فصلنامه مطالعات روانشناسی و علوم تربیتی

دوره ۸، شماره ۲، تابستان ۱۴۰۱ صفحات ۱۳۱-۱۴۱

ISSN: 2476-5090

www.uctjournals.com

هوشمندسازی پلیس

محمدرضا حیدری[۱] و امیرحسین محمدی[۲]

۱. دانشجوی دکتری مدیریت فناوری اطلاعات، مدیریت خدمات و توسعه فناوری، دانشکده مدیریت دانشگاه آزاد اسلامی واحد تهران مرکزی

Msra.h1360@gmail.com

۲. مهندسی فناوری اطلاعات، گرایش شبکه های کامپیوتری، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران

Amirmg88@gmail.com

چکیده

با پیشرفت روزافزون فن‌آوری اطلاعات امروزه مباحثی از قبیل: حکومت هوشمند؛ سرمایه انسانی هوشمند؛ محیط هوشمند؛ زندگی هوشمند و اقتصاد هوشمند روزبه‌روز در حال گسترش است. تعامل این عناصر، هوشمندسازی جامعه را تعیین می‌کند. از طرفی افزایش چشمگیر برخی از مقوله‌های جرم شامل قتل، جرائم مرتبط با مواد مخدر و همچنین سرقت‌های شدید باعث شده است رهبری دستگاه‌های اجرای قانون و همچنین دولت‌ها متوجه شوند که استفاده از روش‌های سنتی پلیس به تنهایی موفق به کاهش جرم نخواهد شد. از این رو یک تلاش هماهنگ برای تشویق آژانس‌های دادرسی پلیس در جامعه برای تشدید استفاده و اجرای سیستم‌های پلیس الکترونیکی و هوشمندسازی پلیس انجام گرفته است. هدف این پژوهش بررسی هوشمندسازی پلیس و زمینه‌ها و ابعاد آن می‌باشد.

کلیدواژه‌ها: هوشمندسازی، فن‌آوری اطلاعات، پلیس الکترونیک، هوشمندسازی پلیس

مقدمه

ساخت جامعه هوشمند کیفیت زندگی بالاتری را به همراه خواهد داشت. توسعه سازمان‌ها به سمت الگوی هوشمندسازی یکی از چالش‌های پیش روی جامعه امروز است. جوامع بطور مداوم در حال توسعه و اتخاذ فن‌آوری های فناوری اطلاعات و ارتباطات به منظور ایجاد بسترهایی است که دولت‌ها، مشاغل و شهروندان بتوانند با هم ارتباط برقرار کرده و با هم همکاری کنند و ارتباطات لازم را بین شبکه‌ها (از مردم، مشاغل، فناوری‌ها، زیرساختها، انرژی و فضاها) فراهم کنند(Brutti *et al*, 2019, p: 25).

فناوری اطلاعات و ارتباطات (ICT) و هوشمندسازی

فناوری اطلاعات و ارتباطات (ICT) و هوشمندسازی در جامعه ما همه گیر است. فناوری اطلاعات و ارتباطات همچنین با فناوری های دیگر، مانند فناوری نانو، بیوتکنولوژی و فناوری عصبی ارتباط دارد. این به اصطلاح همگراییNBIC از اواخر دهه ۱۹۹۰ به طور فزاینده ای مشاهده می‌شود. هوشمندسازی به هر جنبه ای از زندگی ما نفوذ می کند: این فناوری که در زندگی امروزه مستقر است (به عنوان مثال از طریق تغییر افکار)، بین ما (از طریق رسانه‌های اجتماعی مانند فیس بوک)، بیشتر و بیشتر در مورد ما می‌داند (از طریق داده‌های بزرگ و تکنیک هایی مانند تشخیص احساسات)، و به طور مداوم در حال یادگیری رفتار ما است. ربات‌ها و نرم افزار رفتار هوشمندانه‌ای دارند و می‌توانند عواطف را تقلید کنند. هوشمندسازی جامعه مرزهای تواناییهای ما را تحت فشار قرار می‌دهد و انواع فرصت‌ها را ارائه می‌دهد، اما مرزهای اخلاقی ما را نیز به چالش می-کشد. از جمله این فن‌آوری‌ها می‌توان به اینترنت اشیاء، روباتیک، بیومتریک، فناوری اقناعی، واقعیت مجازی و تقویت شده و سیستم عامل‌های دیجیتال، هوش مصنوعی، محاسبات مه اشاره کرد. بسیاری از شرکت های فن‌آوری پیش‌بینی می کنند که IoTدر زندگی روزمره ما در آینده حضور گسترده خواهد داشت. بسیاری از فن‌آوری‌هایی بخشی از IoT است: مانند عینک-های واقعیت افزوده که از اینترنت استفاده می‌کنند تا در زمان واقعی به کاربران اطلاعات اضافی درباره محیط خود ارائه دهند، یا یک دوربین بیومتریک که می‌تواند برای تشخیص چهره‌ها به یک پایگاه داده آنلاین وصل شود. توسعه IoT و روباتیک کاملاً مرتبط است. درست مانند دستگاه‌های IoT، روبات‌ها اکثراً مجهز به سنسور برای خواندن محیط خود هستند. آنها به طور فزاینده‌ای به ابر متصل می‌شوند تا داده‌ها را به اشتراک بگذارند و تجزیه و تحلیل کنند، و بر اساس آن تحلیل‌ها اقدامات مستقلی انجام دهند. اگرچه برخی از مسائل در نتیجه با هم همپوشانی دارند، رباتیک مجموعه مشکلات معقول اخلاقی خاص خود را ایجاد می کند(Royakkers *et al*, 2018, P: 127). رونق اینترنت اشیا (IoT) و موفقیت سرویس‌های ابری غنی به سرعت ظهور یک پارادایم محاسباتی جدید به نام محاسبات مه را تسریع کرده‌است که پردازش داده‌ها را در نزدیکی منابع خود ترویج می‌دهد.مه که مکمل ابر است، قول می‌دهد بسیاری از ویژگی‌های جذاب مانند تاخیر پایین، هزینه پایین، چند مستاجری بالا، مقیاس پذیری بالا، و تقویت اکوسیستم IoT را ارائه کند.اگرچه مفهوم مه به طور گسترده در بسیاری از مناطق به کار گرفته شده‌است، اما هنوز به طور کامل مورد تحقیق قرار نگرفته است(Li *et al*, 2018, P:122). از خدمات آنلاین مانند نتفلیکس و فیسبوک گرفته تا چت بات در تلفن‌ها و در خانه مانند Siri و Alexa، به طور روزانه شروع به تعامل با هوش مصنوعی (AI) می‌کنیم. هوش مصنوعی برنامه نویسی رایانه‌ها برای انجام کارهایی است که به طور معمول به هوش انسانی نیاز دارد. این شامل توانایی درک و نظارت بر اطلاعات بصری / مکانی و شنیداری، تعقل و پیش بینی، تعامل با انسان و ماشین ها و یادگیری و بهبود مداوم است.. به زودی، هوش مصنوعی راه‌های تعامل با دولت ما نیز نفوذ خواهد کرد. از شهرهای کوچک ایالات متحده گرفته تا کشورهایی مانند ژاپن، سازمانهای دولتی به دنبال هوش مصنوعی برای بهبود خدمات شهروندی هستند (Mehr, 2017, pp:1-2).

