مدل مفهومی فضای سایبر از دیدگاه کاربرد علوم داده در امنیت سایبری

سید نصیب اله دوستی مطلق[۱]، علی اصغر نوروزی[۲]

[۱]عضو هیات علمی دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی
doustimotlagh@chmail.ir
[۲]محقق دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی
alianorouzi@chmail.ir

چکیده

دوام، رشد و توسعه هر کشوری در گروی امنیت ملی آن است. از مهم‌ترین جنبه‌های امنیت ملی در دنیای امروزی، امنیت سایبری است. در سال‌های اخیر حجم، تنوع، نرخ تولید و پیچیدگی تهدیدها و حملات سایبری افزایش چشم‌گیری داشته است. علوم داده و یادگیری ماشین حوزه‌های پژوهشی در حال رشدی هستند که راهکارهای مناسبی را برای مواجهه با این چالش‌ها ارائه می‌دهند. در حقیقت، روش‌های یادگیری ماشین و علوم داده عنصر کلیدی برای خودکار و هوشمند کردن سامانه‌های امنیتی شده‌اند. برای استفاده دقیق و همه جانبه از علوم داده در ارتقای امنیت سایبری نیاز به مدل مفهومی فضای سایبر است. در پژوهش حاضر جهت ارائه مدل مفهومی از رویکرد کیفی استفاده شده است. برای این منظور در مصاحبه با نخبگانِ امنیت فضای سایبر و علوم داده سه مفهوم ۱) کاربر، محتوا و خدمات، ۲) حکمرانی و ۳) زیرساختِ به مثابه ابعاد اساسی مدل فضای سایبر از دیدگاه کاربرد علوم داده در امنیت سایبری مورد شناسایی قرار گرفتند و سپس مؤلفه‌های هر یک از این ابعاد استخراج شدند.

کلمات کلیدی: فضای سایبر، امنیت فضای سایبر، علوم داده، یاد گیری ماشین، ارزیابی امنیت سایبری.

۱ مقدمه

فضای سایبر در عصر کنونی، بخش مهمی از زندگی افراد، اقتصاد کشورها، سیاست و حتی مسائل امنیتی و نظامی شده است و قابل چشم پوشی نیست. از مهم‌ترین مسائل مطرح در فضای سایبر امنیت آن است. با افزایش و تکامل حملات در فضای سایبر، نیاز به وجود سامانه‌های خودکار برای تکمیل تجزیه و تحلیل انسانی بیش از پیش احساس می‌شود. علاوه بر این، یافتن آسیب‌پذیری‌ها و رخنه‌ها به مساله‌ای بسیار دشوار تبدیل شده است. اندازه فضای سایبر و حجم داده‌ها و اطلاعات موجود در آن چنان در حال رشد است که به نظر

غیر ممکن است که بدان از کجا باید شروع کرد. حفاظت از داده‌ها و سامانه‌های رایانه‌ای در مقابل حملات سایبری یکی از حیاتی‌ترین وظایف امنیت سایبری است. لازمه این امر استفاده از روش های حفاظت دقیق و خودکار (یا نیمه‌خودکار) است. حفاظت دقیق و خودکار با علوم داده امکان‌پذیر می‌شود.

علوم داده ترکیبی از ابزار، روش‌ها و الگوریتم‌ها برای پردازش و تحلیل داده‌ها و استخراج دانش از آن‌ها است. علوم داده از اشتراک علوم و فنونی همچون آمار، هوش مصنوعی و به خصوص روش‌های یادگیری ماشین، داده‌کاوی، روش‌های بصری‌سازی، پایگاه داده‌ها و روش‌های پردازش داده ایجاد شده است [۵]. به دلیل اهمیت علوم داده و کاربردهای زیاد آن، در سال‌های اخیر راه‌کارهای متعددی برای استفاده از علوم داده به منظور تشخیص رخدادها و حملات سایبری (چه از قبل شناخته‌شده و چه ناشناخته) و محافظت از سامانه‌های حساس پیشنهاد و عملیاتی شده است [۶][۷]. با استفاده از علوم داده در امنیت سایبری، الگوها و رفتارهای پیچیده حمله‌کنندگان شناسایی می‌شود، قابلیت‌های شناسایی و جلوگیری از حملات سایبری بهبود پیدا می‌کند، اطلاعات در مورد تهدیدات سایبری افزایش می‌یابد و اشتراک گذاری فوری اطلاعات در مورد تهدیدات تسهیل می‌گردد. برای استفاده دقیق و همه جانبه از علوم داده در ارتقای امنیت سایبری نیاز به مدل مفهومی فضای سایبر است.

