Archive of SID



# نقش زیرساخت‌های هوشمند برای حفاظت از اماکن حساس در مدیریت و برنامه‌ریزی شهری (مطالعه موردی حمله داعش به مجلس)

بهادرپسندیده طالمی[1]
گروه جغرافیا و برنامه ریزی شهری،واحدزاهدان،دانشگاه آزاد اسلامی،زاهدان،ایران
bahadorpasandideh@gmail.com

چکیده
در این مقاله ابتدا به مدیریت شهری و شهرهای آینده پرداخته شده و برخی ویژگی‌های شهرهای آینده بررسی گردیده است. در ادامه برنامه‌ریزی و مدیریت شهری برای آمایش اماکن حساس و امنیتی مورد مطالعه قرار گرفته و برخی مناطق در کشورهای مختلف که در آن‌ها اماکن حساس در مناطقی خاص تجمیع شده بررسی گردیده است. سپس مقاله به نقش فناوری در ایجاد امنیت پرداخته و برخی فناوری‌های ضدتروریسم قابل‌کاربرد در اماکن شهری را ارایه کرده است. در همین زمینه مطالعه‌ای تطبیقی در زمینه کاربرد فناوری‌های هوشمند نظیر اینترنت اشیا و دوربین‌های هوشمند برای ایجاد و تقویت امنیت در شهرهای آینده‌نگر چین انجام شده است. در همین راستا برابر سناریویی فرضی، نقش فناوری‌های هوشمند و زیرساخت‌های آن در حفظ و ارتقای امنیت اماکن حساس شهری نمایش داده شده است. همچنین در مقایسه‌ای موردی به حمله داعش به مجلس شورای اسلامی پرداخته شده و نشان داده شده است که چگونه نبود زیرساخت‌ها و فناوری‌های هوشمند، باعث عدم کشف حمله تروریستی به اماکن حساس گردید. برای این کار مفاهیمی مانند ماتریس هشدار تهدید و علائم و نشانه‌های تهدید نیز تعریف و ارایه شده است. در این مقاله پژوهشگر به دنبال تبیین نقش ورود فناوری‌ها در عرصه مدیریت شهری و به‌منظور افزایش حفاظت و مراقبت از اماکن حساس است و با بررسی اجمالی مواردی مانند شهرهای آینده‌گرای چین و نیز برخی حوادث تروریستی مانند حادثه حمله داعش به مجلس شورای اسلامی، به لزوم توجه مدیریت و برنامه‌ریزی شهری به ایجاد زیرساخت‌های مناسب فناورانه برای حفظ و ارتقای امنیت اماکن حساس می‌پردازد. پژوهشگر در این راه و برای نمایش لزوم ایجاد زیرساخت‌های فناوری‌های نوین و بهره‌گیری از آن‌ها، از دو فناوری اینترنت اشیا و دوربین‌های هوشمند با قابلیت پردازش تصاویر بهره می‌گیرد تا توانایی آن‌ها در ایجاد قابلیت پیش‌بینی و پیشگیری از وقوع حملات تروریستی در اماکن حساس را نشان دهد.
روش تحقیق در این مقاله تحلیلی – استنباطی و از نظر هدف کاربردی بوده و چگونگی جمع‌آوری اطلاعات به صورت اسنادی – کتابخانه‌ای است.

واژگان کلیدی: مدیریت و برنامه‌ریزی شهری، زیرساخت‌های هوشمند، اماکن حساس و اینترنت اشیا (IOT).



www.SID.ir

Archive of SID



مقدمه

جهان با سرعتی باورنکردنی نسبت به گذشته در حال تغییر است اما با این حال آشکارا می‌توان گفت که حتی سرعت این تغییرات هم در مقایسه با تغییراتی که در آینده رخ خواهد داد بسیار ناچیز خواهد بود. بسیاری از تحولات، فناوری‌ها، پیشرفت‌ها و ... در عصر حاضر حاصل همکاری‌ها و هم‌افزایی‌های میان‌رشته‌ای است. به‌طور طبیعی موضوع مدیریت و برنامه‌ریزی شهری نیز مانند تمام رشته‌های علمی دیگر از این قاعده مجزا نیست و با ورود پدیده‌هایی مانند شهرهای هوشمند و آینده‌گرا، این رشته علمی نیز در حال تطابق خود با پدیده هوشمندسازی است. زیرساخت‌های هوشمند، عناصر پاسخگویی تلقی می‌شوند که شرایط و تغییر الگوهای استفاده خود را به‌طور خودکار به کاربرانشان منتقل می‌کنند. از طرفی آمایش و جانمایی اماکن حساس و امنیتی در شهرها مقوله‌ای بسیار جدی و مهم است که در سال‌های اخیر توجهات بسیاری را به خود جلب کرده است. در بسیاری از نقاط جهان اماکن حساس امنیتی و پلیسی دارای انواع روش‌های حفاظتی و مراقبتی هستند که این روش‌ها با توجه به رشد فناوری‌های مختلف، به‌طور روزمره دچار تحول و بهبود می‌گردند.

حملات تروریستی به دلیل ویژگی‌های خاص خود چالش‌های عمده‌ای را پیشِ روی سازمان‌های انتظامی - امنیتی قرار می‌دهند که مقابله با آن‌ها نیز روش‌های خاصی را می‌طلبد. چون بهترین راهبرد در برابر هر تهدید پیش‌بینی و پیشگیری از وقوع آن است در این مقاله پژوهشگر به دنبال ارایه روشی مؤثر در ارایه هشدار در مورد احتمال وقوع یک حمله تروریستی با رویکرد به‌کارگیری نظام علائم و نشانه‌ها در بستر فناوری‌های نوین جمع‌آوری اطلاعات است. یکی از رویکردهای مهم در ایجاد امنیت از طریق اعمال مدیریت و برنامه‌ریزی شهری، استفاده از مفهوم و فناوری اینترنت اشیا (IOT) و دوربین‌های هوشمند است که در این مقاله از آن‌ها به‌عنوان بستری برای پیاده‌سازی مفهوم نقش فناوری و زیرساخت‌های آن در برنامه‌ریزی شهری در ارتقای امنیت اماکن حساس استفاده شده است. این پژوهش پس از بیان مقدمه، طرح مسئله، اهمیت و ضرورت موضوع و طرح هدف‌ها، سوال‌های اصلی و فرعی، در بخش‌های انتهایی تمامی فرآیندهای پیش‌گفته را در یک سناریوی تهدید تروریستی فرضی اِعمال کرده و نتایج را نمایش داده است. در فرجامِ کار نیز پژوهشگر پیشنهادهایی برای فعالیت‌های پژوهشی آینده ارایه کرده است.



www.SID.ir

Archive of SID



بیان مسئله

رشد سریع فناوری در حوزه‌های علمی مختلف بر امور مختلف تأثیر شگرفی گذاشته است. از جمله این امور می‌توان به تأثیر شگرف تکنولوژی بر مدیریت و برنامه‌ریزی شهری اشاره کرد که باعث شده مفهوم شهرهای آینده‌گرا یا شهرهای هوشمند بسیار شایع شود و فکر بسیاری از برنامه‌ریزان، طراحان و مدیران امور شهرسازی، مدیریت و معماری را متوجه خود کند. رشد دانش‌های دیجیتالی از طرفی باعث توسعه فناوری‌هایی شده است که می‌توانند برای حفظ و ارتقای امنیت اماکن حساس و امنیتی به کمک بیایند و به‌طور چشمگیری هزینه‌های مادی و انسانی این کار را کاهش دهند.

در سالیان اخیر اقدام‌های تروریستی متعددی توسط گروهک‌های تروریستی شرق و غرب کشور انجام شده است. بسیاری از این اقدامات در محیط‌های شهری به وقوع پیوست. به‌عنوان مثال تنها گروهک جهاد و توحید در بازه زمانی کمتر از دو سال (۴ اردیبهشت ۱۳۸۸ تا یکم اردیبهشت ۱۳۹۰) اقدام به انجام دست‌کم ۲۵ عملیات تروریستی کرد (پایگاه اطلاع‌رسانی وزارت اطلاعات-۱۳۹۵/۰۵/۱۳). حمله داعش به حرم امام و مجلس شورای اسلامی و عملیات‌های مشابه دیگر آسیب‌پذیری اماکن حساس شهری در برابر اقدامات تروریستی را نشان می‌دهد که ناشی از پیچیدگی، ناهمگونی و تنوع این نوع حملات است. علاوه‌براین حضور شهروندان عادی و مجتمع‌های فرهنگی – اجتماعی، وجود نهادهای دولتی و ... زمینه و شرایط مستعد برای حمله و اقدامات تروریستی گروهک‌ها را فراهم می‌کند. پژوهشگر در این تحقیق به دنبال بررسی این موضوع است که نقش فناوری‌های ضدتروریسم و ضرورت ایجاد زیرساخت‌های لازم برای به‌کارگیری آن‌ها را در مدیریت و برنامه‌ریزی شهری را تبیین نماید.

