KNO-1204-5006

یک چارچوب هوشمند یکپارچه برای پیشگیری و تشخیص سرقت خودرو مبتنی بر تحلیل داده‌های سنسوری و الگوهای جرم

آرمان رحمتی لپوندانی[1*]، سعید شعبانزاده[2]، مهدی نیاجلیلی[3]

[1*] کارشناسی ارشد مهندسی مکانیک گرایش ساخت و تولید دانشگاه جامع امام حسین(ع) ، تهران، ایران
Armanrahmatilapevandani@gmail.com

[2] کارشناسی ارشد مهندسی مکانیک گرایش طراحی کاربردی دانشگاه بوعلی سینا ،همدان،ایران saeid.shabanzadh.3@gmail.com

[3] هیأت علمی ، گروه مهندسی مکانیک، دانشگاه ملی مهارت، تهران، ایران، Mniajalili@tvu.ac.ir

چکیده

سرقت خودرو و قطعات جانبی آن همچنان یکی از چالش‌های اساسی امنیت شهری در بسیاری از کشورها به شمار می‌رود و پیامدهای اقتصادی، اجتماعی و روانی قابل‌توجهی برای مالکان خودرو و نهادهای مسئول به همراه دارد. با وجود توسعه طیف گسترده‌ای از سامانه‌های ضدسرقت، بسیاری از راهکارهای موجود ماهیتی واکنشی داشته و عمدتاً پس از وقوع سرقت فعال می‌شوند؛ در نتیجه توان محدودی در پیشگیری مؤثر از وقوع جرم دارند. پیشرفت فناوری‌های حسگری، ارتباطی و تحلیلی در سال‌های اخیر، فرصت مناسبی را برای طراحی سامانه‌های هوشمند با رویکرد پیش‌دستانه فراهم ساخته است. در این مقاله، یک چارچوب هوشمند و یکپارچه برای پیشگیری و تشخیص سرقت خودرو ارائه می‌شود که بر تلفیق داده‌های سنسورهای داخلی خودرو، فناوری‌های موقعیت‌یابی و ارتباطی نظیر GPS و GSM، و تحلیل الگوهای جرم‌شناختی استوار است. روش پژوهش مبتنی بر تحلیل تطبیقی مطالعات پیشین، شناسایی تهدیدهای رایج در سرقت خودرو و استخراج معیارهای کلیدی ارزیابی سامانه‌های امنیتی است. بر این اساس، یک معماری چندلایه شامل لایه حسگری، لایه تحلیل داده و لایه تصمیم‌گیری طراحی شده است که امکان پایش مداوم وضعیت خودرو و شناسایی رفتارهای مشکوک را فراهم می‌کند. ارزیابی چارچوب پیشنهادی به‌صورت سناریومحور و تحلیلی انجام شده و عملکرد آن در مواجهه با سناریوهای مختلف از جمله سرقت کامل خودرو، سرقت قطعات و استفاده غیرمجاز بررسی شده است. نتایج حاصل از این ارزیابی‌ها نشان می‌دهد که رویکرد پیشنهادی می‌تواند دقت تشخیص را افزایش داده، نرخ هشدارهای کاذب را کاهش دهد و زمان واکنش سامانه را در مقایسه با سامانه‌های متداول به‌طور محسوسی بهبود بخشد. این پژوهش می‌تواند به‌عنوان مبنایی برای توسعه سامانه‌های ضدسرقت هوشمند و پیاده‌سازی‌های عملی آینده مورد استفاده قرار گیرد.

واژگان کلیدی: سرقت خودرو، سامانه ضدسرقت، تحلیل داده‌های سنسوری، GPS/GSM، اینترنت اشیای خودرو

