تاثیر امنیت سایبری بر هوشمندسازی دولت الکترونیک با چارچوب امنیتی ارائه خدمات

چکیده

با گسترش نوآوری در فناوری اطلاعات، جهان در حال تجربه تکامل هوشمند سازی و پیدایش شهرهای هوشمند است. دستگاه‌های هوشمند در بسیاری از شهرها مورد استفاده قرار می‌گیرند. خانه ها، اتومبیل‌ها، اماکن عمومی و سایر سیستم‌های اجتماعی اکنون در مسیر اتصال به "اینترنت اشیا" هستند. در روند هوشمند سازی، به شرط تامین امنیت و انتظارات ما از حریم خصوصی، ایجاد فرصت‌های اقتصادی و اجتماعی جدید مورد انتظار خواهد بود. این پژوهش با در نظر گرفتن ضرورت گسترش هوشمند سازی و توجه به اهمیت امنیت در این حوزه، به تبیین عوامل تاثیر گذار پرداخته است که منجر به ارائه مدل می‌شود. این مطالعه از منظر هدف، کاربردی و از جهت گردآوری اطلاعات، توصیفی- همبستگی است. گردآوری داده‌ها از طریق پرسشنامه محقق ساخته و با جامعه‌ی نمونه ای شامل ۱۲۰ نفر از متخصصین مدیریت فناوری اطلاعات و کارشناسان حوزه امنیت سایبری فعال در شهر تهران با روش نمونه گیری غیراحتمالی (در دسترس) و همچنین تجزیه و تحلیل داده‌ها از طریق نرم‌افزار پی ال اس انجام شده است. آلفای کرونباخ برای تمامی سازه ها بالاتر از ۷/. و مقدار میانگین واریانس استخراج شده بالاتر از ۵/. بوده و روایی و پایایی سازه‌ها تایید شد. در مدل ارائه شده مشخص می‌شود که توجه به چالش های مدرن امنیت سایبری به عنوان تاثیر مستقیم و همچنین، اصول تشکیل پایگاه امنیت و چارچوب ارائه خدمات هوشمند به عنوان عوامل میانجی در گسترش هوشمند سازی در دولت الکترونیک تاثیر معنا داری دارد.

کلمات کلیدی:

دولت الکترونیک، توسعه هوشمند، هوشمند سازی، امنیت سایبری، پایگاه امنیت، خدمات هوشمند

۱. مقدمه:

در دوران دیجیتال، همگام سازی میان عناصر ذی‌نفع در زنجیره های تولید، برای رونق بخشیدن به فعالیت های کارآفرینی و مساعد برای هوشمند سازی، امری ضروری است(Schiavone et al., 2020). پیشرفت های اخیر فناوری و معماری در شبکه‌های نسل پنجم [1]با شروع استقرار در جهان، ارز شمندی خود را ثابت کرده اند. همراه با تکامل سریع، خطرات، تهدیدها و آسیب پذیری های سیستم برای کسانی که قصد بهره برداری از آن شبکه ها را دارند ، به وجود می آید. نقض داده‌ها، سرقت ID ، شکستن رمز کپچا[2] و سایر موارد این چنینی به عنوان چالش‌های جدید مطرح است و میلیون‌ها نفر از افراد و سازمان ها را نیز تحت تأثیر قرار داده و حفظ امنیت سایبری را به یک نگرانی اساسی تبدیل کرده است(Bhatele et al., 2019).

در سال ۲۰۱۰ ، کمتر از ۵۰ میلیون بدافزار منحصر به فرد وجود داشت که برای جامعه امنیتی شناخته شده بود. در سال ۲۰۱۲، تعداد آنها دو برابر، حدود ۱۰۰ میلیون شد و در سال ۲۰۱۹، بیش از ۹۰۰ میلیون مورد، بدافزار وجود داشت که برای جامعه امنیتی شناخته شد و طبق آمار موسسه AV-TEST در آلمان، این تعداد احتمالاً رشد خواهد کرد. جرایم اینترنتی و حملات می‌توانند خسارات مالی مخربی به بار آورند و سازمانها و افراد را نیز تحت تأثیر قرار دهند (ibm, 2019) هزینه سالانه اقتصاد جهانی برای جرایم اینترنتی ۴۰۰ میلیارد دلار است(Fischer, 2015). تعداد سوابق نقض شده در هر سال از ۵ سال آینده تقریباً سه برابر خواهد شد. بنابراین، ضروری است که سازمان‌ها برای کاهش ضرر و زیان، از یک رویه امنیت سایبری قوی استفاده کنند(Papastergiou et al., 2019).

دنیای سایبری و گسترش هوشمند سازی بر همه موجودات از سطح فردی- سازمانی گرفته تا سطح ملی- بین المللی تأثیر می‌گذارد و مواردی نظیر (الف) وجود هستی شناختی جدید دیجیتال (ب) جریان جدید داده ها (ج) تسریع سریع سرعت در ارتباطات (د) کالایی سازی داده ها و (ه) گسترش بازیگران درگیر را ایجاد می‌کند(Garnett & James, 2020) توجه به اهمیت سرعت رشد و نوآوری‌های بدیعی که در این مسیر اتفاق افتاده و توانسته با سرعت زیاد فراگیری در سطح جهانی را شکل دهد، این ضرورت را ایجاد می‌کند تا با شناخت صحیح از فرآیند هوشمند سازی با رویکرد صیانیت از امنیت تدوین گردد تا به بررسی چالش های مدرن ایجاد شده جهت شناخت تهدیدات ناشی از فناوری‌های هوشمند (هوش‌مصنوعی[3]، یادگیری ماشین، زنجیره بلوک، یادگیری عمیق، تجزیه و تحلیل داده های بزرگ، علوم داده، اینترنت اشیاء و ...) پرداخته شود.

---

[1] 5g

[2] captcha

[3] AI

۲. پیشینه نظری و تجربی

۲. ۱. مجموعه هوشمند

شبکه هوشمند یکی از مهمترین کاربردهای اینترنت اشیا است. با توسعه و بکارگیری فناوری‌های اطلاعاتی و ارتباطی در سیستمهای سنتی، بهبود سیستم‌های فیزیکی-سایبری شبکه هوشمند نیز افزایش می‌یابد. همانطور که شبکه های هو شمند با گسترش خود سطح بالاتری از رفاه را برای افراد می‌آورند اما باید توجه دا شت که سیستم های شبکه هوشمند مبتنی بر اینترنت اشیا، دارای معماری پیچیده و شامل دستگاه ها و زیرساخت های حیاتی هستند. این زیر ساخت‌ها حاوی سیستم های ارتباطی بوده که در صورت عدم رعایت شرایط امنیت سابری، می‌توانند منجر به نقصان امنیت ملی و یا بر هم خوردن نظم عمومی شوند. این سیستم های ممکن است در برابر حملات سایبری آسیب پذیر باشند. بنابراین ، تلاش زیادی برای افزایش امنیت شبکه هوشمند در صنعت، دولت و دانشگاه وجود دارد(Gunduz & Das, 2020).

ظهور اتوماسیون و دیجیتالی سازی منجر به این می شود که زیرساخت‌های حیاتی به طور فزاینده‌ای به هم پیوند خورده و به طور چشمگیری سطوح حمله آنها را افزایش دهد (Europol, 2020). آژانس های نظارتی، مانند آژانس امنیت سایبری اتحادیه اروپا (ENISA) و وزارت امنیت داخلی (DHS) در ایالات متحده، دستورالعمل‌های امنیتی را برای حمایت از اجرای استانداردهای بالای امنیتی زیر ساخت های مهم ارائه می‌دهند. این دستورالعمل‌ها بر اساس استفاده از استانداردهای بین المللی (مانند ISO 27001 برای امنیت IT ، یا ISA 62443 برای امنیت فناوری عملیاتی) برای مشخصات خاص زیرساخت های حیاتی نمایه می‌شوند(Libor, 2017). با این حال ، تعریف رویکرد امنیتی مناسب برای یک مورد خاص زیرساختی حیاتی ، کاری پیچیده و دست و پا گیر است ، زیرا این امر به مجموعه بسیار خاصی از نیازها و ارزیابی ریسک بستگی دارد.

۲. ۱. ۱. هوش مصنوعی

ظهور هوش مصنوعی توجه محققان را به یک الگوی جدید استاندارد زندگی جلب کرده است. این انقلاب در سراسر جهان برای سهولت زندگی با استفاده از دستگاه‌های هوشمند مانند سنسورهای هوشمند، محرک‌ها و بسیاری از دستگاه‌های دیگر پذیرفته شده است. دستگاه‌های مجهز به هوش مصنوعی، هوشمندتر و قادر به انجام یک کار خاص هستند که باعث صرفه جویی در منابع و زمان زیادی می‌شود. رویکردهای مختلفی در ادبیات موجود برای مقابله با مسائل مختلف زندگی واقعی مبتنی بر سیستم های هوش مصنوعی در دسترس است(Qinxia et al., 2021). پیشرفت های اخیر در هوش مصنوعی (AI) ، به ویژه در یادگیری ماشین (ML) و یادگیری عمیق (DL) ، و ادغام آنها در سیستم های مبتنی بر نرم افزار از همه حوزه ها، چالش های جدید مهندسی سیستم های مبتنی بر هوش مصنوعی مدرن را ایجاد می کند .این سیستم‌ها، داده‌های فشرده ای دارند، به طور مداوم در حال تحول هستند، خود را سازگار می‌کنند و

رفتار آنها دارای درجه ای از عدم اطمینان است (که به طور معمول پذیرفته می شود) .این ویژگی‌ها به منظور تضمین کیفیت در هنگام توسعه و بهره برداری در محیط های زنده، نیازمند رویه های سازگار و جدید تضمین کیفیت (QA) سازگار و تحلیلی از حوزه مهندسی نرم افزار (SE) هستند(Qinxia et al., 2021).