عوامل هوشمند سازی

برای هوشمند سازی هر نهاد و سازمانی باید عواملی محیا باشند تا هوشمندسازی به طور صحیح و اصولی انجام پذیرد. ایـن عوامل عبارتند از:

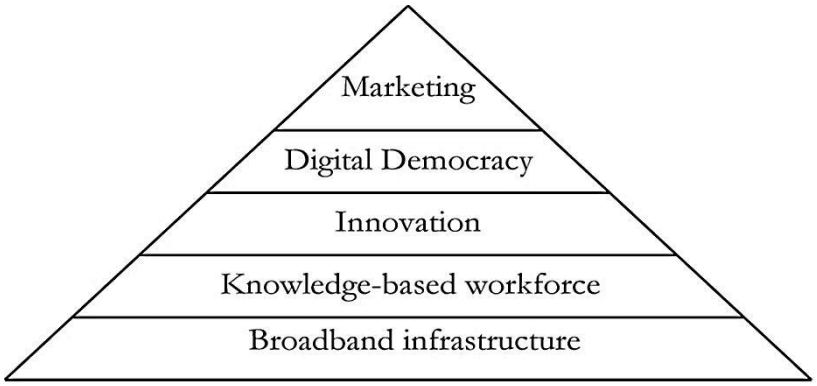
زیر ساخت های پهنای باند که مبنایی برای ارزیابی ظرفیت محلی در خصوص ارتباطات دیجیتالی است. زیرا وابستگی فزاینده شرکت ها و موسسات به ارتباطات و داده ها، باعث افزایش اهمیت پهنای باند به عنوان یک زیرساخت ارتباطی شده و این عامل را به عنوان کاتالیزوری برای توسعه و بهبود بدل نموده است.

نیروی کار دانش بنیان به عنوان مبنایی برای اندازه گیری ظرفیت جمعیت واجد شرایط برای فعالیت های دانش بنیان محسوب می شود. این جمعیت، تنها به فارغ التحصیان دانشگاهی در علوم و مهندسی محدود نمی شود، بلکه نیروهایی که در کارخانه ها ،آزمایشگاه های تحقیقاتی کار می کنند و به نوعی با تولید دانش و ارائه خدمات پژوهشی مرتبط هستند، را نیز پوشش می دهد.

نوآوری به عنوان معیاری با هدف ارزیابی میزان توانایی جوامع در ایجاد محیط های نوآورانه ای است که توانایی جذب طبقه خاق و کسب و کارهای خلاقانه را داشته باشند. البته باید این نکته را مدنظر قرار داد که نوآوری در بسیاری از موارد به ایجاد خوشه هایی با تکنولوژی بالا اشاره داشته و به معنای یافتن روش هایی با هدف ارتقا سطح کیفی خدمات ارائه شده به مشتریان است.

دموکراسی دیجیتالی، معیاری است که دولت و برنامه های بخش های دولتی و خصوصی را از منظر میزان غلبه بر شکاف های دیجیتالی و حصول اطمینان از امکان دسترسی برابر همه اقشار جامعه به پهنای باند و بهره گیری از اطلاعات ارزیابی می کند.

بازاریابی معیاری است که جذابیت کالا و میزان رقابت آن ها را مورد سنجش قرار می دهد. از سوی دیگر، بازاریابی موثر به عنوان یک عامل کلیدی، نقش مهمی را در کمک به توسعه اقتصادی، افزایش پهنای باند و زمینه سازی برای برای جذب نیروی کار ایفا می نماید (Stratigea, 2012, P: 380).



شکل شماره۱: عوامل هوشمند سازی(Stratigea, 2012, P: 380)

تحقیقات نشان می‌دهد که بسیاری از پیشرفت‌های موجود در فن‌آوری های غالب جامعه هوشمند مغایر با شش مضمون حریم خصوصی، استقلال، امنیت، کرامت انسانی، عدالت و توازن قدرت می‌باشد. موج جدید دیجیتالیزاسیونه، فشار بر این ارزشهای عمومی است. برای شکل‌دهی مؤثر جامعه دیجیتالی به روشی مسوولانه از نظر اجتماعی و اخلاقی، ذینفعان باید درک کاملی از آنچه که ممکن است در این زمینه وجود دارد، داشته باشند. باید نظارت بیشتر در زمینه‌های حفظ حریم خصوصی و حفاظت از داده‌ها، تبعیض، استقلال، کرامت انسانی و توازن نابرابر قدرت به خوبی ساماندهی گردد (Royakkers *et al*, 2018, P: 127).

تنظیم داده های بزرگ و شفافیت الگوریتم ها

دیجیتالی شدن جهان مادی، بیولوژیکی و اجتماعی فرهنگی ما منجر به جهانی در حال گسترش دیجیتالی داده‌ها می شود. در آن دنیای دیجیتال، داده‌هایی که پردازش و تجزیه و تحلیل می شوند، پایه‌ای را برای افراد و همچنین سیستم‌های خودکار برای تصمیم گیری فراهم می کند که متعاقباً تأثیر آن بر دنیای فیزیکی است. برای انواع خدمات و محصولات ضروری، ما به طور فزاینده ای از فن‌آوری های دیجیتال استفاده می کنیم و به سیستم های دیجیتال وابسته می شویم: در مراقبت‌های