اهمیت و ضرورت تحقیق

همچنین کشورمان در حال حاضر در مسیر توسعه قرار دارد و بهبود فرآیندها و روش‌هایی که بتواند به باعث ارتقای مدیریت و برنامه‌ریزی شهری گردد بسیار مهم است. از طرفی اقصی نقاط کشورمان شاهد عملیات در شهرها و هراس‌افکنی تروریست‌ها بوده است که باعث می‌گردد فشار بر سازمان‌های پلیسی و امنیتی را افزایش یابد. به همین دلیل لازم است تا از همه راه‌کارهای ممکن برای حفظ و ارتقای امنیت اماکن و به‌ویژه اماکن حساس و مقابله با حملات تروریستی استفاده شود. یکی از این راه‌کارها تبیین و احصای نقش طراحی، آمایش، مدیریت و برنامه‌ریزی شهری در افزایش امنیت اماکن حساس است. اما تاکنون کمتر به نقش این عامل مهم در افزایش امنیت پرداخته شده است. به همین دلیل نیاز به پژوهش‌ها و تحقیقاتی وجود دارد که بتواند به رابطه مستقیم و بسیار مهم مدیریت و برنامه‌ریزی شهری و امنیت اماکن حساس بپردازد. به همین دلیل لازم است تا نقش ایجاد زیرساخت‌های لازم برای استفاده از فناوری‌هایی که می‌توانند برای حفظ و ارتقای امنیت اماکن حساس و مقابله با حملات تروریستی به‌کار روند، در مدیریت و برنامه‌ریزی شهری تبیین گردد.

هدف‌های تحقیق

هدف اصلی

بررسی و تبیین توانش ایجاد و استفاده از زیرساخت‌های هوشمند برای حفاظت از اماکن حساس در مدیریت و برنامه‌ریزی شهری.

هدف فرعی

۱- بررسی و مطالعه تطبیقی نقش مدیریت و برنامه‌ریزی شهری در تأمین و ارتقای امنیت در برخی نقاط جهان.

۲- معرفی توانش (پتانسیل) برخی فناوری‌های نوین قابل‌اجرا در مدیریت و برنامه‌ریزی شهرها برای حفظ و ارتقای امنیت اماکن حساس.

۳- نمایش توانش بسیار زیاد مدیریت و برنامه‌ریزی شهری در کاهش هزینه‌های انسانی و مادی نیروهای پلیسی و امنیتی.



www.SID.ir

فرضیه و سؤال‌های تحقیق

فرضیه تحقیق

فرضیه این تحقیق این است که برنامه‌ریزی و مدیریت شهری آینده‌گرا می‌تواند با ایجاد زیرساخت‌های لازم و به‌کارگیری فناوری‌های نوین، به حفظ و ارتقای چشمگیر امنیت اماکن حساس کمک نماید.

سؤال اصلی

نقش برنامه‌ریزی و مدیریت شهری در حفظ و ارتقای امنیت اماکن حساس چیست؟

سؤال‌های فرعی

۱- آیا مدیریت و برنامه‌ریزی شهری در تأمین و ارتقای امنیت در نقاط دیگر جهان نقش دارد؟

۲- چه فناوری‌هایی وجود دارد که قابلیت اجرا در مدیریت و برنامه‌ریزی شهرها برای حفظ و ارتقای امنیت اماکن حساس را داشته باشند؟

۳- آیا مدیریت و برنامه‌ریزی شهری در کاهش هزینه‌های انسانی و مادی نیروهای پلیسی و امنیتی نقش دارد؟

روش تحقیق

چون هدف این پژوهش نمایش بررسی و تبیین توانش ایجاد و استفاده از زیرساخت‌های هوشمند برای حفاظت از اماکن حساس در مدیریت و برنامه‌ریزی شهری است، بنابراین این تحقیق از نظر هدف کاربردی، و از نظر چگونگی گردآوری اطلاعات، روش اسنادی – کتابخانه‌ای و آینده پژوهی است.

۱- مدیریت شهری و شهرهای آینده

پیش‌بینی شده تا ۱۵ سال آینده بیش از پنج میلیارد نفر از ساکنان زمین ساکن شهرها باشند. بنابراین در چنین شرایطی باید پیش از اینکه در شهرها با چنین جمعیتی روبه‌رو شویم خود را آماده کنیم. در سال های اخیر بیش از ۴۰۰ شهر و شهرک هوشمند در نقاط مختلف در سطح دنیا ساخته شده است و روزبه‌روز به تعداد افرادی که قصد دارند زندگی در شهرهای هوشمند را تجربه کنند افزوده می‌شود. آن‌ها بر این باورند استفاده از فناوری های جدید در حوزه دیجیتال که در زندگی امروز ما جای خود را باز کرده است، می‌تواند نوید بخش زندگی بهتر و آسان‌تر برای بشر باشد. برخلاف آنچه تصور می‌شود ساختمان‌های مرتفع و توسعه زیرساخت های حمل‌ونقل تنها نیاز شهرهای آینده نخواهد بود بلکه بیش از هر چیز در این شهرها به سامانه‌های هوشمند نیاز داریم. بدون تردید با پیشرفت فناوری، روزبه‌روز به فهرست فناوری‌ها و امکاناتی که باید در شهرهای هوشمند فراهم باشد افزوده خواهد شد. اکنون بیش از هر زمان دیگری شاهد توسعه روزافزون فناوری‌های نوین در شهرها هستیم. در چنین شرایطی باید برای زندگی در شهرهای هوشمند آماده شویم. از دیدگاه علمی شهر هوشمند شهری است که در آن از طریق به‌کارگیری هوشمندانه منابع طبیعی و با هدف توسعه اقتصادی پایدار و بهبود کیفیت زندگی، روی منابع انسانی و سرمایه‌های اجتماعی، حمل‌ونقل و ارتباطات بر پایه فناوری اطلاعات و فناوری دیجیتال سرمایه‌گذاری شود. به‌نظر می‌رسد این مفاهیم بیانگر ویژگی‌ها و مشخصات زندگی آینده بشر و به‌عبارتی شهرهای آینده است. پس می‌توان نتیجه‌گیری کرد در آینده بشر زندگی در شهرهای هوشمند را تجربه خواهد کرد. شهرهای هوشمند متناسب با گسترش فناوری های نوین و افزایش تقاضای شهروندان به امکانات جدید طراحی می‌شود و این شهرها پنجره‌ای به‌سوی دنیای جدیدی است که در آن آخرین دستاوردهای حوزه فناوری گردهم آمده اند تا بشر بتواند زندگی باکیفیت‌تر و ساده‌تری را تجربه کند. در این شهرها که براساس زیرساخت‌های زندگی دیجیتال طراحی می‌شود، نیازهای افراد به روشی هوشمندانه و با استفاده از آخرین فناوری‌های روز دنیا



www.SID.ir

Archive of SID



تأمین می‌شود. اگرچه زیرساخت‌های فیزیکی از مهم‌ترین و ضروری‌ترین نیازهای توسعه زندگی شهرنشینی است، اما این روزها شهرها بیش از پیش به فناوری‌های روز دنیا نیاز دارند. از این‌رو مفهوم شهرهای هوشمند به‌عنوان یک ابزار مهم و راهبردی در روند توسعه ضرورت‌های شهرهای آینده موردتوجه قرار گرفته است. محیط زندگی هوشمند، اقتصاد هوشمند، حمل‌ونقل هوشمند، زندگی هوشمند و از همه مهم‌تر شهروندان هوشمند از معیارهای اصلی شهرهای هوشمند آینده است. امروزه چه بخواهیم و چه نخواهیم زندگی ما براساس ادبیاتی از جنس فناورهای نوین تعریف تازه‌ای پیدا کرده است. از دیدگاه بعضی افراد هوشمندی عبارت است از یافتن راهکارهایی برای چالش‌های مختلف در شهرها به کمک حسگرهایی که داده‌هایی را از سطح شهر جمع‌آوری کرده و تجزیه‌وتحلیل می‌کنند.

بعضی شهرها از پایه و اساس به عنوان یک شهر هوشمند بنا می‌شوند که به زیرساخت‌های موردنیاز برای توسعه زندگی شهری هوشمند مجهز شده است. از جمله این زیرساخت‌ها، امکانات لازم برای ایجاد و به‌کارگیری فناوری‌های دیجیتال و نوین و زیرساخت‌های ارتباطی لازم برای استفاده عملی از این فناوری‌ها است. از جمله بسترهای ارتباطی در عصر جدید، اینترنت اشیا، ارتباطات نسل ۵ تلفن همراه و ... است.