هدف این پژوهش ارائه مدل مفهومی برای فضای سایبر از دیدگاه کاربرد علوم داده در ارتقای امنیت سایبری است. این مدل شامل سه بعد اساسی ۱) کاربر، محتوا و خدمات، ۲) حکمرانی و ۳) زیرساخت است. بعد اول شامل مؤلفه‌های تحلیل داده‌ها، تحلیل، پیش‌بینی و واکنش به تهدیدها و حملات و شبکه‌های اجتماعی است. بعد حکمرانی شامل مؤلفه‌های قوانین، ارزیابی، حکمرانی داده، تصمیم‌گیری مبتنی بر داده، بودجه، بومی‌سازی و استفاده از شرکت‌های خصوصی، ظرفیت‌سازی، آموزش، تحقیق و توسعه و مرکز فرماندهی واحد است. بعد زیرساخت نیز حاوی مؤلفه‌های مرکز عملیات امنیت سایبری، شبکه‌های ارتباطی مناسب برای تحلیل و تشخیص تهدیدها و حملات، سخت‌افزار مناسب برای تحلیل و تشخیص تهدیدها و حملات، فناوری ابر برای ذخیره و تحلیل داده‌ها و زیرساخت مناسب کلان داده‌ها (موازی، توزیع‌شده) است. از این مدل و ابعاد و مؤلفه‌های آن می‌توان برای تبیین نقش علوم داده در ارتقای امنیت سایبری و همچنین ارزیابی وضعیت کشور یا یک سازمان در حوزه امنیت سایبری و علوم داده بهره برد.

۲ مروری بر کارهای دیگران

فضای سایبر شامل اینترنت، شبکه‌ها، سامانه‌ها، لوازم جانبی، داده‌ها و کاربران در محیط اطلاعات است. این محیط بهم پیوسته برای حاکمیت جهانی، تجاری، نظامی و امنیت ملی حائز اهمیت است (Caton, 2019). به دلیل پیچیدگی بالای فضای سایبر از مدل‌های گوناگونی برای توصیف و تحلیل آن استفاده می‌شود. در ادامه برخی از این مدل‌ها مرور می‌شوند.

۱.۲ مدل سه لایه وزارت دفاع آمریکا

از منظر وزارت دفاع آمریکا، فضای سایبر در سه بعد مجزا ولی کاملا درهم تنیده و پیوسته تشریح می‌گردد که همواره با افراد، سازمان‌ها و سامانه‌ها در تعامل است. این ابعاد عبارتند از: فیزیکی (مانند گوشی‌های همراه)، اطلاعاتی (مانند توزیع اطلاعات) و شناختی یا فکری (مانند ادراک و برداشت)[۷]. شکل ۱ ابعاد به هم پیوسته فضای سایبر و نحوه ارتباط آن‌ها را نشان می‌دهد. بعد فیزیکی از سامانه‌های فرماندهی و کنترل، تصمیم‌گیرنده‌های کلیدی و زیرساخت‌های حمایتی تشکیل شده است. این بعد شامل شبکه‌های ارتباطی، انسان، امکانات C2، روزنامه‌ها، کتاب‌ها، برج‌های مایکروویو، لپ‌تاپ‌ها، تلفن‌های هوشمند یا هر چیز دیگرِ قابل اندازه‌گیری شهودی است. بعد فیزیکی مرتبط با محدوده‌های نظامی، ملی، اقتصادی و جغرافیایی است. بعد اطلاعاتی کجایی و چگونگی جمع‌آوری، پردازش، ذخیره، انتشار و حافظت از اطلاعات را شامل می‌شود. بعد شناختی شامل ذهن کسانی است که عمل‌های انتقال، دریافت، پاسخ یا کنش را روی اطلاعات انجام می‌دهند. این بعد به پردازش اطلاعات، ادراک، قضاوت و تصمیم‌گیری افراد یا گروه‌ها اشاره دارد. عناصر این بعد تحت تاثیر عواملی مانند اعتقادات فردی و فرهنگی، هنجارها، آسیب‌پذیری‌ها، انگیزه‌ها، احساسات، تجربیات، اخلاق، آموزش، سلامت روان، هویت‌ها و ایدئولوژی‌هاست.

