

تحلیل تهدیدهای بهره‌برداری از اینترنت رفتارها در سازمان‌های امنیتی

رضا طوسی^۱، مجید اصغرزاده^۲

چکیده

اینترنت رفتارها IoB، مهم‌ترین جریان تکنولوژی استراتژیک در سال ۲۰۲۱ می‌باشد و فناوری است که فعالیت‌های افراد را بصورت دیجیتالی ردیابی کرده و از نتیجه آن برای اثرگذاری بر رفتارها، تغییر یا اصلاح آن استفاده می‌کند این فناوری، به تجزیه و تحلیل داده‌های رفتاری که از اینترنت اشیا و منابع دیگر جمع‌آوری شده و سپس تلاش برای استفاده مؤثر از آن، اشاره می‌کند. این داده‌ها از طریق فناوری‌های پوشیدنی، فعالیت‌های آنلاین فردی، و سایل برقی خانگی جمع‌آوری می‌شوند که می‌توانند اطلاعات ارزشمندی در مورد رفتار و علاقه کاربران ارائه دهند. همچنین فناوری اینترنت رفتارها دارای ابعاد گسترده امنیتی است و دولت‌ها و سازمان‌های اطلاعاتی تلاش می‌کنند از این حوزه جهت گردآوری اطلاعات و داده‌های گسترده از شهروندان و رهبران کشور هدف استفاده کنند تا بعد از تجزیه و تحلیل و کسب شناخت دقیق، روندها و رویدادها را درک کنند و آن‌ها را در مسیر دلخواه خود قرار دهند. هدف پژوهش، احصاء و تحلیل تهدیدهای مترتب بر استفاده از اینترنت رفتارها در سازمان‌های امنیتی است. جامعه آماری تحقیق شامل صاحب‌نظران حوزه فناوری اطلاعات و ارتباطات و بخش‌های عملیاتی سازمان‌های امنیتی با حجم ۶۵ نفر است و با استفاده از پرسش‌نامه محقق ساخته ۱۰ سؤالی در طیف لیکرت، برای هر سؤال فرعی پرسش در نظر گرفته شده است. روایی پرسش‌نامه بر مبنای نظرخواهی از صاحب‌نظران و اعتبار آن نیز از طریق آلفای کرونباخ (۰.۸۷) صورت گرفته است. نتیجه پژوهش حاکی از آن است که به‌کارگیری فناوری اینترنت رفتارها به‌عنوان یکی از فناوری‌های نوین، در سازمان‌های امنیتی با تهدیدها و چالش‌هایی مواجه است که در صورت عدم توجه به رفع آنها، کارآمدی، برتری و اشراف اطلاعاتی، بهره‌وری، توان امنیتی و عملیاتی در سامانه‌های امنیتی و اطلاعاتی را تحت تأثیر قرار خواهد داد.

کلیدواژه‌ها: /اینترنت رفتارها، /اینترنت اشیا، تحلیل تهدید، سازمان‌های امنیتی، روان‌شناسی رفتاری

۱- کارشناسی ارشد پدافند غیر عامل (امنیت ملی)- نویسنده مسئول r1356.tousi1356@gmail.com

۲- استادیار روان‌شناسی تربیتی و عضو هیئت علمی دانشکده فارابی masgharzadeh22@gmail.com

مقدمه

اینترنت رفتارها با استفاده از نوآوری‌ها و پیشرفت‌های نوظهور فن آوری از جمله الگوریتم‌های یادگیری ماشین، به ثبت، تجزیه و تحلیل، درک و پاسخ به انواع رفتارهای انسانی کمک می‌کند به گونه‌ای که امکان پیگیری و تفسیر رفتار افراد را فراهم می‌کند ضمن اینکه این فناوری توصیفی و پیشگیرانه است به این معنی که در تجزیه و تحلیل رفتار کاربر و تشخیص تأثیر متغیرهای روان‌شناختی جهت تحقق نتیجه خاص کمک می‌کند ضمن اینکه بر انتخاب کاربران نیز تأثیر می‌گذارد و شرکت‌ها و سازمان‌ها را قادر می‌سازد تا با تجزیه و تحلیل تجربه کاربران محصولات و خدمات خود را بهبود بخشند در واقع بهبود کارایی و کیفیت محصول یا خدمت هدف اصلی اینترنت رفتارها است. در این راستا اینترنت رفتارها را می‌توان ترکیبی از سه حوزه فناوری، تجزیه و تحلیل داده‌ها، و علوم رفتاری در نظر گرفت و در ادامه علوم رفتاری را به چهار حوزه تصمیمات، احساسات، پیشرفت و رقابت تقسیم نمود. (ترابی، ۱۴۰۰)

اینترنت اشیا ارتباط متقابل بین دستگاه‌هاست که به ایجاد طیف گسترده‌ای از منابع داده جدید منجر می‌شود. این داده‌ها ممکن است فقط به شما به عنوان مشتری اختصاص داشته باشند، برای مثال داده‌هایی که از طریق اپلیکیشن شرکتی ارائه کرده‌اید. اما شرکت‌ها بیشتر اطلاعات غیراختصاصی مشتریان را از طریق «اشتراک‌گذاری» دستگاه‌های متصل به اینترنت جمع‌آوری می‌کنند. یک دستگاه، برای مثال تلفن هوشمند می‌تواند فعالیت‌های آنلاین و همچنین مکان جغرافیایی شما را در دنیای واقعی دنبال کند. برای شرکت‌ها برقراری ارتباط بین تلفن هوشمند با لپ‌تاپ، دستیار صوتی خانگی، دوربین‌های منزل یا خودرو و حتی سوابق تلفن هوشمندتان (پیام‌ها و تماس‌های تلفنی) دشوار نیست. شرکت‌ها با این کار می‌توانند اطلاعات بسیار بیشتری در مورد شما (چیزهایی که دوست دارید یا ندارید، گرایش‌هایتان در رأی‌دادن و نحوه خرید شما) کسب کنند. (مرکز ملی فضای مجازی، ۱۳۹۹).

فناوری‌های جدید به علت ماهیت جذاب و نوآورانه خود بدون توجه به تهدیدهای آشکار و پنهان این فضا، مورد پذیرش عمومی قرار خواهد گرفت. این پذیرش عمومی و گسترده موجب بروز چالش‌های هویتی، فرهنگی، سیاسی و اقتصادی خواهد شد و احتمال بروز چالش‌های امنیتی را در پی خواهد داشت. در عصر سایبر با درهم‌تنیده شدن گستره زندگی و تکنولوژی‌های غیربومی تهدیدهای نوینی متوجه سازمان‌ها به‌ویژه سازمان‌های امنیتی و در نهایت امنیت ملی خواهد شد. از آنجایی که این تکنولوژی‌ها عموماً بومی نبوده و متعلق به کشورهای متخاصم و یا هم‌پیمانان آنها است، چالش‌هایی را متوجه سازمان‌های امنیتی و امنیت ملی خواهد کرد. (قهرودی و همکاران، ۱۳۹۴: ۸۳).

اینترنت رفتار یک پایگاه داده بزرگ بالقوه برای مجرمان سایبری است که می‌توانند از آن بهره ببرند. حقایق انحصاری در مورد مشتریان نیز در صورت قرارگرفتن در آغوش کاربران غیراخلاقی می‌تواند به خطر بیفتد. باین‌حال، بسیاری از آژانس‌ها و مشاغل همگی شروع به رسیدگی به این موضوع کرده‌اند. پروتکل‌های جدید امنیت سایبری نیز ممکن است وارد سبک زندگی شوند که استفاده از فناوری اینترنت رفتار را ایمن‌تر می‌کند. نگرانی‌های حریم خصوصی یکی دیگر از دغدغه‌های اینترنت رفتارها است، زمانی که آژانس‌ها، اطلاعات زیادی در مورد روحیات مشتریان، رفتار، علاقه‌مندی‌ها و ناپسندی‌های مشتریان خود جمع‌آوری می‌کنند، مشتریان این حق را دارند که از حقوق حفظ حریم خصوصی خود استفاده کنند. (وبگاه <http://lavancom.com>، ۱۴۰۰)

برای پیاده‌سازی و به‌کارگیری این فناوری در سازمان‌های امنیتی، چالش‌های فراوانی پیشروی آن قرار دارد که یکی از مهم‌ترین این چالش‌ها، چالش‌های امنیتی و روان‌شناختی خواهد بود که نیاز است تهدیدات و چالش‌های باید به تفصیل مورد بررسی قرار گیرند. در واقع مسئله اصلی پژوهش حاضر بدیع ناشناخته بودن مولفه‌ای بنام اینترنت رفتارها در سازمان‌های اطلاعاتی و وجود تهدیدهایی که با معرفی، و تبیین ادبیات نظری می‌توان تهدیدهای های آن در راستای فعالیت‌های اطلاعاتی و عملیاتی در سازمان‌های امنیتی به‌دقت شناسایی و معرفی گردد. باتوجه‌به روند بی‌سابقه ورود و نفوذ سرسام‌آور فناوری‌های نوین در امور شخصی و سازمانی و وجود تهدیدها و چالش‌های متعدد این فناوری‌ها بنا به دلایل مختلف از قبیل غیربومی بودن سخت‌افزاری و نرم‌افزاری آنها، نداشتن دانش و فرهنگ استفاده صحیح و.... بنابراین هدف از پژوهش حاضر پیرامون تهدیدهای فناوری موصوف، شناسایی چالش‌ها و تهدیدهای پیش روی آن و کمک به حفظ و ارتقای امنیت کاربران و جامعه هدف بوده و تضمین استمرار موفقیت سازمان‌های امنیتی - اطلاعاتی و جلوگیری از پیشامدهای ناگهانی و غافلگیرانه از طریق انتخاب راهبردهای مناسب در برابر بروز و ظهور فناوری‌های نوین از طریق مقابله با تهدیدات آنها موردنظر است.

پیشینه پژوهش

ردیف	عنوان تحقیق	نتیجه تحقیق
۱	فرست ها و تهدیدات امنیتی اینترنت رفتار، ماهنامه برآورد، سال نهم، شماره ۱۰۳ مهر ۱۴۰۰	اینترنت رفتارها بدون تردید دارای مزایای گسترده‌ای برای افراد، شرکت‌ها و دولت‌ها است که مهم‌ترین آنها آسان‌تر کردن مدیریت زندگی در سطح فردی، مدیریت کسب‌وکار توسط شرکت‌ها و مدیریت جامعه توسط دولت‌ها است. در این راستا این امکان در دسترسی کشورها و دستگاه‌های اطلاعاتی قرار گرفته تا از طریق اینترنت و هوش مصنوعی بازیگر هدف خود را عمیقاً شناخته و بر آن تأثیرات جدی بگذارد.
۲	کمک به سنجش رفتار طرفدار محیط‌زیست توسط اینترنت اشیا. دانشکده Qianhu، دانشگاه Nanchang، anchang PR China، 330031	این مقاله رویکردهای فعلی اندازه‌گیری رفتار را بررسی کرده، مزایا و معایب اندازه‌گیری رفتار را با داده‌های اینترنت اشیا در مقابل رفتار سنتی مقایسه می‌کند،
۳	اینترنت رفتار (IOB) و سیستم‌های هوش مصنوعی قابل توضیح برای تأثیرگذاری بر رفتار اینترنت اشیا Haya Elayan, Moayad Aloqaily, Member, IEEE, and Mohsen Guizani, Fellow, IEEE (15 sep 2021)	برای ردیابی، کنترل و تأثیرگذاری بر رفتار افراد برای کسب منفعت. امروزه استفاده از اینترنت اشیا (IoT)، رایانش ابری و هوش مصنوعی (AI) ردیابی و تغییر رفتار کاربران را از طریق تغییر رفتار از طریق اینترنت اشیا آسان‌تر کرده است. این مقاله مفهوم اینترنت رفتار (IOB) و ادغام آن با تکنیک‌های هوش مصنوعی قابل توضیح (XAI) را برای ارائه تجربه قابل اعتماد و مشهود در فرایند تغییر و بهبود رفتار کاربران، معرفی و بحث می‌کند.
۴	اینترنت رفتارها پژوهشکده فضای مجازی گزارش شماره ۴۷ دی ماه ۱۳۹۹	مقوله IOB هنوز در مراحل اولیه قرار دارد؛ ولی از آنجایی که داده‌ها و تحلیل‌های بیشتری در دسترس قرار می‌گیرد (گسترش دسترسی به اطلاعات از طریق IoT)، شرکت‌ها باید مطمئن شوند که از هرگونه رفتار یا روند مصرف‌کننده آگاهی دارند. با استفاده از روش‌های مفید مدیریت داده‌ها و معرفی برنامه‌های آموزشی و امنیت سایبری می‌توان شرایط خوبی برای امنیت داده‌ها فراهم کرد.

