Sciences and Techniques of Information Management
Volume 10, Issue 3, 2024
University of Qom

Identifying Crime Prediction Strategies in Schools Using the Internet of Things (IOT)

Saman Abdolahi
Assistant Professor, Department of Law, Naragh Branch, Islamic Azad University, Naragh, Iran.
mr.samanabdolahi@gmail.com

Abstract

Purpose: The establishment and implementation of information and communication technology (ICT) in combating crime have made some societies more modern and innovative in crime detection. Accordingly, societies equipped with modern capabilities have greater opportunities. To enhance identification and intervention in this area, it is essential to propose a system that utilizes social tools from the Internet of Things to support the identification of criminals and the prediction of crime in the real world. One of the most critical areas for implementing the Internet of Things (IoT) to predict crimes is within schools. Students represent both the most vital and vulnerable components of the educational system and the national capital of any country. Therefore, it is essential to leverage modern technologies for crime prediction in schools. The purpose of this study is to investigate the role of the Internet of Things in predicting crimes in schools.

Method: This article is focused on its purpose and employs quantitative methods and surveys for implementation. The statistical population for this research consists of experts and criminologists in Tehran in 2023. The sample size was determined using the formula for an indefinite population. In a pilot study involving 30 questionnaires, the variance of the original sample was found to be 0.32. Ultimately, 157 individuals were selected as the sample using a simple random sampling method. The instrument used in this research is a researcher-developed questionnaire focused on the Internet of Things in schools, specifically regarding crime prediction. The data collected were analyzed using statistical inference tests and structural equation modeling.

Findings: The structural relationship analysis revealed that the direct effect of "Internet of Things capabilities" on crime prediction, with a coefficient of 0.81, indicates that these capabilities can significantly contribute to predicting crime in schools. In second place, the "Internet of Things applicability in identifying crime patterns, with a coefficient of 0.63, significantly influences crime prediction in schools. Finally, the "Internet of Things functional requirements in schools, with a coefficient of 0.52, also impacts crime prediction in educational settings. Overall, these modeling results align with the inferential findings from testing the hypotheses.

Conclusion: By using the Internet of Things in environmental design and maintenance, we can enhance local safety and environmental control, identify crime patterns, increase police awareness of criminal activity, conduct crime analysis, and utilize artificial intelligence algorithms. This approach enables us to accurately predict the occurrence of crimes in specific locations and take proactive measures to prevent them. Therefore, specialized systems and infrastructures for the development of

Cite this article: Abdolahi, S. (2024). Identifying Crime Prediction Strategies in Schools Using the Internet of Things (IOT). *Sciences and Techniques of Information Management*, 10(3): 325-350.
https://doi.org/10.22091/ STIM.2025.10372.2063

Received: 2024-09-18 ; **Revised:** 2024-11-03 ; **Accepted:** 2024-12-10 ; **Published online:** 2024-09-23
 Article type: Research Article **Published by:** University of Qom.

the Internet of Things (IoT) in schools and other critical and sensitive locations should be utilized effectively, and appropriate platforms should be established to support their development. Therefore, planners, policymakers, and criminologists can leverage real data to significantly manage crime prevention processes in schools, thereby reducing the incidence of crime as the infrastructure develops.

Keywords: Internet of Things, Schools, Students, Crime prediction, Crime prevention.

علوم و فنون مدیریت اطلاعات
دوره ۱۰، شماره ۳، ۱۴۰۳

شناسایی راهبردهای پیش‌بینی جرایم در مدارس با استفاده از اینترنت اشیا

سامان عبدالهی
استادیار، گروه حقوق، واحد نراق، دانشگاه آزاد اسلامی، نراق، ایران. mr.samanabdolahi@gmail.com

چکیده

هدف: راه‌اندازی و پیاده‌سازی فناوری اطلاعات و ارتباطات و به کارگیری آن در مقابله با جرایم در هر جامعه باعث شده برخی جوامع در جرم‌یابی مدرن‌تر و پیشگام‌تر باشند. بر این اساس، چنین جوامعی با ظرفیت‌هایی مدرن، دارای فرصت‌های بیشتری هستند و برای شناسایی و مداخله در این حوزه، پیشنهاد سیستمی مبتنی بر ابزارهای اجتماعی اینترنت اشیا، برای پشتیبانی از شناسایی مجرمان و پیش‌بینی جرم در دنیای واقعی لازم و ضروری به نظر می‌رسد. یکی از مهم‌ترین اماکنی که لازم است اینترنت اشیا برای پیش‌بینی جرایم به کار گرفته شود، مدارس هستند. دانش‌آموزان نیز مهم‌ترین و حساس‌ترین عناصر نظام آموزشی و سرمایه‌های ملی هر کشوری بوده و لازم است در زمینه پیش‌بینی جرایم در مدارس، از فناوری‌های نوین استفاده کرد. بر همین اساس، هدف پژوهش حاضر بررسی نقش اینترنت اشیا در پیش‌بینی جرایم در مدارس است.

روش: این پژوهش از نظر هدف کاربردی و از نظر شیوه اجرا، کمّی و پیمایشی است. جامعه آماری پژوهش کارشناسان و جرم‌شناسان شهر تهران در سال ۱۴۰۲ هستند که از طریق فرمول حجم نمونه جامعه نامعین و در یک بررسی آزمایشی از ۳۰ پرسشنامه، واریانس نمونه اولیه ۰/۳۲ به دست آمده که در نهایت ۱۵۷ نفر با روش تصادفی ساده به عنوان نمونه انتخاب شدند. ابزار پژوهش حاضر، پرسشنامه محقق‌ساخته اینترنت اشیاء در مدارس مبتنی بر پیش‌بینی جرم است که داده‌های آن از طریق آزمون‌های استنباط آماری و مدل‌سازی معادله ساختاری تحلیل شده‌اند.

یافته‌ها: در تحلیل روابط ساختاری نتایج حاصل از مدل‌سازی نشان داد که اثر مستقیم «قابلیت‌های اینترنت اشیا» بر پیش‌بینی جرم با ضریب (۰/۸۱) گویای این واقعیت است که «قابلیت‌های اینترنت اشیا» می‌تواند بر پیش‌بینی جرم در مدارس موثر باشد. در جایگاه دوم نیز «کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم» با ضریب (۰/۶۳) بر پیش‌بینی از جرم در مدارس تاثیر داشته و نهایتاً «الزامات عملکردی اینترنت اشیا در مدارس» با ضریب (۰/۵۲) بر پیش‌بینی از جرم در مدارس تاثیر دارد. در مجموع، این نتایج حاصل از مدل‌سازی با نتایج استنباطی در آزمون فرضیات همسو و هم‌جهت است.

استناد به این مقاله: عبدالهی، سامان (۱۴۰۳). شناسایی راهبردهای پیش‌بینی جرایم در مدارس با استفاده از اینترنت اشیا. *علوم و فنون مدیریت اطلاعات*، ۱۰(۳): ۳۲۵-۳۵۰. https://doi.org/10.22091/STIM.2025.10372.2063

تاریخ دریافت: ۱۴۰۳/۰۶/۲۸ ؛ **تاریخ اصلاح:** ۱۴۰۳/۰۸/۱۳ ؛ **تاریخ پذیرش:** ۱۴۰۳/۰۹/۲۰ ؛ **تاریخ انتشار آنلاین:** ۱۴۰۳/۰۷/۰۲

نوع مقاله: پژوهشی **ناشر:** دانشگاه قم

نتیجه‌گیری: با به کارگیری اینترنت اشیا از طریق طراحی و نگهداری محیطی، افزایش ایمنی محلی و کنترل محیطی، شناسایی الگوهای جرم، افزایش آگاهی پلیس از وقوع جرم، تحلیل جرم و الگوریتم هوش مصنوعی می‌توان وقوع جرایم در هر مکانی را به طور دقیق پیش‌بینی کرد و مانع از بروز این جرایم شد. بنابراین، باید سیستم‌ها و زیرساخت‌های تخصصی توسعه اینترنت اشیا در مدارس و همه مکان‌های مهم و حساس، به صورت تخصصی به کار گرفته شوند و برای پیشرفت آنها بسترهای مناسب فراهم گردد. از این‌رو برنامه‌ریزان، سیاستگذاران و جرم‌شناسان می‌توانند بر پایه داده‌های واقعی، روندهای پیشگیری از جرایم را در مدارس تا اندازه زیادی تحت کنترل خود درآورند و به‌ازای هر مقدار توسعه در این زیرساخت، به همان اندازه از وقوع جرایم پیشگیری کنند.

کلیدواژه‌ها: اینترنت اشیا، مدارس، دانش‌آموزان، پیش‌بینی جرم.