شکل ۱: ابعاد به هم پیوسته فضای سایبر [۷]

۲.۲ مدل زیمت و اسکودیس

مدل زیمت و اسکودیس [۸] دارای چهار دامنه زیرساخت/سیستم‌ها، محتوا/کاربرد، مردم/اجتماع و حکمرانی است. در شکل ۲ این چهار دامنه نشان داده شده است. دامنه زیرساخت/ سامانه‌ها شامل اجزای فیزیکی و زیرساخت فنی است. دامنه محتوا/کاربرد شامل پایگاه‌های اطلاعاتی و سازوکارهای دسترسی و پردازش

دامنه حکمرانی		
دامنه زیرساخت/سامانه‌ها	دامنه محتوا/کاربرد	دامنه مردم/اجتماع

شکل ۲: مدل زیمت و اسکودیس [۸]

اطلاعات است. دامنه مردم/اجتماع شامل ارتباطات و تعاملات بین انسان‌ها و اطلاعات است. درنهایت، دامنه حکمرانی شامل سازوکارهای مدیریتی و نظارتی برای حکمرانی بر سه دامنه دیگر است.

۳.۲ مدل شورای عالی فضای مجازی

فضای مجازی کشور، پوششی بسیار وسیع در حوزه‌های مختلف فضای مجازی (بستر، خدمات، محتوا، کاربر، مقررات و امنیت) دارد که محدوده آن، با شرط قرار گرفتن خدمت‌دهنده یا کاربر در قلمرو حاکمیتی نظام جمهوری اسلامی ایران، قابل تعریف است. بر این اساس در اسناد شورای عالی فضای مجازی کشور مدل شش لایه‌ای برای فضای سایبر تبیین شده است که در شکل ۳ قابل مشاهده است [۱].

شکل ۳: مدل شش لایه شورای عالی فضای مجازی [۱]

۴.۲ مدل‌های دیگر

تقی‌پور و اسماعیلی [۲] یک مدل مفهومی به عنوان الگو و زیرساخت شناختی برای دفاع سایبری جمهوری اسلامی ایران پیشنهاد داده‌اند. این مدل شامل سه بعد بازدارندگی، پدافند (دفع) و برگشت‌پذیری (تاب‌آوری) است. بازدارندگی مانع ذهنی محکمی را برای دشمنان ایجاد می‌کند تا با افزایش هزینه‌های حملات سایبری، در مرحله طرح‌ریزی و قبل از آن، عملیات حمله را با تزلزل مواجه سازد. پدافند به معنای دفاع در مقابل حملات است و به دو نوع عامل و غیر عامل دسته‌بندی می‌شود. برگشت‌پذیری نیز عبارت است از توانایی یک سازمان برای مقاومت، واکنش و بازیابی در حملات سایبری.

رمضان‌زاده و همکاران [۳] یک مدل مفهومی برای ارزیابی قدرت سایبری نیروهای مسلح با تأکید بر بعد بازدارندگی سایبری ارائه کرده‌اند. این مدل دارای مؤلفه‌های پنج‌گانه استحکام‌سازی، پاسخ به تهاجم سایبری، پشیمان‌کنندگی دشمن (اقدام متقابل)، بازیابی و استمرار عملیات (افزونگی) است. همه این مؤلفه‌ها مربوط به بعد بازدارندگی سایبری هستند و می‌توانند در شناسایی و اولویت‌بندی سرمایه‌های سایبری نیروهای مسلح به منظور ایجاد زمینه بازدارندگی سایبری در مقابل تهدیدات، مفید باشند.