۵	طراحی سیستم‌های اینترنت رفتارها Mahyar T. Moghaddam University of Southern Denmark	در این مقاله یک چارچوب مفهومی برای طراحی سیستم‌های IoB ارائه شده و مدل مفهومی بر اساس یک مطالعه اکتشافی با ترکیب ارزشیابی تحصیلی با مصاحبه خبرگان طراحی شده است.
۶	اینترنت رفتارها (IoB) و نقش آن در ارائه خدمات به مشتری (Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Shanay Rab, Suman Rajiv ۲۰۲۱)	پیوند دادن انسان‌ها و رایانه‌ها برای تجزیه و تحلیل رفتار به یک نقطه عطف نیاز دارد. IoB از داده‌های رفتاری استفاده می‌کند و سپس پتانسیل آن را ارزیابی می‌کند. شرکت‌ها روش‌های مختلفی را برای توسعه تکنیک‌هایی برای تولید و فروش کالا برای مصرف‌کنندگان تحلیل، آزمایش و اعمال کرده‌اند. داده‌ها می‌توانند مبنای رشد، بازاریابی و استراتژی‌های فروش را برای کسب و کارها فراهم کنند.
۷	کتاب روان‌شناسی تحلیل اطلاعات نوشته مجید اصغرزاده انتشارات دیده‌بان سال ۱۳۹۸	در این مجلد به مباحثی نظیر روان‌شناسی شناختی (اعصاب‌شناسی روان‌شناسی تغییر ذهن و...) - احساس و ادراک (معز و ساختارهای آن - ادراک - شکل‌گیری برداشت - سندهای علمی و...) - متغیرهای مداخله‌گر در تحلیل اطلاعات - سازوکارهای ذهن (ساختارهای و فرایندهای ذهنی) - شخصیت، هیجان و پردازش اطلاعات - کارورزی و تربیت تحلیل‌گران اطلاعاتی پرداخته شده است.
۸	تهدیدات و فرصت‌های به‌کارگیری اینترنت اشیا در یک سامانه امنیتی (پایان‌نامه - ابراهیم نصیری اردلی - ۱۴۰۰)	نگارنده ضمن بررسی تهدیدات و فرصت‌های به‌کارگیری اینترنت اشیا در یک سامانه امنیتی به راه‌های برون‌رفت از چالش‌های این فناوری پرداخته است.

مبانی نظری:

اینترنت:

اینترنت یکی از بزرگ‌ترین اختراعات قرن اخیر است که در روند ارتباطی بشر تأثیر شگرفی گذاشته و دنیای بشری را به طور کامل متحول نموده است. در واقع اینترنت یکی از بهترین راه‌های برقراری ارتباط با سایرین است. (اکبری، ۱۴۰۱؛ وبگاه ivsi.ir)

اینترنت اشیا:

اینترنت اشیا یک شبکه گول پیکر از اشیا متصل است که شامل افراد نیز می شود. اینترنت اشیا رابطه بین مردم - مردم، مردم - اشیا و اشیا با اشیا خواهد بود. (مورگان، ۲۰۱۴: ۶۶)

اشیا در این تکنولوژی به هر دستگاهی که دارای سنسور جهت تبادل اطلاعات است خطاب می شود، سنسورهای دما، ترافیک، تشخیص حرکت و تشخیص گازها نمونه ای از سنسورهایی است که به عنوان شیء در اینترنت اشیا بکار گرفته می شوند، تمامی این سنسورها اطلاعاتی را به دستگاه مقصد می فرستند تا بر اساس این اطلاعات تصمیماتی اتخاذ کنند. بزرگ ترین فایده اینترنت اشیا این است که به ما امکان می دهد تا با دنیای آنالوگ پیرامون خود (ماشین ها، مردم، حیوانات، گیاهان، و چیزهای دیگر) به زبان دیجیتال با تمام فواید ارتباطات دیجیتال سخن بگوییم. (ازبک زایی، ۱۳۹۵)

به صورت خلاصه "اینترنت اشیا" فناوری مدرنی است که در آن برای هر موجودی (انسان، حیوان و یا اشیا) قابلیت ارسال داده از طریق شبکه های ارتباطی، اعم از اینترنت یا اینترنت، فراهم می گردد. فرایند ارسال داده ها در فناوری اینترنت اشیا بدین ترتیب است که به سوژه مورد نظر یک شناسه یکتا و یک پروتکل اینترنتی (IP) تعلق می گیرد که داده های لازم را برای پایگاه داده مربوطه ارسال می کند. داده هایی که توسط ابزارهای مختلف از قبیل گوشی های تلفن همراه و انواع رایانه ها و تبلت ها قابل مشاهده خواهند بود. (نصیری، ۱۴۰۰)

اینترنت اشیا ایجاد اتصال میان هر دستگاه و وسیله ای (حتی موجودات زنده) با اینترنت (با یکدیگر) است. (تائبی، ۱۳۹۵: ۵)

توانایی های اینترنت اشیا:

۱. **اشیای بی جان و جاندار به یکدیگر متصل می شوند:** هر چیزی که بتوان یک حسگر را به آن متصل کرده و آنرا به اینترنت متصل کند و بتواند به یک اکوسیستم جدید وصل شود این دامنه گسترش یافته حتی ارگانیزم های زنده از قبیل گیاهان، حیوانات، مزرعه و انسان ها را نیز در بر می گیرد.

۲. **از حسگرها برای جمع آوری داده ها استفاده می کند:** در اینترنت اشیا حسگرها به یکدیگر و سیستم ها متصل می شوند و به درک اطلاعات می پردازند یا اطلاعاتی را که خوراک داده ای

حسگرهای دیگر است تولید می‌کند و شرکت‌ها و افراد از اطلاعات تولید شده توسط این حسگرها استفاده می‌کنند.

۳. قسمتی از شبکه IP را تغییر می‌دهد که ارتباط برقرار کند: اینترنت اشیا اطلاعاتی در باره وضعیت خود، محیط اطراف، مردم، سیستم‌های نرم‌افزاری و ماشین‌ها را در اختیار ما قرار می‌دهد. زمان و حجم ارسال این اطلاعات قابل کنترل است و تمام این وسایل یک هویت دیجیتال خواهند داشت و همانند یک انسان قادر به شناسایی شدن هستند (تائی، ۱۳۹۵).

فرایند ارسال داده‌ها در فناوری اینترنت اشیا بدین ترتیب است که به سوژه موردنظر یک شناسه یکتا و یک پروتکل اینترنتی تعلق می‌گیرد که داده‌های لازم را برای پایگاه داده مربوطه ارسال می‌کند. داده‌هایی که توسط ابزارهای مختلف از قبیل گوشی‌های تلفن همراه و انواع رایانه‌ها و تبلت‌ها قابل مشاهده خواهند بود. فرایند ارسال داده‌ها در فناوری اینترنت اشیا نیازی به تعامل «انسان با انسان» یا «انسان با رایانه» نخواهد داشت و داده‌ها به صورت اتوماتیک و بر اساس تنظیمات انجام شده و در زمان‌های مشخص (معمولاً به صورت دائم و لحظه‌ای) ارسال می‌گردند. (اسکندری، ۱۳۹۲)

در حال حاضر کاربردهای فناوری‌های مختلف اینترنت / وب و اینترنت اشیا مانند وب ۲، وب ۳، جهان هوشمند، محاسبات سبز و ... به ادغام جهان اجتماعی، فیزیکی و مجازی سرعت می‌بخشد. می‌توان پیش بینی کرد که جهان سایبری تشکیل شده از کامپیوترها، با جهان اجتماعی تشکیل شده از افراد و جهان فیزیکی متشکل از اشیا در آینده تلفیق خواهد شد. به بیان دیگر ابرجهان ۱ از IoT^3/WoT^2 تشکیل شده است و تأثیر عمیقی بر زندگی و کار افراد ایجاد می‌کند. اینترنت اشیا به ما فرصت‌ها و چالش‌های جدیدی ارائه می‌دهد و اگر این فناوری درست به کار برده شود، برای کار و زندگی آینده تحولی عظیم و نو به وجود خواهد آورد. (همان)

^۱ Hyper world

^۲ Web of trust

^۳ Internet of things

ویژگی‌های تکنولوژی اینترنت اشیا:

باتوجه به آنچه که در قسمت قبل ذکر شد، طبیعتاً در ارزیابی مسائل و چالش‌های اخلاقی مربوط به تکنولوژی اینترنت اشیا می‌بایست ویژگی‌های خاص آن را مدنظر قرار داد. براین اساس، برخی محققان به ویژگی‌ها و خصلت‌هایی از اینترنت اشیا اشاره می‌کنند که ممکن است مسبب مسائل اخلاقی باشد:

۱- **حضور همه‌جایی** [Ubiquity, omnipresence]: IOT همیشه و همه جا در اشیا پیرامونی وجود دارد. به تعبیر بهتر کاربر به وسیله آن بلعیده خواهد شد.

۲- **کوچک‌سازی، نامرئی‌بودن** [Miniaturization, invisibility]: رایانه‌ها ناپدید و ابزارها کوچک‌تر و کوچک‌تر خواهند شد. بنابراین، از هرگونه بازرسی، ممیزی، کنترل کیفیت و رویه‌های حسابرسی دوری می‌کنند.

۳- **ابهام** [Ambiguity]: تمایز میان اُبژه‌های [آنچه مشاهده می‌گردد] طبیعی، مصنوعات و موجودات دشوارتر خواهد شد که پیامد جابجایی از یک مقوله به مقوله دیگر است که با ابتناء بر برچسب‌ها، طراحی پیشرفته و جذب در شبکه‌های جدید مصنوعات صورت می‌پذیرد و در این صورت مسائل جدی درباره هویت و مرزهای سیستم پدیدار خواهد شد.

۴- **شناسایی دشوار** [Difficult identification]: پس از اتصال به IOT، اشیا هویت خواهند داشت. دسترسی به ارتش اشیا و مدیریت این هویت‌ها ممکن است منافع زیادی را ایجاد کند و در نتیجه مسائل جدی امنیتی و کنترلی به وجود آورد.

۵- **ارتباط فزاینده** [Ultra-connectivity]: ارتباطات به تعداد زیاد افزایش پیدا می‌کند و به مقیاس‌های بی‌سابقه‌ای از اشیا و افراد می‌رسد. در نتیجه، مقدار داده‌ها و محصولات جابه‌جاشده به میزان قابل توجهی افزایش پیدا خواهد کرد (Big Data) و آن‌ها می‌توانند به صورت مخربی مورد استفاده قرار گیرند.

۶- **رفتار خودمختار و غیرقابل پیش‌بینی** [Autonomous and unpredictable behavior]: اشیا متصل به اینترنت ممکن است به‌طور هوشمند و خودانگیخته در وقایع انسانی دخالت کنند. مردم به همراه اشیا بخشی از محیط‌های IOT خواهند بود، بنابراین، سیستم‌های ترکیبی با رفتار غیرمنتظره خلق می‌شود.