۱. مقدمه

وقتی که نیروی پلیس یک رفتار مجرمانه در حال ارتکاب را کشف می‌کند، به این معنی است که در یک دوره زمانی خاص، آنها از آنچه اتفاق می‌افتد و کجا اتفاق می‌افتد، آگاه هستند (توندیس و مولهاوزر[1]، ۲۰۱۹، ص۲۸). پیشگیری از جرم زمانی محقق می‌شود که بتوان شرایط تحقق جرایم را پیش‌بینی کرد. بر همین اساس لازمه پیشگیری از جرایم، پیش‌بینی است. راه‌اندازی و پیاده‌سازی فناوری اطلاعات و ارتباطات و به کارگیری آن در مقابله با جرایم در هر جامعه، باعث شده برخی جوامع در جرم‌یابی مدرن‌تر و پیشگام‌تر باشند. بر این اساس، چنین جوامعی با ظرفیت‌هایی مدرن، دارای فرصت‌های بیشتری هستند و برای شناسایی و مداخله در این حوزه، پیشنهاد سیستمی مبتنی بر ابزارهای اجتماعی اینترنت اشیا (IoT)[2]، برای پشتیبانی از شناسایی مجرمان و پیش‌بینی جرم در دنیای واقعی لازم و ضروری به نظر می‌رسد. اینترنت اشیا را می‌توان ارتباط بین حسگرها و محرک‌ها با هدف به اشتراک گذاشتن اطلاعات در چارچوب متحد تعریف کرد؛ به طوری که عملکرد مشترکی را برای ایجاد کاربردهای خلاقانه فراهم کنند (گابی[3] و همکاران، ۲۰۱۳، ص۱۶۴۵؛ ابراهیمی، تدین و صیادحقیقت، ۱۴۰۰، ص۴).

کاربرد اینترنت اشیا در مکان‌های متعددی مورد توجه قرار گرفته است. یکی از مهم‌ترین اماکنی که لازم است اینترنت اشیا برای پیش‌بینی جرایم به کار گرفته شود، مدارس هستند. دانش‌آموزان نیز مهم‌ترین و حساس‌ترین عناصر نظام آموزشی و سرمایه‌های ملی هر کشور به‌شمار می‌آیند. مدرسه به عنوان یکی از مهم‌ترین مؤسسات رسمی و آموزشی هر کشوری که همه کودکان با رسیدن به سن مدرسه وارد آن می‌شوند، موظف است با ارتقای سطح دانش و آگاهی، آمادگی‌های لازم و مفید را برای آنها فراهم کند و دانش‌آموزان را در برابر رفتارهای پرخطر و امنیت اجتماعی ناسالم حفظ کند. امروزه اگر اقدامات لازم برای پیش‌بینی، کنترل و کاهش آسیب‌های اجتماعی[4] انجام نشود، بدون شک سرمایه‌های ارزشمند مادی، معنوی، انسانی و اجتماعی که دانش‌آموزان هستند، از دست خواهند رفت (بارنت[5]، ۲۰۲۰، ص۱۹). بر همین اساس لازم است در زمینه پیش‌بینی جرایم در

1. Tundis & Mühlhäuser
2. Internet of things
3. Gubbi

٤. محیط مدرسه ممکن است مسائل مختلفی را در مورد دانش‌آموزان آشکار نماید: شکست تحصیلی، مردود شدن‌های مکرر، غیبت مکرر، رفتارهای اخلال‌گر و آشوب‌گر، تخریب و ویران‌گری، خشونت، اخراج دائمی، توجه صرف مربیان به دانش‌آموزان نخبه، خودداری و تردید مربیان در وارد کردن دانش‌آموزان در امور مدرسه، عدم دسترسی دانش‌آموزان به آموزگاران، فقدان انضباط، شلوغ بودن کلاس‌ها... (کاری یو، ۱۳۸۱، ص۲۷۸).

5. Barnett

مدارس از فناوری‌های نوین استفاده کرد. از همین‌رو، پس از وقوع شبکه جهانی وب، اینترنت اشیا با توجه به افزایش چشمگیر اینترنت می‌تواند انقلاب بعدی باشد و این سازه به‌دنبال ایجاد پلی بین دنیای واقعی و مجازی است که توانمندی ایجاد شبکه‌ای یکپارچه از میلیاردها اشیا با قابلیت اتصال بی‌سیم به یکدیگر، جهت تبادل اطلاعات دارد (اصغری‌نژاد، رزقی‌شیرسوا و خانزادی، ۱۴۰۳، ص۱۵۲). لذا، با توجه به اهمیت اینترنت اشیا در مدارس امروزی، ضرورت استفاده از این فناوری برای پیش‌بینی جرایم احساس می‌شود. به عبارت دیگر، ابزارهای اینترنت اشیا دارای سازندگانی هستند که از قابلیت دسترسی به اطلاعات این ابزارها برخوردار بوده و از امکان کنترل آنها نیز بهره‌مند هستند (صادقی و ناصر، ۱۳۹۹، ص۸۶).

بنابراین، لزوم کنترل آن توسط مراجع ذی‌صلاح یک ضرورت مهم است. اهمیت کاربرد فناوری‌های نوین در مدارس، به قابلیت وصل شدن ابزارآلات مختلف به اینترنت، و هوشمند شدن آن‌ها با دستور گرفتن از یک منبع مشخص در بستر اینترنت اشیا امکان‌پذیر است. در چنین شرایطی یک سیستم مبتنی بر اینترنت اشیا پیشنهاد می‌شود که هدف آن تقویت ارتباط بین شهروندان و نیروهای پلیس است که این سیستم بر روی دستگاه‌های تلفن‌های هوشمند متمرکز بوده و بر روی یک رویکرد معماری جدید تکیه می‌کند. آنچه به عنوان هدف اصلی در این پژوهش دنبال می‌شود، شناسایی راهبردهای پیش‌بینی جرایم در مدارس با استفاده از اینترنت اشیا است که در بسیاری از کشورها دنبال شده و تجارب موفقی از آن در دسترس است. با توجه به اهمیتی که پیشگیری از جرم در مدارس دارد، بنابراین، کشف هر راهبرد جدیدی باید با آغوش باز مورد استقبال قرار گیرد. از این‌رو با توجه به جدید بودن موضوع اینترنت اشیا در ایران، اولاً پیشینه‌های این حوزه بسیار محدود بوده و ثانیاً، می‌توان اهمیت و ضرورت آن را بسیار لازم دانست.

در این راستا، پژوهش حاضر درصدد پاسخ به این سوال است که چه راهبردهایی برای پیش‌بینی جرایم در مدارس با استفاده از اینترنت اشیا وجود دارد؟ بر همین اساس هدف پژوهش حاضر بررسی نقش اینترنت اشیا در پیش‌بینی جرایم در مدارس است.

۲. ادبیات مفهومی و نظری

ادبیات مفهومی این پژوهش بر دو حوزه مهم متمرکز است. اول اینترنت اشیا را تعریف و بررسی می‌کند و در گام دوم کاربرد اینترنت اشیا در مدارس را از لحاظ پیش‌بینی جرم مورد مطالعه قرار می‌دهد. ادبیات نظری هم به طور مفصّل الزامات عملکردی اینترنت اشیا در مدارس، قابلیت‌های اینترنت اشیا در مدارس و کاربردپذیری اینترنت اشیا را در شناسایی الگوهای جرم بررسی می‌کند.

۲-۱. الزامات عملکردی اینترنت اشیا در مدارس

اینترنت اشیا سیستمی از دستگاه‌های به هم پیوسته است که هنگام برقراری ارتباط با اینترنت، منابع و داده‌ها را به طور ایمن به اشتراک می‌گذارند. استفاده فراگیر از اینترنت اشیا توسعه اختراعات متعددی ازجمله اتوماسیون خانگی، فناوری پوشیدنی، آتش‌نشانی هوشمند، اندازه‌گیری هوشمند، تولید پیشرفته و ساختمان‌های هوشمند را تسهیل کرده و زندگی را برای انسان آسان‌تر نموده است (مظهر[1] و همکاران، ۲۰۲۲، ص۲). همچنین سیستم‌های امنیتی مبتنی بر اینترنت اشیا، مانند دوربین‌ها، از ارتکاب جرم پیشگیری، فعالیت‌های مشکوک را نظارت و دسترسی مجاز به محل مدرسه را تضمین می‌کنند. سیستم‌های واکنش اضطراری، مانند سنسورها و آلارم‌های متصل، می‌توانند به نهادهای ذی‌ربط هشدار دهند و دستورالعمل‌های ضروری را برای مقابله و پیشگیری به‌کار گیرند (مالاسو[2] و همکاران، ۲۰۲۴، ص۲۹۴). علاوه‌بر این، اینترنت اشیا از طریق افزایش یادگیری از راه دور، از بروز بسیاری از خطرات احتمالی در مسیر مدرسه پیشگیری می‌نماید. طبیعتاً دستگاه‌های اینترنت اشیا در مدارس امنیت بسیاری از دانش‌آموزان را در مسیر تردد در مناطق پرخطر تضمین می‌کند (مالاسو و همکاران، ۲۰۲۴، ص۲۹۴). علاوه‌بر این، دستگاه‌های معمولی اینترنت اشیاء که در مدارس یافت می‌شوند، عبارتند از: لپ‌تاپ، تبلت، سیستم‌های روشنایی، گرمایش، تهویه، دوربین‌های امنیتی و قفل‌ها، چاپگرها و دستگاه‌های کپی، بردهای هوشمند و نمایشگرهای تعاملی. بنابراین، درک پذیرش گسترده دستگاه‌های اینترنت اشیا در مدارس به دلیل مزایایی که برای تجارب یادگیری پیشرفته ایجاد می‌کنند، آسان است (مالاسو[3] و همکاران، ۲۰۲۳، ص۱۳۶). پیشرفت‌های اخیر در فناوری اینترنت اشیا و ارتباط آنها با جرم‌شناسی، نشان می‌دهد که مسأله اینترنت اشیا پدیده نوظهوری برای پیش‌بینی هوشمندانه و واقع‌گرایانه مرتبط با جرایم احتمالی هستند. با استقرار سیستم مبتنی بر اینترنت اشیا در بیشتر جوامع، مدیران و برنامه‌ریزان می‌توانند با استفاده از سنسورهای جاسازی‌شده، محیط را بهتر کشف کنند. آن‌ها می‌توانند در هر زمان به تحولات محیطی و سایر اطلاعات دسترسی پیدا کنند. با اینکه تکنولوژی‌های نوین نظیر شهرهای هوشمند، کنترل‌های الکترونیکی، محتواهای الکترونیکی و تجهیزات هوشمند توانسته‌اند تأثیر مثبتی بر تغییرات جامعه داشته باشند؛ اما هنوز نتوانسته‌اند چالش‌های امنیتی جامعه را به‌خوبی رفع کنند. به طور کلی، توجه به الزامات عملکردی اینترنت اشیا در مدارس می‌تواند زمینه پیش‌بینی جرایم را فراهم نماید که به‌تبع

1. Mazhar
2. Malasowe
3. Malasowe

آن از جرایم در مدارس پیشگیری کند.