در پیش بینی کار آینده و گسترش و کاربرد تکنیک های هوش مصنوعی در پیشگیری از حمله سایبری ، باید از تفاوت بین اهداف فوری و دیدگاه‌های بلند مدت آگاه بود. بسیاری از تکنیک های هوش مصنوعی در پیشگیری از حمله سایبری مرتبط هستند، همچنین در حال حاضر، در بسیاری از حملات سایبری مشکلاتی وجود دارد که به اقدامات پیچیده‌تری نیاز دارند(Anwar & Hassan, 2017).

۲. ۱. ۲. تجزیه و تحلیل داده های کلان[۴]

داده های بزرگ با در نظر گرفتن راه حل‌های موثر، به وسیله‌ی بهبود سرعت، افزایش دهنده امنیت شبکه می‌شود تا فضای واقعی تهدید درک شود. از طریق یادگیری ماشینی می‌توان خطرات ناشناخته از جمله تهدیدات یک فناوری پیشرفته را تجزیه و تحلیل و برطرف کرد. تجزیه و تحلیل داده‌های بزرگ، همراه با جریان شبکه، گزارش‌ها و رویدادهای سیستم، می‌توانند بی‌نظمی و فعالیت‌های مشکوک را کشف کنند، می‌توانند یک سیستم تشخیص نفوذ را ایجاد کنند، که با توجه به پیچیدگی روزافزون تخلفات سایبری این امر ضرورت بیشتری یافته است. امنیت سایبری ارکان اساسی تجربه دیجیتالی است، بنابراین ابتکارات دیجیتالی سازمان‌ها باید از ابتدا الزامات مربوط به امنیت و حریم خصوصی این داده‌ها را در سایبر و حریم خصوصی در نظر بگیرند. بنابراین، تجزیه و تحلیل داده های بزرگ نقش مهمی در کاهش تخلفات امنیت سایبری ناشی از متنوع ترین روش‌ها ، تضمین امنیت داده‌ها و حریم خصوصی آنها، یا حمایت از سیاست های اشتراک اطلاعات امن به نفع امنیت سایبری دارد(Banotra et al., 2021).

از سوی دیگر با پیشرفت مستمر معماری شبکه ارتباطی برای ادغام طیف متنوعی از دستگاه ها با نیازهای منحصر به فرد برای پارامترهای مختلف شبکه، منجر به ایجاد چالش های پیچیده‌ای برای امنیت شبکه شده است. تحولات اخیر در شبکه‌های نسل پنجم و با ارائه نرخ و سرعت بالاتر داده‌ها ، رشد همه جانبه ارتباطات داده را تسهیل کرده است. چنین افزایش عظیمی در ترافیک داده‌ها و دستگاه‌های متصل شبکه، معنای آسیب پذیری، تهدید و حملات بیشتر و در نتیجه خسارات فاجعه بار از نظر مالی، اجتماعی و انسانی را در بر دارد. بنابراین، بررسی و تجزیه و تحلیل این داده‌های بزرگ برای فعالیت های مشکوک با روش های سنتی قابل حصول نیست در این زمینه، انتظار از هوش مصنوعی و یادگیری ماشین آن است که نقشی اساسی در حل مشکلات بهینه سازی ان پی سخت[۵] و پیچیده داشته باشد (Yao et al., 2019).

[4] Big Data

[5] NPhard

۲. ۱. ۳ بلاک‌چین و اینترنت اشیا

امنیت سایبری یک نیاز مبرم برای دولت‌ها، مشاغل و افراد است که با تغییرات سریع فناوری و تغییر چشم انداز، آسیب سایبری را افزایش می‌دهد. تعداد زیادی راه حل برای رفع نیازهای امنیتی در حال تغییر ارائه شده است که یکی از این راه حل‌ها مبتنی بر بلاک‌چین است. بلاک‌چین یک فناوری زیربنایی امیدوارکننده است و دارای قابلیت استفاده در جنبه‌های مختلف امنیت سایبری است. به عنوان مثال، ویژگی‌های زنجیره بلوک مانند تمرکز زدایی، قابل تأیید و تغییر ناپذیری می‌توانند برای دستیابی به اصالت ، قابلیت اطمینان و یکپارچگی داده ها تسهیل کنند(Parizi et al., 2020).

در سال های اخیر، بلاک‌چین و اینترنت اشیا فناوریهای مطلوبی معرفی شدند که توانایی مدیریت کارآمد، صحیح، موثر اقتصادی استفاده از دارایی را دارند. در اینترنت اشیا (IoT) ، دستگاه های هوشمند یا حسگرها، اطلاعات را جمع‌آوری می‌کنند. ساخت اطلاعات امن، خود سازمان یافته و خود سازگار در بلاک‌چین مورد توجه قرار می‌گیرد. بلاک‌چین دفتری توزیع شده و غیرمتمرکز است که دارای بلوک‌های معاملات به ترتیب زمانی بر روی یکدیگر است. از نظر امنیت و اعتماد به فدراسیون شرکت ها در یک پلت فرم کمک می کند. اعتماد کاربران در استفاده از فناوری های بلاک چین وIoT مشهود است.پس می‌توان گفت حفظ امنیت اطلاعات مورد نیاز با استفاده از تکنیک های بلاک چین و IoT راه حل مناسبی خواهد بود(You et al., 2019).

۲. ۲. اصول تشکیل پایگاه امنیت

برای اطمینان از سه هدف مهم امنیت سایبری، یعنی در دسترس بودن، محرمانه بودن و یکپارچگی، می‌توان از چند اصل ساده اما مؤثر پیروی کرد. که این اصول شامل: تمرکز، دسترسی، پروتکل و پشتیبان گیری است (Panimalar et al., 2018). هر کدام از چهار اصل مطرح شده را می‌توان اینگونه تعریف کرد:

۲. ۲. ۱. **تمرکز بر سیستم‌های قبلی**: تثبیت میزان در دسترس بودن، محرمانه بودن و یکپارچگی منابع تحت تأثیر بزرگترین چالش‌ها قرار می‌گیرد و از این رو با تمرکز بر روی سیستم‌های حیاتی و ارائه بهترین محافظت حاصل می‌شود، در حالی که روش‌های دیگر برای محافظت از سیستمهای پیشین کمتری استفاده می‌شود (Yu et al., 2010).

۲. ۲. ۲. **کاربران مختلف با سطح دسترسی متفاوت**: چه داده هایی از طرف چه کسی قابل دستیابی است تا بتواند بر اساس چه نوع کاربر باشد و هیچ فردی نباید به همه داده ها و اطلاعات دسترسی پیدا کند. این به معنای حداقل امتیازات برای مسئولیت خاص است. از این رو، تغییر در مسئولیت مستقیماً با تغییر امتیازات متناسب است (Tang & Chen, 2007).

۲. ۲. ۳. **ارائه دفاع مستقل (پروتکل)**: چندین پروتکل تأیید هویت برای یک کار واحد، ایده به مراتب بهتری از یک پروتکل واحد است. این امر خطر حملات سایبری موفقیت آمیز را به شدت کاهش می‌دهد و اصل اساسی

افزایش کار مهاجم است، زیرا وی مجبور است چندین کار را انجام دهد تا چندین لایه محافظتی را بشکند (Ahmad et al., 2009)

۲. ۴. **پشتیبان گیری**: شکست می تواند رخ دهد اما برنامه ریزی عواقب پس از شکست می تواند آسیب های شدید به سیستم، شبکه یا فرد را کاهش دهد. این یک تکنیک بسیار مؤثر است و در زمینه های مختلف عملی است. نگهداری سوابق در مورد همه تخلفات: کارمندان امنیت سایبری باید سوابق همه تخلفات را حفظ کنند و باید دائماً مطالعات انجام شود و اقدامات حفاظتی ایجاد شود. این روند باید سریع باشد، زیرا هکرها منتظر نیستند؛ آنها مهارتهای خود را افزایش می دهند و همچنین ابزارهای حمله سایبری را بهبود می بخشند (Panimalar et al., 2018).

۲. ۳. چارچوب ارائه خدمات در امنیت سایبری هوشمند

علم داده های امنیت سایبری مبتنی بر داده ا ست ، از رو شهای یادگیری ما شینی ا ستفاده می کند ، تلاش برای تعیین کمیت خطرات سایبری ، ترویج رو شهای استنباطی برای تجزیه و تحلیل الگوهای رفتاری ، تمرکز بر ایجاد هشدارهای پا سخ امنیتی ، و در نهایت به دنبال بهینه سازی عملیات امنیت سایبری ا ست. از این رو ، ما به طور خلا صه در مورد یک چارچوب لایه ای پردازش داده های متعدد بحث می کنیم که به طور بالقوه می تواند برای کشـــف بینش امنیتی از داده های خام برای ساخت سیستم های امنیتی سایبری هو شمند مورد ا ستفاده قرار گیرد ، به عنوان مثال ، سیستم کنترل دسترسی مبتنی بر قاعده سیاست یا سیستم تشخیص و جلوگیری از نفوذ. برای تصمیم گیری هوشمند مبتنی بر داده در سیستم امنیت سایبری حا صل ، درک مشکلات امنیتی و ماهیت داده های امنیتی مربوطه و تجزیه و تحلیل گ سترده آنها مورد نیاز ا ست. برای این منظور ، چارچوب معرفی می گردد که نه تنها تکنیک های یادگیری ما شین را برای ایجاد مدل امنیتی در نظر می‌گیرد بلکه یادگیری و پویایی تدریجی را برای به روز نگه دا شتن مدل و تولید پا سخ متناظر ، که می تواند موثرتر و هوشـمندانه تر باشـد ، در نظر می گیرد. برای ارائه خدمات مورد انتظار شـکل ۲ نمای کلی از چارچوب را نشان می دهد ، شامل چندین لایه پردازش ، از داده های رویداد امنیتی خام گرفته تا خدمات.