۷- **هوش ترکیبی** [Incorporated intelligence]: اشیاء به عنوان جانشینانی برای حیات اجتماعی دیده می‌شوند. آن‌ها امتداد ذهن و بدن انسانی خواهند بود. محرومیت از این ابزارها منجر به مشکلاتی خواهد شد.

۸- **کنترل دشوار** [Difficult control]: کنترل و حکمرانی IOT تنها با تعداد زیادی از هاب‌ها، سوئیچ‌ها و داده‌ها امکان‌پذیر نخواهد بود. بلکه به دلیل اینکه جریان اطلاعات آسان شده و انتقال‌ها سریع‌تر، ارزان‌تر، و بسیار گسترده‌تر می‌باشد، کنترل آن به ویژه در سطح حکومتی بسیار دشوار خواهد بود.

۹- **هوش تعبیه‌شده و ذهن گسترش‌یافته** [Embedded intelligence and extended mind]: اشیای دینامیک و هوشمند، با رفتارهای جدید، به عنوان ابزارهای گسترش ذهن و بدن انسان به حساب می‌آیند.

۱۰- **بیگ دیتا** [Big Data]: IOT محدوده‌ای از تولید، ذخیره‌سازی و جریان پردازش فوق‌العاده‌ای در سطح اگزایبیت و فراتر از آن است.

۱۱- **غیرقابل پیش‌بینی بودن و عدم قطعیت** [Unpredictability and uncertainty]: توسعه IOT منجر به رفتارهای نوظهور خواهد شد بدون اینکه کاربر دارای دانش لازم کار با محیط IOT باشد. (همان)

تهدیدهای اینترنت اشیاء برای سامانه‌های نظامی و امنیتی:

تهدیدهایی که در سامانه‌های نظامی و امنیتی اینترنت اشیاء وجود دارند واقعاً گسترده و قابل توجه هستند. در این بخش سعی می‌شود تعدادی از آنها عنوان شود. (بهشتی آتشگاه و همکاران، ۱۳۹۷: ۷۲)

۱. پراکندگی و گسترده‌گی گره‌ها

در اینترنت اشیاء گره‌ها و خوشه‌ها از نظر فیزیکی می‌توانند از یکدیگر بسیار دور باشند. نقطه مقابل شبکه‌های حسگر بی‌سیم که گره‌ها باید در یک شعاع مشخص فعالیت می‌کنند. این ویژگی به گره‌های اینترنت اشیاء این امکان را می‌دهند که در مناطق هدف، بدون هیچ‌گونه محدودیت ارتباطی فعالیت کنند. همچنین تراکم آنها نیز می‌تواند بسیار زیاد باشد. در مأموریت‌های نظامی و امنیتی غالباً اندازه گره‌ها به

شکلی طراحی می‌شوند که بسیار کوچک و نامحسوس باشند از این رو می‌توان تعداد قابل توجهی از این گره‌ها را در فضای موردنظر استفاده کرد بدون آنکه برای دشمن جلب توجه کنند. (همان).

2. نامتجانسی و ناهمگنی

ناهمگونی و نامتجانسی گره‌های اینترنت اشیا غالباً ارتباطات و شبکه‌های اینترنت اشیا را دچار مشکل می‌کند. لایه‌های مختلف اینترنت اشیا از پروتکل‌های ارتباطی و ساختار داده‌های متناسب با منابع موجود در گره‌های لایه موردنظر تنظیم و انتخاب می‌شوند. این گوناگونی تکنولوژی‌ها اقدامات امنیتی متفاوتی را طلب می‌کنند. از این رو طراحی یک سیستم امنیتی یکپارچه چالش برانگیز خواهد بود. اجرای فرایندهای تعامل پذیری نیز به زمان‌های تأخیر افزوده می‌کند که در سامانه‌های فوق حساس تهدید قابل توجهی محسوب می‌شود. از این رو پیشنهاد می‌شود که حتی الامکان از تکنولوژی‌های ارتباطی و ساختار داده‌ای همگون استفاده شود. (همان).

۳. زیر ساخت و تجهیزات غیربومی

متأسفانه، این تهدید از جمله مهم‌ترین عواملی است که برای راه‌اندازی سامانه‌های نظامی و امنیتی اینترنت اشیا ایجاد مشکل می‌کند. این نوع تجهیزات بسیار مستعد درهای پستی هستند. پروتکل‌های ارتباطی، تجهیزات شبکه‌ای و سرویس‌های رایانش ابری مناسب و بومی برای اینترنت اشیا توسط نهادهای داخلی تولید نشده‌اند. از طرف دیگر استفاده از زیرساخت‌ها و تجهیزات غیربومی مشکلات و فرایند تأمین امنیت و محرمانگی را که پیش‌تر عنوان کردیم را دوچندان می‌کنند. در نهایت می‌توان نتیجه گرفت قدم اول در طراحی این شبکه‌ها تشکیل تیم‌های تحقیق و توسعه در جهت تأمین تجهیزات موردنیاز است. (همان)

۴. شناسایی و الگویابی دشوار

در شرایط فعلی می‌توان بیان کرد که تعداد قابل توجهی از هم‌وطنان عزیزمان مصادیقی از اینترنت اشیا را در محل زندگی یا کار خود استفاده می‌کنند. متأسفانه شرکت‌های داخلی در تأمین و عرضه این تجهیزات نقش بسیار کم‌رنگی دارند و تقریباً تمامی آنها به شکل وارداتی و بدون هیچ‌گونه نظارتی وارد شده‌اند. در حال حاضر تمامی آنها وارد پهنای باند شبکه‌ای کشور قرار دارند و یا از آن اطلاعات دریافت یا وارد آن می‌کنند. تمامی این تجهیزات می‌توانند مستعد درهای پستی باشند؛ بنابراین در زمان‌های

مقتضی می‌توانند ایجاد مشکل و ترافیک مضر کنند. حال آنکه با شرایط عنوان شده نظارت، شناسایی و الگوبابی حملات و فعالیت‌های آنها تقریباً غیرممکن است. (بهشتی آتشگاه و همکاران، ۱۳۹۷: ۷۲)

۵. هزینه عملیاتی پایین و انعطاف‌پذیری

شبکه اینترنت اشیا بسیار منعطف و با زیرساخت حداقلی قابل راه‌اندازی است. راه‌اندازی این نوع شبکه‌ها وابسته به تعداد مشخصی گره یا زیرساخت ندارد. می‌توان به آنها قابلیت تحرک و جابه‌جایی داد و با پشتیبانی از پروتکل‌های مختلف و ابعاد کوچک، قدرت اجرایی فراوانی را ارائه می‌دهد. در چنین حالتی دشمن و افراد متخاصم می‌توانند به راحتی آنها را در محیط تعبیه کنند تا مأموریت‌های خود شامل جمع-آوری اطلاعات یا انجام حملات را انجام دهند. حتی در صورت شناسایی و یا نابودی آنها هیچ هزینه قابل توجهی متوجه آنها نخواهد بود. این ویژگی در کنار قابلیت گسترش و پراکندگی باعث می‌شود اینترنت اشیا به عنوان یک تکنولوژی مناسب برای مأموریت‌های آفندی نظامی و امنیتی محسوب شود. (همان)

۶. پروتکل‌های ارتباطی ناامن

در اینترنت اشیا از پروتکل‌های ارتباطی مختلفی استفاده می‌شود. این پروتکل‌ها غالباً در دودسته رنج کوتاه و بلند مورد استفاده قرار می‌گیرند. پروتکل‌های رنج کوتاه مانند زیگبی، بلوتوث، Z-Wave و غیره هستند و پروتکل‌های رنج بلند شامل پروتکل‌هایی نظیر لورا، سیگفاکس، سلولار، RF و غیره هستند. همان‌طور که مشاهده می‌شود این پروتکل‌ها و پشته‌های آنها توسط توسعه‌دهندگان خارجی عرضه و پشتیبانی می‌شود. یکی از مهم‌ترین اصل‌ها در شبکه‌های اینترنت اشیا داشتن کانال‌ها و لینک‌های ارتباطی امن است. در این حالت با توجه به اینکه سیاست‌های انتقال، اقدامات محرمانگی و امنیت، باند فرکانسی و کانال‌های ارتباطی توسط آنها تعیین می‌شود، حفظ امنیت دشوار به نظر می‌رسد. (همان)

۷. حملات دست جمعی

تجهیزات اینترنت اشیا به خودی خود توانمند به نظر نمی‌رسند؛ از این رو حساسیتی نسبت به آنها وجود ندارد. معمولاً این دستگاه‌ها با توان پردازشی پایین، مجهز به چند حسگر یا محرک هستند. مانند ساعت-های هوشمند یا تجهیزات اتوماسیون منازل. حال آنکه با کنار هم قرار گرفتن آنها می‌توانند حملات DDoS ترتیب دهند یا اینکه اطلاعات جمعیتی یک محل را برای سیستم مرکزی و کنترل خود ارسال

کنند. حملات گسترده با هویت‌های گوناگون وظیفه کشف و خنثی‌سازی را دشوارتر می‌کند. (بهشتی آتشگاه و همکاران، ۱۳۹۷ : ۷۲)

۸. هدف قراردادن کاربردهای مختلف

اینترنت اشیا در مراکز و کاربردهای مختلف نفوذ پیدا کرده است. از محیط خانه گرفته تا کارخانه‌ها، پالایشگاه‌ها، فروشگاه‌ها، مراکز عمومی و حمل‌ونقلی می‌توانیم شاهد حضور این تجهیزات باشیم. از این رو این دستگاه‌ها دسترسی مناسب و جامعی از سطح اجتماع به دست می‌آورند. از طرفی الگوی مصرفی و رفتاری تمام کاربران تجهیزات فوق نسبت به دیگری متفاوت است و عملاً توسعه و ساخت یک سیستم پویای شناسایی دسترسی و فعالیت‌های غیرمجاز را پیچیده می‌کند. کشور ما مجموعه فرهنگ محور، اقلیم محور، دینی و بر اساس ارزش‌های دیرینه بنا نهاده شده که جمع‌آوری دقیق این اطلاعات و مطالعه مستندات به دشمنان فرصت واردآوردن ضربات به شدت مهلک را فراهم می‌کند. (رضانی و همکاران، ۱۳۹۹ : ۱۹۹).

تهدیدهای به‌کارگیری اینترنت اشیا در سازمان‌های امنیتی:

- ۱) نبود ممیزی مناسب برای انتخاب تجهیزات هوشمند.
- ۲) تنوع و پیچیدگی زیاد مأموریت‌ها و عملیات در فرایندهای اطلاعاتی و عملیاتی.
- ۳) تنوع زیاد ابزار و فناوری‌های نوین و پیشرفته و شگردهای مورد استفاده مجرمان امنیتی.
- ۴) پیچیدگی دانش اطلاعاتی و امنیتی.
- ۵) ترک خدمت برخی از مدیران متخصص و باتجربه از سازمان‌های امنیتی.
- ۶) تأخیر در واگذاری اعتبارات لازم برای اجرای برنامه‌های تجهیز سازمان‌های امنیتی.
- ۷) توجه ناکافی به آموزش کارکنان در برنامه‌های جانشین‌پروری در سازمان‌های امنیتی.
- ۸) ضعف نگرش برخی از مدیران به تجهیزات پیشرفته به‌عنوان یک سرمایه راهبردی در سازمان‌های امنیتی.
- ۹) ضعف نگرش راهبردی نسبت به هوشمندسازی سازمان‌های امنیتی.
- ۱۰) وجود برخی از مدیران محتاط و گریزان از خطر در سازمان‌های امنیتی.
- ۱۱) فقدان برنامه عملیاتی در به‌کارگیری تجهیزات هوشمند و اینترنت اشیا در فرایندها و مأموریت‌های عملیاتی و اطلاعاتی.

۱۲) اراده ناکافی مدیران برای تغییر تجهیزات سنتی فعلی متناسب با شرح وظایف و مأموریت‌های عملیاتی و اطلاعاتی.