بهداشتی، بانکی، رسانه‌ها، آموزش و پرورش یا سیستم دادگستری. دیجیتالی شدن جامعه در حال ورود به مرحله جدیدی است و تمایز بین آنلاین و آفلاین را تار کرده است: ما دنیای زندگی هستیم. تحولات در زمینه داده‌های بزرگ، الگوریتم های هوشمند مبتنی بر هوش مصنوعی عناصر ضروری فن آوری‌های مورد بحث در بالا هستند. به عنوان مثال، این پیشرفت‌ها با دستگاه‌های IoT که اطلاعات را به ابر (داده‌های بزرگ) ارسال می‌کنند و در همان زمان توسط داده ها و الگوریتم‌های موجود از ابر هدایت می شوند، برای انجام یک عمل خاص در دنیای فیزیکی هدایت می‌شوند. داده‌ها و الگوریتم‌های بزرگ به تصمیم گیری در بخش‌های دولتی و خصوصی، از کشف تقلب یا احتمال بازگشت مجدد، گرفته تا تشخیص‌های پزشکی کمک می کند. در برخی مناطق، الگوریتم‌های هوشمند و سیستم‌های هوشمند در حال حاضر تصمیم گیری را از مردم گرفته‌اند، به عنوان مثال، با هواپیماهای بدون سرنشین مسلح، یا در اتومبیل‌های هوشمند. فن‌آوری‌های موجود در برنامه‌های مشاوره در تلفن هوشمند ما در چراغ‌های خیابانی هوشمند، می‌توانند اقناع کننده باشند و ممکن است به طرز ظریفی رفتار و استقلال ما را تحت تأثیر قرار دهند. به دلیل دیجیتالی شدن، اکنون تجارت سرسام آور اطلاعات وجود دارد. "داده های بزرگ" گاهی به "طلای جدید" گفته می شود. داده ها با ارزش هستند زیرا تصمیمات بهتری را ممکن می سازد ، به عنوان مثال، درمورد اینکه مصرف کنندگان باید نشان دهند کدام تبلیغ یا کدام افراد باید به عنوان کلاهبردار بالقوه مورد بررسی قرار گیرند. ما قبلاً موضوعات مختلفی راجع به حریم خصوصی بحث کرده ایم و داده های بزرگ به دلیل استفاده مجدد و ترکیب های احتمالی منابع داده های مختلف، چالش خاصی را در این رابطه ارائه می دهند. به نظر می رسد ترکیب و استفاده مجدد از داده های بزرگ با اصل محدودیت هدف مغایرت دارد که یکی از ارکان قانون حمایت از داده ها است. نویسندگان مختلف استدلال می کنند که قانونگذاری و نظارت در عصر داده های بزرگ باید بیشتر بر مسئولیت شرکت ها (پاسخگویی) و نحوه استفاده از داده ها تمرکز کند.اما مخالفان می گویند که اصل محدودیت هدف مکانیزم مهمی برای مقابله با جمع آوری بی پروا و چاقی های داده است. علاوه بر این، مشخصه مهم داده های بزرگ این است که از قبل مشخص نیست که بینش ها را می توان از داده ها گرفت. محققان نشان دادند که براساس لایکهای فیس بوک، می توان ترجیح جنسی، گرایش مذهبی و سیاسی شخصی، خصوصیات شخصی و استفاده از مواد اعتیادآور را تشخیص داد. مقامات همچنین به دنبال پتانسیل داده های بزرگ هستند. یک مثال سیستم ضد تقلب هلندی به نام System Risk Indication (SyRI) است که داده های مربوط به جریمه ها، بدهی ها، مزایا، آموزش و ادغام را در یک محیط دیجیتالی امن رمزنگاری، ترکیب و تجزیه و تحلیل می کند تا به منظور جستجوی مؤثرتر در افرادی که سوء استفاده می کنند از مزایا یا معایب استفاده کنند. تکنیک های داده کاوی (تجزیه و تحلیل داده‌ها) و الگوریتم‌ها (همراه با هوش مصنوعی، به ویژه تکنیک‌هایی مانند یادگیری عمیق) از مقادیر زیادی از داده‌هایی که در سالهای اخیر در دسترس هستند، بی‌نهایت بهره می‌برند. داده‌ها فایل های مربیگری را برای نرم افزار خودآموز تشکیل می‌دهند: هرچه داده نرم‌افزار بیشتر شود، باهوش‌تر می‌شود. شرکت‌هایی مانند فیس بوک و گوگل دارای نرم‌افزاری برای تشخیص چهره هستند که به لطف بسیاری از عکس‌هایی که هر روز کاربران بارگذاری می‌کنند، به سرعت بهبود می‌یابند. نرم افزار ترجمه نیز در حال پیشرفت است زیرا می‌تواند تعداد زیادی از اسناد رسمی ترجمه شده از سازمان ملل و کمیسیون اروپا را جلب کند. در سالهای اخیر، بحث در مورد نظارت بر الگوریتم‌های اساسی در سیستم‌های خودکار از زوایای مختلف به وجود آمده است. دولت آلمان اخیراً مقاله‌ای را منتشر کرده است که می‌گوید سیستم عامل‌های آنلاین مانند گوگل و فیسبوک، باید اطلاعات بیشتری در مورد نحوه عملکرد الگوریتم‌های آن ها به عنوان مثال، هنگام فیلتر کردن اخبار یا نتایج جستجو ارائه دهند (Royakkers *et al*, 2018, P: 138-139)

مزایا و معایب هوشمندسازی

استفاده روزافزون از فناوری اطلاعات و ارتباطات همچنین به معنای هوشمندسازی تعامل بین مردم و همچنین بین افراد و سازمانها از طریق واقعیت افزوده و فضای مجازی و سیستم عامل های دیجیتال است. بنابراین دیجیتالی شدن در دنیای اجتماعی فرهنگی ما نفوذ می‌کند: خرید، معاملات، گوش دادن به موسیقی، تماس با دوستان، اقدام و یافتن تاریخ چیزهایی هستند که بطور فزاینده ای بصورت آنلاین انجام می‌دهیم. ظهور رسانه‌های اجتماعی و سایر خدمات آنلاین در اواخر دهه

۱۹۹۰ و در اواخر قرن تأثیر زیادی بر نحوه ارتباط ما گذاشت. خدمات نقش مهمی در فرهنگ و شکل‌گیری هویت به دست آورده‌اند. به عنوان مثال زندگی کنونی با تلفن هوشمند در هم تنیده شده است که ارتباط بین دنیای واقعی و مجازی را تشکیل می‌دهد. سیستم عامل‌های دیجیتال معاملات هوشمند و کارآمد را فعال می‌کنند. از طریق این سیستم عامل‌های دیجیتال، فرم‌های سازمانی کاملاً جدیدی بعد از سال ۲۰۱۰ ظاهر شدند. نمونه‌هایی از Airbnb و Uber هستند که طی چند سال به بازیگران اصلی اقتصادی تبدیل شده‌اند (Frenken & Schor, 2017, pp: 7-8). دیجیتالیزاسیون و هوشمندسازی همچنین مشکلات جرم جدی را به همراه دارد. اینترنت یا دستگاههای متصل به اینترنت می توانند به خودی خود هدف جنایت قرار بگیرند، مانند حملات هکری یا DDoS (توزیع انکار سرویس) که وب سایت ها یا سیستم ها را فلج می کند. تجربه نشان می دهد که تقریباً هر سیستم دیجیتالی قابل هک شدن است. به عنوان مثال، در سال ۲۰۱۲ ، محققان دانشگاه تگزاس به وزارت امنیت داخلی آمریکا نشان دادند که چقدر هک کردن و کنترل یک هواپیمای بدون سرنشین نظامی نسبتاً ساده است. با جعل هویت شخصی که دستگاه را کنترل می کند، به راحتی می‌توان دسترسی غیرمجاز به یک دستگاه را بدست آورید. در حقیقت ترس از تروریسم سایبری در محافل سیاست وجود دارد. هکرها همچنین می توانند به اطلاعات حساس دسترسی پیدا کنند و این اطلاعات را به افراد خلافکار بدهند. علاوه بر استخراج اطلاعاتی که از دستگاه های هوشمند برای آنها با ارزش است، جنایتکاران می توانند کنترل دستگاه های هوشمند را به دست گیرند. مسئله امنیت به دلیل این واقعیت که دستگاه های IoT به یکدیگر متصل هستند، پیچیده تر می شود. بنابراین، برای مثال، هک کردن یک دستگاه قهوه با موفقیت می تواند به شما امکان دسترسی به ماشین یا باز کردن درب جلو را بدهد. علاوه بر این، این نوع مسئله امنیتی برای بسیاری از تولید کنندگان لوازم الکترونیکی مصرفی جدید است. کلاهبرداری از هویت یک مشکل بزرگ اجتماعی است. کلاهبرداری از هویت عبارت است از به دست آوردن، تصاحب، تملک یا ایجاد شناسه‌های کاذب عمدی، ارتکاب یا قصد ارتکاب رفتار غیرقانونی. بیومتریک پیشرفته باید تقلب در هویت را کاهش دهد. گذرنامه ها امروزه دارای تراشه‌ای با اسکن صورت و اثر انگشت های دیجیتال هستند. در انگلستان از اسکن عنبیه استفاده می کنند. علاوه بر راحتی استفاده برای کاربران، به رسمیت شناختن بیومتریک همچنین از نظر امنیتی این مزیت را دارد که کاربر باید از نظر جسمی حضور داشته باشد. این امر با جعل اسناد، سرقت کارت و افشای رمزهای عبور، خطر تقلب را کاهش می‌دهد (Royakkers *et al*, 2018, P: 133-134).