رحیم‌اف و موحدی [۴] یک الگوی راهبردی برای ارزیابی عملیات سایبری پیشنهاد داده‌اند. آن‌ها استدلال می‌کنند که توان انجام موفق عملیات سایبري، باعث افزایش قدرت سایبري، ایجاد بازدارندگی سایبري و کاهش تهدیدات سایبري می‌شود. بنابراین ارزیابی فعالیت‌هاي سایبري جهت شناسایی ضعف‌ها و قوت‌ها و بررسی میزان اثربخشی فعالیت‌ها اجتناب‌ناپذیر است. به این منظور، رحیم‌اف و موحدی یک الگوی راهبردی شامل سه بعد ارزیابی طراحی و طرح‌ریزي، ارزیابی آمادگی رزمی و ارزیابی اجرا پیشنهاد می‌دهند. این بعدها به ده مؤلفه و هفتادوسه شاخص تقسیم‌بندی شده‌اند.

۳ مدل پیشنهادی

پس از مصاحبه با نخبگان، ابعاد مدل مفهومی ارزیابی موارد زیر انتخاب شدند:

- کاربر، محتوا و خدمات
- حکمرانی
- زیرساخت

مدل مرجع برای انتخاب این ابعاد مدل شش لایه مرکز ملی فضای مجازی بود. به دلیل این که در اینجا دیدگاه امنیت سایبری داریم، لایه امنیت حذف شد. در حقیقت امنیت در تمام ابعاد به صورت ضمنی وجود دارد. قابل ذکر است که تمام موارد امنیتی در این مدل مفهومی، مربوط به امنیت غیر عامل هستند. لایه‌های کاربر، محتوا و خدمات در یک بعد ادغام شدند، زیرا که دیدگاه پژوهش علوم داده است و جدا کردن این سه لایه منجر به پیچیدگی غیر ضروری مؤلفه‌ها می‌شد. هر بعد دارای سه تا هشت مؤلفه است. برخی از مؤلفه‌ها نیز به زیرمؤلفه‌ها شکسته شده‌اند تا پیچیدگی کاهش یابد. شکل ۴ و جدول ۱ ابعاد، مؤلفه‌ها و زیرمؤلفه‌های مدل مفهومی ارزیابی استخراجی از مصاحبه نخبگی را نشان می‌دهد.

بعد کاربر، محتوا و خدمات شامل شبکه‌های اجتماعی و کلیه افراد مرتبط با فضای مجازی، داده‌ها، اطلاعات داخلی و راداری، متن ایمیل‌ها، تعاملات و اطلاعات ردوبدل شده در شبکه‌های ارتباطی و اجتماعی، ذخیره و پردازش اطلاعات، تحلیل، پیش‌بینی و واکنش به تهدیدها و حملات، به‌روزرسانی سامانه‌ها، خدمات اتوماسیون، برنامه‌های کاربردی، خدمات مبتنی بر وب، پست الکترونیکی، سامانه فایل‌ها و غیره است.

بعد حکمرانی شامل اقدامات قانونی، سازمان‌دهی، ظرفیت‌سازی، تنظیم قوانین و مقررات، ارزیابی، بودجه و بومی‌سازی است.

بعد زیرساخت شامل هر سازوکار مرتبط با زیرساخت و معماری، سخت‌افزار و پروتکل‌ها، رایانه‌های راداری، حسگرها، سامانه‌های کنترلی، ابر و غیره است.

در ادامه برخی از اصطلاحات موجود در مؤلفه‌ها و زیرمؤلفه‌ها توضیح داده می‌شود.

- آسیب‌پذیری در مقوله امنیت سایبری نقطه ضعفی است که می تواند توسط مجرمان سایبری برای دسترسی غیر مجاز به یک سامانه رایانه‌ای مورد سو استفاده قرار گیرد.