۲. ۳. ۱. جمع آوری اطلاعات امنیتی

گام کلی برای جمع آوری و مدیریت داده های امنیتی از منابع مختلف داده بر اساس یک مشکل امنیتی خاص و پروژه در داخل شرکت است. منابع داده را می توان در چندین دسته گسترده مانند شبکه ، میزبان و ترکیبی طبقه بندی کرد (Sarker et al., 2020).

۲. ۳. ۲. آماده سازی داده های امنیتی

پس از جمع آوری داده های امنیتی خام از منابع مختلف با توجه به دامنه مسئله ای که در بالا بحث شد ، این لایه وظیفه آماده سازی داده های خام برای ساخت مدل را با اعمال فرآیندهای مختلف ضروری دارد. با این حال ، همه داده های جمع آوری شده به روند ساخت مدل در حوزه امنیت سایبری کمک نمی کنند (Zhao et al., 2014)

۲. ۳. ۳. مدل سازی امنیتی مبتنی بر یادگیری ماشین

این مرحله اصلی است که از طریق استفاده از علم داده های امنیت سایبری ، بینش و دانش از داده ها استخراج می شود. در این بخش ، ما به ویژه بر مدل سازی مبتنی بر یادگیری ماشین تمرکز می کنیم زیرا تکنیک های یادگیری ماشین می توانند چشم انداز امنیت سایبری را به طور قابل توجهی تغییر دهند. ویژگی ها یا ویژگی های امنیتی و الگوهای آنها در داده ها بسیار جالب است که برای استخراج بینش های امنیتی کشف و تجزیه و تحلیل می شوند. برای رسیدن به هدف ، درک عمیق تر از داده ها و مدل های تحلیلی مبتنی بر یادگیری ماشین با استفاده از تعداد زیادی از داده های امنیت سایبری می تواند موثر باشد (Han et al., 2011).

۲. ۳. ۴. یادگیری و پویایی افزایشی

در چارچوب ما ، این لایه به دنبال نهایی کردن مدل امنیتی حاصل با در نظر گرفتن اطلاعات اضافی با توجه به نیاز است. این می تواند با پردازش بیشتر در چندین ماژول امکان پذیر باشد. به عنوان مثال ، ماژول پس پردازش و بهبود در این لایه می تواند نقشی در ساده سازی دانش استخراج شده با توجه به نیازهای خاص با در نظر گرفتن دانش خاص دامنه داشته باشد. از آنجا که مدلهای طبقه بندی یا پیش بینی حمله مبتنی بر تکنیکهای یادگیری ماشین به شدت به داده های آموزش متکی هستند ، به سختی می توان آن را به مجموعه داده های دیگر تعمیم داد ، که این برای برخی از برنامه ها قابل توجه است. برای رفع این نوع محدودیت ها ، این ماژول مسئول استفاده از دانش دامنه به صورت طبقه بندی یا هستی شناسی برای بهبود ارتباط حمله در برنامه های امنیت سایبری است (Sarker et al., 2019).

۲. ۴. چالش‌های مدرن امنیت سایبری

امروزه، فضای مجازی به یک منبع محبوب و اجتناب ناپذیر برای به اشتراک گذاری اطلاعات و سایر فعالیت‌های حرفه‌ای از جمله تجارت، خرید، معاملات بانکی، تبلیغات، خدمات و غیره تبدیل شده است. این افزایش تصاعدی استفاده از فضای مجازی منجر به افزایش تصاعدی جرایم سایبری نیز شده است. دلیل اصلی این افزایش، استفاده از برنامه‌های وب تقریباً در همه جنبه‌های زندگی است. برنامه‌های وب عاری از خطاهای طراحی نیستند و مجرمان اینترنتی از این خطاها برای دستیابی غیرقانونی به سیستم ها سوء استفاده می‌کنند(Lun et al., 2016). همچنین امنیت سایبری به یکی از موضوعات مورد علاقه و با اهمیت در سراسر جهان تبدیل شده است و شامل تامین امنیت اطلاعات به وسیله‌ی شناسایی، جلوگیری و پاسخ به حملات سایبری است(Bada et al., 2019). سازوکارهای دفاعی که توسط سازمان‌های مختلف برای محافظت از فضای سایبری استفاده می‌شود، برای تامین امنیت در برابر آسیب‌های امنیتی روزافزون کافی نیستند. بنابراین، امنیت سایبری یکی از مهمترین چالش‌های علمی است که در دهه اخیر توجه محققان و متخصصان را به خود جلب کرده است. تعداد زیادی پژوهش در حوزه های مختلف سایبری انجام شده است که هر یک دارای ویژگی‌های خاصی برای رسیدگی به موارد مختلف نقض امنیت هستند(Lun et al., 2016).

بر طبق پژوهش همایون[6] و همکاران که به بررسی تهدیدات و آسیب پذیری‌های امنیت سایبری با روش نقشه برداری سیستماتیک انجام شده، پنج مورد از مهم‌ترین چالش‌های امنیت سایبری، حمله‌ی بندآوری خدمات[7]، بدافزار[8]، فیشینگ[9]، تزریق به پایگاه داده[10] و حمله‌ی شخص میانی[11] بیان شده است(Humayun et al., 2020). در ادامه به توضیح این چالش‌ها پرداخته شده است.

۲. ۴. ۱. **حمله‌ی بندآوری خدمات** (Denial-of-service): حمله‌ی بندآوری خدمات نوعی از برجسته ترین و مهمترین حملات دنیای سایبری امروز است. این نوع حملات با مکانیسم‌های ساده اما بسیار قدرتمند، تهدیدی عظیم برای جامعه فعلی اینترنت است(Mahjabin et al., 2017). Dos حمله رایجی در اینترنت است که هم برای کاربر و هم برای ارائه دهندگان خدمات مشکلات فراوانی ایجاد می‌کند. حمله‌ی بندآوری خدمات، با افزایش ارسال تعداد بسته‌ها از طریق شبکه و ایجاد ترافیک مخرب در شبکه، سبب از بین بردن قدرت ارتباطی و محاسباتی شبکه می‌شوند.(Mallikarjunan et al., 2016).

۲. ۴. ۲. **بدافزار** (Malware): بدافزار نوعی برنامه نرم‌افزاری است که اهداف مضر مهاجمان را برآورده می‌کند. بدافزارها، برای دستیابی به اهداف مهاجمان طراحی شده است. این اهداف شامل اختلال در عملکرد سیستم، دسترسی به سیستم محاسبات و منابع شبکه و جمع آوری اطلاعات حساس بدون اجازه کاربر است. در نتیجه، بدافزار اغلب تهدید جدی ایجاد می‌کند(Bayer et al., 2006). در عصر اینترنت، بدافزارها (مانند ویروس‌ها[12]، تروجان‌ها[13]، جاسوس‌افزارها[14]، باج‌افزارها[15]، ربات‌ها[16] و غیره) تهدیدهای امنیتی جدی علیه کاربران اینترنت ایجاد کرده‌اند که این تهدیدات، هر روزه تکامل یافته‌تر و پیشرفته‌تر می‌شوند(Ye et al., 2017).

۲. ٤. ۳. فیشینگ (Phishing): اصطلاح فیشینگ نوعی اصطلاح ماهیگیری است و همچنین عمل فیشینگ همانند فرآیند ماهیگیری است به‌صورتی که مهاجم با استفاده از طعمه، اطلاعات شخصی یا محرمانه قربانی را به سرقت می‌برد(Purkait, 2012). به عبارت دیگر فیشینگ یک عملیات فریب مقیاس پذیر است که به موجب آن از جعل هویت برای به‌دست آوردن اطلاعات از یک قربانی استفاده می شود(Lastdrager, 2014). فیشینگ از چند دهه پیش تهدیدی در دنیای سایبریِ بوده و هم اکنون نیز وجود دارد. در طول سال‌ها با خلاقیت فیشرها در برنامه ریزی و اجرای حملات، فیشینگ رشد و تکامل یافته است(Chiew et al., 2018).

۲. ۴. ۴. **تزریق به پایگاه داده** (SQL injection attack): تزریق به پایگاه داده SQL یکی از انواع تهدیدات است که برنامه‌های تحت وب، برنامه‌های موبایل و حتی برنامه‌های دسکتاپ که به پایگاه داده متصل هستند را در برمی‌گیرد. با اجرای تزریق SQL، مهاجم می‌تواند به برنامه یا پایگاه داده دسترسی کامل پیدا کند تا بتواند

---

[6] Humayun
[7] Denial-of-service (Dos)
[8] Malware
[9] Phishing
[10] SQL injection attack
[11] Man-in-the-middle attack
[12] Viruses
[13] Trojans
[14] Spyware
[15] Ransomware
[16] Bots

داده‌های قابل توجهی را غیرمسئولانه حذف یا تغییر دهد. برنامه‌هایی که ورودی کاربر را به درستی تأیید نمی کنند، آن‌ها را در مقابل تزریق SQL آسیب پذیر می کند. (SQLIA) زمانی اتفاق می‌افتد که یک مهاجم بتواند مجموعه‌ای از عبارات مخرب SQL را از طریق دستکاری داده‌های ورودی کاربر برای اجرای توسط پایگاه داده back-end در یک پرس و جو وارد کند. با استفاده از این نوع تهدیدها، برنامه‌ها می‌توانند به راحتی هک شده و اطلاعات محرمانه توسط مهاجم را به سرقت برند(Alwan & Younis, 2017).