پیشینه تحقیق

پژوهشی با عنوان، بسترهای نرم افزاری شهر هوشمند: رویکرد مدولار برای دستیابی به قابلیت همکاری در شهرهای هوشمند توسط بروتی و همکاران در سال ۲۰۱۹ انجام گرفت. هدف این پژوهش بررسی بسترهای نرم افزاری شهر هوشمند و ارائه رویکردی برای دستیابی به قابلیت همکاری در شهرهای هوشمند بود. در نتیجه این پژوهش رویکرد را پیشنهاد کرد که توصیف یک روش و یک پلت فرم ICT چند لایه مدولار و مقیاس پذیر برای حل مشکل قابلیت همکاری متقابل دامنه در زمینه برنامه های شهر هوشمند بود (Brutti *et al*, 2019). پژوهشی با عنوان، مه(FOG) مجازی: چارچوب محاسبات مه مجازی سازی برای اینترنتی از اشیا توسط لی و همکاران در سال ۲۰۱۸ انجام گرفت. در این پژوهش، مجازی سازی شی برای غلبه بر موانع ناشی از محدودیت‌های منابع بر روی گره‌های سطح حسی بررسی می‌شود، در حالی که مجازی سازی خدماتی به آسانی برای ایجاد برنامه‌های مناسب برای کاربران نهایی مورد بررسی قرار می‌گیرد.علاوه بر این، مجازی سازی عملکرد شبکه برای انجام انعطاف‌پذیری تامین خدمات شبکه مورد مطالعه قرار می‌گیرد.مجازی سازی شی، مجازی سازی عملکرد شبکه و مجازی سازی خدمات، یک چارچوب لایه‌ای که شامل اشیا هوشمند، مه و ابر است، برای نشان دادن درک مه مجازی در امتداد پیوستار IoT ارایه شده است(Li *et al*, 2018). پژوهشی با عنوان، چارچوب مراقبت از سلامتی تشخیص بیماری IoT بر پایه ابر محورتوسط ورم و سود توسط در سال ۲۰۱۸ انجام گرفت. در چند سال گذشته، انتشارات ام-مرکز مراقبت از سلامتی بر اساس مطالب اینترنت (IoT) پایه ریزی شده که ویژگیهای چندبعدی و خدمات در زمان واقعی را فراهم کرده اند. این انتشارات برنامه ای از میلیونها نفر را به طور منظم برای بدست آوردن جدیدترین اطلاعات سلامتی به منظور سبک زندگی سلامت‌تر تدارک دیده اند. القای ابزار IoT در محیط مرکز سلامتی ویژگیهای متعدد این اطلاعات را بازسازی کرده‌اند.

بیشترین داده های ایجاد شده توسط ابزار IoT در محدوده مراقبت از سلامتی روی ابر بجای اتکای مجزا روی ذخیره سازی محدود و منابع محاسباتی ابزاری آنالیز شده که به صورت دستی کار می کنند. نسبت به این مفهوم، IoT ابر محور بر اساس چارچوب هشدار ام-مراقبت از سلامتی پیشنهاد می دهد که بیماری اصلی را با شدت سطح آن پیش‌بینی کند. ترمینولوژیهای کلیدی برای ایجاد مقیاسهای سلامتی هدایت شده- کاربر با کشف مفهوم علوم محاسباتی کشف شده اند. نمونه اصلی طراحی برای مراقبت سلامتی دانشجویی هوشمند برای سناریو نشر طراحی شده است. نتایج بعد از پردازش مقیاسهای سلامتی در یک مفهوم خاص محاسبه شده اند. در این پژوهش، داده های سلامتی دیدگاه دانشجویی سیستماتیک با استفاده از مجموعه داده های UCI و سنسورهای پزشکی برای پیش بینی شدت بیماری متفاوت دانشجو ایجاد شده است. دستورالعملهای تشخیص با استفاده از الگوریتمهای طبقه بندی متفاوت آخرین یافته های علمی بکار رفته و نتایج بر اساس دقت، حساسیت، ویژگی و اف-مقیاس محاسبه شده اند. نتایج آزمایشی نشان می دهد که روش شناسی پیشنهادی روش های خط اصلی برای پیش بینی بیماری عملکرد بهتری دارند(Vermal& Sood, 2018). پژوهشی با عنوان، حفظ محرمانه بودن در سیستم مدیریت انرژی مجتمع کاربر برای محاسبات ابری توسط تیان و همکاران در سال ۲۰۱۸ انجام گرفت. تحت توسعه فناوری اطلاعات و ارتباطات، این مقاله در مورد مدیریت انرژی یکپارچه کاربردهندگان مبتنی بر ابر برای بهبود بهره وری انرژی در یک جامعه هوشمند، که یک مدل دوسطحی است که براساس یک مرکز انرژی و بارگیران تکیه می کند، مورد بحث قرار می گیرد. علاوه بر این، برای رسیدگی به موضوع حفظ محرمانگی برای سرویس ابری، یک مکانیزم پنهان سازی اطلاعات براساس توابع نقشه برداری خطی طراحی شده است که نیاز و فرآیندهای پنهان سازی اطلاعات مربوطه مشخص می شود. نتایج عددی اثربخشی مدل پیشنهادی و روش محاسبات ابری را نشان می دهد(Tian *et al*, 2018).