۲- مدیریت و برنامه‌ریزی شهری و امنیت

همواره در فرآیند مدیریت و برنامه‌ریزی شهری مقوله امنیت یکی از موضوعات مهم بوده است. در بسیاری از نقاط جهان، برای تأمین امنیت اماکن حساس از رویکرد تجمیع این مناطق در یک منطقه خاص کمک گرفته می‌شود. از دیرباز و از عهد باستان، طراحی بسیاری از شهرهای جهان بر اساس امنیت بوده است. داشتن دیوار، برج و بارو و انواع تمهیدات دیگر در شهرهای قدیم، مؤید نقش همیشگی امنیت در طراحی، برنامه‌ریزی و مدیریت شهری است. با بررسی منابع مرتبط با دوره ساسانی می‌توان چنین نتیجه گرفت که ساختار اصلی شهرهای ساسانی شامل کهندژ، شارستان، شار میانی و بیرونی، بازار و میدان بوده که کهندژ محل استقرار حکومت و فرمانروای شهر بوده است و شارستان که خود به دو قسمت شارستان میانی و شارستان بیرونی تقسیم می‌شد، سکونتگاه دیوانیان، اشراف و سپاهیان بود. مجموعه‌ای است مرکب از کاخ‌ها، آتشگاه اصلی، دیوان‌ها، سربازخانه‌ها، ذخایر، خزاین و انبارهای آذوقه. این دژ در مرکز یا بالاترین نقطه شهر و مهم‌ترین نقطه سوق‌الجیشی ساخته و با دیوارهای سنگین محافظت می‌شد. این دژ در دوره اسلامی به کهندژ یا قهندژ معروف بود [حبیبی، از شار تا شهر، ص ۳۲–۳۳]. این بخش، در مرکز و بهترین نقطه شهر و اغلب در سطحی بالاتر از سایر نقاط جای داشت و توسط دروازه‌ای به خارج راه داشت. کهندژ جایگاه و سکونتگاه پادشاه، حکام و درباریان بود و فضایی دارای سیستمی خودکفا بود و نیازهای ساکنانش را در درون همان فضای محصور تأمین می‌کرد. برای کهندژ، برج و بارو و خندقی جهت حفاظت ساکنانش ساخته می‌شد و آتشکده و فضاهای وابسته به آن نیز، اغلب در همین بخش احداث می‌شد [سلطان‌زاده، معماری و شهرسازی ایران، ص ۶۷]. شارستان سکونتگاه دیوانیان، اشراف و سپاهیان بود و دارای حصار و دیگر استحکامات لازم بود. علاوه بر اسرای جنگی، از نیروی کار صنعتگران و کارگران شهرهای دیگر کشور نیز استفاده می‌کردند و آن‌ها را در شهر جدید جای می‌دادند [تقوی‌نژاد و دیلمی؛ معماری، شهرسازی و شهرنشینی ایران، ص ۱۶۲]. در عصر کنونی نیز موضوع آمایش و جانمایی مناسب اماکن حساس در شهرها وجود دارد. به‌عنوان مثال بسیاری از مناطق حساس امنیتی در بغداد، در منطقه خضرا یا منطقه سبز بغداد قرار گرفته‌اند. همچنین در اراضی اشغالی، بسیاری از نهادهای امنیتی و سازمان‌های حساس اطلاعاتی در منطقه هاکریا در تل‌آویو مجتمع شده‌اند. در کشورمان نیز مناطقی مانند میدان پاستور را می‌توان محل تجمیع بسیاری از اماکن دولتی و حکومتی حساس دانست. پس مشخص می‌گردد که همواره در طراحی و مدیریت شهری، تأمین امنیت اماکن حساس از اولویت بالایی برخوردار بوده و همواره مورد توجه حاکمان، مسئولان و برنامه‌ریزان قرار داشته است. در بسیاری از پژوهش‌ها تاکنون به نقش مهم طراحی و برنامه‌ریزی و المان‌های



www.SID.ir

آن نظیر طراحی خیابان‌ها، چگونگی استفاده از زمین، تراکم ساختمان‌ها و ... در کاهش ریسک مخاطرات امنیتی اشاره شده است [Armitage, 2013]. ماهیت پیچیده و وابستگی متقابل اجزای مختلف شهرهای هوشمند، چالش‌های اجتماعی، سیاسی، فنی و به‌ویژه امنیتی را در آن‌ها به‌وجود خواهد آورد[Ismagilova, E., Hughes, L., Rana, N, 2020].

۳- نقش فناوری در ایجاد امنیت در شهرها

همان‌طور که پیش از این اشاره شد، شهرهای هوشمند وابستگی زیادی به فناوری خواهند داشت و چون امنیت از جنبه‌های بسیار مهم برنامه‌ریزی شهری است، در نتیجه فناوری‌ها در شهرهای هوشمند آینده نقش انکارناپذیری در تأمین امنیت به عهده دارند. هوش مصنوعی، اینترنت اشیا، حسگرهای هوشمند، ارتباطات سلولی نسل ۵ و ۶ و ... از اجزای بسیار مهمی هستند که می‌توانند به حفظ و ارتقای امنیت در شهرهای هوشمند بسیار کمک کنند. به‌عنوان مثال، جمع‌آوری و تجزیه‌وتحلیل گسترده داده‌ها نقش مهمی در مدیریت و برنامه‌ریزی بهتر شهری در شهرهای هوشمند ایفا می‌کند. برنامه‌ریزان و معماران شهری با استفاده از این داده‌ها می‌توانند زیرساخت‌های هوشمند ایجاد کنند و حتی امکان پیشگیری از مسائلی مانند مشکلات امنیتی و تروریستی را بیابند. فناوری‌های ضد تروریسم کنونی نیز ناگزیر از انطباق خود با بستر و شرایط شهرهای آینده هستند.

۳-۱ فناوری‌های ضدتروریسم

فناوری‌های ضد تروریسم مختلفی در حال حاضر در سطح جهان توسعه یافته و به‌کار رفته‌اند. از فناوری بیومتریک گرفته تا پردازش سیگنال‌های ویدئویی، داده‌کاوی و کلان‌داده‌ها، برای کشف، شناسایی و مقابله با تهدیدات تروریستی استفاده می‌شوند. در واقع می‌توان گفت که هم‌اکنون نیز در بسیاری از نقاط جهان این فناوری‌های نوین ضد تروریسم هستند که نقش اصلی را در مقابله با این تهدیدات بر عهده دارند [Al-Abed, 2012]. در ادامه به‌طور نمونه به کاربرد فناوری‌های هوش مصنوعی، تشخیص چهره و دوربین‌های هوشمند در شهرهای آینده‌گرای چین پرداخته می‌شود و نقش این فناوری‌های نوین در حفظ و ارتقای امنیت نشان داده می‌شود.

۳-۲ مطالعه تطبیقی کاربرد فناوری‌های نوین در ایجاد امنیت: شهرهای آینده‌گرای چین

در چین معاون وزیر علوم و فناوری این کشور اعلام کرد که در آینده نزدیک داده‌کاوی مبتنی بر هوش مصنوعی و یادگیری ماشینی به نیروهای پلیس و امنیت این کشور کمک می‌کند تا با دقتی بسیار بیشتر از قبل اقدامات پیشگیرانه در برابر حملات تروریستی را به اجرا بگذارند و بتوانند حملات تروریستی را کشف کنند [Strittmatter, 2018]. همچنین در شهرهایی مانند ژنگژو، نیروهای امنیتی و پلیس از عینک‌های هوشمند دارای فناوری واقعیت افزوده[1] (AR) که به نرم‌افزارهای پیچیده و نوین تشخیص چهره مجهز هستند استفاده می‌کنند تا بتوانند کار چهره‌زنی و شناسایی مجرمان و افراد تحت تعقیب بین انبوه جمعیت شهری را انجام دهند. نیروهای پلیس با استفاده از این عینک‌ها که به پایگاه‌های داده دولتی متصل هستند برای ارسال تصاویر مجرمان بالقوه و شناسایی آن‌ها با استفاده از فناوری تشخیص چهره بهره می‌برند (Russell 2018). همچنین چین در قالب برنامه نمره اعتبار اجتماعی با استفاده از فناوری‌های نوین در پی اعطای نمره اجتماعی به تک‌تک شهروندان است که این نمره با توجه به نوع رفتار شهروندان این کشور می‌تواند بالا یا پایین برود ودر واقع نشان‌دهنده میزان اعتمادی است که می‌توان به یک شهروند داشت. بستر اصلی انجام این پروژه استفاده از دوربین‌های مداربسته هوشمند با قابلیت‌های تشخیص چهره، تشخیص نوع راه رفتن و ... مبتنی بر هوش مصنوعی است. این سامانه قادر است به کمک بیش از ۶۰۰ میلیون دوربین مداربسته هوشمند، افراد را شناسایی و نام، آدرس، کد ملی و شماره گذرنامه آن‌ها را

[1] Augmented Reality



www.SID.ir

Archive of SID



ارایه کند. برابر اعلام یکی از منابع، وزارت امنیت عمومی چین برای این منظور بیش از ۱،۳ میلیارد تصویر از شهروندان چینی بالای ۱۶ سال را در پایگاه داده ویژه‌ای وارد کرده است (L. Y. Chen 2017).

۳-۳ مطالعه موردی نبود فناوری‌های نوین و شکست در تأمین امنیت اماکن حساس: حمله داعش به مجلس شورای اسلامی

حمله داعش به حرم امام خمینی (ره) و مجلس شورا اسلامی یکی از نمونه‌های عملی است که به‌وضوح نبود فناوری‌های نوین و تأثیر آن در شکست در تأمین امنیت اماکن حساس در مناطق شهری را به نمایش گذاشت. در مورد حمله داعش به تهران گفتنی است که برابر اعلانیه‌ای که وزارت اطلاعات پس از حمله منتشر کرد، مشخص شد که همان‌طور که گفته می‌شد، عناصر حمله از قبل برای نیروهای امنیتی، انتظامی و اطلاعات معرف بودند. در اعلانیه وزارت اطلاعات آمده بود: «... ۵ نفر از عناصر تروریست سابقه‌دار وابسته به گروه‌های وهابی و تکفیری بودند که پس از جذب به گروهک تروریستی داعش، از کشور خارج گردیده و در جنایات این گروهک تروریستی در موصل و رقه مشارکت داشته‌اند». همچنین سریاس صادقی یکی از عوامل حمله تروریستی داعش در تهران، از سه سال قبل از آن به‌طور کامل به‌عنوان یکی از مبلغین داعش در شهرهای مرزی غرب کشور مطرح و شناخته‌شده و تصاویر و سایر اطلاعات آن نیز در دسترس بود. در مقایسه با نمونه‌های سامانه‌های امنیتی موجود در کشور چین، که در بخش ۳-۲ معرفی گردید، در صورت وجود سامانه‌های هوشمند امنیتی نظیر شناسایی چهره و ... جلوگیری از حمله تروریستی داعش با توجه به در دسترس بودن اطلاعات مهاجمان، امکان‌پذیر بود.

۳-۴ فناوری‌های نوین و پیشگیری از حملات تروریستی

با توجه به مطالب قبلی ارایه‌شده در مورد تأثیر فناوری در ایجاد، حفظ و ارتقای امنیت، در این بخش در قالب سناریویی، کاربرد فناوری‌های هوش مصنوعی، تشخیص چهره و دوربین‌های پلاک‌خوان بر بستر اینترنت اشیا را که قابل‌پیاده‌سازی در شهرها هستند در حفظ و ارتقای امنیت، و تشخیص و جلوگیری از حملات تروریستی علیه اماکن حساس (وزارت دفاع و مجلس شورای اسلامی) را بررسی می‌کنیم.