۱۳) توجه بیش از حد مسئولان در امر فناوری و اینترنت اشیا به کمیت به جای کیفیت. (لک، ۱۳۹۹)

اینترنت رفتارها

IoB یک مورد استفاده از اینترنت اشیا است که بر تشویق مشتریان برای افزایش نتایج خاص متمرکز است. IoB را می‌توان به عنوان نقطه ملاقات سه رکن [زیر] مشاهده کرد:

(الف) اینترنت اشیا: اطلاعات مشتری مانند مکان، برنامه روزانه، وضعیت سلامتی و غیره را ارائه می‌دهد.

(ب) روان‌شناسی مصرف‌کننده: به بررسی نیروهای محرک پشت رفتارهای افراد می‌پردازد.

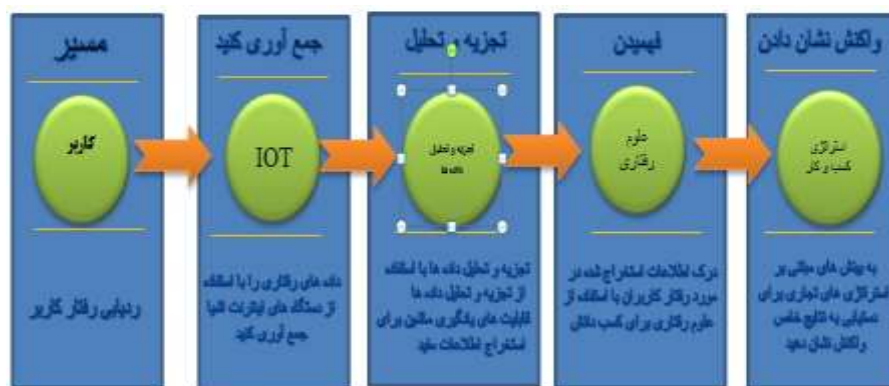
(ج) تجزیه و تحلیل داده‌ها: برای شناسایی الگوهای رفتار و ارائه پیشنهادها، الگوریتم‌ها می‌توانند داده‌های اینترنت اشیا را با مطالعات روان‌شناختی ترکیب کنند. از این سه عامل برای دستیابی به رضایت بلندمدت مشتری و درآمد بالاتر استفاده می‌شود (سینگ و همکاران، ۲۰۲۲: ۱).

اینترنت رفتارها، غبار دیجیتالی زندگی افراد را از منابع مختلف جمع‌آوری می‌کند و سازمان‌های دولتی یا خصوصی می‌توانند از این اطلاعات برای تأثیرگذاری بر رفتار آنها استفاده کنند. (گارتر، ۲۰۲۱).

IoB یکی از برترین گرایش‌های فناوری برای سال ۲۰۲۱ در نظر گرفته شده است. و همه‌گیری COVID-19 عمدتاً مسئول تبدیل شدن IoB به این روند است زیرا نحوه ارتباط مصرف‌کنندگان با برندها را تغییر داده است و باعث شده کسب‌وکارها درباره نحوه ارتباط خود با مشتریان تجدید نظر کنند. (Mohd Javaid ، ۲۰۲۱)

IoB در سه حوزه، دستگاه‌های اینترنت اشیا، تجربه کاربر/جستجو و رفتار عمل می‌کند. این دستگاه‌ها را به اینترنت متصل می‌کند تا رفتار کاربر را ردیابی کند، سپس این رفتار را برای بهبود جستجو و تجربه کاربر تجزیه و تحلیل می‌کند تا بر رفتار آنها برای رسیدن به یک نتیجه خاص تأثیر بگذارد. (سینگ و همکاران، ۲۰۲۲: ۱)

گردشکار اینترنت رفتارها



شکل ۱- گردش کار IoB (العیان و همکاران، ۲۰۲۱)

چالش‌ها و آینده IOB :

۱. امنیت

برخورد با داده‌های حساس و بلادرنگ همیشه نگرانی‌های امنیتی را برای هر کاربر سرویس ایجاد می‌کند. در IoB، لازم است سطح بالایی از امنیت و حفاظت به کاربران نشان داده شود، زیرا انتظار می‌رود داده‌های رفتاری آنها مستعد حملات باشد. حساسیت داده‌ها مجرمان سایبری را برای دسترسی، افشای، جمع‌آوری و بهره‌مندی از آن ترغیب می‌کند.

۲. استفاده اخلاقی

داده‌های رفتاری یک نوع داده حساس و شخصی است و جمع‌آوری، ذخیره یا تجزیه و تحلیل آن باید با شفافیت و استفاده اخلاقی همراه باشد. کاربر این حق را دارد که از این فرایند آگاه باشد و همچنین بداند که حریم خصوصی وی محفوظ است و از سوءاستفاده محافظت می‌شود. یکی دیگر از جنبه‌های استفاده اخلاقی، پیروی نکردن از این اصل است که هدف وسیله را توجیه می‌کند، شرکت‌ها در بیشتر موارد به دنبال سود بیشتر هستند، بدون توجه به تأثیر تغییر رفتار کاربر در زمینه‌های حیاتی مانند سلامت، در نهایت، در چالش‌های اخلاقی، اطمینان از رضایت کاربر هنگام جمع‌آوری و استفاده از داده‌های او برای هر هدفی است.

۳. اثر شترمرغ

اثر شترمرغ پدیده‌ای است که زمانی رخ می‌دهد که ذهن منطقی معتقد باشد چیزی مهم است و ذهن عاطفی انتظار دارد آن را دردناک باشد. مردم قدرت و مزایای استفاده از IoB را درک می‌کنند. با این حال، آنها ممکن است در مورد فرایند ردیابی ناراحت باشند (مشکلات اعتماد) که منجر به اجتناب یا رد آن می‌شود؛ بنابراین، زمانی که شرکت‌ها IoB را پیاده‌سازی می‌کنند، کار بر روی درک فرایند توسط کاربران کافی نیست. آنها همچنین باید برای رفع ناراحتی ناشی از استفاده از این فناوری تلاش کنند.

اینترنت رفتارها (IoB) به دنبال توضیح این است که چگونه داده‌ها به طور مؤثرتری تجزیه و تحلیل و به کار می‌روند تا کالاهای جدید را از نقطه نظر روان‌شناسی انسانی ایجاد و ترویج کنند. سازمان‌ها می‌توانند از IoB به روش‌های مختلفی استفاده کنند، چه عمومی باشند و چه خصوصی که در صورت عدم حفظ چارچوب‌های امنیتی، می‌توانند مورد سوءاستفاده قرار گیرند. اینترنت رفتارها که با نام IoB نیز شناخته می‌شود، مفهومی است که فناوری، روان‌شناسی انسان و بهترین جنبه‌های تحلیل داده‌ها، تحلیل رفتاری و فناوری را ترکیب می‌کند. پلتفرم IoB به کسب‌وکارها ابزارهایی را می‌دهد که برای ایجاد درک کامل از مشتریان خود نیاز دارند. اتصال گجت‌ها به اینترنت اشیاء، نقاط داده جدید (IoT) زیادی تولید می‌کند. هدف IoB مشاهده، تجزیه و تحلیل، درک و واکنش به انواع رفتارهای انسانی است به گونه‌ای که افراد را قادر می‌سازد با استفاده از فناوری در حال تکامل و بهبود الگوریتم‌ها نظارت و درک شوند. (سینگ و همکاران، ۲۰۲۲: ۱).

ویژگی‌های کلیدی IOB

این فناوری نوظهور می‌تواند به طرق مختلف برای شرکت‌ها و سازمان‌ها سودمند باشد. در زیر برخی از ویژگی‌های کلیدی IoB آورده شده است:

۱. بازاریابی مؤثر محصولات

اینترنت اشیاء (IoT) داده‌ها و اطلاعات زیادی تولید می‌کند. هنگامی که این اطلاعات توسط اینترنت رفتارها (IoB) پردازش می‌شود، شناسایی کاربران پلت فرم با تعامل و تجزیه و تحلیل عادات خرید مشتریان آسان می‌شود. این داده‌ها برای پیاده‌سازی استراتژی‌های بازاریابی مؤثر برای مشتریان استفاده می‌شوند و می‌توان تبلیغات هدفمند را به سرعت ارسال کرد.

۲. بهبود تجربه کاربری

شرکت‌ها می‌توانند با استفاده از اطلاعات دقیق جمع‌آوری شده از اینترنت رفتارها (IoB) تجربه استفاده از محصول را برای مشتریان تقویت کنند. این می‌تواند به آنها در بهبود تعامل با مشتری کمک کند.

۳. خدمات بهتر به مشتریان

هرچه مردم از دستگاه‌های اینترنت اشیا بیشتری استفاده کنند، اطلاعات بیشتری در مورد آنها جمع‌آوری می‌شود. نه تنها این داده‌ها می‌توانند به ارائه خدمات بهتر کمک کنند، بلکه می‌توانند به سرعت مشکلاتی را که مشتریان با آن مواجه هستند، را حل کنند. شرکت‌ها با کمک به حل سریع مشکلات فروش، سعی می‌کنند مشتریان خود را راضی نگه دارند.

۴. افزایش ترافیک به وب سایت‌ها

با ظهور اینترنت رفتارها (IoB)، نسخه بهبودیافته سئو، بهینه‌سازی تجربه جستجو (SXO)، برای افزایش ترافیک وب‌سایت و بازاریابی بهتر محصولات و خدمات، توسعه‌یافته است. (۲۰۲۱، wisdomplexus.com).

اهداف و زمینه‌های کاربردی IoB

هدف کلی IoB شامل نظارت، درک و تأثیرگذاری بر رفتارها برای دستیابی به تجارت موردنظر مانند بهبود خدمات مشتری، شخصی‌سازی محصولات و خدمات و در نهایت درآمد و همچنین اهداف اجتماعی است برنامه‌های کاربردی خاص با موارد استفاده از IoB مرتبط هستند این برنامه‌ها شامل برنامه‌های عمومی IoB برای اطمینان از ایمنی (به‌عنوان مثال، سیستم اعتبار اجتماعی دولت چین) و سلامت (انطباق در میان همه‌گیری COVID-۱۹) است و سایر موارد عبارت‌اند از سلامت شخصی، فروش و بازاریابی، تحرک و برنامه‌های بیمه.

جدول ۱ نمونه‌هایی از حوزه‌های کاربردی IoB و اهداف سازمانی آن‌ها

منابع نمونه	اهداف	حوزه کاربردی
(Javaid et al. 2021; Nyman 2012)	درک رفتار مشتری برای تبلیغات هدفمند و توصیه‌های محصول.	بازاریابی دیجیتال و تحقیقات
(Panetta 2019)	ردیابی رفتار راننده برای جلوگیری از رفتار بد رانندگی و پاداش دادن به رفتار خوب رانندگی	تحرک و پویایی
(Javaid et al. 2021; Stary 2021;)	پروتکل‌های بهداشت عمومی، مانند شستن دست‌ها یا پوشیدن ماسک در طول کووید ۱۹ را نظارت و اجرا می‌کند	سلامت عمومی
(Willemssen 2021)	با پیگیری وفاداری به رژیم، نظارت بر امنیت عمومی، اعتبار اجتماعی را ارائه می‌دهد	دولت
(Javaid et al. 2021; Stary 2020)	وضعیت سلامتی را کنترل کنید و اطلاعات لازم مانند برنامه، وضعیت یا نیاز به مداخله پزشکی را به کاربران اطلاع می‌دهد	مراقبت‌های بهداشتی شخصی
(Ganguli 2021)	شناسایی فعالیت‌های مشکوک از طریق موتورهای ریسک برای شناسایی تهدیدها.	امنیت سایبری
(Javaid et al. 2021)	شناسایی و نظارت بر کارمندان برای جلوگیری از غیرمولد بودن و تشویق رفتار مثبت.	روابط محل کار

چالش‌های کلیدی IoB:

۱. **دستکاری برای سود:** بیابید به عنوان مثال به فردی برگردیم که مایل است به رژیم غذایی خود پایبند باشد. اگر این فرد بدن کاملاً سالمی دارد اما توسط یک متخصص مراقبت‌های بهداشتی متقاعد به شروع رژیم غذایی است. به عنوان مثال، می‌توان افراد را متقاعد کرد که در صورت داشتن نگرانی‌های بیش از حد سلامت، برای مراقبت‌های بهداشتی بیشتر هزینه کنند. (سینگ و همکاران، ۲۰۲۲: ۲).

