک اشتراک اساسی در API توییتر که دسترسی به سهمیه ماهانه تنها ۱۰،۰۰۰ توییت را اعطا می‌کند، هزینه ۱۰۰ دلار در هر ماه را متحمل می‌شود (Twitter, 2023). گسترش این کمک‌هزینه برای پوشش یک میلیون توییت به‌طور قابل‌توجهی تعهد مالی را به مبلغ قابل‌توجهی ۵۰۰۰ دلار در ماه افزایش می‌دهد (Twitter, 2023). به دلیل این محدودیت‌های مالی، دامنه تحقیق به‌ناچار محدود و تنها بر روی نمونه محدودی از توییت‌ها متمرکز شد.

در آینده، ما می‌خواهیم الگوریتم‌های نوآورانه‌ای را برای تولید شاخص‌های تهدید سایبری در کشور صرفاً از داده‌های رسانه‌های اجتماعی با استفاده از ابزار قوی‌تر و مدرن‌تر توسعه دهیم. به‌عنوان‌مثال، مایکروسافت اخیراً پارچه مایکروسافت را راه‌اندازی کرده است که شامل انبارداری داده‌های قوی و پیشرفته، مهندسی داده‌ها، یادگیری ماشین، علوم داده و قابلیت تجسم است (Microsoft, 2023). با استفاده از این پلتفرم‌های نوآورانه، ما در نظر داریم از تکنیک‌های یادگیری عمیق مانند شبکه عصبی بازگشتی (RNN) (Ajao et al., 2018)، رمزگذارهای خودکار و غیره استفاده کنیم. ازآنجاکه این مطالعه از ۱۳ اکتبر ۲۰۲۲ شروع به گرفتن پست‌های رسانه‌های اجتماعی مرتبط با سایبری کرد، ایجاد شاخص تهدید سایبری در سطح کشور، توسعه‌ای قابل‌توجه برای این تحقیق خواهد بود. ترکیب شاخص‌های تهدید سایبری مبتنی بر رسانه‌های اجتماعی به همراه داده‌های حمله سایبری از فروشندگان ضد ویروس، دید بسیار جامع‌تری از تهدیدات سایبری جهانی ارائه می‌دهد.

منابع

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, *11*(2), 198.

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, *132*, 103352.

Ajao, O., Bhowmik, D., & Zargari, S. (2018). Fake news identification on twitter with hybrid cnn and rnn models. In *Proceedings of the 9th international conference on social media and society* (pp. 226-230).

Altintasi, C. (2023). Exponential smoothing of quadrature amplitude modulation for power quality disturbance detecting and classification. *IEEJ Transactions on Electrical and Electronic Engineering*, *18*(8), 1245-1254.

Australian Securities & Investments Commissions. (2022). *Guidance for consumers impacted by the optus data breach*. https://asic.gov.au/about-asic/news-centre/news-items/guidance-for-consumers-impacted-by-the-optus-data-breach/

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In *Emerging cyber threats and cognitive vulnerabilities* (pp. 73-92). Academic press.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva papers on risk and insurance. Issues and practice*, *47*(3), 698-736.

Dale, D., McClanahan, K., & Li, Q. (2023). Ai-based cyber event osint via twitter data. In *2023 International Conference on Computing, Networking and Communications (ICNC)* (pp. 436-442). IEEE.

Dempsey, T. (2023). Spreading Lies Through the Cyber Domain. In *European Conference on Cyber Warfare and Security* (Vol. 22, No. 1, pp. 559-566).

Dey, A. K., Gupta, G. P., & Sahu, S. P. (2023). A metaheuristic-based ensemble feature selection framework for cyber threat detection in IoT-enabled networks. *Decision Analytics Journal*, *7*, 100206.

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Analytics*, *1*(1), 6.

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial Intelligence*, *36*(1), 2037254.