۲-۲. قابلیت‌های اینترنت اشیا در مدارس

تا سال ۲۰۲۰، سیستم‌های اطلاعات جغرافیایی (GIS) ابزار یادگیری غیرماشینی بودند که قبلاً برای داده‌های زمانی و مکانی استفاده می‌شدند. اما بعد از سال ۲۰۲۰، سیستم‌های اطلاعات جغرافیایی به عنوان ابزاری برای تحلیل نقاط جرم استفاده شده و توانستند به کاهش نرخ جرم کمک کنند (کونادی[1] و همکاران، ۲۰۲۰، ص۲). بر همین اساس و با استفاده از تحلیل سیستم‌های اطلاعات جغرافیایی به عنوان یک قابلیت مهم در اینترنت اشیا، پیش‌بینی نرخ جرم را می‌توان به عنوان روشی برای ایجاد سیستمی برای یافتن الگوهای آتی جرم و کمک به مجری قانون برای حل جرم که منجربه کاهش نرخ آن در دنیای واقعی می‌شود، تعریف کرد. در این میان، پیش‌بینی جرم به توانایی پیش‌بینی جرایم در آینده، تا سال‌های آینده برای افزایش پیشگیری از وقوع جرم اشاره دارد و این امر می‌تواند با استفاده از رویکردهای سری زمانی برای یافتن روند جرم در آینده از داده‌های سری زمانی محقق شود (سعید و عبدالمحسن[2]، ۲۰۲۳، ص۳). به طور کلی، قابلیت‌های اینترنت اشیا در مدارس با استفاده از روش‌های مختلف ازجمله روش‌های آماری، روش‌های تجسّم پوششی، یادگیری بدون نظارت و تکنیک‌های یادگیری نظارت شده می‌تواند روند جرایم را پیش‌بینی کند. روش‌های تجسّم شامل توضیح بصری ارتباط بین نمای جغرافیایی و سایر داده‌های جرم مانند پروفایل جغرافیایی نقشه‌برداری جرم مبتنی بر سیستم‌های اطلاعات جغرافیایی، پیش‌بینی جرم و نقشه‌برداری نامتقارن است (جانگرا و کالسی[3]، ۲۰۱۹، ص۳۴). توسعه الگوریتم‌های یادگیری ماشینی به محققان تجزیه و تحلیل داده‌های جرم کمک می‌کند تا با استفاده از مدل‌های یادگیری ماشینی تحت نظارت و بدون نظارت، این داده‌ها را تجزیه و تحلیل کنند و آن‌ها را براساس تکنیک‌های پیش پردازش و خوشه‌بندی برای استخراج مکان‌های جرم از داده‌های مشخصی بررسی نمایند. از دیگر قابلیت‌های اینترنت اشیا الگوی مبتنی بر زمان و مکان جرم برای تولید پیش‌بینی‌های دقیق است. علاوه‌بر این، توسعه الگوریتم‌های یادگیری ماشینی به بررسی دلایل وقوع جرم در مناطق خاص با استفاده از الگوریتم‌های یادگیری ماشینی می‌پردازد. یادگیری ماشینی هم بر پایه داده‌های جمع‌آوری شده از سال‌های گذشته و سوابق ارتکاب جرم در همان منطقه به پیش‌بینی از جرم کمک می‌کند (سردانا و همکاران[4]، ۲۰۲۱،

1. Kounadi
2. Saeed & Abdulmohsin
3. Jangra & Kalsi
4. Sardana

ص۴۴). پیشگیری وضعی که به دنبال تغییر وضعیت‌های ماقبل جنایی به منظور انصراف بزهکارانی است که اندیشه مجرمانه در ذهن آنها شکل گرفته و خواهان جامه عمل پوشیدن است (دارابی، ۱۳۹۷، ص۱۳۲)، این قابلیت را دارد که حفاظت از دانش‌آموزان را در برابر موضوعات مختلف مانند قلدری، خشونت، آزار و اذیت و سایر انواع بزهکاری و جرایم شایع در مدرسه ارتقاء دهد. این حفاظت را می‌توان در طول روز در مدرسه اعمال کرد و شامل طیف گسترده‌ای از اقدامات فیزیکی حمایتی مانند دوربین‌های امنیتی است که به نظارت بر فعالیت دانش‌آموزان و مهار تمایل به ارتکاب جرم کمک می‌کند (واتکینز[1]، ۲۰۱۵، ص۱۷). این امر به نوبه خود می‌تواند رفاه نه‌تنها دانش‌آموزان، بلکه معلمان و کارکنان را بهبود بخشد.

اینترنت اشیا از طریق ایمن‌سازی مدارس و کنترل دوربین می‌تواند راهبردهای پیشگیری از جرم را در مدارس توسعه دهد. برخی اقدامات پیشگیرانه از جرم در مدارس از طریق اینترنت اشیا در چند حوزه اصلی تحقق می‌یابد. این اقدامات شامل، طراحی و نگهداری محیطی، سیستم‌های الکترونیکی هوش مصنوعی و واکنش فوری به حادثه است. به طور کلی سیستم اینترنت اشیا در قالب دوربین‌های مداربسته و تحلیل داده‌های آن با کاهش قابل توجه و متوسط جرایم همراه است. بیشترین و ثابت‌ترین اثرات در اماکنی که تحت نظر هستند، بر پایه نظارت مبتنی بر اینترنت اشیا به گسترش دامنه خود در فضای عمومی و خصوصی ادامه می‌یابد و این فرایند با فناوری جدیدی در حال تکامل بوده و به این شکل روند سیاست‌گذاری از اجرا و ارزیابی نتایج باکیفیت سود خواهد برد (پیزا و همکاران[2]، ۲۰۱۹، ص۱۳۶). بر همین اساس، قابلیت‌های اینترنت اشیا و استقرار سیستم مبتنی بر اینترنت اشیا می‌تواند در اماکنی مانند مدارس از بروز بسیاری از جرایم احتمالی پیشگیری کند. از همین‌رو، تاکنون رویکردهای مختلفی در مورد پیشگیری از جرم اتخاذ شده است؛ یکی از این رویکردها، پیشگیری از طریق طراحی محیطی[3] است. این رویکرد از توجه به نقش محیط بشرساز در وقوع جرم ریشه گرفته است (محمدنسل، ۱۳۹۳).

این نوع پیشگیری نخستین بار توسط جرم‌شناس آمریکایی، سی. ری جفری[4] در کتابی با همین عنوان ارائه شد. این نظریه بر این اندیشه مبتنی است که رفتار انسانی در محیط، تحت تاثیر طراحی آن محیط قرار دارد و از شش جزء شامل: تعیین قلمرو، نظارت، کنترل دسترسی، تصویر محیط (حفظ و

1. Watkins
2. Piza, Welsh, Farrington & Thomas
3. CPTED
4. C. Ray Jeffrey

نگهداری محیط)، سخت کردن آماج جرم و فعالیت‌های پشتیبانی تشکیل شده است (محمدی جانکی و قورچی بیگی، ۱۳۸۸، ص۳۴۵). با توجه به این نظریه، اینترنت اشیا از طریق اطلاعات مکانی و زمانی جرم و با استفاده اطلاعات جرایم و براساس درصد اندازه‌گیری دقت کار قبلی، الگوریتم‌هایی برای پیش‌بینی از جرم طراحی می‌کند که دقت بسیار بالایی در پیشگیری از جرم را ممکن می‌سازد (سعید و عبدالمحسن، ۲۰۲۳، ص۲). از طرفی هم سیستم‌های ساختمان هوشمند مانند روشنایی خودکار و سیستم‌های امنیتی، ضمن کاهش هزینه‌ها، احساس امنیت در مدارس و محیط‌های آموزشی را بیشتر می‌کنند. به طور کلی، سیستم‌های امنیتی مبتنی بر اینترنت اشیا، مانند دوربین‌ها، از جرایم پیشگیری می‌کنند، بر فعالیت‌های مشکوک نظارت کرده و دسترسی مجاز به محل مدرسه را تضمین می‌کنند. علاوه‌بر این، سیستم‌های واکنش اضطراری، مانند سنسورها و آلارم‌های متصل، می‌توانند به سرعت به مقامات هشدار دهند و پروتکل‌های اضطراری را در صورت آتش‌سوزی، جراحت یا حوادث دیگر آغاز کنند (مالاسو و همکاران، ۲۰۲۴، ص۲۹۶). این قابلیت و بسیاری از قابلیت‌های دیگر که به آنها اشاره شد، می‌تواند در زمینه پیشگیری و پیش‌بینی جرایم شایع در مدارس مفید باشد.