۲. **دستکاری برای کنترل:** احزاب سیاسی یا دولت‌ها می‌توانند از IoB برای تأثیرگذاری بر مردم استفاده کنند. (همان).

۳. **نگرانی‌های مربوط به حریم خصوصی:** به حداکثر رساندن سود ممکن است چالش برانگیز باشد زیرا تجزیه و تحلیل و ذخیره‌سازی کلان داده شامل داده‌های شخصی حساس زیادی است که به

عملکرد بالایی نیاز دارد. علی‌رغم افزایش مقررات استفاده از داده‌های خصوصی، فناوری‌هایی وجود دارند که پردازش داده‌ها را بدون افشای اطلاعات خصوصی امکان‌پذیر می‌سازند.(همان).

۴. قوانین و مقررات: مقررات مطابق با پیشرفت فناوری نبوده است. مشکلات حقوقی هنوز باید برطرف شود. برای مثال، شیوه‌های امنیت داده معمولاً استاندارد نیستند.(همان)

۵. تهدید ناشی از حملات سایبری: با افزایش اتکای ما به فناوری‌های دیجیتال در زندگی روزمره، آسیب‌پذیری ما نیز در برابر آنها افزایش می‌یابد. با وجود رشد ابزارهای امنیت سایبری و حتی بیمه‌ها، مردم همچنان باید این خطرات را در نظر بگیرند.(همان).

۶. متقاعد کردن مردم برای به اشتراک گذاشتن داده‌های خود: برخی از افراد ممکن است مایل نباشند اطلاعات خصوصی خود را فاش کنند. بیابید وضعیت بیمه خودرو را بررسی کنیم. طبق گفته Deloitte، ۴۷٪ از رانندگان نمی‌خواهند اطلاعات رانندگی آنها به اشتراک گذاشته شود. داده‌های رانندگی شامل جزئیاتی مانند سرعت متوسط، میزان ترمز کامل استفاده شده در هر کیلومتر، مسیرهای رانندگی و غیره است (همان).

IoB با چالش جمع‌آوری، ذخیره و استفاده از داده‌ها مواجه است. نظارت بر سطح دسترسی غیرممکن است و بنابراین، همه سازمان‌ها باید به مسئولیت IoB برای استفاده از آن توجه داشته باشند. نرم‌افزاری که در واقع کاربران را از یک برنامه به یک شبکه کامل متصل می‌کند، همچنان توسط گوگل، فیس‌بوک و آمازون بدون مجوز آنها خریداری می‌شود. علاوه بر این، چالش‌های حقوقی و امنیتی قابل توجهی برای آزادی حریم خصوصی وجود دارد که بین حوزه‌های قضایی در سراسر جهان متفاوت است. در آینده، این تجربه مصرف‌کننده را از ابتدا و انتها بررسی خواهد کرد. این باعث می‌شود که علاقه مصرف‌کننده به محصول شروع شود، سفر او برای خرید تا نقطه خرید، و ایجاد نقاط تماس بیشتر برای ایجاد تعامل مثبت با مشتری. همچنین راه‌های جدیدی برای تعامل با مشتریان برای تعامل با برند قبل از خرید کشف خواهد کرد. مفهوم رفتار اینترنتی شامل یک مرور کلی از رفتار کاربر، از جمله دانش در مورد نحوه زندگی آنها در شبکه‌های اجتماعی و رسانه‌های دیگر است. داده‌ها از طریق وب مصرف‌کنندگان عادی، قهوه‌سازها، ترموستات‌ها، سیستم‌های کنترل خانگی، دستگاه‌های پوشیدنی و غیره به دست می‌آیند. برای کسب اطلاعات در مورد تحولات سبک زندگی هر فرد استفاده می‌شود و به نوبه خود

می‌تواند آگاهی از استفاده از چنین مواردی را فراهم کند. کالاها و خدمات. (Mohd Javaid همکاران، ۲۰۲۱)

روان‌شناسی رفتار:

روان‌شناسی

روان‌شناسی از دو واژه مشتق شده است. واژه روان (Psyche) اشاره به ترکیبی منسجم و سازمان‌یافته از شناخت‌ها احساسات و رفتارها دارد و واژه (Logy) به شناخت این اجزا و درک سازمان و تعاملات موجود بین آنها اشاره دارد. موضوع مورد مطالعه در این علم رفتار است رفتار به هر نوع عکس‌العمل موجود زنده در برابر محرک‌های درونی و بیرونی اطلاق می‌شود رفتار دارای جنبه‌های درونی و بیرونی است (اصغرزاده، ۱۳۹۸: ۵).

روان‌شناسی تغییر ذهن

یکی از زمینه‌های جذاب در روابط فردی و جمعی مقوله تغییر ذهن است چگونه افراد انسانی در روابط شخصی و اجتماعی خود بر دیگران تأثیر می‌گذارند و اساس آن تحول ذهنی و فکری چگونه پدید می‌آید این موضوعی است که نظر دانشمندان علوم‌شناختی را به خود جلب کرده و به طراحی راهکارهایی برای تغییر ذهن خود و دیگران انجام می‌دهد است. (همان).

روان‌شناسی تحلیل اطلاعات و رسانه‌های گروهی

یکی از حوزه‌های کاربردی متأثر از یافته‌های علوم‌شناختی روان‌شناسی تحلیل اطلاعات و رسانه‌های گروهی است روان‌شناسی شناختی در درک خطاهای شناختی که منجر به تصمیمات نادرست می‌گردد و نیز طراحی بهترین شیوه تأثیرگذاری بر افکار عمومی به این حوزه کمک‌های مهمی می‌رساند دستگاه‌های اطلاعاتی یکی از کاربران یافته‌های علوم‌شناختی برای تحلیل اطلاعات هستند رسانه‌های گروهی نیز برای جذب افکار عمومی و تأثیرگذاری بر آن از اصول روان‌شناسی شناختی بهره می‌برند (اصغرزاده، ۱۳۹۸: ۱۳).

روان‌شناسی شناختی و تحلیل اطلاعات در حوزه اطلاعاتی - امنیتی

حوزه اطلاعاتی - امنیتی با حجم وسیعی از داده‌ها که به طور عمده نیز از ابهام برخوردار هستند

بیشتر با فرایندهای ذهنی تحلیلگر هدایت می شود این حوزه با دو نوع عدم قطعیت ذاتی و عمدی دسته‌بندی‌گریبان است از سوی داده‌های تحلیلی آن قدر پیچیدگی ظریفی دارند که خود برای تحلیل گرد چالش تولید می کنند و از طرفی بازیگران آن به طور عمدی در داده‌ها دخل و تصرف کرده و به نوعی داده‌ها را در لفافه می پیچند که خود یک موضوع پیچیده‌ای را ایجاد می کند در چنین وضعیتی است که عامل سوم و مهم ترین عامل تحت عنوان ذهنیت تحلیل گر وارد عمل شده و در کنار این دو موضوع عدم قطعیت ذاتی و عمدی کار تحلیل را به سمت وسوی دشواری هدایت می کند. (اصغرزاده، ۱۳۹۸: ۲۱-۲۲).

سازمان‌های اطلاعاتی - امنیتی (حفاظتی):

سازمان‌های امنیتی در حال ورود به شرایطی هستند که نیروی محرکه آن فناوری، انرژی آن اطلاعات، هدایت کننده آن دانش و مجری آن کارکنان سازمان‌های امنیتی است نیاز اطلاعاتی سازمان‌های امنیتی موجب پیدایش دانش‌ها و نوآوری‌های متعدد در عرصه‌ها و مشاغل متنوع حفاظت اطلاعاتی شده است. در این میان سازمان‌هایی موفق هستند که به کمک ابزارهای مدیریتی و فناوری‌های نوین از فرصت‌های ایجاد شده به نفع خود استفاده کنند (عباسی، بهنود، ۱۳۹۵: ۵).

سازمان‌های اطلاعاتی با تمام سازوکارهای خود در انجام وظایف و مأموریت‌هایشان نیاز به اطلاعات دارند و تلاش می نمایند تا در حوزه قلمرو فعالیت خود اشراف اطلاعاتی داشته باشند به تعبیری هرگونه اقدام و بررسی مستلزم اطلاع از موضوع و سوژه موردنظر بوده و میزان موفقیت هر تشکیلات اطلاعاتی بستگی به آگاهی و اشراف بر محیط و اهداف اطلاعاتی داشته و برای همین منظور یکی از ارکان این سازمان‌ها سیستم جمع‌آوری اخبار و اطلاعات است که با روش‌ها و منابع مختلف و متعدد نقش مؤثری در ایجاد اشراف اطلاعاتی ایفا می نمایند. (جمشیدیان، ۱۳۸۸: ۶).

اطلاعات :

یکی از مهم ترین ستون‌های قدرت ملی و امنیت اطلاعات است اطلاعات هم روند است و هم محصول. هنگامی که جمع‌آوری می شود یک روند است و هنگامی که مورد استفاده قرار می گیرد یک محصول است. (آستانا - نیرمال، ۱۳۹۵: ۲۵).

نقش اطلاعات در تصمیم :

بدون شک هیچ تصمیمی نمی‌تواند در مورد دستیابی به هدف‌های از پیش تعیین شده کاملاً عقلایی و رضایت‌بخش باشد مگر اینکه فرد اطلاعات دقیق و منابع نیروی انسانی متخصص تکنولوژی و امکانات مالی را در دسترس است و همچنین اطلاعات کامل درباره هر یک از گناه‌های بالقوه خود برای هریک از هدف‌ها داشته باشد؛ بنابراین در نظام‌های سیاسی معمولاً اخبار و وقایع حقایق و آمار و ارقام موردنیاز با استفاده از مجموعه‌ای از روش‌های مرتبط به هم به صورت منظم جمع‌آوری می‌گردد که پس از پرورش اخبار و تبدیل آنها به اطلاعات قابل استفاده در اختیار تصمیم‌گیرندگان خط‌مشی و سیاستمداران قرار می‌گیرند تا در تصمیم‌گیری‌ها و اقدامات اجرایی مورد استفاده واقع شود پس سیاستمداران برای اتخاذ یک تصمیم مناسب و رضایت‌بخش باید توان تدارک و تجهیز حقایق و وقایع اطلاعات و داده‌های مفید و به هنگام را به شکل قابل استفاده در برنامه‌ریزی‌ها و تصمیم‌گیری‌ها داشته باشند (بهشتی زاده، ۱۳۹۲: ۱۸)

ضرورت تغییر در سازمان‌های امنیتی

دو دلیل عمده وجود دارد که ضرورت تغییر در سازمان‌های امنیتی را ایجاب می‌کند ۱- نیاز به تغییرات درونی برای تطبیق با رخداد‌های ایجاد شده در خارج از سازمان ۲- علاقه به پیش بینی توسعه در آینده و یافتن راه‌های تطبیق با آن (ادوارد جی اپل، ۲۰۱۱)

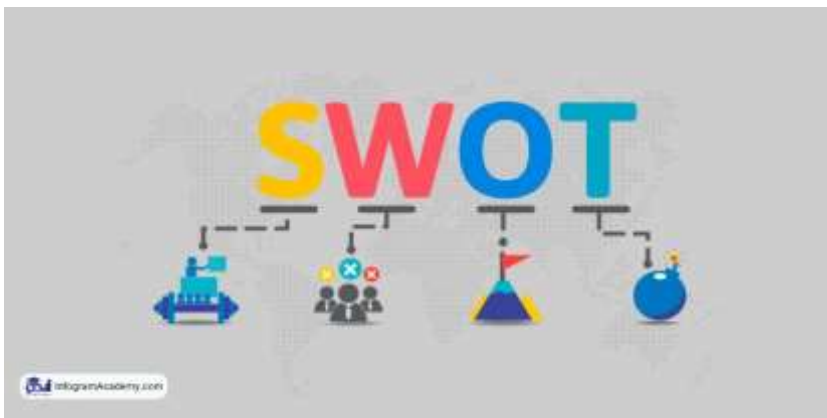
نقش فناوری در مدیریت تغییر

فناوری پیشرفته اطلاعاتی در مدیریت تغییر، مدیران را قادر می‌سازد تا با سازمان، محیط و یکدیگر ارتباط بیشتر و بهتری برقرار نمایند. (همان).