تاریخچه هوشمندسازی پلیس(SPI)

در سال ۲۰۰۸ و ۲۰۰۹، سازمان‌های اجرای قانون در سراسر ایالات متحده با کاهش بودجه که توسط "رکود بزرگ" به وجود آمده بود ، تحت فشار قرار گرفتند. بسیاری از سازمان های اجرای قانون استخدام کار خود را متوقف کردند، بیش از چند آژانس پاسخگوی تماس های غیر اضطراری را متوقف کردند و روش‌های گزارشگری جایگزین را ایجاد کردند. به دلیل کمبود منابع، کارکنان را از وظایف تخصصی بیرون کشیده و به دلیل کمبود منابع، فعالیت‌های پلیس و فعالیت های مربوط به حل مشکلات جامعه متوقف شده است. شرایط بودجه، آژانسها را وادار به تمرکز بیشتر روی پاسخگویی به تماس های خدماتی می کرد. در طول ۴۰ سال گذشته، به استثنای پولیس اطلاعاتی، تمام "ایده های بزرگ" در مورد امنیت عمومی در ادارات محلی و دانشگاه ها سرچشمه گرفته است. در سال ۱۹۷۹، هرمان گلدشتاین (دانشگاه ویسکانسین) با بیان این که پلیس باید حوادث را نه به عنوان رویدادهای منزوی بلکه به عنوان علائم آشکار مشکلاتی که دارای تاریخ و آینده هستند، پلیس را با محوریت حل مسئله ای معرفی کرد. در سال ۱۹۸۰، پیشینه های پلیس اجتماعی هنگامی متولد شد که رابرت تروجانویچ (دانشگاه ایالتی میشیگان) آزمایش گشت زنی فلنت را شروع کرد. در سال ۱۹۸۲، جیمز س. ویلسون و جورج کلینگ " پلیس و امنیت محله" را در ماهنامه آتلانتیک منتشر کردند. در نیویورک سیتی، ویلیام برتون و جک مپل در سال ۱۹۹۳ Comp Stat را تأسیس کردند. در برابر این زمینه از کاهش بودجه و چالش‌های مالی، BJA اولین درخواست هوشمندسازی پلیس(SPI) در ۹ ژوئن سال ۲۰۰۹ منتشر شد. با استفاده از SPI، BJA به دنبال یک نتیجه خاص بود: شناسایی یا تأیید راه حلهای مؤثر (کاهش جرم) و کارآمد (با قیمت مناسب برای اکثر آژانس ها) برای مشکلات مزمن جرم محلی. BJA انتظار داشت که با همکاری دانشمندان پلیس و عدالت کیفری به این نتیجه برسد که بتوانند راه حلها و فرایندهای تئوریهای علم جرم شناسی را با تشخیص روش‌های درست ارزشیابی با توجه به فوریتی که سازمان‌های اجرای قانون برای انجام مسئولیت‌های خود دارد، آزمایش کنند و توسعه دهند (Coldren Jr. *et al*, 2013, p: 277).

تعریف هوشمند سازی پلیس

به گفته BJA (۲۰۱۴)، هوشمند سازی پلیس به عنوان مداخلات گسترده مبتنی بر استفاده از شیوه های پلیس، راهبردها و تاکتیک های مبتنی بر شواهد و داده محور، به منظور پیشگیری و کنترل جرم تعریف کرده است. آنچه که در مورد این تعریف

قابل توجه است این است که طرح های هوشمندسازی پلیس در جهت بهبود عملکرد پلیس به منظور پیشگیری و کنترل جرم در نظر گرفته شده است. با این حال، توجه به اطمینان از اثربخشی، کارآیی و استفاده اقتصادی از این طرحها نیز مورد توجه است (Matlala, 2016, p: 3061). ریکمن (۲۰۱۰) استدلال می کند که پلیس هوشمند تأکید برفعالیت برای جلوگیری از وقوع جرم به جای واکنش در برابر آن را دارد. این نویسنده ادعا می کند که برای تحقق پلیس پیشگیرانه، هوشمند سازی پلیس باید با استفاده از ابزارهای محرک فناوری مانند نرم افزار تحلیلی ، پزشکی قانونی DNA و ICT و قابلیت های نظارت برای پیشگیری و کنترل جرم انجام پذیرد(Matlala, 2016, p: 3062). هوشمند سازی پلیس با تکامل جمعیتی شهروندان مرتبط است. که شامل تراکم جمعیت و میزان شهرنشینی، تغییر در جمعیت، ثبات در رابطه با تحرک ساکنان، الگوهای رفت و آمد و سایر عوامل گذرا است. استفاده از پلیس هوشمند با محیط های پویا اجتماعی و جنایی همراه با تهدیدهای جدید در مورد امنیت عمومی مرتبط است. که این می‌تواند با آنچه که معمولاً به عنوان جرایم اجتماعی شناخته می شود، مرتبط باشد، به عنوان مثال قتل، تجاوز. اسمیت و همکاران (۲۰۰۴) صراحتا پلیس هوشمند را تعریف نمی کنند. با این حال، این نویسندگان بر این عقیده اند که در چارچوب آفریقای جنوبی، پلیس هوشمند مفهومی جامع است که تعدادی از موضوع های مدیریت پلیس را در دوره پسا دموکراتیک شامل می کند. که شامل جنبه های قانونی پلیس، روابط پلیس در جامعه، تشکیل مشارکت برای جلوگیری از جرم، بهبود مدیریت (مدیریت) ایستگاه های پلیس، استفاده موثر از اطلاعات جرم، بهبود اندازه گیری عملکرد پلیس و همچنین ایجاد توانمندسازی قربانی است (Matlala, 2016, p: 3062). بر اساس تعاریف فوق می توان ادعا کرد که پلیس هوشمند بیش از کاربرد فناوری اطلاعات و ارتباطات و سایر دستگاههای فن آوری برای مبارزه با جرم و جنایت، شامل راهبردهای دیگر پلیس همچون حل مسئله و پلیس اجتماع محور است (Matlala, 2016, p: 3062). جدیدترین طرح مشارکت واحد تحقیق و تخصص پلیس که اخیراً تأمین می شود، هوشمندسازی پلیس است. هوشمندسازی پلیس بر این فرض اساسی بنا شده است که سازمانهای اجرای قانون باید در یک شرایط مالی که در آن بودجه های آژانس‌ها محدود و فرصت افزایش کارمندان محدود است، مؤثر، کارآمد و اقتصادی باشند. مؤلفه اصلی هوشمندسازی پلیس، استفاده از سیستمهای نرم افزاری و بانکهای اطلاعاتی برای مشارکت در تجزیه و تحلیل جرم و نقشه برداری، شناسایی نقاط حاد و سایر تلاشهای اطلاعاتی برای حل مسئله است (Alpert *et al*, 2013, p: 37).