۲-۳. کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم

مدارس انبوهی از اطلاعات شخصی ارزشمند در مورد دانش‌آموزان[۱]، کارکنان و والدین ازجمله نام، آدرس، شماره، شغل و... را در اختیار دارند. این داده‌ها دقیقاً همان چیزی است که مجرمان به دنبال آن هستند و می‌توانند برای ارتکاب جرایم مختلفی از قبیل سرقت، کلاهبرداری و... استفاده شوند. بنابراین، دامنه جرایم در مدارس می‌تواند بسیار گسترده باشد (مالاسو و همکاران، ۲۰۲۴، ص۲۹۵). از این‌رو، کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم بسیار مهم هستند. در این راستا تجزیه و تحلیل سیستم اینترنت اشیا در مدارس در مورد عملکرد سیستم افزایش جرم صحبت می‌کند. این سیستم دارای سه کاربر مختلف عموم مردم، افسران پلیس و مدیر است. برای اینکه هر شخصی هر جرمی را گزارش کند، باید با هر وسیله ارتباطی که از طریق اینترنت پشتیبانی می‌شود، از پلتفرم بازدید کند، در هنگام ورود به پلتفرم، کاربر روی دکمه «آپلود یا گزارش جرم» که فرمی را باز می‌کند، کلیک می‌کند. جایی که فرد می‌تواند مشخصات جرم مشکوک مشاهده شده را وارد کند یا حتی در صورت ثبت، هرگونه فایل تصویری جرم را بارگذاری کند. سپس بر روی ارسال کلیک کند.

۱. در مدارس ایران حضور برخی دانش‌آموزان در مسیر تردد مدارس همیشه طعمه مناسبی برای مجرمان حرفه‌ای بوده و با به دست آوردن اطلاعات مهم دانش‌آموزان، امکان سوءاستفاده از آنها فراهم می‌شود.

هنگامی که گزارش جرم با موفقیت انجام شد، شخص یک پیام موفقیت‌آمیز را به عنوان یک اعلان تایید دریافت می‌کند. حساب کاربری افسران پلیس باید از طریق یک پیوند ورود به سیستم دسترسی داشته باشد که قبل از ورود به داشبورد باید تأیید شود. داشبورد به کاربر پلیس اجازه می‌دهد موارد گزارش جرم را مشاهده کند، گزارش‌های جرم را رصد نموده و فوراً خودروی گشت پلیس را برای اقدام فوری مطلع کند. پس از اینکه اعلان با موفقیت انجام شد، همین اطلاعات موجود به منظور بایگانی جهت بررسی و پیش‌بینی ارتکاب جرم در آینده در پایگاه داده ذخیره می‌شود. کاربر مدیر، کاربری با نقش بالا در پلتفرم است، کاربر با ثبت نام عضو جدید نیروی انتظامی و همچنین ثبت جرم جدید در پایگاه داده، به بررسی و نظارت بر فعالیت سایر کاربران در پلتفرم دسترسی دارد و گزارش جرم اکنون برای همه شهروندان آسان و قابل دسترسی است. همه گزارش‌ها در سیستم مدیریت پایگاه داده توزیع شده ذخیره می‌شود که همه عوامل نیروی پلیس از طریق شناسه خود برای ورود به سیستم دسترسی دارند (چاینمرم و آئو[1]، ۲۰۲۳، ص۱۷۰). در چنین وضعیتی کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم نقش تعیین‌کننده‌ای دارند. در نهایت داده‌های اینترنت اشیا چارچوبی آسان برای پیاده‌سازی نقشه جغرافیایی جرم است که به کارآگاهان و سایر افسران مجری قانون کمک می‌کند تا در جرم‌یابی به موفقیت‌هایی دست یابند. این الگو بعضاً برای مقابله با جرایم در هر مکانی مناسب است (ناث[2]، ۲۰۰۶، ص۴۲). به طور کلی اینترنت اشیا سیستمی است که به عموم مردم اجازه می‌دهد تا یک جنایت را گزارش داده و همچنین به نیروی پلیس این امکان را می‌دهد که به راحتی قربانی جرم را از طریق پیوند رایگان و در دسترس گزارش جرم توسط عموم مردم، ردیابی و نظارت کند (چاینمرم و آئو، ۲۰۲۳، ص۱۷۱).

همچنین این امر باعث تسریع آگاهی پلیس از وقوع جرم می‌شود. اصولاً وقوع یک رفتار مجرمانه می‌تواند در هر زمان و هر مکانی رخ دهد. در نتیجه بعید است پلیس در زمان وقوع جرم در صحنه جرم حضور داشته باشد. در صورت عدم حضور در صحنه جرم، اولین مشکل مربوط به زمان آگاهی نیروهای پلیس از ارتکاب جرم است. به طور معمول، اطلاعات اولیه مربوط به گزارش جرم از سمت شهروندان می‌آید. در نتیجه برای ارائه اطلاع دقیق محل وقوع جرم و مجرم به پلیس، لازم است تکنولوژی اینترنت اشیا آگاهی پلیس از وقوع جرم را در کمترین زمان انجام دهد (الحولی[3]، ۲۰۱۷، ص۱۷۶؛ قنبری، ۱۴۰۲، ص۱۴). در همین راستا، رشد حیرت‌انگیز استفاده از هوش مصنوعی در

1. Chinaemerem & Ao
2. Nath
3. Alohali

حوزه‌های حمل و نقل، بهداشت و سلامت و...، بر کسی پوشیده نیست. امروزه نظام عدالت کیفری نیز برای حل برخی از مسائل و مشکلات خود در زمینهٔ پیشگیری از تکرار جرم، به این ابزار فناورانه متکی است (ابراهیمی، ۱۴۰۱، ص۳۳). روش‌های هوش مصنوعی که به عنوان داده‌های واقعی یا داده‌های جرم طبقه‌بندی می‌شوند، تکنیکی برای شناسایی مجرمان به ویژه مجرمان س صایبری را با ارزیابی ورودی‌های به دست آمده از افراد تجویز می‌کند و از طریق گروه‌بندی و یا خوشه‌بندی اطلاعات معتبر (خوشه صفر) با حفظ اطلاعات غیرمعتبر (خوشه ۱) خارج می‌شود. با استفاده از اطلاعات واقعی، داده‌های غیرمعتبر به عنوان اطلاعات جرم و با استفاده از اطلاعات جرم و منفی واقعی به عنوان اطلاعات تایید شده در نظر گرفته می‌شود که سپس به خوشه (۰) اضافه می‌شود. سپس با استفاده از طبقات متعدد، اطلاعات مجرمانه بررسی می‌شود. به عنوان مثال، هیچ نرم‌افزار و سخت‌افزاری برای تشخیص کلاهبرداری وجود ندارد، اما تکنیک‌های مختلف خوشه‌بندی برای مشتریان مختلف با کاراکترها/ اعتبارات نوسانی استفاده می‌شود که در آن بررسی اطلاعات برای مقادیر مختلف وجود دارد و مشخصات مجرم مربوط به جرایم سایبری برای ارزیابی‌های مختلف ارزیابی می‌شود. در روش یادگیری نظارت شده، مدلی برای پیش‌بینی براساس شواهد در شرایط عدم قطعیت شکل می‌گیرد. از طریق محاسبات الگوریتم‌های تطبیقی، نمونه‌های اطلاعاتی را می‌توان حل کرد، که این حل مساله باعث می‌شود رایانه شخصی بهتر خطرات را درک کند. با تعداد بیشتر ادراک، اجرای پیش‌بینی شده رایانه شخصی نیز بهبود می‌یابد. یک محاسبه یادگیری تنظیم‌شده به جمع‌آوری اطلاعات در دسترس فکر می‌کند و نوع واکنش‌های شناخته‌شده به اطلاعات را نشان می‌دهد. در نتیجه محاسبه در آن نقطه، مدلی را برای ارائه انتظارات معقول در پرتو اطلاعات جدید آماده می‌کند (وینا و همکاران[1]، ۲۰۲۲، ص۳). به طور کلی منطق سیستم اینترنت اشیا با استفاده از تکنیک‌های شبیه‌سازی ارزیابی شده و این سیستم یک حالت عملیاتی شبیه‌سازی شده را ارائه می‌دهد که در آن نقش شهروندان و مجرمان توسط شهروندان مجازی و مجرمان مجازی جایگزین و شبیه‌سازی می‌شود. این محیط شبیه‌سازی نه‌تنها برای ارزیابی رفتار و عملکرد الگوریتم‌های پیشنهادی فعلی استفاده می‌شود، بلکه امکان پشتیبانی از تعریف و ارزیابی الگوریتم‌های اضافی پیچیده‌تر را نیز فراهم می‌کند. در واقع، عملکرد واقعی آن براساس برنامه‌های نصب شده بر روی دستگاه‌های تلفن همراه ارزیابی شده و برای تخمین اثربخشی آن باید در مناطق ویژه‌ای مورد آزمون قرار گیرد، تا با برآورد مداخله فوری در مکان و صرفه‌جویی در زمان آن اثبات شود. در سال‌های اخیر داده‌کاوی به عنوان

1. Veena

تکنیک‌هایی به منظور تجزیه و تحلیل داده‌های جرمی که قبلاً از منابع مختلف ذخیره شده‌اند، برای یافتن الگوها و روند جرایم استفاده می‌شود. علاوه‌بر این، می‌توان از داده‌کاوی برای افزایش کارایی در حل سریع‌تر جرایم و همچنین برای اعلام خودکار جرایم استفاده کرد. با این حال، تکنیک‌های مختلفی از داده‌کاوی وجود دارند که به منظور افزایش کارایی کشف جرم، لازم است به طور مناسب انتخاب شوند (تانگساتاپورنواتانا[1]، ۲۰۱۶، ص۱۲۳). به این ترتیب کاربردپذیری اینترنت اشیا می‌تواند در زمینه شناسایی الگوهای جرم در مدارس بسیار موثر باشد.