۲. ۴. ۵. **حمله‌ی شخص میانی** (Man-in-the-middle attack): یک حمله‌ی شخص میانی نوعی حمله سایبری است که در آن یک شخص خارجی غیرمجاز وارد مکاتبه آنلاین بین دو کاربر می‌شود و از دید این دو کاربر پنهان می‌ماند. بدافزاری که در حمله میانی قرار دارد، غالباً اطلاعات فردی و طبقه بندی شده را که به تازگی توسط این دو کاربر ایجاد شده است را کنترل می‌کند و ممکن است آن را تغییر دهد. یک فرد در حمله‌ی شخص میانی به‌عنوان یک پروتکل در خارج از سیستم و بدون آشکار شدن هیچ گونه دستکاری می‌تواند به اطلاعات محرمانه دسترسی پیدا کند؛ آن‌ها را بخواند و تغییر دهد. این مسئله بسیار مخرب است و اکثر سیستم های رمزنگاری بدون داشتن یک احراز هویت مناسب، در معرض هک شدن توسط بدافزاری به نام MITM می‌شوند(Mallik et al., 2019).

جدول(۱). جدول پیشینه ادبیات و منابع پژوهش

نام محقق/سال	عنوان پژوهش	یافته‌های پژوهش
Furstenau et al., 2020	بیست سال تحول علمی امنیت سایبری: یک نقشه‌ی علمی	هدف در این مطالعه انجام یک نقشه برداری علمی در زمینه مطالعه امنیت سایبری به منظور کشف موضوعات فعلی نویسندگان در این زمینه و ایجاد نقشه‌ی علمی به منظور شناسایی موضاعات مهم و چالش‌ها در این حوزه است.
Anwar & Hassan, 2017	استفاده از تکنیک های هوش مصنوعی به منظور پیشگیری از حملات سایبری	امنیت سایبری رشته ای است که می‌تواند بیشترین منفعت را از هوش مصنوعی کسب کند. سخت نرم افزار برای دفاع در برابر حملات قدرتمند در حال توسعه در سیستم‌ها دشوار است. با استفاده از تکنیک‌های هوش مصنوعی این مهم تسهیل می‌شود.
Geluvaraj et al., 2019	آینده امنیت سایبری: نقش اصلی هوش مصنوعی، یادگیری ماشین	حملات هکرهایی که می‌خواهند به داده‌ها و اطلاعات دسترسی پیدا کنند به صورت نمایی در حال افزایش است و روز به روز پیشرفته‌تر

	و یادگیری عمیق در فضای مجازی	می‌شوند. در آینده، هوش مصنوعی نقش مهمی در امنیت سایبری خواهد داشت. بعلاوه، ممکن است در فضای مجازی اختلافات جهانی گسترده به‌وجود آید. که شامل حمله به ساختارهای سازمانی و تاسیسات و همچنین ایجاد اختلال در عملکرد عادی دولت و سیستم های مالی شود.
Leenen & Meyer, 2019	هوش مصنوعی و تجزیه و تحلیل داده‌های کلان در پشتیبانی از دفاع سایبری	در این مقاله با ارائه یک نمای کلی از وضعیت فعلی و شناسایی روندهای نوظهور در زمینه امنیت سایبری، استفاده از تجزیه و تحلیل داده های بزرگ و فناوری های نوظهور برای دفاع سایبری در نظر گرفته شده است. تجزیه و تحلیل داده های بزرگ توانایی مقابله با مجموعه‌های زیادی از داده‌های متنوع، ساختاری و غیر ساختاری را تقریباً در زمان واقعی فراهم می‌کند.
Sarker et al., 2020	علم داده های امنیت سایبری: مروری کلی از دیدگاه یادگیری ماشین	هدف این مقاله به اشتراک گذاشتن نمای کلی از مفهوم سازی، درک، مدل سازی و تفکر در مورد علم داده های امنیت سایبری است. همچنین موارد مختلف کلیدی در تجزیه و تحلیل شناسایی امنیت مورد بحث قرار گرفته است.
Alqahtani & Braun, 2021	بررسی تأثیر کنترل های فنی، مسئولیت پذیری و نظارت بر انطباق امنیت سایبری در سازمان‌های دولت الکترونیک	نقض امنیت سایبری در درجه اول به دلیل استفاده نادرست از سیستم های اطلاعاتی و عدم رعایت اقدامات امنیت سایبری است. عدم رعایت امنیت سایبری یکی از نگرانی های اصلی سازمان هاست. این مطالعه. پنج عامل رسمی و غیررسمی جدید که بر انطباق امنیت سایبری در سازمان‌ها تأثیر می گذارند را مورد شناسایی و ارزیابی قرار داده است.
Huang & Madnick, 2020	آیا قابلیت امنیت سایبری بالا منجر به گشودگی در تجارت دیجیتال می‌شود؟ با میانجی‌گر بلوغ دولت الکترونیکی در نوآوری دیجیتال فرامرزی	خطرات امنیت سایبری تهدیدهای جدیدی را برای تجارت دیجیتال ایجاد می‌کند، دولت ها برای تنظیم نوآوری‌های دیجیتال، سیاست‌های امنیتی سایبری متعددی را در دستور کار خود قرار می‌دهند. این مطالعه برای بررسی رابطه بین قابلیت امنیت ملی سایبری و محدودیت‌های

		تجارت دیجیتال، یک مدل رفتار ملی تجارت سایبری ایجاد کرده است و همچنین یک چارچوب حاکمیتی برای یک سیستم تجارت دیجیتال امن و باز پیشنهاد می‌دهد.
Mora et al., 2019	مطالعه‌ی موردی امنیت سایبری مستقر با تکنولوژی بلاک‌چین به منظور حفظ حریم خصوصی شهروندان و زیرساخت‌های سایبری شهرهای هوشمند	دستگاه های اینترنت اشیا هوشمند متصل به زیرساخت های سایبری در یک شهر هوشمند می‌توانند در معرض تهدیدهای امنیتی قرار بگیرند. در این مقاله تکنولوژی بلاک‌چین نوید بخش تامین کننده امنیت بیان شده و چگونگی کار کرد آن مورد ارزیابی قرار گرفته است.

با توجه به پیشینه و مدل مفهومی مستخرج، جدول سنجش متغیرها که به تشریح سازه، ابعاد وو شاخص ها می‌پردازد.

جدول(۲). سنجش متغیرها

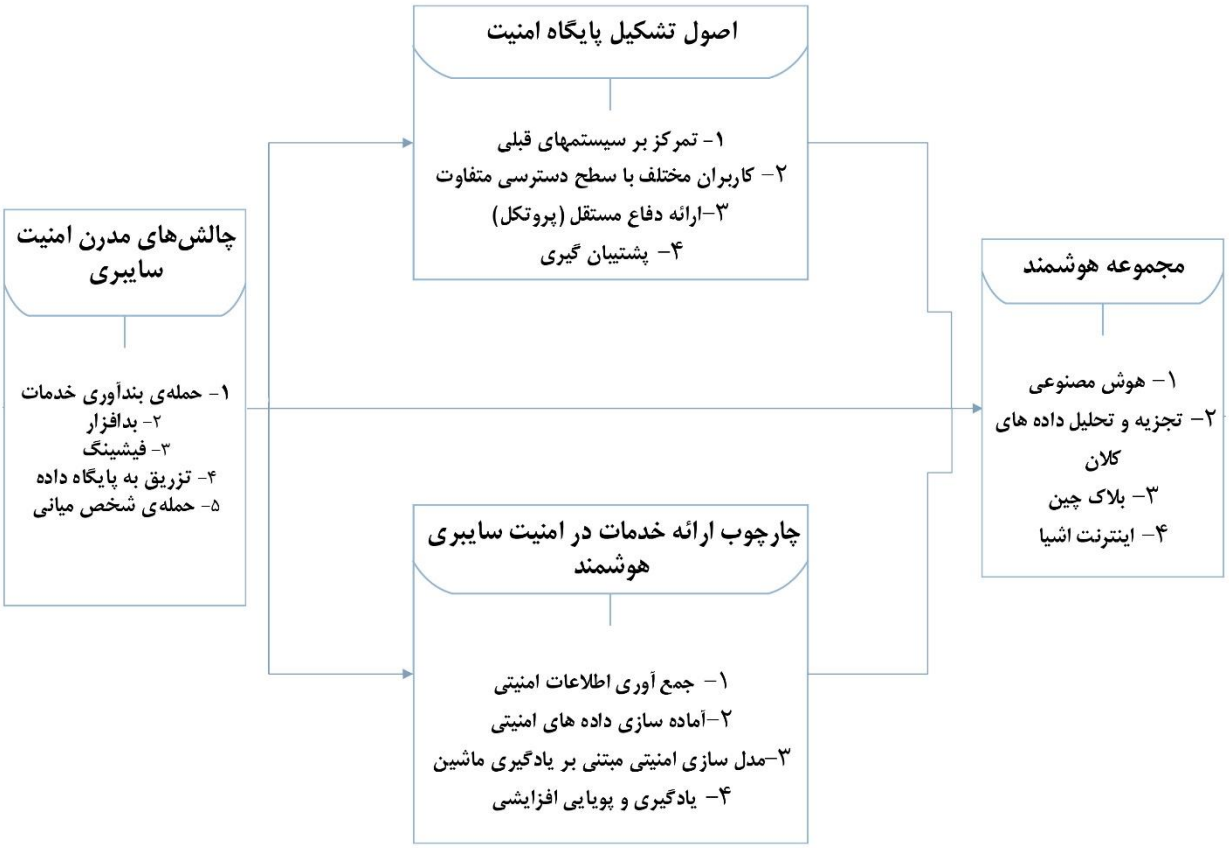
عنوان سازه	ابعاد	شاخص‌ها	منابع
مجموعه هوشمند	هوش مصنوعی	طیف گسترده ای از تقاطع های بین رشته ای بین امنیت سایبری و هوش مصنوعی وجود دارد.	Li, 2018 Zeadally et al., 2020
		پیشرفت در تکنیک های رمزنگاری و هوش مصنوعی (به ویژه یادگیری ماشینی و یادگیری عمیق) نوید بخش توانایی متخصصان امنیت سایبری برای مقابله با تهدیدهای رو به رشد توسط مهاجمان است.	
		فناوری های هوش مصنوعی، مانند یادگیری عمیق، می‌توانند به امنیت سایبری وارد شوند تا مدل های هوشمندی برای طبقه بندی بدافزار و تشخیص نفوذ و سنجش هوش تهدیدآمیز ساخته شود.	
	تجزیه و تحلیل داده‌های کلان	امنیت سایبری در زمینه داده های کلان به عنوان یک مسئله مهم شناخته شده است و یک چالش بزرگ برای جامعه تحقیقاتی است.	Sabar et al., 2018 Leenen & Meyer, 2019