اینترنت اشیا عبارت است از اتصال دستگاه‌های مختلف به یکدیگر و در نهایت گردهم آوردن تمامی مواردی که منجر به پیشرفت یک شهر هوشمند می‌شود. این فن‌آوری طیف گسترده‌ای از دستگاه‌های گزارش‌دهنده مانند حسگرها، دستگاه‌های نظارتی و ... را در برمی‌گیرد و با ادغام و تعامل آزادانه داده‌های گردآوری‌شده توسط آن‌ها می‌تواند سامانه‌های پیچیده شهری را در زمان واقعی مدیریت کند و عواقب ناخواسته آن‌ها را به حداقل برساند. اینترنت اشیا به‌طور کلی به بسیاری از چیزها شامل اشیا و وسایل محیط پیرامون‌مان که به شبکه اینترنت متصل شده‌اند و بتوانند توسط اپلیکیشن‌های موجود در تلفن‌های هوشمند و تبلت کنترل و مدیریت شوند اشاره دارد و به زبان ساده، ارتباط حسگرها و دستگاه‌ها با شبکه‌ای است که از طریق آن می‌توانند با یکدیگر و با کاربرانشان تعامل کنند. این مفهوم می‌تواند به‌سادگی ارتباط یک گوشی هوشمند با تلویزیون باشد یا به پیچیدگی نظارت بر زیرساخت‌های شهری و ترافیک باشد (Brown, 2016).

در این بخش فرآیندی معرفی می‌شود که طی آن قابلیت دریافت اطلاعات از منابع گوناگون (دوربین‌های هوشمند) توسط فناوری اینترنت اشیا[1] (IOT) کمک می‌کند تا داده‌های خام و به ظاهر بی‌ارتباط دریافتی به‌صورت روشمند و با استفاده از ماتریس تولید هشدار[2] و در صورت برآورده نمودن ضابطه‌های نظام نشانه‌ها و علائم[3]، به هشدارهای تهدید تبدیل شوند و به سازمان‌های پلیسی – امنیتی کمک کنند تا تهدیدهای تروریستی را شناسایی، پیش‌بینی و از تحقق آن‌ها جلوگیری کنند. با توجه به داده‌های ورودی مختلف

[1] Internet Of Things
[2] Threat Warning Matrix
[3] Indicators



www.SID.ir

به سازمان‌های پلیسی - امنیتی، تنوع این داده‌ها و قالب آن‌ها و سهم گسترده‌شان در تهیه خوراک اطلاعاتی سازمان‌های پلیسی - امنیتی، فرآیند معرفی‌شده در این بخش با ادغام روشمند این داده‌های متنوع، هشدارهای تهدید احتمالی را با ضریب اعتبار بالاتری نسبت به حالت معمول به این سازمان‌ها ارایه می‌کند. در این شرایط علاوه بر اینکه ارایه هشدارهای تهدیدهای تروریستی از ضریب اعتبار بالاتری برخوردار می‌شوند، بلکه سازمان‌های پلیسی - امنیتی می‌توانند به درجاتی از توانمندی پیش‌بینی و پیشگیری از این نوع تهدیدها دست یابند.

حالا سؤال‌هایی که پیش می‌آید این است که چگونه می‌توان برای بیشینه بهره‌برداری ممکن از این داده‌ها که از منابع اطلاعاتی گوناگون و در قالب‌های متفاوت جمع‌آوری می‌شود در راستای امور عملیاتی و پیش‌بینی و پیشگیری وقوع تهدید استفاده کرد؟ پیکره‌بندی مناسب این کار چگونه است؟ آیا پیاده‌سازی روندهای مناسب برای ارتباط‌دهی داده‌ها با یکدیگر در داده‌های بزرگ[1] می‌تواند به قابلیت‌های عملیاتی سازمان‌های پلیسی - امنیتی بیفزاید؟ زیرساخت‌های فنی و بستر مناسب اجرایی‌سازی این نوع فرآیندها چیست؟ آیا مفهوم و فناوری IOT می‌تواند کاندید مناسبی برای میزبانی این نوع فرآیندهای تحلیلی باشد؟ این بخش از پژوهش به منظور پاسخگویی به این سوال‌ها و ابهام‌ها انجام شده است.

اتخاذ رویکرد و طراحی چارچوب مناسبی که در قالب آن داده‌های جمع‌آوری‌شده از حسگرهای مختلف و منابع اطلاعاتی متفاوت به‌طور عملی در خدمت کار عملیاتی قرار گیرد، می‌تواند داده‌های بزرگ نتیجه‌شده از منابع مختلف را به منشأ دستیابی به توانایی پیش‌بینی و شناسایی طرح‌های تروریستی تبدیل کند. مهم‌ترین وظیفه سازمان‌های پلیسی - امنیتی تولید شناخت دقیق و عینی در خصوص وقایع و رخدادهای پلیسی و امنیتی برای جلوگیری از غافلگیری آنان با رخدادهای پیش‌بینی‌نشده است. پیش‌بینی به معنی درون‌نگری شکلی از اشکال شناخت است که اصولاً به آینده توجه می‌کند تا چگونگی فعالیت کنونی را روشن سازد (حاجیانی، ۱۳۹۱). لازم به ذکر است که پیش‌بینی و آینده‌نگری علمی، فرآیند فنی و تکنیکیِ دقیقی درباره موقعیت (یا وضعیت یا موقعیت‌های متعدد) یک پدیده در شرایط آینده است و بنابراین فارغ از هرگونه جنبه غیب‌گویی و پیشگویی است (حاجیانی، ۱۳۹۱، ص.۲۷). با توجه به مباحث مطرح‌شده می‌توان نتیجه‌گیری کرد که پیش‌بینی و آینده‌نگری یکی از ابعاد مهم و بسیار کاربردی در ایجاد امنیت است که در حوزه مطالعاتی آینده‌پژوهی دنبال می‌شود. مواجهه با حملات تروریستی یکی از غافلگیری‌های عمده سازمان‌های اطلاعاتی در است که به دلیل ماهیت خاص این نوع حملات و کوتاه بودن مرحله حین بحران و تهدید تروریستی، معمولاً سازمان‌های اطلاعاتی اقدام خاصی را در زمان عملی و اجرایی شدن تهدید نمی‌توانند انجام دهند. به همین دلیل آینده‌پژوهی تهدید با هدف پیش‌بینی و پیشگیری از وقوع آن بهترین راهکار برای سازمان‌های پلیسی - امنیتی است. چون تهدیدهای تروریستی دارای ماهیت بسیار پنهان است، مقابله با آن‌ها توجه دقیق‌تر به مشخصه‌های این نوع تهدید را می‌طلبد. این کار با تعیین دقیق سناریوهای محتمل و تدوین دقیق‌تر نظام نشانه‌ها و علائم و به‌کارگیری آن‌ها در ماتریس تولید هشدار و احصای سناریوهای ممکن امکان‌پذیر است.

۳-۴-۱ رابطه آینده‌پژوهی، سناریوهای تهدید، نظام علائم و نشانه‌ها با تولید هشدار و پیش‌بینی تهدید در سازمان‌های پلیسی - امنیتی

تولید هشدار (ترسیم رابطه میان جمع‌آوری و تحلیل اطلاعاتی) ماهیتی آینده‌پژوهانه دارد. چون یکی از بهترین روش‌ها در آینده‌پژوهی امنیتی روش سناریونویسی است، در این بخش از پژوهش نیز از این روش بهره گرفته شده است. گام نخست آینده‌پژوهی در این روش فهرست کردن سناریوهای محتمل است. نوشتن سناریوهای محتمل به چند روش امکان‌پذیر است که از جمله آن‌ها می‌توان به استفاده از خبرگی اشاره کرد. توجه به پیشران‌ها نیز از دیگر عوامل مؤثر بر سناریوهای محتمل است. پیشران‌ها در واقع عواملی هستند که می‌توانند منشأ وقوع یک سناریو شوند. مثلاً اختلاف سران یک کشور قبل و حین یک انتخابات می‌تواند به‌عنوان پیشران آشوب و

[1] Big Data



www.SID.ir

اغتشاش بعد از انتخابات در نظر گرفته شود. به‌طور خلاصه در رویکرد آینده‌پژوهی رخدادهای پلیسی - امنیتی به دنبال فهرست کردن آینده‌های محتمل هستیم تا در مرحله بعد با استفاده از نظام هشدارها و علائم بتوانیم به آینده‌های ممکن برسیم. پس از فهرست کردن آینده‌های محتمل باید به تدوین نظام نشانه‌ها و علائم وقوع یک آینده بپردازیم که در صورت رسیدن علائم و نشانه‌های ویژه یک سناریو به یک سطح آستانه[1] مشخص، آن آینده محتمل به یک آینده ممکن تبدیل می‌شود. به همین دلیل در فرآیند تولید هشدار تهدید مهم‌ترین مرحله شناسایی و تدوین دقیق و کارآمد نشانه‌ها و علائم بروز و ظهور احتمالی یک آینده محتمل است. نکته مهمی که وجود دارد این است که نشانه‌ها و علائم مختص یک یا چند سناریوی تهدید است و نباید برای همه سناریوهای ممکن صدق کند. اگر نشانه و علامتی وجود داشته باشد که همه سناریوهای محتمل را تغذیه و برآورده کند نمی‌توان آن را نشانه و علامت تهدید دانست زیرا هیچ‌گونه داده جدید برای حل معادله امنیتی پیشِ رو و برطرف نمودن مِه ابهام‌برانگیز سناریوهای محتمل به دست نمی‌دهد. به‌عبارت‌دیگر اگر ما نشانه و علامتی را تدوین کنیم که برای تمامی سناریوهای محتمل صدق می‌کند آن نشانه دردی را از ما دوا نمی‌کند زیرا به تشخیص افتراقی نمی‌انجامد. پس از تدوین نشانه‌ها و علائم هر سناریو، تمامی آن‌ها در جدولی مانند جدول ۱ مرتب می‌شوند. جدول حاصل در واقع ماتریس تولید هشدار است. طبق فرآیند استاندارد تولید هشدار، با توجه به شواهد و قراین موجود به هر کدام از علائم سناریوها یک نمره داده می‌شود. نمرات می‌تواند به صورت‌های رایج باشد. به‌عنوان مثال نمره از صفر تا ۱۰ یا بین ۱ تا ۴ ستاره. در پایان با جمع نمره‌هایی که به هر کدام از علائم و نشانه‌ها (از نظر امکان وجود و وقوع) داده می‌شود، احتمال وقوع هر سناریو به دست می‌آید و سناریوها از نظر امکان وقوع اولویت‌بندی می‌شوند.