۳. روش پژوهش

این پژوهش از نظر هدف، کاربردی و از نظر شیوه اجرا، کمّی و پیمایشی است. بر پایه ادبیات نظری، فرض‌هایی برای برررسی رابطه بین پیش‌بینی جرایم در مدارس و استفاده از اینترنت اشیا در نظر گرفته شده است و سپس با شاخص‌سازی این متغیرها، اطلاعات مورد نیاز جمع‌آوری و آزمون‌های متناسب انجام شده است. جامعه آماری پژوهش شامل کارشناسان و جرم‌شناسان شهر تهران در سال ۱۴۰۲ هستند. با توجه به نامعین بودن این افراد، از فرمول حجم نمونه برای جوامع نامعین استفاد ه شده است. برای این کار در یک بررسی آزمایشی، از ۳۰ پرسشنامه واریانس نمونه اولیه معادل ۰/۳۲ برآورد شده و با پذیرش ۰/۰۵ درصد خطا، حجم نمونه طبق فرمول کوکران ۱۵۷ نفر برآورد گردید که با توجه به پرسشنامه‌های تکمیل شده، ۱۵۵ پرسشنامه صحیح مبنای تحلیل قرار گرفته‌اند. روش نمونه‌گیری نیز به صورت تصادفی ساده بوده که پرسشنامه‌های موجود در میان کارشناسان و جرم‌شناسان شهر تهران توزیع و جمع‌آوری شده است. ابزار گردآوری اطلاعات، پرسشنامه محقق‌ساخته اینترنت اشیاء در مدارس مبتنی بر پیش‌بینی جرم است که برپایه ادبیات نظری سوالات هر متغیر طراحی و در طیف ۵ گانه لیکرت استفاده شد. روایی صوری توسط اساتید مربوطه و پایایی آن براساس ضریب آلفا بالای ۰/۷ بدست آمد. تحلیل داده‌ها به کمک آزمون تحلیل رگرسیون خطی و مدل‌سازی معادله ساختاری انجام شده است.

۴. یافته‌ها

یافته‌های این پژوهش در دو بخش ارائه شده است. در بخش اول فرضیات پژوهش با استفاده از تحلیل رگرسیون خطی آزمون شده و در بخش دوم اثر همه متغیرهای مستقل بر وابسته با استفاده از یک مدل معادله ساختاری آزمون شده است. برای استفاده از تحلیل رگرسیون، پیش‌شرط‌های این

1. Thongsatapornwatana

آزمون رعایت گردید. طبق این پیش‌شرط‌ها هر دو متغیر در سطح سنجش فاصله‌ای و توزیع داده‌های گردآوری شده نیز نرمال بوده است.

۴-۱. آزمون نرمالیتی داده‌ها

قبل از انجام آزمون‌های آماری، آزمون نرمالیتی به منظور رعایت پیش‌فرض‌ها گرفته شد. این آزمون‌ها اصل فرض صفر را به کار می‌گیرند تا بررسی کنند که آیا یک نمونه از یک جامعه دارای توزیع طبیعی ناشی می‌شود یا نه. در کل هدف آزمون برای انتخاب آزمون درست جهت تحلیل فرضیه‌های پژوهش است. چرا که براساس نوع توزیع آماری داده‌ها می‌توان نوع آزمون آنها را نیز انتخاب کرد. برای مثال پیش‌فرض آزمون‌های پارامتری، نرمال بودن توزیع آماری متغیرهاست. به طور کلی می‌توان گفت که آزمون‌های پارامتری، عموماً بر میانگین و انحراف معیار استوارند. حال اگر توزیع جامعه نرمال نباشد، نمی‌توان استنباط درستی از نتایج داشت. برای بررسی توزیع آماری متغیرها از آزمون‌هایی استفاده می‌شود. این آزمون‌ها به آزمون‌های نیکویی-برازش معروف هستند. آزمون کولموگروف اسمیرنوف و آزمون کای دو، جزو آزمون‌های نیکویی-برازش هستند. اما با توجه به محدودیت‌های آزمون کای دو، معمولاً برای آزمون نرمال بودن، از آزمون کولموگروف-اسمیرنف و شاپیرو ویلك[1] استفاده می‌شود.

جدول ۱- نتایج آزمون کولموگروف اسمیرنف و شاپیرو ویلک در فرض نرمال بودن توزیع متغیرهای پژوهش

متغیر	کولموگروف اسمیرنوف		شاپیرو ویلک	
	آماره	سطح معناداری	آماره	سطح معناداری
پیش‌بینی جرم	۰/۲۶۱	۰/۲۱۱	۰/۷۶۵	۰/۲۳۶
الزامات عملکردی اینترنت اشیا در مدارس	۰/۲۴۶	۰/۱۶۲	۰/۸۲۶	۰/۳۲۳
قابلیت‌های اینترنت اشیا	۰/۳۲۳	۰/۳۱۳	۰/۸۲۷	۰/۳۴۷
کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم	۰/۳۲۵	۰/۲۵۶	۰/۸۱۵	۰/۳۴۲

جدول (۱) دو مقدار سطح معناداری را برای هر کدام از متغیرها به طور مجزا نشان می‌دهد. این مقادیر در تشخیص نرمال بودن داده‌ها تعیین‌کننده است. چنانچه سطح معناداری در آزمون کولموگروف-اسمیرنوف یا آزمون شاپیرو ویلک بیشتر از ۰/۰۵ باشد، می‌توان داده‌ها را با اطمینان بالایی نرمال فرض کرد. در غیر این صورت نمی‌توان گفت که داده‌ها توزیع‌شان نرمال است. بنابراین، متغیرهای این پژوهش نرمال هستند و در استباط آماری از آزمون‌های نرمال استفاده می‌شود. البته

1. Kolmogorov-Smirnov & Shapiro-Wilk

لازم به ذکر است که در بحث مدل‌سازی معادله ساختاری، شاخص‌های برازش نیز گویای نرمال بودن داده‌هاست.

۴-۲. فرضیه‌های پژوهش

۱) الزامات عملکردی اینترنت اشیا در مدارس بر میزان پیش‌بینی جرم اثرگذار است.

جدول ۱- تحلیل رگرسیون اثر الزامات عملکردی اینترنت اشیا در مدارس بر روی پیش‌بینی جرم

نام متغیر	R	R^2	B	Beta	T	F	Sig
الزامات عملکردی اینترنت اشیا در مدارس	۰/۶۱۲	۰/۳۶۵	۳/۸۳۶	۰/۶۱۲	۸/۹۷۲	۸۰/۴۶۹	۰/۰۰۰

همبستگی (R=۰/۶۱۲) مثبتی بین میزان الزامات عملکردی اینترنت اشیا در مدارس و پیش‌بینی جرم در مدارس وجود دارد. بر همین اساس، مقدار R^2=۰/۳۶۵ نشان می‌دهد که متغیر الزامات عملکردی اینترنت اشیا در مدارس توانسته ۳۶ درصد از واریانس متغیر وابسته (پیش‌بینی جرم) را تبیین نماید. ضریب B=۳/۸۳۶ نشان می‌دهد که به‌ازای هر واحد افزایش در متغیر مستقل (الزامات عملکردی اینترنت اشیا در مدارس)، ۳/۸۳۶ واحد به متغیر وابسته (پیش‌بینی جرم) افزوده می‌شود. با توجه به مقادیر T=۸/۹۷۲، F=۸۰/۴۶۹ و Sig =۰/۰۰۰، رابطه مشاهده شده بین دو متغیر در سطح ۹۹ درصد معنی‌دار است، لذا فرضیه فوق تایید می‌شود.

۲) قابلیت‌های اینترنت اشیا در مدارس بر میزان پیش‌بینی جرم اثرگذار است.

جدول ۲- تحلیل رگرسیون اثر قابلیت‌های اینترنت اشیا در مدارس بر روی پیش‌بینی جرم

نام متغیر	R	R^2	B	Beta	T	F	Sig
قابلیت‌های اینترنت اشیا در مدارس	۰/۷۲۴	۰/۵۲۴	۴/۰۳۵	۰/۷۲۴	۱۰/۶۵۳	۱۱۳/۴۸۲	۰/۰۰۰

براساس نتایج حاصل، همبستگی (R=۰/۷۲۴) مثبتی بین قابلیت‌های اینترنت اشیا در مدارس و پیش‌بینی جرم وجود دارد. بر همین اساس، مقدار R^2=۰/۵۲۴ نشان می‌دهد که متغیر قابلیت‌های اینترنت اشیا در مدارس توانسته ۵۲ درصد از واریانس متغیر وابسته (پیش‌بینی جرم) را تبیین نماید. ضریب B=۴/۰۳۵ نشان می‌دهد که به‌ازای هر واحد افزایش در متغیر مستقل (قابلیت‌های اینترنت اشیا در مدارس)، ۴/۰۳۵ واحد به متغیر وابسته (پیش‌بینی جرم) افزوده می‌شود. با توجه به مقادیر T=۱۰/۶۵۳، F=۱۱۳/۴۸۲ و Sig =۰/۰۰۰، رابطه مشاهده شده بین دو متغیر در سطح ۹۹ درصد معنی‌دار است، لذا فرضیه فوق تایید می‌شود.

۳) کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم در مدارس بر میزان پیش‌بینی جرم

اثرگذار است.