شکل ۴: مدل مفهومی فضای سایبر از دیدگاه کاربرد علوم داده در امنیت سایبری

جدول ۱: ابعاد، مؤلفه‌ها و زیرمؤلفه‌های مدل مفهومی

ابعاد	مولفه‌ها	زیرمولفه‌ها
کاربر، محتوا و خدمات	تحلیل داده‌ها	جمع‌آوری داده‌ها
		پردازش، گزینش و تحلیل داده‌ها
		ذخیره داده‌ها
	تحلیل، پیش‌بینی و واکنش به تهدیدها و حملات	پایش و تشخیص ریسک‌ها و تهدیدها
		کشف، مدیریت و کنترل آسیب‌پذیری‌ها و بدافزار
		واکنش به تهدیدها و حملات و طرح تداوم
		اطلاعات راهبردی تهدید رایانه‌ای
		مدیریت اطلاعات و رخدادهای امنیتی
	شبکه‌های اجتماعی	
حکمرانی	قوانین	تنظیم قوانین مرتبط با داده‌های حساس
		نظارت بر حسن اجرای قوانین و سیاست‌ها
		نحوه اشتراک اطلاعات بین سازمان‌ها
		راهبرد ملی برای امنیت فضای سایبر
	ارزیابی	اجرای مانورهای حملات سایبری
		ارزیابی سامانه‌های موجود
	حکمرانی داده	
	تصمیم‌گیری مبتنی بر داده	
	بودجه	
	بومی‌سازی و استفاده از شرکت‌های خصوصی	
	ظرفیت‌سازی، آموزش، تحقیق و توسعه	
	مرکز فرماندهی واحد	
زیرساخت	مرکز عملیات امنیت سایبری	
	شبکه‌های ارتباطی مناسب برای تحلیل و تشخیص تهدیدها و حملات	
	سخت‌افزار مناسب برای تحلیل و تشخیص تهدیدها و حملات	
	فناوری ابر برای ذخیره و تحلیل داده‌ها	
	زیرساخت مناسب کلان داده‌ها (موازی، توزیع‌شده)	

- تهدید در فضای سایبر یک اقدام یا رویداد منفی بالقوه است که توسط یک آسیب‌پذیری تسهیل شده است. به طور کلی تهدید سایبری یک اقدام مخرب است که به دنبال آسیب رساندن به داده‌ها و یا سرقت داده‌ها و یا تاثیر ناخواسته بر یک سامانه یا برنامه رایانه‌ای است.

- حمله سایبری هر گونه تهاجمی است که سامانه‌های اطلاعاتی رایانه‌ای، شبکه‌های رایانه‌ای یا زیرساخت‌ها را هدف قرار می‌دهد. در این اقدام، مهاجم شخص یا فرایندی است که تلاش می‌کند بدون مجوز به داده‌ها، عملکردها یا سایر مناطق محدود شده سامانه دسترسی پیدا کند. این دسترسی به احتمال زیاد با قصد تخریب است.

- طرح تداوم توانایی یک سازمان و کسب‌وکار برای ادامه ارائه خدمات در سطوح قابل قبولِ از پیش تعریف شده، پس از یک حادثه غیر مترقبه، مانند حمله سایبری است.

- مرکز عملیات امنیت سایبری یک تیم امنیت اطلاعات را در خود جای داده است که مسئول نظارت و تجزیه و تحلیل وضعیت امنیتی سازمان به صورت مداوم است. هدف تیم مرکز عملیات امنیت سایبری شناسایی، تجزیه و تحلیل و پاسخ به حوادث امنیت سایبری با استفاده از ترکیبی از راه‌حل‌های فناوری و مجموعه‌ای قوی از فرایندها است. مراکز عملیات امنیتی معمولا متشکل از تحلیلگران و مهندسان امنیتی و همچنین مدیرانی است که بر عملیات امنیتی نظارت می‌کنند.

- اطلاعات راهبردی تهدید سایبری دانش، مهارت و اطلاعات مبتنی بر تجربه در مورد وقوع و ارزیابی تهدیدات سایبری یا فیزیکی و عوامل تهدید هستند که می‌توانند در کمک به کاهش حملات احتمالی و رویدادهای مضر فضای سایبر مفید باشند [۹].