جدول ۱. ماتریس تولید هشدار (راهنمای کاربری نرم‌افزار تحلیل فرضیه‌های رقیب).

| علائم و نشانه‌ها / سناریوها | سناریوی ۱ | سناریوی ۲ | سناریوی n |
|---|---|---|---|
| ۱ | امتیاز نشانه اول از سناریوی ۱ | امتیاز نشانه اول از سناریوی ۲ | امتیاز نشانه اول از سناریوی n |
| ۲ | امتیاز نشانه دوم از سناریوی ۱ | امتیاز نشانه دوم از سناریوی ۲ | امتیاز نشانه دوم از سناریوی n |
| ۳ | امتیاز نشانه سوم از سناریوی ۱ | امتیاز نشانه سوم از سناریوی ۲ | امتیاز نشانه سوم از سناریوی n |
| ⋮ | ⋮ | ⋮ | ⋮ |
| n | امتیاز نشانه nام از سناریوی ۱ | امتیاز نشانه nام از سناریوی ۲ | امتیاز نشانه nام از سناریوی n |
| جمع نمرات | نمره سناریوی اول | نمره سناریوی دوم | نمره سناریوی nام |

پس از به دست آمدن نمرات به‌دست آمده برای هر کدام از سناریوها و نرمالیزه کردن آن‌ها (چون ممکن است تعداد نشانه‌ها و علائم سناریوهای مختلف با هم یکی نباشد) با توجه به نمره سناریوهای مختلف، به ترتیب ممکن‌ترین سناریوها مشخص می‌گردند. به‌عبارت‌دیگر هرچه نمره یک سناریو بالاتر باشد، احتمال وقوع آن بیشتر است.

۳-۴-۲ نشانه‌ها و علائم سناریوی تحقق تهدید تروریستی

[1] Threshold



www.SID.ir

Archive of SID



تهدیدهای اقدامات تروریستی مانند هر تهدید دیگری دارای نشانه‌ها و علائمی هستند. اگرچه نشانه‌ها و علائم این تهدیدها با توجه به محیط محلی[1] دارای تفاوت‌هایی است اما می‌توان برخی نشانه‌ها و علائم را برای اکثر این نوع تهدیدها برشمرد. در جدول زیر برخی دسته‌بندی‌های مختلف این علائم و مثال‌هایی از وجود آن‌ها را می‌بینیم.

جدول ۲. دسته‌بندی‌های علائم و نشانه‌های تهدید عملیات تروریستی و مثال‌هایی برای آن‌ها (Bennett, 2008) و (RISS, 2004).

| دسته‌بندی نشانه‌ها و علائم تهدید | مثالی از وجود نشانه‌ها و علائم تهدید |
|---|---|
| شناسایی قبل از عملیات | - شناسایی پیاده دو یا چند نفر که هماهنگ با یکدیگر در اطراف یک منطقه حساس در حال شناسایی موقعیت هستند<br>- شناسایی متحرک با استفاده از دوچرخه، موتور، ماشین، قایق و ...<br>- افراد یا خودروهایی که چندین‌بار در اطراف یک مکان حساس دیده شده‌اند<br>- افرادی که مدت‌زمانی در یک خودروی پارک شده اطراف یک مکان حساس نشسته‌اند |
| جست‌وجو و احصای اطلاعات | - تحقیق در مورد عِده و عُده نیروهای امنیتی<br>- تحقیق در مورد روش‌های دسترسی به اماکن حساس<br>- تحقیق در مورد چگونگی دریافت مجوز حمل و نقل‌وانتقالات مواد خطرناک |
| تحقیق در مورد اقدامات امنیتی و سنجش آن | - انجام هشدارهای کاذب (به‌عنوان مثال تهدید به بمب‌گذاری)<br>- تلاش برای نفوذ به موانع امنیتی فیزیکی<br>- تلاش برای سنجش تأمین فیزیکی و روش‌های پاسخ به تهدید در اماکن حساس<br>- تلاش برای شناخت روش‌های عبور دادن سلاح و مهمات از نقاط ایست و بازرسی و پنهان کردن آن‌ها از کشف توسط آشکارساز فلز و بازرسی بدنی |
| نفوذ (در برابر اقدامات تأمین فیزیکی یا امنیت سایبری) | - یک نفوذی وارد یک منطقه ورود ممنوع شده و بخشی از سامانه هدف را تخریب یا دست‌کاری کند<br>- نفوذ به یک شبکه رایانه‌ای<br>- ورود کارکنان غیرمجاز به یک منطقه ممنوعه با هدف جمع‌آوری اطلاعات یا سرقت اجزای مربوط به یک هدف |
| تهیه تجهیزات | - تلاش‌های مشکوک یا غیرمجاز برای دستیابی به خودروها، لباس‌های فرم، کارت‌های ورود یا هویت‌های رسمی یک نهاد یا منطقه حساس<br>- سرقت بی‌سیم‌های یک نهاد<br>- سرقت یا خرید رنگ یا لوگوهای مشابه خودروهای امنیتی و اورژانس |
| شناسایی افراد مشکوک | - افراد یا خودروهایی که چندین بار در یک منطقه حاضر بوده یا رفتار غیرعادی داشته‌اند<br>- افرادی که نزدیک یک منطقه حساس در حال استفاده از دوربین عکاسی یا سایر تجهیزات عکس‌برداری و فیلم‌برداری دیده شده‌اند<br>- افرادی که علاقه‌مند به انداختن عکس با کارکنان امنیتی یا عکس‌برداری از اقدامات تأمینی یک منطقه |

[1] Micro-Environment



www.SID.ir

| | |
|---|---|
| | حساس هستند<br>- افرادی که در حال تهیه عکس و یادداشت‌برداری در منطقه‌ای که توریستی نیست مشاهده شده‌اند |
| اجرای تمرینی عملیات تروریستی | - افراد مشکوکی که بدون دلیل و در یک بازه زمانی درون یک خودروی پارک شده نشسته‌اند<br>- افرادی که در حال مشاهده مکالمات رادیوفرکانسی پلیس و ثبت و ضبط زمان پاسخگویی اورژانس هستند<br>- فیلم‌برداری و عکس‌برداری بدون دلیل موجه<br>- رها کردن اشیایی مانند قطعاتی از بار یک مسافر |
| آماده‌سازی تجهیزات و رفتن به موقعیت | - خشاب‌گذاری و پر کردن سلاح‌ها و آماده‌سازی سایر تجهیزات<br>- رفتارهای مشکوک<br>- نقل‌وانتقال سلاح‌ها |

هر کدام از نشانه‌ها و علائم زیر می‌توانند توسط منابع اطلاعاتی مختلف به دست بیایند و قالب داده‌های آن‌ها نیز متفاوت از یکدیگر باشد. جمع‌آوری این اطلاعات به‌خودی‌خود برای پیش‌بینی تهدیدهای تروریستی کافی نیست زیرا به‌ندرت هر کدام از نشانه‌ها و علائم می‌توانند به‌تنهایی مرتبط با یک تهدید تروریستی قلمداد شود و به نتیجه‌گیری در مورد احتمال وقوع یک حمله تروریستی بیانجامد. به همین دلیل نیاز است تا بستری به وجود بیاید تا همه این علائم و نشانه‌ها که از منابع گوناگون و با قالب‌های متفاوت جمع‌آوری می‌شوند، به‌طور یکپارچه در راستای کشف وجود علائم و نشانه‌های یک حمله تروریستی تحلیل شوند. به همین دلیل نیاز است تا ساختاری برای جمع‌آوری این داده‌ها به‌منظور جمع‌آوری و یکپارچه‌سازی هدفمند و کارآمد آن‌ها به وجود بیاید. ویژگی‌ها و توانایی‌های فناوری IOT می‌تواند ضامن اجرای این هدف باشد که در ادامه بررسی می‌شود.