جدول ۳- تحلیل رگرسیون اثر کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم در مدارس بر روی پیش‌بینی جرم

نام متغیر	R	R^2	B	Beta	T	F	Sig
کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم	۰/۵۸۰	۰/۳۳۰	۳/۳۴۰	۰/۴۸۰	۵/۵۵۱	۳۰/۸۱۴	۰/۰۰۰

براساس نتایج حاصل، همبستگی (R=۰/۴۸۰) مثبتی بین کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم در مدارس و پیش‌بینی جرم وجود دارد و بر همین اساس، مقدار R^2=۰/۳۳۰ نشان می‌دهد که متغیر کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم در مدارس توانسته ۳۳ درصد واریانس متغیر وابسته (پیش‌بینی جرم) را تبیین نماید. ضریب B=۳/۳۴۰ نشان می‌دهد که به‌ازای هر واحد افزایش در متغیر مستقل (کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم در مدارس)، ۳/۳۴۰ واحد به متغیر وابسته (پیش‌بینی جرم) افزوده می‌شود. با توجه به مقادیر T=۵/۵۵۱، F=۳۰/۸۱۴ و Sig =۰/۰۰۰، رابطه مشاهده شده بین دو متغیر در سطح ۹۹ درصد معنی‌دار است، لذا فرضیه فوق تایید می‌شود. برای اطمینان بیشتر در بررسی روابط، مدل معادله ساختاری پژوهش نیز آزمون شده است.

۴-۳. مدل کلی پژوهش

در راستای آزمون فرضیه‌های پژوهش از مدل‌سازی معادله ساختاری نیز برای آزمون مدل پژوهش استفاده است. در این مدل ۲۳ متغیر مشاهده شده وجود دارد که این متغیرها از تجمیع تعداد زیادی گویه حاصل شده‌اند. برخی از متغیرهای مشاهده شده شامل متغیرهای مستقل اصلی پژوهش هستند که در مدل نظری مشخص شده و برای تبیین اثر متغیرهای مستقل بر تبیین پیش‌بینی جرم در مدارس به کار رفته‌اند. در جدول (۴) ساختار اصلی مدل با شاخص‌ها و نمادهای ترسیمی موجود در مدل مشخص شده است.

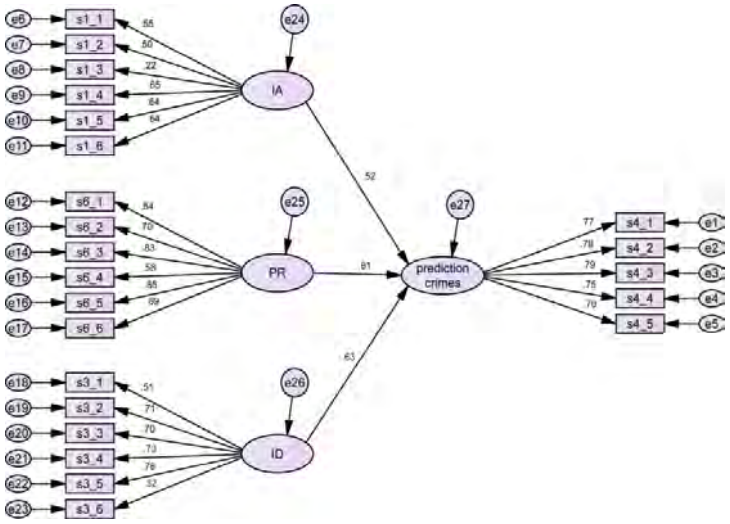
جدول ٤- متغیرها و نمادهای ترسیمی موجود در مدل

شاخص‌های اصلی	شاخص‌های فرعی	نماد ترسیمی
پیش‌بینی جرم Predicting crimes	قلدری	s4_1
	مصرف مواد مخدر	s4_2
	تجاوز و آزار جنسی	s4_3
	خشونت	s4_4
	سرقت	s4_5

شاخص‌های اصلی	شاخص‌های فرعی	نماد ترسیمی
الزامات عملکردی اینترنت اشیا در مدارس IA	تجهیز مدارس به شبکه‌های اینترنتی	s1_1
	نظارت همه‌جانبه در مدارس و امکان کنترل از راه دور	s1_2
	استفاده از بردهای هوشمند تعاملی مانند تبلت‌ها و سایر وسایل ارتباطی	s1_3
	توسعه اپلیکیشن‌های محافظتی در مدارس	s1_4
	امکان دسترسی به تحولات محیطی در هر زمان و مکان	s1_5
	به‌کارگیری الگوی مبتنی بر زمان و مکان جرم برای پیش‌بینی‌های دقیق	s1_6
قابلیت‌های اینترنت اشیا PR	استفاده از رویکردهای سری زمانی برای یافتن روند جرم در آینده	s6_1
	استفاده از تحلیل سیستم‌های اطلاعات جغرافیایی و امکان تحلیل جرم برای پیش‌بینی جرم	s6_2
	تکنیک‌های یادگیری نظارت شده برای پیش‌بینی جرم	s6_3
	استفاده از الگوریتم‌های یادگیری ماشین و تجزیه و تحلیل داده‌های جرم	s6_4
	سیستم‌های الکترونیکی هوش مصنوعی و واکنش فوری به حادثه	s6_5
	نظارت بر فعالیت‌های مشکوک و توسعه ایمن‌سازی و کنترل دوربین در مدارس برای پیشگیری	s6_6
کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم ID	ثبت اطلاعات جرایم در مدارس	s3_1
	استفاده از پلتفرم‌های گزارش جرم	s3_2
	بارگزاری اطلاعات جرم توسط کاربران	s1_3
	رصد جرایم در مدارس و شناسایی الگوهای جرایم	s3_4
	امکان گزارش جرایم توسط مردم	s3_5
	شبیه‌سازی جرایم احتمالی با اطلاعات موجود	s3_6

این متغیرهای آشکار شاخص‌های اصلی متغیرهای مستقل و وابسته هستند که در متغیرهای مستقل در سه بعد و ۱۸ متغیر مستقل تعریف شده‌اند.

متغیرهای مستقل شامل: الزامات عملکردی اینترنت اشیا در مدارس، قابلیت‌های اینترنت اشیا، کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم هستند که هر کدام با ۶ سوال در پرسشنامه تعریف و شاخص‌سازی شده‌اند. همچنین برای متغیر وابسته (پیش‌بینی جرم) نیز پنج بعد اصلی جرایم (قلدری و دعوا، مصرف مواد مخدر، تجاوز و آزار جنسی، خشونت، تقلب و دزدی) وجود دارد.



نمودار ۱- مدل معادله ساختاری برای تبیین پیش‌بینی جرم در مدارس[1]

در مدل فوق دو نوع رابطه تحلیل آماری شده‌اند که در بیان شاخص‌های «الزامات عملکردی اینترنت اشیا در مدارس» (IA) شش شاخص مختلف وجود دارد که (s1_4) یا «توسعه اپلیکیشن‌های محافظتی در مدارس» با ضریب ۰/۶۵، دارای بیشترین وزن در تبیین «الزامات عملکردی اینترنت اشیا در مدارس» بوده و (s1_3) به معنی «استفاده از بردهای هوشمند تعاملی مانند تبلت‌ها و سایر وسایل ارتباطی» نیز با ضریب ۰/۲۲ دارای وزن کمتری در تبیین «الزامات عملکردی اینترنت اشیا در مدارس» است. در تبیین «قابلیت‌های اینترنت اشیا» نیز شاخص «سیستم‌های الکترونیکی هوش مصنوعی و واکنش فوری به حادثه» یا (s6_5) با ضریب ۰/۸۵ دارای بیشترین وزن در تبیین «قابلیت‌های اینترنت اشیا» بوده است. در تعریف «کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم» یا متغیر (ID) نیز شاخص «امکان گزارش جرایم توسط مردم» یا (s3_5) با ضریب ۰/۷۸ بیشترین وزن را در تبیین «کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم» داشته است. به طور کلی همه شاخص‌های تبیینی در مدل فوق با ضرایب بالایی مثبت و معنادار شده‌اند و این به منزله تایید مدل از لحاظ شاخص‌سازی است. در بحث روابط ساختاری، نتایج حاصل از مدل‌سازی نشان داد که اثر مستقیم «قابلیت‌های اینترنت اشیا» بر پیش‌بینی جرم با ضریب (۰/۸۱) گویای این واقعیت است که «قابلیت‌های اینترنت اشیا» می‌تواند بر پیش‌بینی جرم در مدارس موثر باشد. در جایگاه دوم نیز «کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم» با ضریب (۰/۶۳) بر پیش‌بینی جرم در

1. Predicting crimes

مدارس تاثیر داشته و نهایتاً «الزامات عملکردی اینترنت اشیا در مدارس» با ضریب (۰/۵۲) بر پیش‌بینی جرم در مدارس تاثیر دارد. در مجموع، نتایج حاصل از مدل‌سازی با نتایج استنباطی در آزمون فرضیات همسو و هم‌جهت است.