عامل تعیین‌کننده روش کار اطلاعاتی، نوآوری‌های متکی بر فناوری است و از طرفی استفاده از فناوری‌های نوین ناگزیر به نظر می‌رسد؛ چون این فناوری‌ها و نهاد عوامل انسانی، کلید پیشرفت در زمینه حل مشکلات امنیتی تلقی می‌شوند. (مارک فیتین، ۱۳۹۳).

انواع سنتی جمع‌آوری اطلاعات (INTs)^۱ هنوز ارزش بسیار زیادی دارند؛ ولی باید طیفی از اهداف دیجیتال ترکیب شوند تا نمایی کلی از تهدیدها و فرصت‌های موجود ارائه نمایند (آرون برانتلی، ۱۳۹۳).

تحلیل SWOT



شکل ۲ تصویر مفهومی سوات

تعریف SWOT

تجزیه و تحلیل SWOT (قوت‌ها، ضعف‌ها، فرصت‌ها، تهدیدها) یک سازمان را قادر می‌سازد تا استراتژی‌های موردنظرش را تدوین و اجرا نماید قوت‌ها و ضعف‌ها حالت درون‌سازمانی دارند و فرصت‌ها و تهدیدها ناشی از تغییرات محیط بیرونی است. تجزیه و تحلیل SWOT نه تنها باید به شناسایی صلاحیت‌های متمایز عمده سازمان منجر شود؛ بلکه باید به شناسایی فرصت‌هایی که سازمان در حال حاضر به خاطر فقدان منابع مناسب قادر به کسب مزیت از آنها نیست نیز منجر شود (خداداد حسینی، ۱۳۸۵)

تحلیل SWOT یکی از ابزارهای برنامه‌ریزی استراتژیک است و روشی تحلیلی برای دسته‌بندی عوامل مهم درونی و بیرونی اثرگذار بر سازمان و راهبردها و آینده‌های ممکن و شناسایی توانایی‌ها، کاستی‌ها، فرصت‌ها و تهدیدها است. (ستاری خواه، ۱۳۹۸)

گام اول در مراحل برنامه‌ریزی استراتژیک تعیین رسالت، اهداف و مأموریت‌های سازمان است و پس از آن می‌توان از طریق تحلیل SWOT که یکی از ابزارهای تدوین استراتژی است، برای سازمان استراتژی طراحی کرد که متناسب با محیط آن باشد. با استفاده از این تحلیل این امکان حاصل می‌شود که اولاً به تجزیه و تحلیل محیط‌های داخلی و خارجی پرداخته و ثانیاً تصمیمات استراتژیکی اتخاذ نمود که قوت‌های سازمان را با فرصت‌های محیطی متوازن سازد. (لاورنس فاین، ۲۰۰۹).

روش‌شناسی پژوهش

پژوهش حاضر به لحاظ هدف، اکتشافی و کاربردی و از نظر ماهیت توصیفی - تحلیلی با رویکرد آمیخته (کمی و کیفی) که با استفاده از روش موردی - زمینه‌ای اقدام به جمع‌آوری اطلاعات از طریق مصاحبه، پرسش‌نامه، اسناد و مدارک، منابع الکترونیکی و وبگاه‌های معتبر علمی به صورت کتابخانه‌ای و میدانی نموده است. هدف پژوهش، احصاء و تحلیل تهدیدهای مترتب بر استفاده از اینترنت رفتارها در سازمان‌های امنیتی است. جامعه آماری تحقیق شامل صاحب‌نظران حوزه فناوری اطلاعات و ارتباطات و بخش‌های عملیاتی سازمان‌های امنیتی با حجم ۶۵ نفر است و با استفاده از پرسش‌نامه محقق ساخته ۱۰ سؤالی در طیف لیکرت، برای هر سؤال فرعی پرسش در نظر گرفته شده است. روایی پرسش‌نامه بر مبنای نظرخواهی از صاحب‌نظران و اعتبار آن نیز از طریق آلفای کرونباخ (۰.893) صورت گرفته است.

یافته‌های پژوهش

نتایج تجزیه و تحلیل سؤالات پژوهشی نشان داد پرسش‌شوندگان معتقدند ۹۳٫۸ درصد تهدیدهای فناوری اینترنت رفتارها، در قالب سوالات مطرح شده در حد خیلی زیاد و زیاد بر استفاده از فناوری اینترنت رفتارها در سازمان‌های امنیتی به درستی شناسایی شده است. و به کارگیری فناوری اینترنت رفتارها به عنوان یکی از فناوری‌های نوین، در سازمان‌های امنیتی با تهدیدها و چالش‌هایی مواجه است که در صورت عدم توجه به رفع آنها، کارآمدی، برتری و اشراف اطلاعاتی، بهره‌وری، توان امنیتی و عملیاتی در سامانه‌های امنیتی و اطلاعاتی را تحت تأثیر قرار خواهد داد.

آمار توصیفی گویه‌های پرسش‌نامه:

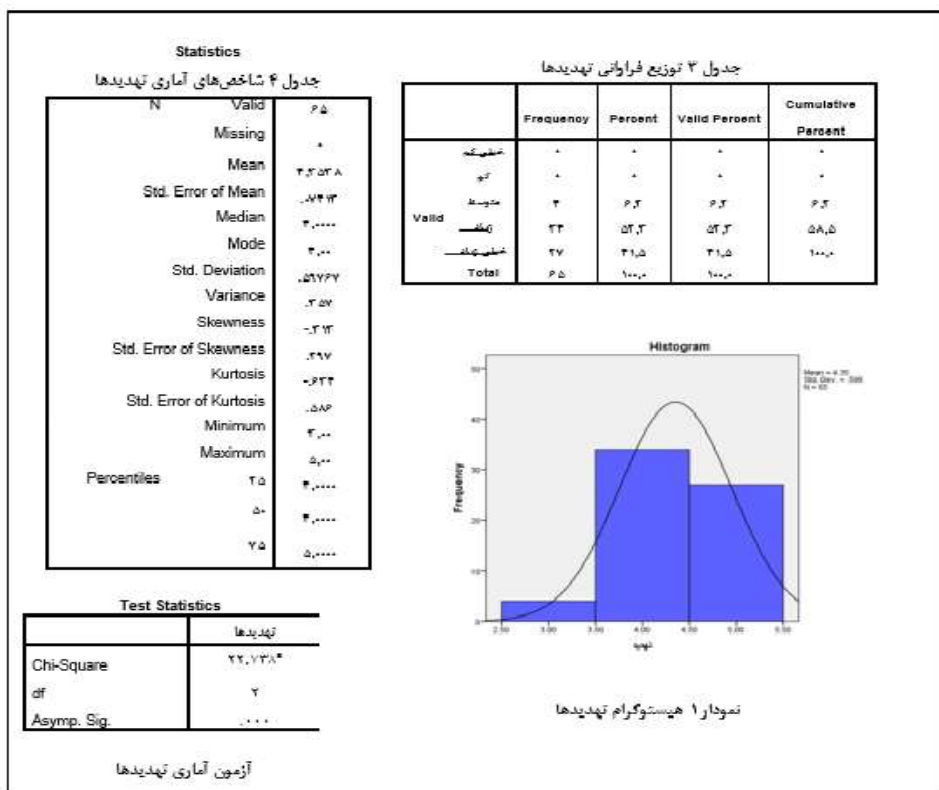
بر اساس نظرسنجی انجام شده، درصد انتخاب هر گزینه از سوی پاسخگویان در جدول ۲ درج شده است، بیشترین توافق در هر سؤال رنگی شده است.

ردیف	شرح گویه	گزینه مورد نظر				
		کاملاً موافقم	موافقم	معتدلاً موافقم	معتدلاً مخالفم	کاملاً مخالفم
۱	سرویس‌های اطلاعاتی حریف به چه میزان می‌توانند از طریق فناوری اینترنت رفتارها به کارکنان جامعه حفاظت شونده تقرب نمایند؟	۰	۰	۱۲,۳	۳۳,۸	۵۳,۸
۲	تا چه میزان امکان هک و نقوذ به تجهیزات فناوری اینترنت رفتارهای مورد بهره‌برداری سازمان‌های اطلاعاتی و امنیتی امکان‌پذیر و محتمل است؟	۱,۵	۳,۱	۱۲,۳	۳۵,۴	۴۷,۷
۳	تا چه میزان امکان پیاده‌سازی ستاره‌های فریب توسط حریف بر علیه سازمان‌های اطلاعاتی و از طریق فناوری اینترنت رفتارها امکان‌پذیر و محتمل است؟	۰	۳,۱	۱۵,۴	۴۳,۱	۳۸,۵
۴	تا چه میزان احتمال نقض امنیت فیزیکی (حوزه‌های پیشگیری) از طریق کنترل تردد‌ها توسط سرویس حریف یا گروه‌ها برای سازمان‌های اطلاعاتی و امنیتی با استفاده از فناوری اینترنت رفتارها می‌تواند تهدید را باشد؟	۰	۴,۶	۱۵,۴	۴۴,۶	۳۵,۴
۵	تا چه میزان احتمال سرقت اطلاعات جمع‌آوری و ذخیره شده در بانک‌های اطلاعاتی سازمان‌های اطلاعاتی و امنیتی با استفاده از فناوری اینترنت رفتارها توسط سرویس‌های حریف و گروه‌های معاند امکان‌پذیر است؟	۳,۱	۹,۲	۱۸,۵	۳۰,۸	۳۸,۵
۶	تا چه میزان وابسته بودن فناوری اینترنت رفتارها از نظر علمی و تجهیزاتی به خارج از کشور می‌تواند برای سازمان‌های اطلاعاتی و امنیتی تهدید را باشد؟	۰	۱,۵	۱۲,۳	۳۲,۳	۵۳,۸
۷	تا چه میزان جانشینی و نصب نام‌صحیح تجهیزات اینترنت رفتارها می‌تواند برای سازمان‌های اطلاعاتی و امنیتی تهدید آفرین باشد؟	۰	۳,۱	۱۶,۹	۳۳,۸	۴۶,۲
۸	تا چه میزان فناوری اینترنت رفتارها می‌تواند زمینه‌ساز مقاصد مرتبط با عدم رعایت صیانت شرعی و حریم خصوصی، برای کارکنان سازمان‌های اطلاعاتی و امنیتی تهدید آفرین باشد؟	۳,۱	۱۲,۳	۲۷,۷	۳۰,۸	۲۶,۲
۹	تا چه میزان فناوری اینترنت رفتارها می‌تواند زمینه‌ساز اقدامات تروریستی علیه کارکنان نخبه و فرماندهان رده‌های بالایی نیروهای مسلح را فراهم آورد؟	۰	۶,۲	۷,۷	۳۰,۸	۵۵,۴
۱۰	تا چه میزان امکان افشای هویت و ماهیت رفتاری کارکنان و خانواده‌های آنها از طریق فناوری اینترنت رفتارها برای سرویس‌های اطلاعاتی حریف امکان‌پذیر است؟	۰	۰	۱۳,۸	۲۹,۲	۵۶,۹

تهدیدهای به کارگیری اینترنت رفتارها در سازمان‌های امنیتی

۱ تجزیه و تحلیل توصیفی سؤال‌های مربوط به تهدیدهای بکارگیری اینترنت رفتارها به صورت کلی:

در قسمت پایین نسبت به تجزیه و تحلیل سؤال‌های مربوط به تهدیدهای بکارگیری اینترنت رفتارها پرداخته شده است.