۳-۴-۳ ویژگی‌های IOT و استعداد آن برای میزبانی از داده‌های امنیتی غیرهمگون و ادغام و یکپارچه‌سازی آن‌ها

پیشرفت‌های جدید در فناوری‌های ICT به‌ویژه در سامانه‌های تحلیلگر چندحسگری[1] و تحلیل داده‌های بزرگ ساخت و توسعه سامانه‌هایی که می‌توانند داده‌های دریافتی از منابع اطلاعاتی متفاوت، شامل داده‌های ساختاریافته و ساختارنیافته و داده‌های به‌لحظه و آفلاین را جمع‌آوری و پردازش کنند ممکن ساخته است. در نتیجه چنین سامانه‌ای می‌تواند به‌عنوان بستری برای جمع‌آوری اطلاعات از منابع ناهمگون (شامل حساسه‌ها و پایگاه‌های داده) عمل کند و در نتیجه پاسخگوی الگوریتم‌های تهدیدی باشد که می‌تواند فعالیت‌های تروریستی بالقوه را احصا و ارزیابی نماید. نزدیک‌ترین فناوری به این مفهوم IOT است (Sundmaeker and Guillemin, 2010) که هماهنگی و همکاری تعداد زیادی از اشیای فیزیکی و مجازی متصل به اینترنت را در جهت ارایه خدمات به انسان را در حوزه‌های وسیع امکان‌پذیر می‌سازد. ایده IOT شامل اکتساب اطلاعات از منابعی مانند بخش حمل‌ونقل، تجارت، ترافیک، دوربین‌های مداربسته و ... (که حسگرها نامیده می‌شوند) و پردازش آن‌ها در سطحی وسیع‌تر است (Smith, 2012). IOT با کلیه وسایلی سروکار دارد که قادر به مشاهده و پایش محیط پیرامونی خود با استفاده از قابلیت حسگری (شامل حسگرهای فیزیکی (مانند وسیله‌های الکترونیکی) و حسگرهای مجازی (مانند پایگاه‌های داده)) هستند. بنابراین IOT می‌تواند بستری برای پشتیبانی و میزبانی از انواع داده‌هایی باشد که پیشتر به آن‌ها اشاره شد. همچنین به یاد داشته باشید که IOT از مولفه‌های اصلی شهرهای هوشمند هستند که می‌توانند در ایجاد امنیت هوشمند نیز مهم‌ترین نقش را ایفا کنند. از این طریق نیز فناوری IOT می‌تواند خود را به‌عنوان کاندیدی مناسب برای کمک به سازمان‌های اطلاعاتی – امنیتی در مواجهه با رخدادهای ضدامنیتی در مناطق شهری معرفی کند.

[1] Multi-Sensor System



www.SID.ir

پس از فناوری IOT می‌توان به‌طور گسترده برای جمع‌آوری و تصویرسازی اطلاعات محیط پیرامونی بهره برد. با این وجود این سامانه‌ها به‌خودی‌خود نمی‌توانند برای پیش‌بینی حملات تروریستی استفاده شوند. به همین دلیل نیاز به پیکره‌بندی مناسب یک فرآیند اطلاعاتی و معماری متناسب یک سامانه متناظر میزبان است تا بتوان با استفاده از این پیش‌زمینه‌ها به توانایی پیش‌بینی یک حمله تروریستی دست یافت.

۳-۴-۳-۱ معماری بهینه فرآیند تحلیل اطلاعات منابع مختلف با به‌کارگیری مفهوم و فناوری اینترنت اشیا

همان‌طور که اشاره شد یکی از کارکردهای اصلی فناوری IOT توانایی آن در جمع‌آوری و پردازش اطلاعات از حسگرهای (اشیای فیزیکی و مجازی که توانایی پایش محیط پیرامونی خود و ارتباط با دیگر اشیای فیزیکی و مجازی را دارند) ناهمگون است. معماری مدنظر برای استفاده از اینترنت اشیا در این پژوهش مفهومی سه لایه است:

- لایه اول: لایه جمع‌آوری داده از منابع اطلاعاتی مختلف که مجهز به یک میان‌افزار[1] است؛
- لایه دوم: پایگاه داده‌ای برای ذخیره و نگهداری اطلاعات مرتبط با اعمال تروریستی (حاوی نشانه‌ها و علائم تهدید برای اماکن و شرایط مختلف و به‌طور کلی ماتریس هشدار)؛
- لایه سوم: لایه استدلال[2] برای بررسی مطابقت اطلاعات ورودی با مصداق‌های احتمالی موجود در پایگاه داده (نشانه‌ها و علائم تهدید) و سنجش میزان تطابق آن با سطح آستانه ارایه هشدار تهدید.

لایه اول فرآیند تحلیل اطلاعات با استفاده از فناوری IOT شامل لایه جمع‌آوری اطلاعات از منابع مختلف است. در این لایه یک میان‌افزار حسگرها وجود دارد که داده‌های دریافتی از حسگرهای مختلف را جمع‌آوری، فیلتر و به یک قالب استاندارد تبدیل می‌کند. دلیل نیاز به فیلتر کردن اطلاعات این است که با افزایش داده‌های ورودی نه تنها به سخت‌افزارهای پیچیده‌تر (و در نتیجه گران‌تر) نیاز است بلکه زمان پردازش داده‌ها نیز به‌طور چشمگیری افزایش می‌یابد. به همین دلیل به نظر می‌رسد نیاز به فیلترکردن اطلاعات دریافتی از حسگرها و منابع اطلاعاتی مختلف با به‌کارگیری ضوابط کارآمد و دقیق وجود دارد. قالب استاندارد نهایی باعث ایجاد اطمینان از نمایش تعاملی و یکپارچه اطلاعات دریافتی از تمامی منابع می‌شود. در این مرحله برچسب اطلاعات مکانی[3] هر کدام از داده‌ها نیز در قالبی یکسان ارایه می‌شود تا در مرحله‌های بعدی استفاده شود. به یاد داریم که هدف نهایی ما از این فرآیند رسیدن به توانایی پیش‌بینی حمله تروریستی است. پس باید با توجه به سناریوهای تهدید موجود برای هر مکان به ارزیابی آن‌ها با استفاده از منابع اطلاعاتی تغذیه‌کننده بستر میزبان (زیرساخت مبتنی بر IOT) پرداخت.

در لایه دوم معماری این فرآیند پایگاه داده شامل سناریوهای تهدید و نشانه‌ها و علائم بروز تهدید (ماتریس هشدار) وجود دارد. این پایگاه داده از نوع فعال[4] خواهد بود که نسبت به اطلاعات ورودی واکنش نشان می‌دهد. داده‌های خروجی مرحله اول با اطلاعات موجود در پایگاه داده معماری مدنظر مقایسه می‌شوند. در این پایگاه داده برای اماکن حساس که مستعد هدف قرارگرفتن در حملات تروریستی هستند تهدیدهایی (سناریوها) وجود دارد و علائم و نشانه‌های آن تدوین شده که همان ماتریس هشدار تهدید است.

---

[1] Middleware

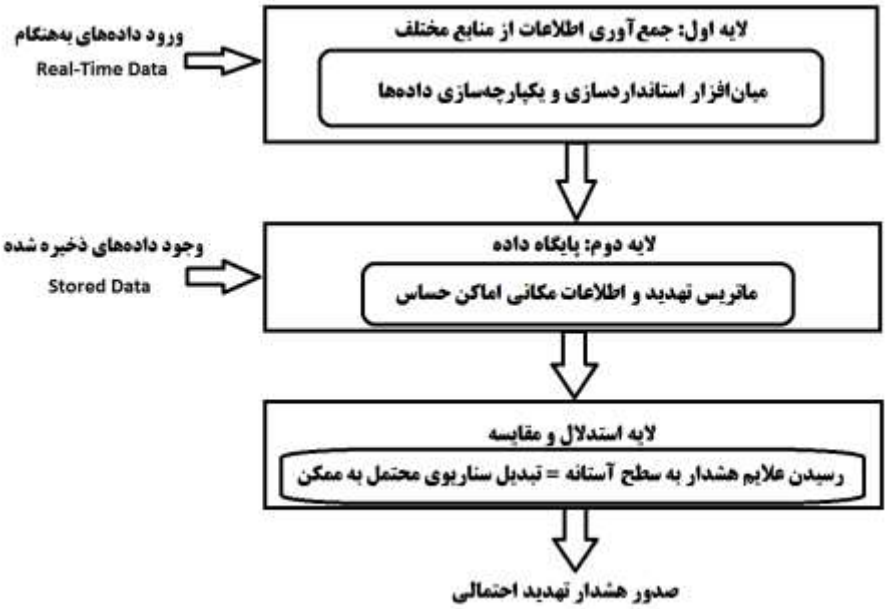
در عمومی‌ترین درک، میان‌افزار یک نرم‌افزار رایانه‌ای است که خدماتی به نرم‌افزارهای کاربردی ورای آن‌هایی که از طریق سیستم‌عامل موجود است ارائه می‌دهد. بنابراین میان‌افزار مشخصاً قسمتی از یک سیستم‌عامل، سامانه مدیریت پایگاه داده‌ها یا یک نرم‌افزار کاربردی نیست. میان‌افزارها کار توسعه‌دهنده را در برقراری ارتباط و انجام‌دادن کارهای ورودی / خروجی (I/O) ساده می‌کند و آن‌ها می‌توانند به هدف مشخص برنامه‌یشان متمرکز شوند.

[2] Reasoning
[3] Geo-Tagging
[4] Proactive Database



www.SID.ir

در لایه سوم از معماری مدنظر اطلاعات ورودی از منابع اطلاعاتی و حسگرها با اطلاعات موجود در لایه دوم مقایسه می‌شود و در صورت وجود انطباق با نظام علائم و نشانه‌ها و نیز برآوردن یک سطح آستانه هشدار، یک هشدار تهدید در قالب شناسایی و پیش‌بینی تهدید تروریستی صادر می‌شود.




شکل ۱. معماری بهینه فرآیند تحلیل اطلاعات منابع مختلف با به‌کارگیری مفهوم و فناوری IOT

در لایه استدلال وزن هر کدام از علائم و نشانه‌ها با توجه به شرایط زمانی و مکانی نیز مشخص می‌شود. تمامی فرآیندهای ارایه شده در بخش‌های قبلی ضمن یک سناریوی فرضی در بخش بعد به‌طور عملی به‌کار گرفته می‌شوند تا چگونگی کارکرد تمامی این عناصر با یکدیگر مشخص گردد.