Gurajala, S., White, J. S., Hudson, B., Voter, B. R., & Matthews, J. N. (2016). Profile characteristics of fake Twitter accounts. *Big Data & Society*, *3*(2), 2053951716674236.

Kaspersky. (2023a). *Cyber threat statistics*.

Kaspersky. (2023b). *Daily exploit cyber threat statistics*.

Kaspersky. (2023c). *Daily local infections cyber threat statistics*.

Kaspersky. (2023d). *Daily mailicious mail cyber threat statistics*.

Kaspersky. (2023e). *Daily network attack cyber threat statistics*.

Kaspersky. (2023f). *Daily on-demand cyber threat statistics*.

Kaspersky. (2023g). *Daily ransomware cyber threat statistics*.

Kaspersky. (2023h). *Daily spam cyber threat statistics*.

Kaspersky. (2023i). *Daily web threats cyber threat statistics*.

Kaye, B. (2022). *Australia's No. 1 health insurer says hacker stole patient details*. Reuters. https://www.reuters.com/technology/after-telco-hack-australia-faces-wave-data-breaches-2022-10-20/

Keshk, M., Sitnikova, E., Moustafa, N., Hu, J., & Khalil, I. (2019). An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems. *IEEE Transactions on Sustainable Computing*, *6*(1), 66-79.

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2022). Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. *Security Journal*, 1.

Kotsias, J., Ahmad, A., & Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, *32*(1), 35-51.

Maathuis, C., & Godschalk, R. (2023, February). Social Media Manipulation Deep Learning based Disinformation Detection. In *International Conference on Cyber Warfare and Security* (Vol. 18, No. 1, pp. 237-245).

Merritt, K. (2022). *Optus confirms 2.1 million customers affected by cyberattack*. Total Telecom. https://totaltele.com/optus-confirms-2-1-million-customers-affected-by-cyberattack/

Microsoft Documentation. (2020). *Choosing a natural language processing technology in azure*. https://docs.microsoft.com/en-us/azure/architecture/data-guide/technology-choices/natural-language-processing.

Microsoft Documentation. (2021). *Microsoft power automate*.

Microsoft Documentation. (2023). *Anomaly detection*.

Microsoft. (2022a). *Microsoft dataverse*.

Microsoft. (2022b). *Microsoft power bi documentation*.

Microsoft. (2023). *Microsoft fabric*.

Morgan, S. (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Ravinder, M., & Kulkarni, V. (2023). Intrusion detection in smart meters data using machine learning algorithms: A research report. *Frontiers in Energy Research*, *11*, 1147431.

Ren, H., Xu, B., Wang, Y., Yi, C., Huang, C., Kou, X., ... & Zhang, Q. (2019, July). Time-series anomaly detection service at microsoft. In *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining* (pp. 3009-3017).

Shi, D., Guo, Z., Johansson, K. H., & Shi, L. (2017). Causality countermeasures for anomaly detection in cyber-physical systems. *IEEE Transactions on Automatic Control*, *63*(2), 386-401.

Statista Research Department. (2022). *Consumer loss through cyber crime worldwide in 2017, by victim country*. https://www.statista.com/statistics/799875/countries-with-the-largest-losses-through-cybercrime/

Sufi, F. (2021). AI-Landslide: Software for acquiring hidden insights from global landslide data using Artificial Intelligence. *Software Impacts*, *10*, 100177.

Sufi, F. (2022a). A decision support system for extracting artificial intelligence-driven insights from live twitter feeds on natural disasters. *Decision Analytics Journal*, *5*, 100130.

Sufi, F. (2022b). AI-GlobalEvents: A Software for analyzing, identifying and explaining global events with Artificial Intelligence. *Software Impacts*, *11*, 100218.

Sufi, F. (2022c). AI-SocialDisaster: An AI-based software for identifying and analyzing natural disasters from social media. *Software Impacts*, *13*, 100319.