تعریف پلیس الکترونیکی

درست مانند پلیس هوشمند، هیچ توافق کلی درباره معنای مفهوم پلیس الکترونیکی (e-policing) وجود ندارد. برای نشان دادن این نکته، پلیس الکترونیکی گاهی اوقات به عنوان ارائه خدمات و اطلاعات بین پلیس و شهروندان از طریق اینترنت تعریف می شود. از طرف دیگر، بوندو و تریپاتی(۲۰۰۷) استدلال می کنند که کاربرد سیستم های پلیس الکترونیکی به پلیس این امکان را می دهد که از وب سایت‌ها، نامه‌های الکترونیکی و نمابر به عنوان یک روش جایگزین برای برقراری ارتباط با مردم استفاده کند. اگرچه این تعریف اهمیت ICT در تقویت ارتباط بین پلیس و ساکنان را نشان می دهد، اما این تعریف محدود است زیرا جنبه های دیگر کاربرد الکترونیکی را تعریف نمی کند. همچنین شایان ذکر است که پلیس الکترونیکی را به عنوان استفاده از دستگاه های تکنولوژیکی به منظور ضبط، ذخیره، تجزیه و تحلیل و به اشتراک گذاری اطلاعات پلیس می داند. محققین همچنین استدلال می کند که پلیس الکترونیکی مستلزم اتوماسیون فرآیندهای دستی ضبط، ذخیره و تجزیه و تحلیل داده های پلیس است. علاوه بر این، این مفسران ابتکارات شامل: پلیس الکترونیکی را برای ایجاد پایگاه داده های ملی مانند مدیریت پرونده های پرونده ای، آمار جرایم، اطلاعات جرایم، ژئو پولیس و گواهی‌های سلامت موتوروسایل نقلیه بیان می کند. در مقایسه با تعریف قبلی، می‌توان ادعا کرد که تعریف دوم جامع تر است زیرا مفهوم را فراتر از ارتباطات الکترونیکی بین پلیس و شهروندان می‌برد. با این وجود، تلاشهایی هماهنگ از طرف آژانس‌های پلیس مانند سرویس پلیس نامیبیان برای موقعیت‌یابی پلیس الکترونیکی مخصوصا در مورد اتوماسیون، ذخیره و تجزیه و تحلیل داده های پلیس و همچنین ایجاد پایگاه های داده صورت گرفته است.

تفاوت پلیس الکترونیکی و پلیس هوشمند

بر اساس تجزیه و تحلیل تعاریف تحقق پلیس هوشمند، می توان نتیجه گرفت که پلیس هوشمند مفهومی گسترده است که شامل استفاده از روشهای مختلف پلیس، فناوری اطلاعات و ارتباطات (ICT) و همچنین نوآوری های فناوری برای جلوگیری و کنترل جرم است. بنابراین می‌توان چنین ادعا کرد که پلیس الکترونیکی، یعنی استفاده از سیستم های ICT برای ضبط، تجزیه و تحلیل، انتشار و ذخیره داده های پلیس که در واقع بخشی از پلیس هوشمند است. همچنین نتیجه می گیرد که به عنوان یک رویکرد از فعالیت پلیس، هوشمندسازی پلیس در اقدامات پیشگیری از جرم ضروری است. دلیل این امر این است که در این روش آژانس‌های پلیس امکان می دهد تا از نوآوری های فن آوری برای اطمینان از کارآیی و کارآمدی پلیس استفاده کنند(Matlala, 2016, p: 3063).

مزایا هوشمندسازی پلیس

پلیس یک منطقه بحرانی از حاکمیت دموکراتیک است که در آن حتی یک عمل منفرد موجبات آشفتگی کل بافت جامعه را فراهم می آورد. به عنوان اولین پاسخ دهنده ، پلیس مجبور است از اعمال توازن ظریف بهره ببرد و کار خود را بطور حرفه‌ای و منظم به پیش ببرد. در پشت پرده این جنبه مهم پلیس، هوشمند سازی پلیس به وجود می‌آید که تفکر انتقادی را به کل نیروهای اجرای قانون افزوده است. اهمیت ایده اصلاحات در پلیس باید شامل نسخه برتر هوشمندسازی پلیس باشد که شامل: میزان حساسیت، مدرن و همراهی، هوشیاری و پاسخگویی، قابلیت اطمینان و پاسخگویی و دانش فنی و آموزش خوب باشد. الگوی هوشمند سازی پلیس دارای کلیه ورودی ها و خروجی هایی است که به دستگاه های اجرای قانون اجازه می دهد تا خود را به یک مدل مدرن و ماهرتر تبدیل کنند. هوشمند سازی پلیس این پتانسیل را دارد تا شکاف های موجود در پلیس را کنترل کند و از مناطق بحرانی که بیشتر اوقات منجر به انتقاد می‌شود، مراقبت کند. بنابراین محوریت توانمندسازی مأمورین اجرای قانون باید در راستای جهت‌گیری جامعه، اخلاق غیرحزبی و حساسیت نسبت به مشکلات آن دسته از افراد و گروههای فرعی جامعه باشد که آزادی و حساسیت آنها در معرض خطر بیشتری است. زنان، کودکان، بی سرپرست، روستایان فقیر، فقیرنشینان، زاغه نشینان شهری، اقلیت‌های فرهنگی و مذهبی و افرادی را که بتوان از نظر جسمی و روحی به چالش کشیده همه در این طبقه قرار می‌گیرند. تمرکز برای ایجاد ظرفیت باید به هر عامل اجرای قانون کمک کند تا این سیستم ارزش را درونی کند (Kapoor, 2015, Pp: 4-5). یک اصل اساسی هوشمند سازی پلیس تضمین همکاری مؤثر بین سازمانهای اجرای قانون و سایر ذینفعان، از جمله دادستانها، سازمانهای جامعه و محققانی است که هرکدام در حفاظت از مردم نقش اساسی دارند. هوشمندسازی پلیس، مشارکت بین همه ذینفعان جامعه را که هنگام تدوین جدول زمانی استراتژی کاهش جرم و جنایت جامع، باید حضور داشته باشند، سهیل کرده است. با این روش جوامع با سابقه طولانی خشونت مزمن توانسته‌اند جنایات خشونت آمیز را کاهش دهند، جان‌ها را نجات دهند و در نتیجه امنیت جامعه را بهبود بخشند (Elliott, 2014, p:8).

ویژگی های هوشمندسازی پلیس

هوشمندسازی پلیس(SPI)، امروز نشان دهنده پیشرفت طبیعی در تکامل و پیشرفت علوم پلیس است که توسط ویژگی های زیر نشان داده شده است:

SPI به صورت محلی هدایت می شود. BJA و وزارت دادگستری نیاز ندارند که SPI های محلی رویکرد خاصی برای کنترل جرم اتخاذ کنند. انتظار این است که تجزیه و تحلیل کامل روی رویکردهای به کار گرفته شده تأثیر بگذارد.