جدول ۵- برآورد وزن‌های رگرسیونی روابط ساختاری موجود در مدل با نرم‌افزار Amos

	Estimate	S.E.	C.R.	P	Label
PC ← IA	1.292	.182	7.110	***	
PC ← PR	1.523	.210	7.240	***	
PC ← ID	1.865	.252	7.412	***	
s1_1 ← IA	1.000				
s1_2 ← IA	.800	.143	5.596	***	
s1_3 ← IA	1.267	.196	6.451	***	
s1_4 ← IA	1.270	.193	6.571	***	
s4_1 ← PC	1.000				
s4_2 ← PC	.896	.074	12.065	***	
s4_3 ← PC	.913	.075	12.203	***	
s4_4 ← PC	.881	.076	11.633	***	
s4_5 ← PC	.698	.065	10.799	***	
s1_5 ← IA	1.320	.202	6.527	***	
s1_6 ← IA	1.036	.159	6.516	***	
s6_4 ← PR	1.263	.180	7.022	***	
s6_3 ← PR	1.593	.185	8.593	***	
s6_2 ← PR	1.145	.145	7.883	***	
s6_1 ← PR	1.000				
s6_5 ← PR	1.738	.201	8.648	***	
s6_6 ← PR	1.452	.187	7.761	***	
s3_4 ← ID	1.528	.212	7.193	***	
s3_3 ← ID	1.299	.184	7.075	***	
s3_2 ← ID	1.471	.207	7.100	***	
s3_1 ← ID	1.000				
s3_5 ← ID	1.887	.255	7.388	***	
s3_6 ← ID	.683	.164	4.161	***	

به منظور بررسی تفاوت معنادار اثر متغیر آشکار بر پنهان، به وزن‌های رگرسیونی مراجعه می‌شود.

مقدار (C.R) مقداری است که نسبت بحرانی خوانده می‌شود. این مقدار که از محاسبه نسبت مقدار برآورد شده غیراستاندارد برای پارامتر[1] به خطای معیار (S.E) محاسبه شده، برای همان پارامتر حاصل می‌شود، و نشان می‌دهد که در صورت رد فرضیه صفری که مقدار این پارامتر را برابر صفر قرار می‌دهد، تا چه حد احتمال خطا وجود دارد. مقادیر سه ستاره (***) در قسمت (P) به معنای تایید فرضیه با مقدار صفر است. در جدول (۵) قضاوت کردن به وجود تفاوت معنادار بین ضریب محاسبه شده و صفر، به صفر درجه خطا منجر می‌شود. با توجه به اینکه تا ۵ درصد میزان خطا قابل قبول است، بنابراین نتیجه نهایی این است که پارامتر محاسبه شده در تمامی موارد دارای تفاوت معنادار با صفر است. در مجموع، این اظهارات برای نمونه‌های بزرگ‌تر جامعه آماری مناسب است.

۵. نتیجه‌گیری

برای شناسایی راهبردهای پیش‌بینی جرایم در مدارس با استفاده از اینترنت اشیا شاخص‌های زیادی وجود دارند که برخی از آنها نسبت به سایر شاخص‌ها اثرگذاری بیشتری بر پیش‌بینی جرم دارند. آنچه به عنوان شواهد علمی در این زمینه می‌تواند پشتوانه نظری برای طرح فرضیه در این زمینه باشد، اسناد و رویکردهایی است که می‌توانند سطح این اثرگذاری را مشخص کنند. به طور کلی یافته‌های نظری و میدانی نشان داده که پیش‌بینی جرم در مدارس وابسته به سه مولفه مهم الزامات عملکردی اینترنت اشیا در مدارس، قابلیت‌های اینترنت اشیا و کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم است. بر همین اساس پیش‌بینی جرم مهم‌ترین راهبرد پیشگیری از وقوع آن است. بر همین اساس اگر فرایندهای پیش‌بینی جرم در اماکن به درستی انجام شود، می‌توان نرخ جرایم را کاهش داد. یکی از مهم‌ترین اماکنی که لازم است راهبردهای پیش‌بینی جرایم در آنها به صورت هوشمندانه دنبال شود، مدارس هستند. مدارس باید به طور فعال طیف وسیعی از راهبردهای پیش‌بینی و پیشگیری از جرم را برای کاهش احتمال و پیامد رفتار مجرمانه اتخاذ کنند. این استراتژی‌ها از تقویت تا نگهداری زیرساخت‌های فیزیکی، سیستم‌ها و فرآیندهای الکترونیکی را شامل می‌شود. از طرفی مدارس موظفند محیط کار و یادگیری ایمن و مطمئن را برای همه دانش‌آموزان و متولیان امر آموزش فراهم کنند. محدود کردن وقوع و پیامدهای رفتارهای مجرمانه، تأثیر مثبتی بر درک مدرسه به عنوان مکانی امن دارد و می‌تواند سلامت و رفاه کلی مدرسه را بهبود بخشد. همچنین باید برخی اهداف مجرمانه در مدارس غیرقابل دسترس شوند و انجام رفتار مجرمانه بسیار دشوار یا بی‌فایده شود. این اهداف از طریق اجرای اقدامات امنیتی فیزیکی، الکترونیکی و یا رویه‌ای که مانع، انکار، به تاخیر انداختن و یا کشف فعالیت

1. Estimate

مجرمانه می‌شود، انجام می‌شود.

علاوه‌بر این، آگاهی و آموزش امنیت سایبری باید به موضوعی تبدیل شود که به دانش‌آموزان، معلمان و مدیران آموزش داده می‌شود. برخی از مسائل خاصی که باید در برنامه‌های آموزشی پوشش داده شوند، می‌تواند شامل شناسایی تلاش‌های فیشینگ و بهترین شیوه‌های رمز عبور باشد. باید به معلمان و دانش‌آموزان اهمیت استفاده از رمزهای عبور قوی برای همه دستگاه‌های اینترنت اشیا آموزش داده شود. مدارس حتی می‌توانند تاریخ‌های دوره‌ای را برای تغییر رمز عبور تعیین کنند، به عنوان مثال، هر ترم این برنامه‌های آموزشی را می‌توان توسط کارکنان آموزشی با تجربه بیشتری تکمیل کرد، یا اگر بودجه اجازه می‌دهد، می‌توان افراد حرفه‌ای را برای ارائه برنامه جامع‌تر امنیت سایبری به کار گرفت. خطرات فزاینده امنیت سایبری مرتبط با اینترنت اشیا نیازمند اقدامات هشیارانه برای محافظت از داده‌های حساس و اطمینان از عملکرد بی‌وقفه مدرسه است. با پذیرش رویکردی فعال و جامع برای امنیت اینترنت اشیا، مدارس می‌توانند از قدرت تحول این فناوری‌ها استفاده کنند و در عین‌حال زیرساخت دیجیتال خود را در برابر تهدیدات بالقوه تقویت نمایند. ایجاد تعادل بین نوآوری و امنیت فقط یک ضرورت نیست. این تعهد به ایجاد یک اکوسیستم آموزشی ایمن و انعطاف‌پذیر برای نسل‌های آینده است. به طور کلی نیاز نهادهای آموزشی و پرورشی به ویژه نیاز مدارس به فناوری اینترنت اشیا می‌تواند نشان‌دهنده حرکت این نهادها به سوی پویایی و ایجاد امنیت فزاینده باشد. با به کارگیری اینترنت اشیا از طریق طراحی و نگهداری محیطی، افزایش ایمنی محلی و کنترل محیطی، شناسایی الگوهای جرم، افزایش آگاهی پلیس از وقوع جرم، تحلیل جرم و الگوریتم هوش مصنوعی، می‌توان وقوع جرایم در هر مکانی را به طور دقیق پیش‌بینی کرد و مانع از بروز این جرایم شد. بنابراین، باید سیستم‌ها و زیرساخت‌های تخصصی توسعه اینترنت اشیا در مدارس و همه مکان‌های مهم و حساس، به صورت تخصصی به کار گرفته شوند و برای پیشرفت آنها بسترهای مناسب فراهم گردد. از این‌رو برنامه‌ریزان و سیاستگذاران و جرم‌شناسان می‌توانند بر پایه داده‌های واقعی، روندهای پیشگیری از جرایم را در مدارس تا اندازه زیادی تحت کنترل خود درآورند و به‌ازای هر مقدار توسعه در این زیرساخت، به همان اندازه از وقوع جرایم پیشگیری کنند.

این پژوهش به دلیل ماهیت مروری آن نمی‌تواند با پژوهش‌های پیشین مقایسه شود. اما می‌توان نتایج آن را در سه حوزه متاثر از برخی پژوهش‌های انجام شده، دانست. به عبارت دیگر، یافته‌های پژوهش در سه حوزه «الزامات عملکردی اینترنت اشیا در مدارس»، «قابلیت‌های اینترنت اشیا در مدارس» و «کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم» هر کدام، از پژوهش‌هایی تاثیر پذیرفته‌اند. در حوزه «الزامات عملکردی اینترنت اشیا در مدارس» این پژوهش از یافته‌های مظهر و

همکاران (۲۰۲۲) و مالاسو و همکاران (۲۰۲۴) بهره برده است. در حوزه «قابلیت‌های اینترنت اشیا در مدارس» این پژوهش از یافته‌های کونادی و همکاران (۲۰۲۰)، سعید و عبدالمحسن (۲۰۲۳)، جانگرا و کالسی (۲۰۱۹) و سردانا و همکاران (۲۰۲۱) بهره برده است. در نهایت در حوزه «کاربردپذیری اینترنت اشیا در شناسایی الگوهای جرم» پژوهش از یافته‌های مالاسو و همکاران (۲۰۲۴)، چاینمرم و آئو (۲۰۲۳) و ناث (۲۰۰۶) استفاده کرده است. به طور کلی، از آنجایی که ظهور محاسبات فراگیر و اینترنت اشیا فرصت‌های بالقوه جدیدی را برای راه‌حل‌های مبتنی بر فناوری برای پیشگیری از وقوع جرم فراهم می‌کند، این یک هدف کلان اجتماعی خواهد بود که برنامه‌های مرتبط با اینترنت اشیا در مدارس به طور جدی دنبال شود.