۳-۴-۴ طراحی سناریوی فرضی وجود تهدید و کاربرد عناصر مختلف پیکره‌بندی ساختار مبتنی بر IOT در پیش‌بینی تهدید و ارایه هشدار

در سناریوی فرضی علائم و نشانه‌های تهدید تروریستی اطراف اماکن حساس (وزارت دفاع و ساختمان مجلس – شکل ۱) را در نظر می‌گیریم.



www.SID.ir

شکل ۲. اماکن حساس و تهدیدهای تروریستی (وزارت دفاع و ساختمان مجلس)

داده‌های ورودی به سامانه نیز از محل چهره‌زنی گشت پلیس، اطلاعات جاسوسی انسانی و نیروهای امنیتی، اطلاعات موجود و ورودی به پایگاه داده، اطلاعات دوربین‌های راهنمایی و رانندگی، دوربین‌های مداربسته و ... تأمین می‌شود (شکل ۲) داده‌های دریافتی از حسگرهای موجود در اطراف این موقعیت داده‌هایی با قالب‌های متفاوت را به بستر سامانه میزبان فرآیند اطلاعات که از ویژگی IOT بهره می‌برد ارسال می‌کنند.

شکل۳. برخی منابع داده ورودی به سامانه (چهره‌زنی دوربین‌های هوشمند مجهز به فناوری تشخیص چهره، منابع انسانی و دوربین‌های تشخیص پلاک خودروها).



www.SID.ir

برای اینکه چگونگی عملکرد معماری و فرآیند ارایه‌شده در این پژوهش مشخص گردد سناریوهای پیش‌بینی حمله تروریستی را در آن اجرا می‌کنیم. این سناریو در دو مرحله پیش از فاز عملیاتی شدن تهدید و در سناریوی بعدی در مرحله به‌لحظه[1] در نظر می‌گیریم.

- در مرحله قبل از عملیاتی شدن تهدید رویدادهای مرتبط با نشانه‌ها و علائم تهدید در پایگاه داده سامانه مبتنی بر IOT درج و ضبط می‌شوند. این مرحله در بازه زمانی تقریباً طولانی انجام می‌شود.

- در فاز عملیاتی به‌لحظه سامانه IOT رویدادهای حیاتی و بسیار مهم را شناسایی می‌کند و هشدارهای پیش‌بینی حمله تروریستی را ارایه می‌کند. برای این کار سامانه از توانایی‌های استدلالی خود پیرامون رویدادهای مرتبط با نشانه‌ها و علائم که در پایگاه داده وجود دارد یا اینکه به صورت به‌لحظه از حساسه‌ها و منابع اطلاعاتی به دست می‌آید استفاده می‌کند.

مرحله پیش از عملیاتی شدن تهدید: این مرحله در یک دوره زمانی فرضی چندهفته‌ای انجام می‌شود. جدول ۳ نشانه‌ها و علائم تهدید را با توجه به آنچه در جدول ۲ به‌عنوان نشانه‌های تهدید تروریستی درج شد ارایه می‌کند.

جدول ۳. رویدادهای کشف شده در مرحله پیش از عملیاتی شدن تهدید.

| نشانه تهدید / رویداد قبل از فاز عملیاتی تهدید | مکان | زمان | حسگر جمع‌آوری‌کننده اطلاعات |
|---|---|---|---|
| خودروی با شماره پلاک ۵۸۳ب۹۳/ایران-۱۴ چندین بار بیرون از ساختمان وزارت دفاع رصد شده است | ساختمان وزارت دفاع | روز اول؛ ساعت ۲۱۰۰<br>روز هفتم؛ ساعت ۱۲۰۰<br>روز دوازدهم؛ ساعت ۲۳۰۰ | دوربین شناسایی و تشخیص پلاک خودروها، دوربین مداربسته اطراف ساختمان وزارتخانه |
| افرادی چندین‌بار در خودروهای پارک‌شده به‌مدت بیش از یک ساعت دیده شده‌اند | ساختمان وزارت دفاع | روز سوم؛ ساعت ۱۳۳۰<br>روز هشتم؛ ساعت ۱۸۴۵ | دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی |
| افرادی چندین‌بار در خودروهای پارک‌شده به‌مدت بیش از یک ساعت دیده شده‌اند | ساختمان مجلس | روز دوم؛ ساعت ۱۰۰۰<br>روز نهم؛ ساعت ۱۴۰۰ | دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی |
| افراد مشکوک در حال عکس‌برداری از محیط دیده شده‌اند | ساختمان وزارت دفاع | روز سوم؛ ساعت ۱۲۰۰<br>روز سیزدهم؛ ساعت ۱۶۰۰<br>روز شانزدهم؛ ساعت ۱۹۴۵ | دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی |
| افراد مشکوک در حال عکس‌برداری از محیط دیده شده‌اند | مرکز کنفرانس | روز پنجم؛ ساعت ۲۰۳۰<br>روز بیست‌سوم؛ ساعت ۱۹۲۰ | دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی |
| درخواست‌هایی برای دسترسی به اماکن حساس | ساختمان وزارت دفاع | روز هجدهم؛ ساعت ۱۷۴۵ | عامل انسانی / درخواست شده از طریق تلفن |
| به صدا درآمدن اشتباه سامانه امنیتی | سالن کنفرانس | روز نهم؛ ساعت ۲۲۰۰ | عامل انسانی |
| تلاش برای نفوذ به شبکه | شبکه وزارت | روز دوم؛ ساعت ۱۳۰۰ | عامل انسانی / اطلاع‌رسانی توسط |

[1] Real-Time



www.SID.ir

| | | | |
|---|---|---|---|
| | دفاع | روز دوازدهم؛ ساعت ۱۸۰۰ | مسئول امنیت شبکه |
| گم شدن یک اسلحه | اعلام نشده | روز دوم؛ ساعت ۰۹۳۰ | عامل انسانی / گزارش شده توسط پلیس / ثبت در پایگاه داده فعال |
| پرسه زدن یک شخص | سالن کنفرانس | روز چهارم؛ ساعت ۰۷۱۰<br>روز پانزدهم؛ ساعت ۱۱۳۵ | فناوری فعال ردیابی افراد / دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی |
| پرسه زدن یک شخص | ساختمان وزارت دفاع | روز ششم؛ ساعت ۲۱۲۰<br>روز شانزدهم؛ ساعت ۰۸۳۰<br>روز بیست‌وپنجم؛ ساعت ۱۵۴۵ | فناوری فعال ردیابی افراد / دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی |
| شخص در حال یادداشت‌برداری | ساختمان مجلس | روز سوم؛ ساعت ۲۱۰۰<br>روز چهاردهم؛ ساعت ۱۹۳۰ | دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی / گشت پلیس |
| شخص در حال یادداشت‌برداری | وزارت دفاع | روز هشتم؛ ساعت ۱۴۴۰<br>روز سیزدهم؛ ساعت ۱۶۳۰<br>روز بیست‌ودوم؛ ساعت ۲۰۴۵ | دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی / گشت پلیس |
| شخص در حال یادداشت‌برداری | سالن کنفرانس | روز دوم؛ ساعت ۱۲۳۰ | دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی / گشت پلیس |
| شخص در حال یادداشت‌برداری | وزارت دفاع | روز هفتم؛ ساعت ۱۸۲۰<br>روز بیست‌وپنجم؛ ساعت ۱۷۳۵ | دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی / گشت پلیس |
| شخصی که مجهز به نقشه و تجهیزات مسیریابی دیده شده است | سالن کنفرانس | روز ششم؛ ساعت ۰۹۴۵ | دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی / گشت پلیس |

رویدادهای جدول ۳ در پایگاه داده سامانه درج و با ابزارهایی که استفاده از فناوری مهیا می‌کند (از جمله راهکارهای مدیریت داده) مدیریت می‌شوند. این داده‌ها در مسیر ورود به سامانه از میان‌افزاری که در بخش قبلی توصیف شد عبور می‌کنند و در قالب مناسب قرار می‌گیرند.



www.SID.ir

فاز عملیات (به‌هنگام): این فاز شامل رویدادهایی است که حین عملکرد به‌لحظه سامانه IOT دریافت می‌شوند. این رویدادها به صورت به‌لحظه وارد سامانه می‌شوند و در پردازش آن‌ها از رویدادهایی که در مرحله پیش از عملیات در پایگاه داده ثبت شده‌اند نیز کمک گرفته می‌شود تا آن‌ها نیز وارد بخش استدلال شوند و به دستیابی بهتر به نتیجه و ارایه هشدار با صحت بیشتر کمک کنند. همان‌طور که پیش از این ارایه شد رویدادهای مرحله پیش از عملیاتی شدن تهدید مرتبط با هشت دسته علائم تهدید ارایه شده در جدول ۲ هستند. برای اینکه اطلاعات و داده‌های مرحله پیش از عملیاتی شدن تهدید، داده‌های به‌هنگام و نشانه‌ها و علائم تهدید تروریستی به‌خوبی با یکدیگر همبسته شوند دو عملیات نگاشت انجام می‌شود: نخست نگاشت بین نمونه‌های رویدادهایی که از علائم حملات تروریستی هستند (ستون اول جدول ۳) و دسته‌بندی نشانه‌ها و علائم تهدید تروریستی (ستون اول جدول ۲) و دوم نگاشت بین رویدادهایی که از علائم حملات تروریستی هستند (ستون اول جدول ۳) و رویدادهایی که از حساسه‌های مختلف جمع‌آوری شده است (ستون اول جدول ۴).