SPI بر نقش علم و تحقیقات در بررسی اثربخشی پلیس متمرکز است. کمبود شواهد علمی مربوط به استراتژی ها و تاکتیک های پلیس نیاز به تمرکز بیشتر بر روی روش های ارزیابی دقیق دارد.

SPI از همان آغاز به کارگیری طرح های ارزیابی تجربی یا شبه تجربی است.

SPI چند بعدی است سایت های محلی باید رویکردهای چند وجهی را برای حل مشکلات مشخص شده از طریق تجزیه و تحلیل روش ها توسعه دهند. رویکردهای یک بعدی احتمالاً نشانگر تحلیل ضعیف است.

SPI نتایج گرا است انتظار می رود مشارکت های پژوهشی SPI یافته هایی را در مورد اثربخشی استراتژیهای اجرا شده بدست آورند.

SPI در تلاش برای نوآوری است. آژانس های با بودجه SPI باید رویکردهای جدیدی را برای پیشگیری از جرم و کنترل جرم، کاربردهای جدید رویکردهای موجود یا کاربردهای رویکردهای مبتنی بر شواهد که قبلاً در حوزه قضایی بودجه اجرا نشده بودند، تهیه و آزمایش کنند(Coldren Jr. *et al*, 2013, p: 278).

پنج مؤلفه اصلی پلیس هوشمند

مؤلفه اصلی پلیس هوشمند شامل: اندازه گیری عملکرد و مشارکت تحقیقاتی، توسعه و همکاری، مدیریت تغییر سازمانی، هدف گذاری استراتژیک، استفاده بهتر از اطلاعات و سایر سیستم های داده و اطلاعات می‌باشد. که شرح آن در ادامه بیان گردیده است.

اندازه گیری عملکرد و مشارکتهای تحقیقاتی: SPI هدفمندانه به تحقیقات منظم در مورد پیاده سازی و نتیجه نوآوری ها نیاز دارد. بنابراین، اعضای جامعه SPI باید با مستندسازی دقیق از فعالیتهای عملی، بهبود اندازه گیری عملکرد و اندازه گیری نتایج با استفاده از استراتژی ها و طرح های ارزیابی مقایسه ای، کیفیت دانش خود را در مورد شیوه های موثر پلیس و اعتماد به نفس آنها نسبت به یافته های تحقیق بهبود بخشند.

توسعه و همکاری: سالهاست که جامعه قانونی به رسمیت شناخته اند و سازمان های پلیس باید روابط مؤثر و ارتباطی مؤثر با شهروندان و رهبران جامعه برقرار کنند تا بتوانند کار خود را به صورت مؤثر انجام دهند. ابتکار عمل جدید پلیس (بخصوص مواردی که متخلفان یا محلات را هدف قرار می دهد)، بدون آموزش عمومی، دستیابی و داشتن اطلاعات، در بیشتر موارد، امکان پذیر نیست و یا توصیه نمی شود.

مدیریت تغییر سازمانی: نوآوری و تغییر، دو هدف اصلی SPI ، به طور طبیعی منجر به نقش های جدید، پیش بینی ها و فرآیندهای داخلی و خارج از سازمان می شود. اعضای جامعه SPI باید برای تغییر سازمانی برنامه ریزی کنند، موانعی را برای تغییر موفقیت آمیز سازمانی پیش بینی کنند و راهکارهایی را برای کاهش مقاومت داخلی و خارجی در برابر تغییر ایجاد کنند.

هدف‌گذاری استراتژیک: با دقت و توجه به داده ها و تعیین چگونگی تأثیرگذاری یا تأثیرپذیری آنها از محیط جنایی، تصمیم گیران اجرای قانون می‌توانند، فعالیت های استراتژیک را که بیشترین احتمال دستیابی به نتیجه مطلوب را دارند، انجام دهند. سایت های SPI به طور استراتژیک تلاش های پلیس و منابع مربوط به نقاط حاد جرم و یا تکرار جرم و ازدیاد جرم را هدف قرار دهند.

استفاده بهتر از اطلاعات و سایر سیستمهای داده و اطلاعات: هوشمندسازی پلیس نیاز به استفاده صحیح و کارآمد از داده ها و منابع اطلاعاتی دارد. داده های پلیس هوشمند فراتر از منابع اطلاعاتی پلیس سنتی است. سیستم پلیس هوشمند از اطلاعات پلیس و همچنین داده‌هایی در مورد تماس با خدمات، جرائم گزارش شده، دستگیری‌ها و شکایاتی که با مکان‌های نقاط حاد جرم در ارتباط است، استفاده می کند. پلیس هوشمند همچنین شامل داده های تحقیقاتی، داده ها از نهادهای خارجی و داده های سازمان های دادگستری خارجی است.

BWC ابزاری برای هوشمندسازی پلیس

BJA از طریق طرح هوشمندسازی پلیس (SPI)، در سال ۲۰۱۱ بودجه‌ای را برای خرید، استقرار و ارزیابی BWC ها(دوربین نصب شده روی بدن پلیس) به اداره پلیس ققنوس (آریزونا) (PPD) و شرکای تحقیقاتی آن در دانشگاه ایالتی آریزونا (ASU) اهدا کرد. BWC از پشتیبانی بسیاری از سازمان های اجرای قانون، گروه‌های مدافع حقوق شهروندی، سازمان های حقوق مدنی، سیاستمداران و دولت فدرال برخوردار است. ارزیابی BWCs، به رهبری شرکای تحقیقاتی در دانشگاه ایالتی آریزونا، بر شش حوزه مهم متمرکز شده است: انطباق فعال‌سازی دوربین افسر، درک افسر از پوشیدن و کاربرد دوربین‌های بدن، تأثیر بر

عملکرد شغلی افسران، تأثیر در انطباق و همکاری عمومی، تأثیر در مسئولیت‌پذیری افسران و تأثیر در روند رسیدگی به پرونده های خشونت خانگی و نتایج آن. تیم SPI ققنوس تعدادی از مزایای درک شده BWC به شرح زیر اعلام کرد:

۱. این فناوری ممکن است مأمورین را از انجام رفتارهای غیرحرفه ای یا رفتارهای نادرست باز دارد و همچنین ممکن است اعضای جامعه را از رفتارهای نامناسب، پرخاشگرانه و مقاوم باز دارد. و ممکن است تعامل بالقوه خشونت آمیز بین پلیس و جامعه را خنثی سازد. یعنی BWCs ممکن است باعث فرهنگ سازی بهینه در جامعه شود.

۲. این فناوری پتانسیل ثبت سوء رفتار، استفاده از زور و سایر رفتارهای مشکل یا رفتارهای غیرحرفه ای را دارد. برعکس، این پتانسیل را نیز دارد که یک افسران برای رد ادعای رفتار نادرست از آن استفاده کنند.