		تجزیه و تحلیل داده‌های کلان و هوش مصنوعی می تواند دفاع سایبری را بهبود بخشد.	
	بلاک چین	فناوری بلاک چین به دلیل گستره و سیعی از کاربردهای بالقوه در حوزه‌ی امنیت، مورد توجه بسیاری قرار گرفته است.	Zhuang et al., 2021 Hasanova et al., 2019
		فناوری بلاک چین در زمینه های تحقیقاتی ، از جمله کاربرد آن در شبکه هو شمند برای امنیت سایبری ، توجه قابل توجهی را به خود جلب کرده است.	
		بسیاری از برنامه ها قربانی حملات سایبری موفق شده اند. با توجه به افزایش تقا ضا برای ارز رمزنگاری شده و چالش های امنیتی فعلی آن، نیاز به فناوری بلاک چین محسوس است.	
	اینترنت اشیا	بسیاری از سازمانها لزوماً از تعداد زیادی از دستگاههای اینترنت اشیا که در حال حاضر استفاده می کنند و اینکه چگونه دستگاههای اینترنت اشیا ممکن است متفاوت از دستگاههای فناوری اطلاعات معمولی (IT) بر امنیت و امنیت سایبری تأثیر بگذارند، آگاهی ندارند.	Sani et al., 2019 Boeckl et al., 2019 Scarfò, 2017
		با پیشرفت چشمگیر در استقرار اینترنت اشیا (IoT) در زیرساخت شبکه هوشمند، تقاضا برای امنیت سایبری به سرعت در حال رشد است.	
		امروزه، تکامل دنیای اینترنت اشیا نویدبخش انفجار تعدادی دستگاه متصل به اینترنت است. این مساله ذاتاً، به طرز چشمگیری مشکلات امنیتی را افزایش می‌دهد.	
اصول تشکیل پایگاه امنیت	تمرکز بر سیستمهای قبلی	تثبیت میزان در دسترس بودن، محرمانه بودن و یکپارچگی منابع تحت تأثیر بزرگترین چالش‌ها قرار می‌گیرد	Yu et al., 2010
		و از این رو با تمرکز بر روی سیستم‌های حیاتی و ارائه بهترین محافظت حاصل می شود،	
		در حالی که روش‌های دیگر برای محافظت از سیستمهای پیشین کمتری استفاده می شود	

	کاربران مختلف با سطح دسترسی متفاوت	چه داده هایی از طرف چه کسی قابل دستیابی است تا بتواند بر اساس چه نوع کاربر باشد و هیچ فردی نباید به همه داده ها و اطلاعات دسترسی پیدا کند.	Hou et al., 2020 Kumaresan & Shanmugam, 2020
		تهدیدات امنیتی داده ها در هنگام دسترسی به داده ها، منجر به دسترسی غیرمجاز، تغییر و افشای داده ها می شود و بر محرمانه بودن و یکپارچگی داده ها تأثیر می گذارد	
		رایانش ابری برای ارائه خدمات مختلف در سطوح مختلف دسترسی کاربر پیچیده تر می شود	
	ارائه دفاع مستقل (پروتکل)	چندین پروتکل تأیید هویت برای یک کار واحد، ایده به مراتب بهتری از یک پروتکل واحد است.	Ahmad et al., 2009 Wang et al., 2020
		احتمال موفقیت مهاجم با افزایش پروتکول کاهش می یابد، زیرا وی مجبور است چندین کار را انجام دهد تا چندین لایه محافظتی را بشکند	
		استفاده ارز تکنولوژی IOT می تواند به افزایش پروتکل ها کمک کند	
	پشتیبان گیری	**مطالعات و اقدامات حقفاظتی باید به سرعت انجام شود و همیشه به روز باشد**	Panimalar et al., 2018 Ali & Awad, 2018
		کارمندان امنیت سایبری باید سوابق همه تخلفات را حفظ و نگهداری کنند	
		پشتیبان گیری از طریق بررسی مداوم ترافیک شبکه ، اطمینان از دسترسی به تنظیمات سیستم و نظارت بر رفتار سیستم باید از سرقت اطلاعات از طریق شبکه های هوشمند جلوگیری کند.	
چارچوب ارائه خدمات در امنیت	جمع آوری اطلاعات امنیتی	متخصصان با استفاده از قدرت دادهها نقش مهمی در امنیت سایبری فراهم می‌کنند	Foroughi & Luksch, 2018 Serrano et al., 2014
		سالها ست که نیاز به اشتراک اطلاعات به عنوان یک نیاز اصلی توسط جامعه امنیت سایبری شناخته شده است.	
		همه‌ی داده‌های جمع آوری شده به روند ساخت مدل در حوزه امنیت سایبری کمک نمی‌کنند.	Zhao et al., 2014

سایبری هوشمند	آماده سازی داده های امنیتی	استخراج الگوهای حادثه امنیتی یا بینش داده‌های امنیت سایبری و ساخت مدل مربوط به داده، کلید ایجاد یک سیستم امنیتی به صورت خودکار و هوشمند است.	Sarker et al., 2020 Kissoon, 2020
		جمع آوری و تجزیه و تحلیل عمیق داده‌ها می‌تواند تسهیل کننده امنیت شود.	
	مدل سازی امنیتی مبتنی بر یادگیری ماشین	تکنیک‌های یادگیری ماشین مجموعه‌ای از مدل‌های ریاضی برای حل مسائل مختلف است. پیش بینی، طبقه بندی، ارتباط داده‌ها، مفهوم سازی داده‌ها کارهاییست که به منظور توصیف امنیت سایبری مورد بهره برداری قرار می‌گیرد.	Martínez Torres et al., 2019 Xin et al., 2018 Thomas et al., 2020
		با توسعه اینترنت، حملات سایبری به سرعت در حال تغییر است و وضعیت امنیت سایبری مناسب نیست، با توجه به بررسی‌ها راه حل را می‌بایست مدل سازی‌ها در یادگیری ماشین (ML) و یادگیری عمیق (DL) جست.	
		با استفاده از الگوریتم های ML می‌توان مدل‌هایی از رفتارها ایجاد کرد و از این مدل ها به عنوان مبنایی برای پیش بینی داده های تازه وارد به منظور افزایش امنیت استفاده کرد.	
	یادگیری و پویایی افزایشی	رویکردهای سنتی امنیت سایبری مبتنی بر پایگاه داده‌های دانش قدیمی هستند و برای ایستادگی در برابر نسل جدید تهدیدات سایبری باید به صورت مستمر به‌روز شوند.	Usman et al., 2019 Geluvaraj et al., 2019
		در سال های اخیر، سیستم عامل‌های مختلف محاسباتی مبتنی بر الگوریتم‌های یادگیری به عنوان یک منبع مفید برای مدیریت و بهره برداری از داده‌های تولید شده برای استخراج اطلاعات معنی دار ظاهر شده اند.	
		بدافزارهای ذسل جدید و حملات سایبری، با روش های سنتی امنیت سایبری د شوار ا ست. آنها با گذ شت زمان تو سعه می یابند، بنابراین رویکردهای جدیدتر و پویایی لازم است.	
چالش‌های مدرن امنیت سایبری	حمله‌ی بندآوری خدمات	این نوع حملات با مکانیسم‌های حمله ساده اما بسیار قدرتمند، تهدیدی عظیم برای جامعه فعلی اینترنت است.	Mahjabin et al., 2017 Mallikarjunan et al., 2016
		Dos حمله رایجی در اینترنت است که هم برای کاربر و هم برای ارائه دهندگان خدمات مشکلات فراوانی ایجاد می‌کند.	
	بدافزار	در عصر اینترنت، بدافزارها تهدیدهای امنیتی جدی علیه کاربران اینترنت ایجاد کرده‌اند.	Ye et al., 2017 Chowdhury et al., 2018
		تهدیدات بدافزارها، هر روزه تکامل یافته‌تر و پیشرفته‌تر می‌شوند.	

		نفوذ اطلاعات حساس توسط نرم افزار مخرب یا بدافزار یک تهدید جدی سایبری در سراسر جهان است که تأثیر فاجعه باری بر مشاغل، سازمان های تحقیقاتی، اطلاعات ملی و همچنین افراد دارد.	
فیشینگ	فیشینگ از چند دهه پیش تهدیدی در دنیای سایبرِی بوده و هم اکنون نیز وجود دارد.		Chiew et al., 2018 Thomas, 2018 Das et al., 2019
	در طول سال‌ها با خلاقیت فیشرها در برنامه ریزی و اجرای حملات، فیشینگ رشد و تکامل یافته است.		
	امروزه یکی از دشوارترین چالش های امنیت اطلاعات، فیشینگ است.		
	فیشینگ یک حمله امنیت سایبری شناخته شده است که طی سال‌های اخیر به سرعت افزایش یافته است.		
تزریق به پایگاه داده	تزریق به پایگاه داده SQL یکی از انواع تهدیدات است که برنامه های تحت وب، برنامه های موبایل و حتی برنامه های دسکتاپ که به پایگاه داده متصل هستند را در برمی‌گیرد.		Alwan & Younis, 2017 Vyamajala et al., 2018
	تزریق SQL به عنوان روشی برای اجرای نمایش داده های SQL و بازیابی اطلاعات حساس از یک پایگاه داده متصل به وب سایت شناخته شده است		
حمله‌ی شخص میانی	اکثر سیستم های رمزنگاری بدون داشتن یک احراز هویت منا سب، در معرض هک شدن تو سط بدافزاری به نام MITM می‌شوند.		Mallik et al., 2019 Natarajan, 2019 Pingle et al., 2018
	امروزه مهاجمان سعی در حمله به داده‌های شبکه با روش حمله ی شخص میانی دارند. الگوریتم یادگیری ما شین در حال ارائه راه حل های بی شماری برای این حمله سایبری است.		
	حمله‌ی شخص میانی یکی از ا صلی ترین حملاتی ا ست که در هک‌های رایانه ای به کار گرفته می‌شود.		