داده‌های جدول ۴ (جدول شاخص‌های آماری) نشان می‌دهد که میانگین، میانه و انحراف استاندارد توزیع به ترتیب ۴,۳۵ و ۴,۰۰ و ۵۹۷/۰ است. توزیع از کجی منفی جزئی برخوردار بوده و در نقطه اوج خود نسبت به توزیع نرمال دارای خوابیدگی است. (نمودار ۱) کمینه و بیشینه نمرات بعد از محاسبه متغیرهای سوالات مربوط به تهدیدها و گرد کردن نیز بین ۳ تا ۵ در نوسان است. توزیع مربوط به فراوانی (جدول ۳) نیز نشان می‌دهد که ۹۳,۸ درصد پاسخ‌دهندگان در حد زیاد و خیلی زیاد نسبت به محتوای سوالات تهدیدها نظر مساعدی دارند. داده‌های جدول ۷۳-۴ (آزمون خی‌دو) حاکی از آن است که ارزش خی‌دوی مشاهده شده (۲۲,۷۳۸) با درجه آزادی (۲) از ارزش خی‌دوی بحرانی (۲۱,۷) در سطح $P < 0.00$ بزرگ‌تر است، در نتیجه سؤال‌های مربوط به تهدیدات اینترنت رفتارها با (۲۰,۷۳۸ درصد) با ۹۹ درصد اطمینان تأیید می‌شود.

تجزیه و تحلیل توصیفی سؤال‌های مربوط به تهدیدهای بهره‌گیری از اینترنت رفتارها در سازمان‌های اطلاعاتی و امنیتی به صورت کلی:

تجزیه و تحلیل توصیفی سؤال‌های مربوط به تهدیدهای بهره‌گیری از اینترنت رفتارها در مجموع به شرح زیر است:

Ranks		
ردیف	گویه‌های تهدیدهای به کارگیری اینترنت رفتارها در سازمان‌های اطلاعاتی و امنیتی	Mean Rank
۱	سرویس‌های اطلاعاتی حریف به چه میزان می‌توانند از طریق فناوری اینترنت رفتارها به کارکنان جامعه حفاظت شونده تقرب نمایند؟	6.20
۲	تا چه میزان امکان هک و نفوذ به تجهیزات فناوری اینترنت رفتارهای مورد بهره‌برداری سازمان‌های اطلاعاتی و امنیتی امکان‌پذیر و محتمل است؟	5.74
۳	تا چه میزان امکان پیاده‌سازی سناریوهای فریب توسط حریف بر علیه سازمان‌های اطلاعاتی و امنیتی از طریق فناوری اینترنت رفتارها امکان‌پذیر و محتمل است؟	5.40
۴	تا چه میزان احتمال نقض امنیت فیزیکی (حوزه‌های پیشگیری) از طریق کنترل تردها توسط سرویس حریف یا گروه‌ها برای سازمان‌های اطلاعاتی و امنیتی با استفاده از فناوری اینترنت رفتارها می‌تواند تهدید را باشد؟	5.16

۵	تا چه میزان احتمال سرقت اطلاعات جمع‌آوری و ذخیره شده در بانک‌های اطلاعاتی سازمان‌های اطلاعاتی و امنیتی با استفاده از فناوری اینترنت رفتارها توسط سرویس‌های حریف و گروه‌های معاند امکان‌پذیر است؟	4.78
۶	تا چه میزان وابسته بودن فناوری اینترنت رفتارها از نظر علمی و تجهیزاتی به خارج از کشور می‌تواند برای سازمان‌های اطلاعاتی و امنیتی تهدیدزا باشد؟	6.22
۷	تا چه میزان جانمایی و نصب ناصحیح تجهیزات اینترنت رفتارها می‌تواند برای سازمان‌های اطلاعاتی و امنیتی تهدیدآفرین باشد؟	5.58
۸	تا چه میزان فناوری اینترنت رفتارها می‌تواند زمینه‌ساز مفاسد مرتبط با عدم رعایت صیانت شرعی و حریم خصوصی، برای کارکنان سازمان‌های اطلاعاتی و امنیتی تهدیدآفرین باشد؟	3.70
۹	تا چه میزان فناوری اینترنت رفتارها می‌تواند زمینه‌ساز اقدامات تروریستی علیه کارکنان نخبه و فرماندهان رده‌های بالایی نیروهای مسلح را فراهم آورد؟	5.98
۱۰	تا چه میزان امکان افشای هویت و ماهیت رفتاری کارکنان و خانواده‌های آنها از طریق فناوری اینترنت رفتارها برای سرویس‌های اطلاعاتی حریف امکان‌پذیر است؟	6.24

جدول ۵ تفسیر خروجی پایایی

Case Processing Summary			
		N	%
Cases	Valid	65	100.0
	Excluded ^a	0	.0
	Total	65	100.0
a. Listwise deletion based on all variables in the procedure.			

جدول ۶ آمار قابلیت اطمینان

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.866	.870	10

جدول ۷ رتبه‌بندی سوال‌های مربوط به فرصت‌های بکارگیری اینترنت رفتارها

باتوجه به جدول ۶ میزان آلفای کرونباخ مشاهده شده 0.870 بوده که حدوداً نزدیک به عدد یک بوده و از مقدار 0/7 بزرگ تر است که این عدد نشان می دهد گویه های تهدید های بکارگیری اینترنت رفتارها از اعتبار و پایایی مناسب برخوردار است.

داده های جدول ۷ نشان می دهد که از میان ده تهدید به کارگیری اینترنت رفتارها در سازمان های اطلاعاتی و امنیتی ، امکان افشای هویت و ماهیت رفتاری کارکنان و خانواده های آنها از طریق فناوری اینترنت رفتارها ، (بارزش رتبه ای ۶,۲۴) و احتمال زمینه سازی مفاسد مرتبط با عدم رعایت صیانت شرعی و حریم خصوصی (بارزش رتبه ای ۳,۷۰) به ترتیب از بیشترین و کمترین ارزش رتبه ای برخوردار هستند. سایر ارزش های رتبه ای در جدول قابل مشاهده است.

جدول ۸- آماره آزمون

Test Statistics ^a	
N	65
Chi-Square	۵۹,۷۷۰
df	۹
Asymp. Sig.	.000
a. Friedman Test	

تهدیدهای به کارگیری اینترنت رفتارها در سازمان های امنیتی، شامل تقرب سرویس های اطلاعاتی حریف به کارکنان جامعه حفاظت شونده، امکان هک و نفوذ به تجهیزات فناوری اینترنت رفتارها، پیاده سازی سناریوهای فریب توسط حریف بر علیه سازمان های اطلاعاتی و امنیتی، احتمال نقض امنیت فیزیکی (حوزه های پیشگیری) از طریق کنترل تردها توسط سرویس حریف یا گروهک ها برای سازمان های اطلاعاتی و امنیتی، احتمال سرقت اطلاعات جمع آوری و ذخیره شده در بانک های اطلاعاتی سازمان های اطلاعاتی و امنیتی، وابسته بودن فناوری اینترنت رفتارها از نظر علمی و تجهیزاتی به خارج از کشور، جانمایی و نصب ناصحیح تجهیزات اینترنت رفتارها، زمینه ساز مفاسد مرتبط با عدم رعایت صیانت شرعی و حریم خصوصی، زمینه سازی اقدامات تروریستی علیه کارکنان نخبه و فرماندهان رده های بالایی نیروهای مسلح، افشای هویت و ماهیت رفتاری کارکنان و خانواده های آنها و غیره است.

نتیجه نهایی را می‌توان در جدول ۸ مشاهده کرد با توجه به مقدار χ^2 دو محاسبه شده (۵۹,۷۰) با درجه آزادی ۹ و همچنین سطح معنی‌داری آزمون، مقدار $P.V$ برابر صفر شده است که کمتر از مقدار ($\alpha=0.05$) است. در نتیجه چنین استنباط می‌شود که گویه‌های مربوط به تهدیدهای بهره‌گیری از اینترنت رفتارها با ۹۹ درصد اطمینان تأیید می‌شود.

۲-۳. نتایج و بحث روی نتایج

نتیجه‌گیری ۱ (برگرفته از مبانی نظری):

اینترنت رفتار بدون تردید دارای مزایا و فرصت‌های گسترده‌ای برای افراد، شرکت‌ها، سازمان‌ها و دولت‌ها است که مهم‌ترین آن‌ها آسان‌تر کردن مدیریت زندگی در سطح فردی، مدیریت کسب‌وکار توسط شرکت‌ها و مدیریت جامعه توسط دولت‌ها است. به تعبیری دیگر، اینترنت رفتار با آسان کردن همه کارها در تمامی سطوح و ابعاد زندگی فردی و اجتماعی، عملاً انقلابی بنیادین در جوامع انسانی ایجاد خواهد کرد. با این حال اینترنت رفتار همچون اینترنت بدن و اینترنت اشیاء، دارای پیامدهای امنیتی است. لازم به اشاره است که چالش‌های امنیتی که فناوری اینترنت رفتار با آن روبروست، عمدتاً شبیه مواردی است که به‌طور کلی اینترنت اشیاء نیز با آن مواجه بوده و هست، با این تفاوت که در هنگام درگیر شدن دستگاه‌های اینترنت رفتار با تهدیدات امنیتی، گاهی مسئله مرگ و زندگی و تداوم امنیت ملی مطرح است. علاوه بر این، اطلاعات جمع‌آوری شده از اینترنت رفتار، چالش‌های دیگری در حوزه امنیت سایبری ایجاد می‌کند. یکی از مهم‌ترین این چالش‌ها مسئله حفظ حریم خصوصی است؛ بنابراین باید امنیت اینترنت رفتار به‌گونه‌ای تأمین شود که حریم خصوصی اولین قربانی آن نباشد. در این زمینه سؤالات مهمی پیشروی دولت‌ها، شرکت‌ها و متخصصان است، از جمله اینکه چه کسی و برای چه هدفی می‌تواند به داده‌های بسیار شخصی افراد دسترسی پیدا کند. در این راستا باید اشاره کرد که با ادامه رشد اینترنت به اشکال مختلف، باید مسائل قانونی و سیاست‌های مربوط به استفاده صحیح از این فناوری‌ها، طراحی و مدون شوند.

جدول ۹ تهدیدهای احصاء شده حاصل از مصاحبه با نخبگان

تجمع شده تهدیدهای به کارگیری اینترنت رفتارها در سامانه‌ها امنیتی بر اساس تحقیق و مصاحبه با اندیشمندان:

ردیف	تهدیدها
۱	امکان تقرب سرویس‌های اطلاعاتی حریف به کارکنان جامعه حفاظت شونده از طریق فناوری اینترنت رفتارها
۲	امکان هک و نفوذ به تجهیزات فناوری اینترنت رفتارهای مورد بهره‌برداری سازمان‌های اطلاعاتی و امنیتی
۳	امکان پیاده‌سازی سناریوهای فریب توسط حریف بر علیه سازمان‌های اطلاعاتی و امنیتی از طریق فناوری اینترنت رفتارها
۴	احتمال نقض امنیت فیزیکی (حوزه‌های پیشگیری) از طریق کنترل تردها توسط سرویس حریف یا گروهک‌ها برای سازمان‌های اطلاعاتی و امنیتی با استفاده از فناوری اینترنت رفتارها
۵	احتمال سرقت اطلاعات جمع‌آوری و ذخیره شده در بانک‌های اطلاعاتی سازمان‌های اطلاعاتی و امنیتی با استفاده از فناوری اینترنت رفتارها توسط سرویس‌های حریف و گروه‌های معاند
۶	وابسته بودن فناوری اینترنت رفتارها از نظر علمی و تجهیزاتی به خارج از کشور
۷	جانمایی و نصب ناصحیح تجهیزات اینترنت رفتارها
۸	احتمال زمینه‌سازی مفاسد مرتبط با عدم رعایت صیانت شرعی و حریم خصوصی، برای کارکنان سازمان‌های اطلاعاتی و امنیتی
۹	زمینه‌سازی برای اقدامات تروریستی علیه کارکنان نخبه و فرماندهان رده‌های بالایی نیروهای مسلح توسط سرویس اطلاعاتی حریف با استفاده از بستر اینترنت رفتارها
۱۰	امکان افشای هویت و ماهیت رفتاری کارکنان و خانواده‌های آنها از طریق فناوری اینترنت رفتارها

باتوجه به کمبود منابع نظری پیرامون فناوری اینترنت رفتارها از نظر کتاب، پایان‌نامه، مقاله و... و اینکه عمده مطالب و رویکردهای مبانی نظری و ادبیات تحقیق و تحلیل محتوای مرتبط با موضوع پژوهش در حوزه اقتصادی و بازاریابی تمرکز دارد و موردی از مبانی نظری در حوزه سازمان‌های اطلاعاتی موجود نبود؛ بنابراین پژوهشگر برای استخراج تهدیدهای این فناوری در سازمان‌های امنیتی و اطلاعاتی متوسل به مصاحبه‌های میدانی از اندیشمندان و صاحب‌نظران در این حوزه نموده که تهدیدهای احصاء شده اینترنت رفتارها در سازمان‌های اطلاعاتی و تحلیل آنها در سازمان‌های اطلاعاتی به شرح جدول ۹ است.