۳. این فناوری با افزایش یادآوری یک حادثه هنگامی که مأمور در حال تکمیل گزارش میدانی خود است، و همچنین بعداً در دادگاه ، می تواند اثربخشی پاسخ پلیس در قبال جرم به طور کلی و خشونت خانگی را به طور خاص افزایش دهد. اقدامات. همچنین می توان از این ویدئو به عنوان شاهد استفاده کرد که ممکن است به میزان بالاتر دستگیری، اتهام، تعقیب و محکومیت منجر شود (Katz *et al*, 2015, pp: 1-2).

نتیجه گیری

نتایج پژوهش BJA جامعه SPI را تشویق می کند تا هر یک از مؤلفه‌های هوشمندسازی پلیس را به عنوان نوآوری پلیس هوشمند در نظر بگیرند. مشارکتهای سنتی و غیر سنتی با مقامات دولتی، سازمانهای جامعه و سایر نهادهای خدمات عمومی بر اجرای موفقیت آمیز راهبردهای پلیس‌هوشمند موثر است. از پلیس هوشمند کل جامعه نه تنها از طریق صرفه‌جویی در هزینه و بهبود مشکلات جرم، بلکه از طریق ارتقاء احساس و همکاری افراد، بهره مند خواهد شد.

منابع

Ahmad Khan, Minhaj & Salah, Khaled. 2017. IoT security: Review, blockchain solutions, and op, Minhaj Ahmad Khan, Khaled SalahPublished in Future Generation Comp, Syst, Pp: 1-33, DOI:10.1016/j.future.2017.11.022.

Alpert, Geoffrey P. & Rojek, Jeff & Hansen, J. Andrew. 2013. Building Bridges Between Police Researchers and Practitioners: Agents of Change in a Complex World, Final Report to the National Institute of Justice, University of South Carolina, December.

Bureau of Justice Assistance (BJA). 2017. Smart Policing Initiative, Data. Analysis. Solutions, U.S. Department of Justice, Applications Due: January 26, pp:1-36.

Brutti, Arianna & SabbataAngelo, Piero De & Nicola, Frascella & Raffaele, Gessa & Cristiano, Ianniello & Stefano, Novelli & Pizzut, Giovanni. 2019. Smart City Platform Specification: A Modular Approach to Achieve Interoperability in Smart Cities, The Internet of Things for Smart Urban Ecosystems, pp :25-50, DOI https://doi.org/10.1007/978-3-319-96550-5_2.

Coldren Jr., James R. & Huntoon, Alissa & Medaris, Michael. 2013. Introducing Smart Policing: Foundations, Principles, and Practice, Vol: 16 issue: 3, PP: 275-286, https://doi.org/10.1177/1098611113497042.

Elliott, Vivian. 2014. THINKING "SMART" ABOUT 21ST CENTURY POLICING COLLABORATIVE APPROACHES TO PUBLIC SAFETY, October, Vol: 96 No: 9, pp: 7-11, icma.org/pm

Frenken, Koen & Schor, Juliet. 2017. Putting the sharing economy into perspective. Environmental Innovation and Societal Transitions, 23, Pp: 3–10, journa hom epage: www.elsevier.com/locate/eist.

Katz, Charles M. & Kurtenbach, Mike & Choate, David E. & White, Michael D. 2015. Phoenix, Arizona, Smart Policing Initiative: Evaluating the Impact of Police Officer Body-

Worn Cameras, Bureau of Justice Assistance, NCJRS Abstract, pp: 1-20, http://www.ncjrs.gov/ App/publications/abstract.aspx?ID=272350.

Kapoor, Vineet. 2015. The 'T-2' of the S.M.A.R.T. Police: A Relook at Police Capacity Building, The Indian Police Journal, April-June, Vol. LXII , No. 2, pp:4-19.

Liang, Xiaohui & Zhang, Kuan & Shen, Xuemin & Lin, Xiaodong. 2014. Security and privacy in mobile social networks: challenges and solutions, IEEE Wireless Communications, Vol: 21, Issue: 1, Pp: 33 – 41, DOI: 10.1109/MWC.2014.6757895.

Li, Jianhua & Jin, Jiong & Yuan, Dong & Zhang, Hongke. 2018. Virtual Fog: A Virtualization Enabled Fog Computing Framework for Internet of Things, Process Safety and Environmental Protection, IEEE Internet of Things Journal, Vol: 5, Issue: 1, Feb, Pp: 121 – 131, DOI: 10.1109/JIOT.2017.2774286.

Matlala, Ramolobi L.G. 2016. Defining e-policing and smart policing for law enforcement agencies in Gauteng Province, Vol: 3, Issue: 12, Pp: 3058-3070, http://valleyinternational.net/ index.php/our-jou/theijsshi.

Mehr, Hila. 2017. Artificial Intelligence for Citizen Services and Government, artificial intelligence for citizen services and government, pp:1-19.

Pop, Madalin-Dorin & Proetean, Octavian. 2018. A Comparison between Smart City Approaches in Road Traffic Management, Journal: Procedia - Social and Behavioral Sciences, Vol: 238, Pp: 29-36, https://doi.org/10.1016/j.sbspro.2018.03.004.

Royakkers, Lambèr & Timmer, Jelte & Kool, Lindavan Est, Rinie. 2018. Societal and ethical issues of digitization, Ethics and Information Technology, 20, pp:127–142. https://doi.org/10.1007/s10676-018-9452-x

Rauch, Erwin & Dallasega, Patrick & Matt, Dominik T. 2016. The Way from Lean Product Development (LPD) to Sma, Procedia CIRP 50, Pp: 26–31, http://creativecommons.org/licenses/by-nc-nd/4.0/.

Realini, Carolina E. & Marcos, Begonya. 2014. Active and intelligent packaging systems for a modern society, Meat Science, Vol: 98, Issue: 3, November, Pp: 404-419, https://doi.org/ 10.1016/j.meatsci.2014.06.031.

Stratigea, Anastasia. 2012. The concept of 'smart cities'. Towards community development?, in H. Bakis, ed,. Digital Territories – Case Studies, Special Issue, NETCOM, 26: 3–4, pp: 375–388.

Tian, Nianfeng & Ding, Tao & Yang, Yongheng & Guo,Qinglai & Sun, Hongbin & Blaabjerg, Frede. 2018. Confidentiality preservation in user-side integrated energy system management for cloud computing, Applied Energy, Vol: 231, Issue: 1, December, Pp: 1230-1245, https://doi.org/10.1016/j.apenergy.2018.09.068

Verma, Prabal& Sood, Sandeep K. 2018. Cloud-centric IoT based disease diagnosis healthcare framework, Elsevier Journal of Parallel and Distributed Computing, Vol: 116, June, Pp: 27-38, https://doi.org/10.1016/j.jpdc.2017.11.018