۶. پیشنهادها

با توجه به نقش سازنده اینترنت اشیا و فناوری در مدارس لازم است در همه مدارس یک واحد مشاوره امنیتی در چارت سازمانی مدارس در نظر گرفته شود تا این واحد برای حمایت از مدارس برای شناسایی خطرات محلی آنها و توسعه راهبردهای پیشگیری از جرم و کاهش خطر، اقدامات فوری انجام دهد. همچنین این واحد امنیتی در مدارس می‌تواند از تجارب مدارسی که ارتکاب جرایم را تجربه کرده‌اند و یا درگیر این معضل هستند، استفاده کرده و راه را برای ارتکاب جرم در مدرسه خود ببندد. علاوه‌بر این، استفاده از اطلاعات دوربین‌های مداربسته همیشه به عنوان یک مولفه مثبت مورد توجه بوده است. بنابراین، نصب دوربین مداربسته در مدارس باید با الزامات قانونی مطابقت داشته باشد و مدارس باید هنگام نصب و مدیریت سیستم‌های دوربین مداربسته به جنبه‌های پیشگیرانه آنها توجه ویژه‌ای داشته باشند. تجهیز مدارس به سیستم‌های اینترنت اشیا این قابلیت را برای پلیس فراهم می‌آورد، که با کوچک‌ترین تحریک پلیس بتوانند بدون معطلی خود را به مدرسه برسانند.

منـابـع

ابراهیمی، ش. (۱۴۰۱). پیشگیری از تکرار جرم از طریق هوش مصنوعی؛ مقتضیات و محدودیت‌ها. *آموزه‌های حقوق کیفری*، ۱۹(۲۳): ۵۴-۳۳. https://doi.org/ 10.30513/cld.2023.4345.1701

ابراهیمی، م.، تدین، م.، صیاد حقیقی، م. (۱۴۰۰). الگوریتم‌های اعتماد در اینترنت اشیا: بررسی، تحلیل و ارائه معیارهای ارزیابی. *پردازش علائم و داده‌ها*، ۱۸(۲): ۲۸-۳. https://doi.org/10.52547/jsdp.18.2.3

اصغری‌نژاد، س.، رزقی‌شیرسوار، ه.، خانزادی، خ. (۱۴۰۳). بررسی وضعیت توسعه اینترنت اشیاء در مدارس مبتنی بر آینده‌پژوهی. *جامعه‌شناسی آموزش و پرورش*، ۱۰(۱): ۱۶۰-۱۵۲.

https://doi.org/10.22034/ijes.2024.2017649.1517

دارابی، ش. (۱۳۹۷). *پیشگیری از جرم در مدل مردم‌سالار سیاست جنایی*. چاپ دوم. میزان.

صادقی، ح.، ناصر، م. (۱۳۹۹). ارائه چارچوب حقوقی مسئولیت‌پذیری در عملکرد ابزارهای اینترنت اشیا در بستر دولت الکترونیک؛ تبیین الگوی سیاستگذاری موثر. *سیاستگذاری عمومی*، ۶(۳): ۱۰۳-۸۱.

https://doi.org/10.22059/jppolicy.2021.79493

قنبری، م. (۱۴۰۲). شناسایی و ردیابی مجرمان از طریق اینترنت اشیا. *کارآگاه*، ۱۷(۶۳): ۱-۲۳.

https://doi.org/10.22034/det.2023.1273131.1387

کاری یو، ر. (۱۳۸۱). مداخله روان‌شناختی- اجتماعی زودرس در پیشگیری از رفتارهای مجرمانه. ترجمه علی حسین نجفی ابرندآبادی. *تحقیقات حقوقی*، ۵(۳۵-۳۶): ۳۰۴-۲۶۷.

محمد نسل، غ. (۱۳۹۳). *پیشگیری از جرم از طریق طراحی محیطی*. بنیاد حقوقی میزان.

محمدی جانکی، ف.، قورچی بیگی، م. (۱۳۸۸). نقش طراحی محیطی در پیشگیری از جرم. *مطالعات حقوق خصوصی*، ۳۹(۲): ۳۶۷-۳۴۵.

References

Alohali, B. (2017). *Detection protocol of possible crime scenes using Internet of Things (IoT)*. In: Cybersecurity breaches and issues surrounding online threat protection (pp. 175-196). IGI Global.

Asgharinezhad, S., Rezghi Shirsavar, H. & Khanzadi, K. (2024). Investigating the Status of Internet of Things Development in Schools based on the Future Research. *Sociology of Education*, 10(1): 152-160. [in persian]

Barnett, J.A. (2020). *Examining School Safety and Security: A Situational Crime Perspective.* The University of Southern Mississippi, Honors Theses.

Cario, R. (2002). Early psychosocial intervention in the prevention of criminal behavior. *Legal Research Quarterly*, 5(35-36): 267-304. [in persian]

Chinaemerem, C.E. & Ao, A. (2023). An Intelligent Crime System Using Internet of Things [IoT] and Web Technological Tools for Instance Crime Reporting and Notification. *IRE Journals*, 9(6): 165-174.

Darabi, Sh. (2018). *Crime prevention in the democratic model of criminal policy*. Second edition. Mizan. [in persian]

Ebrahimi, M., Tadayon, M. & Sayad Haghighi, M. Trust Management in Internet of Things: Review,

Analysis and Establishment of Evaluation Criteria. *Signal and Data Processing*, 18(2): 3-28. https://doi.org/10.52547/jsdp.18 [in persian]

Ebrahimi, Sh. (2022). Prevention of Recidivism through Artificial Intelligence; Requirements and Limitations. *Criminal Law Doctrines*, 19(23): 33-54. https://doi.org/10.30513/cld.2023.4345.1701 [in persian]

Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7): 1645-1660.

Jangra, M. & Kalsi, S. (2019). Naïve Bayes approach for the crime prediction in Data Mining. *International Journal of Computer Applications*, 178(4): 33-37.

Kounadi, O., Ristea, A., Araujo, A. & Leitner, M. (2020). A systematic review on spatial crime forecasting. *Crime science*, no. 9: 1-22.

Mahmoodi Janaki, F. & Ghorchi Beigi, M. (2009). Environmental design and crime prevention. *Law Quarterly*, 39(2): 345-367. [in persian]

Malasowe, B.O., Aghware, F.O., Okpor, M.D., Edim, E.B., Ako, R.E. & Ojugo, A.A. (2024). Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech). *NIPES-Journal of Science and Technology Research*, 6(2): 293-311.

Malasowe, B.O., Akazue, M.I., Okpako, E.A., Aghware, F.O., Ojie, D.V. & Ojugo, A.A. (2023). Adaptive Learner-CBT with Secured Fault-Tolerant and Resumption Capability for Nigerian Universities. *International Journal of Advanced Computer Science and Applications*, 14(8): 135-142. https://doi.org/10.14569/IJACSA.2023.0140816

Mazhar, M.S., Saleem, Y., Almogren, A., Arshad, J., Jaffery, M.H., Rehman, A.U. & Hamam, H. (2022). Forensic analysis on internet of things (IoT) device using machine-to-machine (M2M) framework. *Electronics*, 11(7): 1-23.

Mohammad Nasl, Gh. (2014). *Crime prevention through environmental design*. Mizan Legal Foundation. [in persian]

Nath, S.V. (2006). *Crime pattern detection using data mining*. In: 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology Workshops (pp. 41-44). IEEE.

Piza, E.L., Welsh, B.C., Farrington, D.P. & Thomas, A.L. (2019). CCTV surveillance for crime prevention: A 40 year systematic review with meta analysis. *Criminology & public policy*, 18(1): 135-159.

Qanbari, M. (2023). Identifying and tracking criminals through the Internet of Things. *Karagah*, 17(63): 1-23. https://doi.org/10.22034/det.2023.1273131.1387 [in persian]

Sadeghi, H. & Naser, M. (2020). Providing a legal framework for accountability in the operation of "Internet of Things" tools in the context of e-government. *Iranian Journal of Public Policy*, 6(3): 81-103. https://doi.org/10.22059/jppolicy.2021.79493[in persian]

Saeed, R.M. & Abdulmohsin, H.A. (2023). A study on predicting crime rates through machine learning and data mining using text. *Journal of Intelligent Systems*, 32(1).

Sardana, D., Marwaha, S. & Bhatnagar, R. (2021). Supervised and unsupervised machine learning methodologies for crime pattern analysis. *International Journal of Artificial Intelligence and Applications (IJAIA)*, 12(1): 43-58.

Thongsatapornwatana, U. (2016). *A survey of data mining techniques for analyzing crime patterns.* In: 2016 Second Asian Conference on Defence Technology (ACDT) (pp. 123-128). IEEE.

Tundis, A. & Mühlhäuser, M. (2019). *The role of Information and Communication Technology (ICT) in modern criminal organizations*. In: Organized Crime and Terrorist Networks; Routledge: London, UK.

Veena, K., Meena, K., Teekaraman, Y., Kuppusamy, R. & Radhakrishnan, A. (2022). C SVM classification and KNN techniques for cyber crime detection. *Wireless Communications and Mobile Computing*, no. 8:1-9.

Watkins, N.J. (2015). *Situational Crime Prevention in Schools: Implications for Victimization, Delinquency, and Avoidance Behaviors.* Doctoral dissertation. College of Humanities and Social Sciences: George Mason.