جدول ۴. نمونه‌هایی از رویدادهایی که در مرحله به‌لحظه ارایه می‌شوند.

| ردیف | نشانه و علامت عملیات تروریستی | موقعیت مکانی | حساسیت محیط محلی | حسگر جمع‌آوری‌کننده رویداد | اعلان / عدم اعلان هشدار |
|---|---|---|---|---|---|
| ۱ | حرکت غیرعادی یک خودرو | ساختمان وزارت دفاع | کم | فناوری فعال کشف‌کننده حرکت غیرعادی | عدم اعلان هشدار |
| ۲ | حرکت غیرعادی یک خودرو | ساختمان وزارت دفاع | متوسط | فناوری فعال کشف‌کننده حرکت غیرعادی | - عدم اعلان هشدار برای یک رویداد منفرد<br>- اعلان هشدار برای تکرار چندباره یک رویداد |
| ۳ | حرکت غیرعادی یک خودرو | ساختمان وزارت دفاع | زیاد | فناوری فعال کشف‌کننده حرکت غیرعادی | اعلان هشدار حتی برای یک رویداد منفرد |
| ۴ | حرکت غیرعادی یک خودرو | ساختمان مجلس | کم | فناوری فعال کشف‌کننده حرکت غیرعادی | - عدم اعلان هشدار برای یک رویداد منفرد<br>- اعلان هشدار برای تکرار چندباره یک رویداد |
| ۵ | حرکت غیرعادی یک خودرو | ساختمان مجلس | متوسط | فناوری فعال کشف‌کننده حرکت غیرعادی | اعلان هشدار حتی برای یک رویداد منفرد |
| ۶ | حرکت غیرعادی یک خودرو | ساختمان مجلس | زیاد | فناوری فعال کشف‌کننده حرکت غیرعادی | اعلان هشدار حتی برای یک رویداد منفرد |
| ۷ | مشاهده خودوریی که برای مدت طولانی و بدون دلیل موجه در مکان حساس پارک شده است | ساختمان وزارت دفاع | کم | دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی – گشت پلیس | اعلان هشدار حتی برای یک رویداد منفرد |



www.SID.ir

| | | | | | |
|---|---|---|---|---|---|
| ۸ | مشاهده خودوریی که برای مدت طولانی و بدون دلیل موجه در مکان حساس پارک شده است | ساختمان وزارت دفاع | متوسط | دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی – گشت پلیس | اعلان هشدار حتی برای یک رویداد منفرد |
| ۹ | مشاهده خودوریی که برای مدت طولانی و بدون دلیل موجه در مکان حساس پارک شده است | ساختمان وزارت دفاع | زیاد | دوربین‌های هوشمند متصل به پایگاه‌های داده حکومتی – گشت پلیس | اعلان هشدار حتی برای یک رویداد منفرد |

در جدول بالا هشدارهای تهدید با توجه به وزن و سطح هر نشانه و علامت که در ماتریس تولید هشدار (ماتریس تهدید) مشخص شده است ارایه می‌شود. اگر وزن این نشانه و علائم به یک میزان آستانه برسد، سامانه یک هشدار تهدید ارایه می‌کند. به این شیوه ماتریس تهدید و نشانه‌ها و علائم تهدید با استفاده از قابلیت‌های IOT، حسگرهای آنلاین و به‌لحظه، داده‌های جمع‌آوری شده در پایگاه داده فعال و یک فرآیند پیش‌پردازش توسط یک میان‌افزار وارد کار عملیاتی سامانه می‌شوند و منجر به دستیابی سازمان پلیسی – امنیتی به توانایی و قابلیت شناسایی تهدید و پیش‌بینی و تولید هشدار می‌گردد.

۴- جمع‌بندی و نتیجه‌گیری

در این مقاله به نقش زیرساخت‌های هوشمند برای حفاظت از اماکن حساس در مدیریت و برنامه‌ریزی شهری پرداخته شد. دیدیم که چگونه ایجاد، پیاده‌سازی زیرساخت‌های فناوری‌های هوشمند و به‌کارگیری آن‌ها در طراحی، مدیریت و برنامه‌ریزی شهری می‌تواند به حفظ و ارتقای امنیت اماکن حساس کمک کند. ضمن یک مقایسه تطبیقی با شهرهای آینده‌گرای چین و مطالعه موردی حمله داعش به تهران، برابر یک سناریوی فرضی از فناوری‌های هوش مصنوعی، دوربین‌های هوشمند و ... در بستر اینترنت اشیا برای نمایش چگونگی حفظ و ارتقای امنیت اماکن حساس استفاده شد. در این پژوهش چگونگی کاربرد IOT در تحلیل داده‌های موجود در پایگاه‌های داده بزرگ با توجه به مولفه‌های ماتریس تهدید بررسی شد. همان‌طور که در متن به آن اشاره شد IOT با توجه به ویژگی‌های خود می‌تواند کاربردهای ویژه‌ای در تحلیل داده‌های مختلفی که از حساسه‌ها و منابع گوناگون و با قالب‌های متنوع جمع‌آوری شده‌اند داشته باشد؛ توانایی که از آن به‌عنوان ویژگی پردازش چندحسگری یاد می‌شود. در صورت پیاده‌سازی فرآیند ارایه‌ده در این پژوهش، هزینه‌های مادی و معنوی سازمان‌های پلیسی – امنیتی به‌شدت کاهش می‌یابد و داده‌های خام استخراج‌شده از حساسه‌های مختلف به‌طور تهدیدمحور (با توجه به قرارگیری ماتریس تولید هشدار در فرآیند تحلیل اطلاعات) و هدفمند و بر اساس تهدیدهای مشخص‌شده برای اماکن حساس مدنظر تحلیل و دسته‌بندی می‌شود و برای تولید هشدار و ایجاد توانایی پیش‌بینی تهدید و پیشگیری از تحقق آن به‌کار می‌رود.

۵- پیشنهاد برای پژوهش‌های آینده

پیشنهاد می‌شود پژوهشگران علاقه‌مند به این حوزه‌های کاری در مطالعه‌ها و تحقیق‌های آینده خود به موارد زیر بپردازند:

۱) بررسی چالش‌ها و مزیت‌های پیاده‌سازی فناوری‌های هوشمند پیش‌گفته در بستر شبکه ملی اطلاعات؛

۲) بررسی چالش‌ها و مزیت‌های پیاده‌سازی فناوری‌های هوشمند پیش‌گفته در شبکه نسل ۵ تلفن همراه؛

۳) معماری لازم برای یکپارچه‌سازی فناوری‌های هوشمند با تجهیزات زیرساختی شهری؛



www.SID.ir

۴) بررسی توانش فناوری‌های نوین دیگری مانند کوآدکوپترها در ارتقای امنیت در مدیریت شهری.

منابع و مأخذ

[۱] حبیبی، محسن. از شار تا شهر، تهران: دانشگاه تهران، ۱۳۷۵.
[۲] سلطان‌زاده، حسین. معماری و شهرسازی ایران به روایت شاهنامه فردوسی. تهران: دفتر پژوهش‌های فرهنگی، ۱۳۷۷.
[۳] تقوی‌نژاد دیلمی، محمدرضا. معماری، شهرسازی و شهرنشینی ایران در گذر زمان، تهران: انتشارات یساولی، ۱۳۶۳.
[۴] خلاصه‌ای از اقدامات گروهک تروریستی تکفیری سنندج موسوم به توحید و جهاد؛ پایگاه اطلاع‌رسانی وزارت اطلاعات به آدرس http://www.vaja.ir؛ تاریخ درج خبر: ۱۳۹۵/۰۵/۱۳؛ تاریخ بازیابی از اینترنت: ۱۳۹۵/۱۱/۱۵.
[5] B. T. Bennett, “Understanding, Assessing and Responding to Terrorism”, Protecting Critical Infrastructure and Personnel John Wiley & Sons, Inc., (2008).
[6] “RISS/ROCIC Special Research Report”, Indicators of Terrorist Activity: Stopping the Next Attack In the Planning Stages, (2004).
[7] Brown, Eric (13 September 2016). "Who Needs the Internet of Things?". *Linux.com*. Retrieved 23 October 2016.[13] Sanchez, R. Strategic Learning and Knowledge Management, Wiley, Chichester, 1996.
[8] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, “Vision and Challenges for Realising the Internet of Things”, (2010) March, ISBN 978-92-79-15088-3, doi:10.2759/26127, © European Union, (2010).
[9] I. G. Smith, O. Vermesan, P. Friess and A. Furness, “The Internet of Things 2012 New Horizons”, ISBN: 978-0-9553707-9-3, http://www.internet-of-thingsresearch.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf.
[10] Stephen E. Fienberg, Knowledge Management and Data Mining for Homeland Security, Springer, 2008, NewYork, p-198.
[11] "What is Middleware?". *Middleware.org*. Defining Technology. 2008. Archived from the original on June 29, 2012. Retrieved 2013-08-11.
[12] Armitage R 2013 *Crime prevention through housing design: Policy and practice* New York, NY
: Palgrave Macmillan 24-26.
[13] Ismagilova, E., Hughes, L., Rana, N.P. *et al.* Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Inf Syst Front* (2020). https://doi.org/10.1007/s10796-020-10044-1.
[14] Al-Abed M, Charrier C, Rosenberger C (2012) Evaluation of biometric systems. In: Yang J (ed) New trends and developments in biometrics. INTECH, pp 149–169. https://www.intechopen.com/books/new-trends-and-developments-in-biometrics/evaluation-of-biometric-systems



www.SID.ir

[15] Strittmatter K (2018) Absolute Kontrolle. Sueddeutsche Zeitung, 1 February. http://www.sueddeutsche.
de/digital/digitale-ueberwachung-in-china-absolute-kontrolle-1.3849464
[16] Russell J (2018) Chinese police are using smart glasses to identify potential suspects. TechCrunch, 8 February. https://techcrunch.com/2018/02/08/chinese-police-are-getting-smart-glasses/



www.SID.ir