Sufi, F. (2022d). Identifying the drivers of negative news with sentiment, entity and regression analysis. *International Journal of Information Management Data Insights*, *2*(1), 100074.

Sufi, F. (2023a). A new AI-based semantic cyber intelligence agent. *Future Internet*, *15*(7), 231.

Sufi, F. (2023b). A new social media-driven cyber threat intelligence. *Electronics*, *12*(5), 1242.

Sufi, F. (2023c). Automatic identification and explanation of root causes on COVID-19 index anomalies. *MethodsX*, *10*, 101960.

Sufi, F. (2023d). Social media analytics on Russia–Ukraine cyber war with natural language processing: Perspectives and challenges. *Information*, *14*(9), 485.

Sufi, F., & Alsulami, M. (2021a). Automated multidimensional analysis of global events with entity detection, sentiment analysis and anomaly detection. *IEEE Access*, *9*, 152449-152460.

Sufi, F., & Alsulami, M. (2021b). Knowledge discovery of global landslides using automated machine learning algorithms. *IEEE Access*, *9*, 131400-131419.

Sufi, F., & Alsulami, M. (2022a). A novel method of generating geospatial intelligence from social media posts of political leaders. *Information*, *13*(3), 120.

Sufi, F., & Alsulami, M. (2022b). AI-based automated extraction of location-oriented COVID-19 sentiments. *Comput. Mater. Contin.(CMC)*, *72*(2), 3631-3649.

Sufi, F., & Khalil, I. (2022). Automated disaster monitoring from social media posts using AI-based location intelligence and sentiment analysis. *IEEE Transactions on Computational Social Systems*.

Sufi, F., Alam, E., & Alsulami, M. (2022a). Automated analysis of Australian tropical cyclones with regression, clustering and convolutional neural network. *Sustainability*, *14*(16), 9830.

Sufi, F., Alsulami, M., & Gutub, A. (2023). Automating global threat-maps generation via advancements of news sensors and AI. *Arabian Journal for Science and Engineering*, *48*(2), 2455-2472.

Sufi, F., Razzak, I., & Khalil, I. (2022b). Tracking anti-vax social movement using AI-based social media monitoring. *IEEE Transactions on Technology and Society*, *3*(4), 290-299.

Ten, C. W., Hong, J., & Liu, C. C. (2011). Anomaly detection for cybersecurity of the substations. *IEEE Transactions on Smart Grid*, *2*(4), 865-873.

Tetaly, M., & Kulkarni, P. (2022). Artificial intelligence in cyber security–A threat or a solution. In *AIP Conference Proceedings* (Vol. 2519, No. 1). AIP Publishing.

Turnbull, T. (2022). *Optus: How a massive data breach has exposed australia*. BBC News. https://bbc.com/news/world-australia-63056838

Twitter. (2023). *About twitter api*.

Xu, S., Qian, Y., & Hu, R. Q. (2019). Data-driven network intelligence for anomaly detection. *IEEE Network*, *33*(3), 88-95.

Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security. *Artificial Intelligence Review*, *56*(11), 12407-12438.

Yang, J., Zhou, C., Yang, S., Xu, H., & Hu, B. (2017). Anomaly detection based on zone partition for security protection of industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, *65*(5), 4257-4267.

Zhao, R., Ouyang, W., Li, H., & Wang, X. (2015). Saliency detection by multi-context deep learning. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 1265-1274).

Zibak, A., & Simpson, A. (2019). Cyber threat information sharing: Perceived benefits and barriers. In *Proceedings of the 14th international conference on availability, reliability and security* (pp. 1-9).

استناد به این مقاله: بلوچ روز، ئائمه، و شادروان، سوده. (۱۴۰۳). سیستم اطلاعاتی جهانی تهدیدات سایبری با هوش مصنوعی و شبکه عصبی کانولوشنال. *فصلنامه پژوهش‌های نوین در شهر هوشمند*، ۳(۱)، ۵۰-۷۰.