نتیجه‌گیری ۲ (برگرفته از مصاحبه با اندیشمندان و صاحب‌نظران):

باتوجه‌به تهدیدهای احصا شده برای اینترنت رفتارها در سطح سازمان‌های امنیتی و اطلاعاتی، چنین نتیجه‌گیری می‌شود به‌منظور مقابله با تهدیدات اشاره شده در سامانه‌های امنیتی و جلوگیری از غافلگیری و پیشگیری از شکست حفاظتی:

۱- می‌توان با ارتقاء بینش اطلاعاتی کارکنان حفاظت شونده نسبت به تهدیدات ناشی از تقرب سرویس‌های اطلاعاتی حریف به از طریق تدوین، برنامه‌ریزی و اجرای دوره‌های آموزشی کاربردی و کارگاهی و تولید محتوا و مدیاهای آموزشی نسبت به کاهش اثرات ناشی از تهدیدات مرتبط با تقرب سرویس‌ها مقابله نمود.

۲- می‌توان از طریق فراهم نمودن بورسیه‌های دانشجویی و اعزام به فرصت مطالعاتی برای ارتقاء سطح دانش فناوری (از نظر وسعت و عمق) کارکنان فنی و عملیاتی سازمان‌های اطلاعاتی و امنیتی کمبودهای ناشی از تهدیدهای سخت‌افزاری و نرم‌افزاری را در سامانه‌های امنیتی به حداقل رساند.

۳- می‌توان با تجهیز سامانه‌ها و شبکه‌های ارتباطی و رایانه‌ای سازمان‌های اطلاعاتی و امنیتی به آنتی‌ویروس و فایروال‌های قدرتمند و بومی برای مقابله با هک و نفوذ و سرقت اطلاعات و اجرای سیاست اعتماد صفر در تعامل با سامانه‌ها و کاربران سازمان‌های اطلاعاتی و امنیتی تهدیدهای ناشی از افشاء و نشت اطلاعات را به حداقل رساند.

۴- دیده بانی مستمر فناوری از طریق مراکز فنی و سایبری سازمان‌های امنیتی از طریق پوشش فناوری و پایش فناوری با جانمایی و نصب صحیح تجهیزات مرتبط با IOB و جمع‌آوری اطلاعات از احتمال نقض امنیت فیزیکی سامانه‌ها سرقت اطلاعات جمع‌آوری شده توسط این سامانه‌ها مقابله خواهد شد.

۵- با توجه به اینکه تجهیزات و فناوری مورد استفاده در اینترنت اشیا و اینترنت رفتارها عمدتاً وارداتی و متعلق به کشورهای متخاصم می‌باشند و امکان جاسازی بد افزارها، درهای پشتی، ذخیره و ارسال اطلاعات به آدرس از پیش تعیین شده (به منظور سرقت اطلاعات)، شناسایی کارکنان نظامی و خانواده آنها از طریق بستر همین فناوری‌ها و تقرب، جلب همکاری، تهدید، تطمیع آنها همگی از تهدیدات متصوره فناوری اینترنت رفتارها برای سازمان‌های امنیتی می‌باشد که نیاز به سرمایه‌گذاری در امر بومی‌سازی زیرساخت‌های نرم‌افزاری و سخت‌افزاری و آموزش کارکنان و خانواده

این سازمان ها پیرامون تهدیدات شناسایی شده را ضروری می نماید.

منابع

- اختری، محمد. (۱۳۹۴)، تجزیه و تحلیل نگرانی های امنیتی در اینترنت اشیا، اولین کنفرانس بین المللی حسابداری و مدیریت در هزاره سوم، رشت، شرکت پیش گامان پژوهش های نوین.
- امیری، عبدالرضا. (۱۳۸۸)، مطالعه فرصت ها و تهدیدات ناشی از ظهور فناوری های نوین اطلاعاتی: گامی به سوی تدوین راهبرد در ناجا، فناوری اطلاعات و پلیس، فصلنامه پژوهش های مدیریت انتظامی، سال چهارم، تهران. ایران.
- اصغرزاده، مجید . (۱۳۹۸) ، روان شناسی تحلیل اطلاعات ، تهران ، انتشارات دیده بان
- آستانه، ان سی. نیرمال، آنجالی . (۱۳۹۵) ، مدیریت اطلاعات و امور امنیتی ، تهران ، پژوهشکده مطالعات کاربردی قلم
- باغبان اورندی، محمود. (۱۳۹۹)، وضعیت فناوری اینترنت اشیا در ایران، معاونت راهبری فنی، مرکز ملی فضای مجازی.
- بهشتی آتشگاه، محمد، برتری، مرتضی. عارف، محمدرضا. بیات، مجید. (۱۳۹۷)، اینترنت اشیا، نظامی: مفهوم و چالش های امنیتی. نهمین کنفرانس ملی فرماندهی و کنترل ایران، تهران، دانشگاه خوارزمی. انجمن علمی فرماندهی و کنترل ایران.
- بهشتی زاده، محمد . (۱۳۹۲)، اصول بررسی اطلاعاتی ، تهران ، انتشارات دانشکده اطلاعات
- حکیم، امین؛ فرشچی، علیرضا. (۱۳۹۱)، کاربرد فناوری های همگرا در شکل دهی به فضای رزم آینده، مرکز مطالعات دفاعی و امنیت ملی سپاه دانشگاه امام حسین (ع). تهران. ایران.
- سیف، علی اکبر، ۱۳۶۶، آموزش به کمک روش های تغییر رفتار ف نشریه رشد معلم ، شماره ۴۰ ، مهر ۱۳۶۶
- رضائی، رسول. موحدی صفت، محمدرضا، (۱۳۹۹). رتبه بندی تهدیدهای اینترنت اشیا در محیط نظامی، فصلنامه علمی امنیت ملی، مقاله هفتم. تهران.
- سخایی، محمدجواد. (۱۳۹۴)، فناوری های اینترنت اشیا برای سال های ۲۰۱۷ و ۲۰۱۸ از نگاه گارتر – فابک (فناوری اطلاعات برای کسب و کار).
- کریمی قهرودی، محمدرضا؛ کیان خواه احسان، (۱۳۹۴)، چالش آفرینی اینترنت اشیا بر ارکان امنیت ملی کشور، فصلنامه امنیت ملی، سال چهارم، شماره ۱۶.

- فناوری‌های اینترنت اشیا برای سال‌های ۲۰۱۷ و ۲۰۱۸ از نگاه گارتنر.
- قیصری، محمد. یزدان نژاد، فاطمه. عرب، سعیدرضا. رضایی، کیاناز. (۱۳۹۸)، استانداردها و چالش‌های اینترنت اشیا، انتشارات علوم رایانه. مرکز تحقیقات اینترنت اشیا ایران.
- ستاری خواه علی. (۱۳۹۸)، آینده پژوهی و سناریو نویسی کاربردی، تهران، قرارگاه پدافند هوایی خاتم الانبیاء(ص) آجا
- مرادیان، محسن. (۱۳۹۸)، مبانی نظری امنیت، تهران، دانشکده علوم و فنون فارابی
- خداداد حسینی، سید حمید. عزیزی، شهریار (۱۳۸۵)، مدیریت و برنامه‌ریزی استراتژیک (رویکردی جامع)، تهران، انتشارات صفار-اشراقی
- نادى، حمیدرضا. خلیلی، ابراهیم. (۱۳۹۱) مدیریت سازمان‌های امنیتی، تهران، دانشکده علوم و فنون فارابی مرکز پژوهش‌های علمی
- Mahyar T. Moghaddam, Henry Muccini, Julie Dugdale, Mikkel Baun Kjærgaard, " Designing Internet of Behaviors Systems" in ICSA 2022 proceedings: International Conference on Software Architecture.
- Haya Elayan, Moayad Aloqaily, Mohsen Guizani, Internet of ehavior (IoB) and Explainable AI Systems for Influencing IoT Behavior, arXiv:2109.07239v1 [cs.DC] 15 Sep 2021
- Christian Stary , The Internet-of-Behavior as Organizational Transformation Space with Choreographic Intelligence , Business Informatics, Johannes Kepler University Linz, Linz, Austria, Springer Nature Switzerland AG 2020 M. Freitag et al. (Eds.): S-BPM ONE 2020, CCIS 1278, pp. 113–132, 2020.
- Jiayi Sun, Wensheng Gan, Han-Chieh Chao, Philip S. Yu, Weiping Ding, Internet of Behaviors: A Survey, arXiv:2211.15588v1 [cs.DB] 28 Nov 2022
- Ossama H. Embarak, " Internet of Behaviour (IoB)-based AI models for personalized smart education systems, Procedia Computer Science 203 (2022) 103–110

- SIDDHARTH SINGH KHATI, SUNIL K SINGH, AKASH SHARMA, " Secure Internet of Behavior (IOB): challenges and future Directions, Cyber Security Insights Magazine, Vol 02, 2022
- Javaid, M., Haleem, A., Singh, R. P., Rab, S., & Suman, R. (2021). Internet of Behaviours (IoB) and its role in customer services. Sensors International, 2, 100122.
- Molla, Alemayehu; Hoang, Giang; and Oshodin, Osemwonyemwen, "Conceptualising the Internet of Behaviours (IoB): A Multi-Level Perspective and Research Agenda" (2021). ACIS 2021 Proceedings. 57.
- Haya Elayan, Moayad Aloqaily, Fakhri Karray, Mohsen Guizani, Internet of Behavior (IoB) and Explainable AI Systems for Influencing IoT Behavior , arXiv:2109.07239v2 [cs.DC] 10 May 2022
- Kidd. Chrissy. What is the Internet of Behavior? IoB Explained. BMC Blogs – BMC Website. December 16, 2019. Available at: <https://www.bmc.com/blogs/iob-internet-of-behavior/>.

سایت

- <http://lavancom.com/portal/magazine/lavan-magazine/smart-life/2277-iob>
- <https://www.farsnews.ir>
- <https://paydarymelli.ir>
- <https://nbic.ir>
- <https://technoway.ir/>
- <https://www.analyticssteps.com>
- <https://itrexgroup.com>
- <https://scholar.google.co.in/citations?user=rfyiwvsAAAAJ&hl=en>
- <https://www.tekkiwebsolutions.com/blog/internet-of-behavior/>

- <https://www.themspsummit.com/news/everything-you-need-know-about-internet-behaviors-iob>
- <https://www.techopedia.com/definition/34552/internet-of-behaviors-iob>
- <https://www.rackspace.com/solve/internet-behavior-what-it>
- <https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021/>