شکل(۱)، چارچوب مفهومی پژوهش

۳. یافته ها و روش پژوهش

این پژوهش براساس هدف، کاربردی و از نظر شیوه گردآوری داده‌ها، با توجه عدم دستکاری متغیرها (سرمد، بازرگان و حجازی، ۱۳۸۷)، مطالعه ای توصیفی- همبستگی است. جامعه آماری این پژوهش، کارآفرینانی هستند که در زمان انجام دادن این پژوهش فعال بوده اند. در ادامه داده‌های پژوهش با استفاده از پرسشنامه محقق ساخته الکترونیکی گردآوری شد. با توجه به جامعه آماری، ۷٤٥ نفر کارآفرین فعال در زمان پژوهش با استفاده از روش نمونه گیری تصادفی در دسترس از جامعه محدود (دانیل[17]، ۱۹۹۹)، ۱۱۵ نفر از این کارآفرینان به‌عنوان حجم نمونه مشخص شد. تحلیل داده‌ها با رویکرد کمی و در دو بخش انجام شده است. در بخش اول ویژگی‌های جمعیت شناختی و تجمیع گویه‌ها برای ورود به مدل، با استفاده از نرم‌افزار اس پی اس و بخش دوم از نرم‌افزار پی ال اس برای تحلیل سازه‌ها و روابط بیان شده در چهارچوب مفهومی، استفاده شده است.

[17] Daniel

ویژگی‌های جمعیت شناختی افراد شرکت کننده در این مطالعه در جدول زیر آورده شده اند.

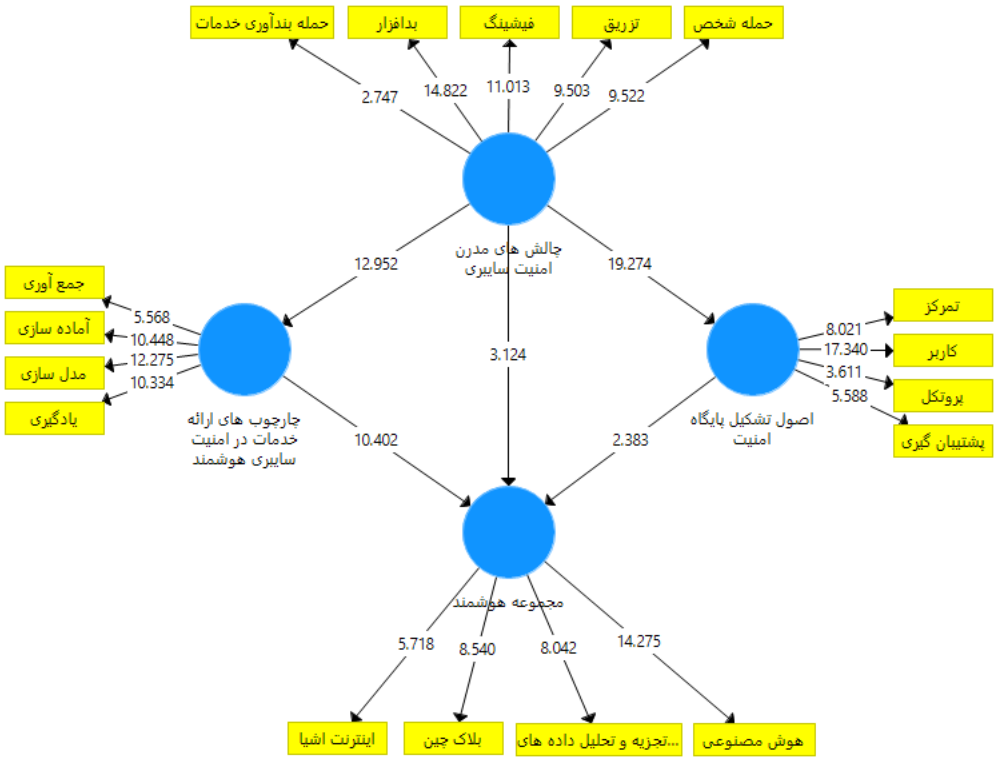
جدول(۳)، ویژگی‌های جمعیت شناختی شرکت کنندگان

شاخص‌ها	گروه‌ها	فراوانی
جنسیت	زن	٤٣
	مرد	٧٧
سن	زیر ۳۰ سال	٣٤
	۳۰ تا ٤٠ سال	٦٢
	بالای ٤٠ سال	٢٤
سابقه کار	٥ تا ۱۰ سال	٣١
	۱۰ تا ۱۵ سال	٤٦
	۱۵ سال به بالا	٤٣
تحصیلات	کارشناسی	٢٩
	کارشناسی ارشد	٦٣
	دکترا	٢٨

لازم به ذکر است، پرسشنامه نهایی این تحقیق به روش مدل‌یابی معادلات ساختاری با رویکرد حداقل مربعات جزئی مورد تجزیه و تحلیل قرار گرفته شده است. در این روش، برازش مدل با استفاده از معیارهای پایایی، روایی همگرا و روایی واگرا بررسی شد. برای بررسی میزان پایایی از دو معیار آلفای کرونباخ و پایایی ترکیبی استفاده شده است. همچنین، روایی پرسشنامه نیز توسط دو معیار روایی همگرا و روایی واگرا بررسی شد. در جدول زیر نتایج مربوط به سازگاری درونی (تحلیل پایایی) آورده شده است:

جدول(۴)، سازگاری درونی متغیرها (روایی همگرا و پایایی ترکیبی)

مولفه	آلفای کرونباخ	پایایی ترکیبی (CR)	AVE
چالش‌های مدرن امنیت سایبری	/٩١٦	/٩٥٤	/٨٧
چارچوب های ارائه خدمات در امنیت سایبری هوشمند	/٩١١	/٩٣٢	/٧٣
اصول تشکیل پایگاه امنیت	/٨٣١	/٩٢١	/٧٥
مجموعه هوشمند	/٨٥١	/٩٤٣	/٨٢



شکل(۲): آزمون معناداری مدل پژوهش

میانگین واریانس استخراج شده برای تمامی سازه‌ها بالاتر از ۰/۵ بوده و روایی سازه‌ها مورد تایید می باشد. آلفای کرونباخ برای سازه‌ها بالاتر از ۰/۷ و پایایی ترکیبی بالاتر از ۰/۷ است. لذا، پایایی سازه‌ها نیز مورد تایید می باشد.

جدول(۵)، ماتریس سنجش روایی واگرا

مولفه	چالش‌های مدرن امنیت سایبری	چارچوب های ارائه خدمات در امنیت سایبری هوشمند	اصول تشکیل پایگاه امنیت	مجموعه هوشمند
چالش‌های مدرن امنیت سایبری	۰/۹۳۲			
چارچوب های ارائه خدمات در امنیت سایبری هوشمند	۰/۶۳۲	۰/۸۵۴		
اصول تشکیل پایگاه امنیت	۰/۶۷۴	۰/۵۳۲	۰/۸۶۶	
مجموعه هوشمند	۰/۶۹۳	۰/۵۷۶	۰/۴۸۹	۰/۹۰۵

با توجه به ماتریس با روایی واگرا مورد تأیید بوده و نتایج فوق نشان میدهد، ابزار پژوهش از روایی و پایایی معتبری برخوردار است.

۳. ۱.ارزیابی برازش مدل

این پژوهش با روش مدل‌یابی معادلات ساختاری با رویکرد حداقل مربعات جزئی انجام گرفته است. برای نشان دادن برازش مدل ساختاری باید مقدار قدر مطلق T-value بیشتر از ۱/۹۶ باشد. بر اساس نمودار زیر تمامی مقادیر بالاتر از ۱/۹۶ می باشد که نشان می‌دهد که برازش مدل ساختاری برقرار می‌باشد.

نتایج نشان می‌دهد که ضریب معناداری مربوط به چالش‌های مدرن امنیت سایبری با تعدیل‌گری چارچوب های ارائه خدمات در امنیت سایبری هوشمند و اصول تشکیل پایگاه امنیت از سطح مناسبی برخوردار است و این بیانگر این است که چارچوب های ارائه خدمات در امنیت سایبری هوشمند و اصول تشکیل پایگاه امنیت توانسته رابطه بین چالش‌های مدرن امنیت سایبری و مجموعه هوشمند را تعدیل نماید. همچنین جهت سنجش کلی مدل اندازه گیری و مدل ساختاری، از شاخصی به نام نیکویی برازش استفاده نموده ایم. فورنل و لارکر سه مقدار ۰/۰۱، ۰/۲۵ و ۰/۳۶ را به‌عنوان مقادیر ضعیف، متوسط و قوی برای آن معرفی نموده اند.

$$GOF = \sqrt{\overline{Com} \times \overline{R^2}} = \sqrt{0.427 \times 0.533} = 0.348$$

تمامی موارد حاکی از برازش قوی برای مدل پژوهش می باشند. نتایج تحلیل مسیر به جهت آزمون فرضیه‌های پژوهش در ادامه آورده شده است:

تمام فرضات تایید شد و نشان‌دهنده اثر معناداری مدل مفهومی است.