۱- مقدمه

سرقت خودرو و قطعات جانبی آن یکی از معضلات مهم امنیت شهری در بسیاری از کشورها محسوب می‌شود و خسارات اقتصادی و اجتماعی قابل‌توجهی به همراه دارد [۴,۵]. افزایش تعداد خودروها و پیچیده‌تر شدن شیوه‌های ارتکاب جرم موجب شده است که سامانه‌های سنتی ضدسرقت، نظیر قفل‌های مکانیکی و دزدگیرهای ساده، کارایی محدودی در شرایط واقعی داشته باشند. این سامانه‌ها غالباً ماهیتی واکنشی دارند و تنها پس از آغاز فرآیند سرقت فعال می‌شوند [۱،۷]. در سال‌های اخیر، پیشرفت فناوری‌های حسگری، ارتباطی و پردازشی زمینه‌ساز توسعه سامانه‌های ضدسرقت هوشمند شده است. استفاده از سنسورهای داخلی خودرو، سامانه‌های موقعیت‌یابی ماهواره‌ای (GPS)، شبکه‌های ارتباطی سیار (GSM) و زیرساخت‌های اینترنت اشیا امکان پایش مداوم وضعیت خودرو و ارسال هشدارهای بلادرنگ را فراهم کرده است [۱۰]. با این حال، بخش قابل‌توجهی از سامانه‌های موجود بر یک فناوری خاص تمرکز دارند و فاقد رویکردی یکپارچه برای تحلیل هم‌زمان داده‌های متنوع هستند. از سوی دیگر، مطالعات جرم‌شناختی نشان می‌دهد که سرقت خودرو پدیده‌ای تصادفی نیست و از الگوهای مشخصی از نظر زمان، مکان و شیوه ارتکاب تبعیت می‌کند [۴]. نادیده گرفتن این الگوها در طراحی سامانه‌های امنیتی می‌تواند اثربخشی آن‌ها را کاهش دهد. بر این اساس، هدف این پژوهش ارائه یک چارچوب هوشمند و یکپارچه برای پیشگیری و تشخیص سرقت خودرو است که با تلفیق تحلیل داده‌های سنسوری و الگوهای جرم‌شناختی، رویکردی پیش‌دستانه و کارآمد را دنبال می‌کند.

۲ -روش‌شناسی پژوهش

روش تحقیق این پژوهش از نوع تحلیلی–توصیفی بوده و با هدف ارائه یک چارچوب مفهومی برای پیشگیری و تشخیص سرقت خودرو طراحی شده است. در این راستا، پژوهش حاضر به‌جای پیاده‌سازی تجربی، بر تحلیل نظام‌مند مطالعات پیشین و تلفیق رویکردهای فنی و جرم‌شناختی تمرکز دارد [۱،۲،۴]. فرآیند انجام پژوهش در چهار مرحله اصلی انجام شده است.

۲,۱ گردآوری و تحلیل منابع

در این مرحله، مقالات علمی مرتبط با سامانه‌های ضدسرقت خودرو، فناوری‌های GPS/GSM، اینترنت اشیای خودرو و مطالعات جرم‌شناختی بررسی شدند [۷،۱۰]. این تحلیل با هدف شناسایی رویکردهای رایج و محدودیت‌های سامانه‌های موجود انجام گرفت.

۲,۲ استخراج معیارهای ارزیابی

بر اساس تحلیل منابع، معیارهایی نظیر نوع تهدید، سطح پیشگیری، زمان تشخیص، نوع واکنش سامانه و میزان کاهش هشدارهای کاذب استخراج شد [۲،۶،۸].

۲,۳ طراحی چارچوب پیشنهادی

چارچوب پیشنهادی با رویکردی چندلایه شامل لایه حسگری، لایه تحلیل داده و لایه تصمیم‌گیری طراحی شد. این نوع معماری در مطالعات پیشین به‌عنوان رویکردی کارآمد برای سامانه‌های امنیتی هوشمند گزارش شده است [۷،۱۰].