- حکمرانی داده مجموعه‌ای از فرایندها، نقش‌ها، استانداردها و معیارهایی است که استفاده موثر و کارآمد از اطلاعات را در توانمند ساختن سازمان یا دولت برای دستیابی به اهداف خود تضمین می‌کند. حکمرانی داده تضمین می‌کند که نقش‌های مرتبط با داده‌ها در سازمان یا دولت به وضوح تعریف شده‌اند [۱۰].

- تصمیم‌گیری مبتنی بر داده اصطلاحی است که برای فرایند و تکنیک تصمیم‌گیری براساس تجزیه و تحلیل داده‌ها و ارزیابی اطلاعات به‌کار می‌رود. در این نوع تصمیم‌گیری از شهود استفاده‌ای نمی‌شود و تنها داده‌ها و اطلاعات استخراج شده از آن‌ها ملاک تصمیمات هستند [۱۱].

- کلان داده‌ها به مجموعه داده‌هایی گفته می‌شود که در حجم و تنوع زیاد و با شتاب بالایی تولید می‌شوند [۱۲].

۴ نتیجه‌گیری و پیشنهاد

در این پژوهش یک مدل مفهومی برای فضای سایبر از دیدگاه کاربرد علوم داده در ارتقای امنیت سایبری پیشنهاد شد. این مدل دارای سه بعد ۱) کاربر، محتوا و خدمات، ۲) حکمرانی و ۳) زیرساخت است. هر بعد نیز به سه تا هشت مؤلفه تقسیم می‌شود. برخی از مؤلفه‌ها نیز به زیرمؤلفه‌ها شکسته می‌شوند.

در ادامه این پژوهش می‌توان براساس این مدل پرسشنامه‌ای طراحی کرد و در اختیار کارشناسان امنیت سایبری و علوم داده قرار داد. با تحلیل آماری نتایج این پرسشنامه، مثلا روش آماري حداقل مربعات جزئی، می‌توان روابط بین مدل، ابعاد و مؤلفه‌ها را مورد بررسی قرار داد تا مدل از لحاظ کمی نیز مورد تایید قرار گیرد. به علاوه، از این مدل می‌توان برای ارزیابی وضعیت امنیت سایبری و علوم داده در فضای سایبری کشور بهره برد.

مراجع

[۱] فیروزآبادی، سیدابوالحسن. درآمدی بر حکمرانی فضای مجازی. انتشارات دانشگاه امام صادق (علیه السلام)، ۱۳۹۹.

[۲] تقی‌پور، رضا و اسماعیلی، علی. طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران. فصلنامه امنیت ملی، ۱۳۹۷.

[۳] رمضان‌زاده، مجتبی، غیوری‌ثالث، مجید، احمدوند، علی‌محمد، آقایی، محسن، و فرخی، ابراهیم نظری. ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تاکید بر بعد بازدارندگی سایبری. فصل‌نامه مدیریت نظامی، ۱۳۹۹.

[۴] رحیم‌اف، هانی و موحدی‌صفت، محمدرضا. الگوی راهبردی ارزیابی عملیات سایبری. فصل‌نامه مدیریت نظامی، ۱۳۹۹.

[5] Martinez, I., Viles, E., and Olaizola, IG. Data science methodologies: current challenges and future approaches. *Big Data Research*, 2021.

[6] Dasgupta, D., Akhtar, Z., and Sen, S. Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, 2022.

[7] Selvarathi, C. A survey on machine learning approach to detect malware. *Turkish Journal of Computer and Mathematics Education*, 2021.

[8] Zimet, E. and Skoudis, E. A graphical introduction to the structural elements of cyberspace. *Cyberpower and national security*, 2009.

[9] Wagner, T. D., Mahbub, K., Palomar, E, and Abdallah, A. E. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, 2019.

[10] Abraham, R., Schneider, J., and Vom Brocke, J. Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 2019.

[11] Garouani, M., Ahmad, A., Bouneffa, M., Hamlich, M., Bourguin, G., and Lewandowski, A. Towards big industrial data mining through explainable automated machine learning. *The International Journal of Advanced Manufacturing Technology*, 2022.

[12] Provost, F. and Fawcett, T. Data science and its relationship to big data and data-driven decision making. *Big data*, 2013.