جدول(۶)، نتایج مدل ساختاری

اثر	مسیر ساختاری	معناداری	ضریب	نتیجه
اثرات مستقیم	چالش‌های مدرن امنیت سایبری ← مجموعه هوشمند	۳,۱۲٤	۰,۲٦٦	تایید
	چالش‌های مدرن امنیت سایبری ← اصول تشکیل پایگاه امنیت	۱۹,۲۷٤	۰,۷۷۰	تایید
	چالش‌های مدرن امنیت سایبری ← چارچوب های ارائه خدمات در امنیت سایبری هوشمند	۱۲,۹۵۲	۰,٦۸٤	تایید
تعدیلگر	چالش‌های مدرن امنیت سایبری ← اصول تشکیل پایگاه امنیت ← مجموعه هوشمند	۲,۳۸۳	۰/۲۱۱	تایید

	چالش‌های مدرن امنیت سایبری ← چارچوب های ارائه خدمات در امنیت سایبری هوشمند ← مجموعه هوشمند	۱۰,٤۰۲	۰,٥۷۷	تایید

۴. نتیجه

امروزه انسان‌ها از طریق تلفن‌های هوشمند، ارتباط و تعامل با یکدیگر را افزایش داده‌اند. این افزایش ارتباط نه تنها درمیان انسان‌ها، بلکه در ارتباط انسان با اشیاء و اماکن پیرامونش را افزایش داده است، به طوریکه، خانه‌ها، اتومبیل‌ها، اماکن عمومی و سایر سیستم‌های اجتماعی اکنون در مسیر اتصال کامل، موسوم به اینترنت اشیا قرار گرفته‌اند. استانداردها در فرآیند هوشمند سازی، در حال تکامل است و منجربه پیشرفت‌های بی‌سابقه در کیفیت زندگی می‌شوند. داده‌ها و اطلاعات حاصل از اجزا در در مجموعه هوشمند تولید و به اشتراک گذاشته می‌شوند، به عنوان مثال در تعریف خدمات عمومی و خصوصی نظیر حمل و نقل هوشمند، امکان اتصال به شبکه‌ای از داده‌های بهم پیوسته مانند موقعیت مکانی، وضعیت لحظه‌ای آب و هوا و همچنین ترافیک، امکان دسترسی فعال خواهد بود. چنین سیستم‌های یکپارچه می‌توانند با افزایش ایمنی عمومی و پاسخ به شرایط اضطراری در بهبود خدمات و رفع حوادث احتمالی کمک کنند. در حفظ این مزیت‌ها، توجه به چالش‌های مهم و درهم پیچیده، امنیت و حریم خصوصی دارای اهمیت خواهد بود. امنیت شامل مراقبت از دسترسی غیرقانونی به اطلاعات و حملاتی است که باعث اختلال در دسترسی به خدمات می‌شود. از آنجا که شهروندان دیجیتالی بیشتر و بیشتر با داده های موجود در مورد مکان و فعالیت های خود کار می‌کنند ، به نظر می‌رسد حریم خصوصی با چالش روبرو شود. (Elmaghraby & Losavio, 2014). از این جهت طراحی سازوکار و مدلی که بتواند در مسیر هوشمند شدن، درک صحیح از امنیت را داشته باشد و حفظ آن را تضمین کند، برای جوامع هوشمند اهمیت پیدا می‌کند.

این پژوهش می‌کوشد تا به بررسی تاثیر چالش‌های مدرن امنیت سایبری بر گسترش هوشمند سازی بپردازد. نتایج مشخص نمود که چالش های مدرن امنیت سایبری، اصول تشکیل پایگاه امنیت و چارچوب ارائه خدمات هوشمند تاثیر مثبتی را بر گسترش هوشمند سازی دارد. علاوه بر تاثیر مستقیم بیان شده، گسترش هوشمند سازی بیشترین تاثیر غیرمستقیم (چالش های مدرن امنیت سایبری) را از چارچوب ارائه خدمات هوشمند می گیرد. بنابراین انتظار می‌رود با در نظر گرفتن چالش های مدرن امنیت سایبری به مدیریت صحیح خطرات امنیتی پرداخته و آن‌را کاهش دهد تا منجربه افزایش منافع شود و همچنین زمینه بهره‌مندی از فرصت‌های اجتماعی، اقتصادی و فرهنگی مجموعه هوشمند را متصور خواهد شد. این موضوع با پژوهش همایون[۱۸] و همکاران که به بررسی تهدیدات و آسیب‌پذیری‌های امنیت‌سایبری با روش نقشه برداری سیستماتیک انجام شده، هماهنگی دارد.

به عنوان پیشنهاد برای تحقیقات آینده برای پژوهشگران علاقه‌مند در این حوزه، شناسایی روند های ایجاد نوآوری در آینده امنیت سایبری پیشنهاد می‌شودکه می‌تواند با تمرکز بر مولفه‌های شناسایی فرصت جدید هوشمند سازی، به کارآفرینی‌های بدیع منتج شود.

[18] Humayun

۵. منابع

Ahmad, I., Abdullah, A. B., & Alghamdi, A. S. (2009). Application of artificial neural network in detection of DOS attacks. *SIN'09 - Proceedings of the 2nd International Conference on Security of Information and Networks*, 229–234. https://doi.org/10.1145/1626195.1626252

Ali, B., & Awad, A. I. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. In *Sensors* (Vol. 18, Issue 3). https://doi.org/10.3390/s18030817

Alqahtani, M., & Braun, R. (2021). *Examining the Impact of Technical Controls, Accountability and Monitoring towards Cyber Security Compliance in E-government Organisations*.

Alwan, Z. S., & Younis, M. F. (2017). Detection and Prevention of SQL Injection Attack: A Survey. *International Journal of Computer Science and Mobile Computing*, *6*(8), 5–17. https://www.researchgate.net/publication/320108029

Anwar, A., & Hassan, S. I. (2017). Applying Artificial Intelligence Techniques to Prevent Cyber Assaults. *International Journal of Computational Intelligence Research*, *13*(5), 883–889.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *ArXiv*. http://arxiv.org/abs/1901.02672

Banotra, A., Gupta, S., Gupta, S. K., & Rashid, M. (2021). Asset Security in Data of Internet of Things Using Blockchain Technology. In *Springer* (pp. 269–281). https://doi.org/10.1007/978-981-15-8711-5_14

Bayer, U., Moser, A., Kruegel, C., & Kirda, E. (2006). Dynamic analysis of malicious code. *Journal in Computer Virology*, *2*(1), 67–77. https://doi.org/10.1007/s11416-006-0012-2

Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The Role of Artificial Intelligence in Cyber Security. In *igi-global.com* (pp. 170–192). https://doi.org/10.4018/978-1-5225-8241-0.ch009

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., Gabel, D., Rourke, O. ', Piccarreta, B., & Scarfone, K. (2019). *NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. 44. https://doi.org/10.6028/NIST.IR.8228

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. In *Expert Systems with Applications* (Vol. 106, pp. 1–20). https://doi.org/10.1016/j.eswa.2018.03.050

Chowdhury, M., Rahman, A., & Islam, R. (2018). Malware analysis and detection using data mining and machine learning classification. *Advances in Intelligent Systems and Computing*, *580*, 266–274. https://doi.org/10.1007/978-3-319-67071-3_33

Das, S., Kim, A., Tingle, Z., & Nippert-Eng, C. (2019). All about phishing exploring user research through a systematic literature review. In *arXiv*. arXiv. http://arxiv.org/abs/1908.05897

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491–497.

https://doi.org/10.1016/j.jare.2014.02.006

Fischer, E. A. (2015). Cybersecurity issues and challenges: In Brief. In *Cyberspace Threat Landscape: Overview, Response Authorities, and Capabilities* (pp. 45–54). www.crs.gov

Foroughi, F., & Luksch, P. (2018). Data science methodology for cybersecurity projects. In *arXiv*. arXiv. https://doi.org/10.5121/csit.2018.80401

Furstenau, L. B., Sott, M. K., Homrich, A. J. O., Kipper, L. M., Al Abri, A. A., Cardoso, T. F., Lo´pez-Robles, J. R., & Cobo, M. J. (2020). 20 years of scientific evolution of cyber security: A science mapping. *Proceedings of the International Conference on Industrial Engineering and Operations Management*, *March*, 314–325. https://www.researchgate.net/profile/Leonardo_Bertolin_Furstenau/publication/340413661_20_Years_of_Scientific_Evolution_of_Cyber_Security_a_Science_Mapping/links/5e91e6234585150839d2b75e/20-Years-of-Scientific-Evolution-of-Cyber-Security-a-Science-Mapping

Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace. In *Lecture Notes on Data Engineering and Communications Technologies* (Vol. 15, pp. 739–747). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-10-8681-6_67

Han, J., Kamber, M., & Pei, J. (2011). Data mining concepts and techniques third edition. *The Morgan Kaufmann Series in Data Management Systems*, *5*(4), 83–124.

Hasanova, H., Baek, U. jun, Shin, M. gon, Cho, K., & Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, *29*(2), e2060. https://doi.org/10.1002/nem.2060

Hou, Y., Garg, S., Hui, L., Jayakody, D. N. K., Jin, R., & Hossain, M. S. (2020). A data security enhanced access control mechanism in mobile edge computing. *IEEE Access*, *8*, 136119–136130. https://doi.org/10.1109/ACCESS.2020.3011477

Huang, K., & Madnick, S. E. (2020). Does High Cybersecurity Capability Lead to Openness in Digital Trade? The Mediation Effect of E-Government Maturity within Cross-border Digital Innovation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3542552

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

Kissoon, T. (2020). Optimum spending on cybersecurity measures. *Transforming Government: People, Process and Policy*, *14*(3), 417–431. https://doi.org/10.1108/TG-11-2019-0112

Kumaresan, S., & Shanmugam, V. (2020). Time-variant attribute-based multitype encryption algorithm for improved cloud data security using user profile. *Journal of Supercomputing*, *76*(8), 6094–6112. https://doi.org/10.1007/s11227-019-03118-8

Lastdrager, E. E. H. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. In *Crime Science* (Vol. 3, Issue 1). SpringerOpen. https://doi.org/10.1186/s40163-014-0009-y

Leenen, L., & Meyer, T. (2019). Artificial Intelligence and Big Data Analytics in Support of Cyber Defense. In *igi-global.com* (pp. 42–63). https://doi.org/10.4018/978-1-5225-8304-2.ch002

Li, J.-H. (2018). Cyber security meets artificial intelligence: a survey *. *Inform Technol Electron Eng*, *19*(12), 1462–1474. https://doi.org/10.1631/FITEE.1800573

Lun, Y. Z., D'Innocenzo, A., Malavolta, I., & Di Benedetto, M. D. (2016). Cyber-Physical Systems Security: a Systematic Mapping Study. *Journal of Systems and Software*, *149*, 174–216. https://doi.org/10.1016/j.jss.2018.12.006

Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, *13*(12), 2017. https://doi.org/10.1177/1550147717741463

Mallik, A., Ahsan, A., Shahadat, M. M. Z., & Tsou, J. C. (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*, *3*(2), 77–92. https://doi.org/10.5267/j.ijdns.2019.1.001

Mallikarjunan, K. N., Muthupriya, K., & Shalinie, S. M. (2016). A survey of distributed denial of service attack. *Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO 2016*, 1–6. https://doi.org/10.1109/ISCO.2016.7727096

Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Review: machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, *10*(10), 2823–2836. https://doi.org/10.1007/s13042-018-00906-1

Mora, O. B., Rivera, R., Larios, V. M., Beltran-Ramirez, J. R., Maciel, R., & Ochoa, A. (2019, February 28). A Use Case in Cybersecurity based in Blockchain to deal with the security and privacy of citizens and Smart Cities Cyberinfrastructures. *2018 IEEE International Smart Cities Conference, ISC2 2018*. https://doi.org/10.1109/ISC2.2018.8656694

Natarajan, J. (2019). Cyber secure man-in-the- middle attack intrusion detection using machine learning algorithms. In *AI and Big Data's Potential for Disruptive Innovation* (pp. 291–316). https://doi.org/10.4018/978-1-5225-9687-5.ch011

Panimalar, A., Pai, G., & Khan, S. (2018). Artificial intelligence techniques for cyber security. *International Research Journal of Engineering and Technology*, *5*(3), 122–124.

Papastergiou, S., Mouratidis, H., & Kalogeraki, E. M. (2019). Cyber security incident handling, warning and response system for the european critical information infrastructures (cyberSANE). *Communications in Computer and Information Science*, *1000*, 476–487. https://doi.org/10.1007/978-3-030-20257-6_41

Parizi, R. M., Dehghantanha, A., Azmoodeh, A., & Choo, K. K. R. (2020). Blockchain in cybersecurity realm: An overview. In *Advances in Information Security* (Vol. 79, pp. 1–5). Springer. https://doi.org/10.1007/978-3-030-38181-3_1

Pingle, B., Mairaj, A., & Javaid, A. Y. (2018). Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use. *IEEE International Conference on Electro Information Technology*, *2018-May*, 192–197. https://doi.org/10.1109/EIT.2018.8500082

Purkait, S. (2012). Phishing counter measures and their effectiveness - Literature review. In *Information Management and Computer Security* (Vol. 20, Issue 5, pp. 382–420). Emerald Group Publishing Limited. https://doi.org/10.1108/09685221211286548

Qinxia, H., Nazir, S., Li, M., Ullah Khan, H., Lianlian, W., & Ahmad, S. (2021). AI-Enabled Sensing and Decision-Making for IoT Systems. In *Complexity* (Vol. 2021). https://doi.org/10.1155/2021/6616279

Sabar, N. R., Yi, X., & Song, A. (2018). A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security. *IEEE Access*, *6*, 10421–10431. https://doi.org/10.1109/ACCESS.2018.2801792

Sani, A. S., Yuan, D., Jin, J., Gao, L., Yu, S., & Dong, Z. Y. (2019). Cyber security framework for Internet of Things-based Energy Internet. *Future Generation Computer Systems*, *93*, 849–859. https://doi.org/10.1016/j.future.2018.01.029

Sarker, I. H., Colman, A., & Han, J. (2019). RecencyMiner: mining recency-based personalized behavior from contextual smartphone data. *Journal of Big Data*, *6*(1). https://doi.org/10.1186/s40537-019-0211-6

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, *7*(1), 1–29. https://doi.org/10.1186/s40537-020-00318-5

Scarfò, A. (2017). The Cyber Security Challenges in the IoT Era. In *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks* (pp. 53–76). Elsevier. https://doi.org/10.1016/B978-0-12-811373-8.00003-3

Schiavone, F., Appio, F. P., Mora, L., & Risitano, M. (2020). The strategic, organizational, and entrepreneurial evolution of smart cities. *International Entrepreneurship and Management Journal*, *16*(4), 1155–1165. https://doi.org/10.1007/s11365-020-00696-5

Serrano, O., Dandurand, L., & Brown, S. (2014). On the design of a cyber security data sharing system. *Proceedings of the ACM Conference on Computer and Communications Security*, *2014-Novem*(November), 61–69. https://doi.org/10.1145/2663876.2663882

Tang, Y., & Chen, S. (2007). An automated signature-based approach against polymorphic internet worms. *IEEE Transactions on Parallel and Distributed Systems*, *18*(7), 879–892. https://doi.org/10.1109/TPDS.2007.1050

Thomas, J. E. (2018). Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *International Journal of Business and Management*, *13*(6), 1. https://doi.org/10.5539/ijbm.v13n6p1

Thomas, T., P. Vijayaraghavan, A., Emmanuel, S., Thomas, T., P. Vijayaraghavan, A., & Emmanuel, S. (2020). Machine Learning and Cybersecurity. In *Machine Learning Approaches in Cyber Security Analytics* (pp. 37–47). Springer Singapore. https://doi.org/10.1007/978-981-15-1706-8_3

Usman, M., Jan, M. A., He, X., & Chen, J. (2019). A survey on representation learning efforts in cybersecurity domain. In *ACM Computing Surveys* (Vol. 52, Issue 6, pp. 1–28). Association for Computing Machinery. https://doi.org/10.1145/3331174

Vyamajala, S., Mohd, T. K., & Javaid, A. (2018). A Real-World Implementation of SQL Injection Attack Using Open Source Tools for Enhanced Cybersecurity Learning. *IEEE International Conference on Electro Information Technology*, *2018-May*, 198–202. https://doi.org/10.1109/EIT.2018.8500136

Wang, L., An, H., & Chang, Z. (2020). Security Enhancement on a Lightweight Authentication Scheme with Anonymity Fog Computing Architecture. *IEEE Access*, *8*, 97267–97278. https://doi.org/10.1109/ACCESS.2020.2996264

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access*, *6*, 35365–35381. https://doi.org/10.1109/ACCESS.2018.2836950

Yao, M., Sohul, M., Marojevic, V., & Reed, J. H. (2019). Artificial Intelligence Defined 5G Radio Access Networks. *IEEE Communications Magazine*, *57*(3), 14–20. https://doi.org/10.1109/MCOM.2019.1800629

Ye, Y., Li, T., Adjeroh, D., & Iyengar, S. S. (2017). A survey on malware detection using data mining techniques. *ACM Computing Surveys*, *50*(3). https://doi.org/10.1145/3073559

You, X., Zhang, C., Tan, X., Jin, S., & Wu, H. (2019). AI for 5G: research directions and paradigms. In *Science China Information Sciences* (Vol. 62, Issue 2). Science in China Press. https://doi.org/10.1007/s11432-018-9596-5

Yu, W., Zhang, N., Fu, X., & Zhao, W. (2010). Self-disciplinary worms and countermeasures: Modeling and analysis. *IEEE Transactions on Parallel and Distributed Systems*, *21*(10), 1501–1514. https://doi.org/10.1109/TPDS.2009.161

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access*, *8*, 23817–23837. https://doi.org/10.1109/ACCESS.2020.2968045

Zhao, S., Leftwich, K., Owens, M., Magrone, F., Schonemann, J., Anderson, B., & Medhi, D. (2014). I-CaN-MaMa: Integrated campus network monitoring and management. *IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World*. https://doi.org/10.1109/NOMS.2014.6838304

Zhuang, P., Zamir, T., & Liang, H. (2021). Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey. *IEEE Transactions on Industrial Informatics*, *17*(1), 3–19. https://doi.org/10.1109/TII.2020.2998479

bm security report, https://www.ibm.com/security/data-breach. Accessed on 20 Oct 2019.

Garnett, H. A., & James, T. S. (2020). Cyber Elections in the Digital Age: Threats and opportunities of technology for electoral integrity. Election Law Journal: Rules, Politics, and Policy, 19(2), 111-126.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 107094.

Europol: Attacks On Critical Infrastructures (2020). https://www.europol.europa.eu/iocta/2015/attacks-on-ci.html. Accessed 10 July 2020

Libor, D. (2017). Concerning measures for a high common level of security of network and information systems across EU (Doctoral dissertation, Тернопіль, ТНЕУ).

سرمد، بازرگان و حجازی، الهه، ۱۳۸۷، روشهای تحقیق در علوم رفتاری .تهران: آگاه.