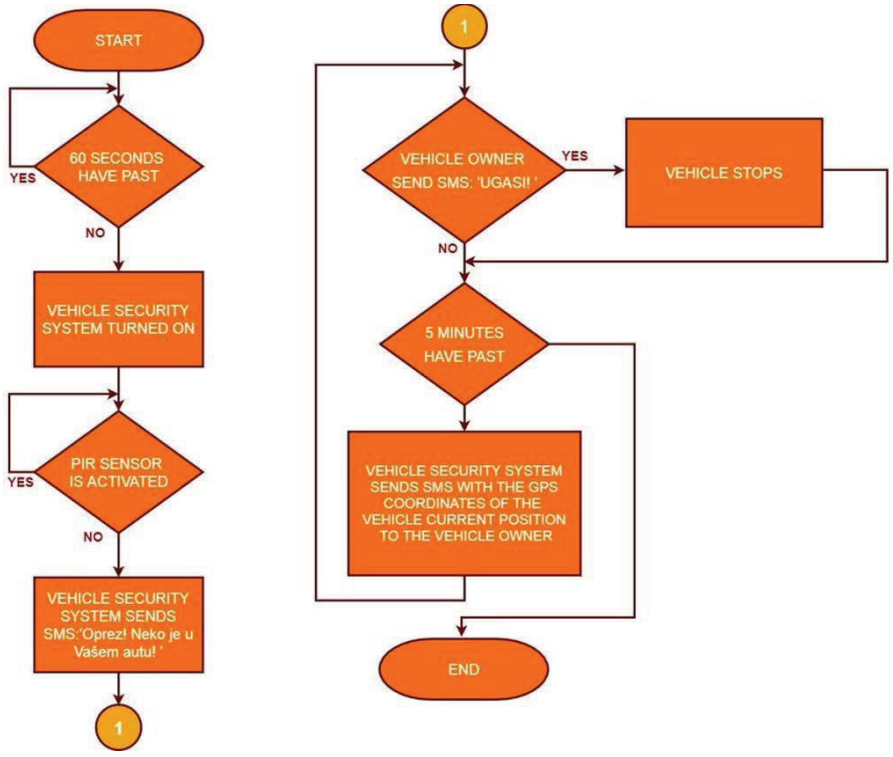
۲,۴ ارزیابی سناریومحور

ارزیابی چارچوب پیشنهادی به‌صورت سناریومحور و تحلیلی انجام شد و سناریوهای مختلف سرقت کامل خودرو، سرقت قطعات و استفاده غیرمجاز مورد بررسی قرار گرفتند. این رویکرد ارزیابی در مطالعات جرم‌شناختی و سامانه‌های ضدسرقت رایج است [۴،۵].

۳-فناوری‌ها و رویکردهای مورد استفاده

در طراحی سامانه‌های ضدسرقت هوشمند، بهره‌گیری از فناوری‌های متنوع حسگری، ارتباطی و تحلیلی نقش کلیدی در افزایش دقت تشخیص و کاهش زمان واکنش ایفا می‌کند. در این پژوهش، چارچوب پیشنهادی بر پایه ترکیب چند رویکرد فناورانه مکمل طراحی شده است. فناوری‌های موقعیت‌یابی جهانی (GPS) و ارتباطات سیار (GSM) از پرکاربردترین ابزارها در سامانه‌های ضدسرقت خودرو محسوب می‌شوند و امکان ردیابی بلادرنگ خودرو، ارسال هشدار به مالک و اجرای فرمان‌های کنترلی از راه دور را فراهم می‌کنند [۱،۷]. با این حال، اتکای صرف به این فناوری‌ها معمولاً منجر به واکنش پس از وقوع سرقت شده و نقش محدودی در پیشگیری فعال دارد. به‌منظور کاهش دسترسی غیرمجاز به خودرو، استفاده از روش‌های احراز هویت هوشمند نظیر سامانه‌های بیومتریک و شناسایی الگوهای رفتاری پیشنهاد شده است که می‌توانند امنیت لایه دسترسی را به‌طور قابل‌توجهی افزایش دهند [۶،۹،۱۱]. در کنار این رویکردها، داده‌های حاصل از سنسورهای داخلی خودرو نظیر شتاب‌سنج، ژیروسکوپ و حسگرهای وضعیت، اطلاعات ارزشمندی درباره حرکت، لرزش و شرایط عملکرد خودرو فراهم می‌کنند. تحلیل هوشمند این داده‌ها امکان شناسایی رفتارهای غیرعادی مانند یدک‌کشی، لرزش غیرمجاز یا تلاش برای سرقت قطعات را فراهم می‌سازد و نقش مهمی در تشخیص پیش‌دستانه تهدید ایفا می‌کند [۱۳]. مطالعات پیشین نشان می‌دهد که استفاده منفرد از هر یک از فناوری‌های مذکور پاسخ‌گوی پیچیدگی شیوه‌های نوین سرقت خودرو نیست. ازاین‌رو، در چارچوب پیشنهادی این پژوهش، تلفیق داده‌های سنسوری، قابلیت‌های ارتباطی و روش‌های تحلیل رفتاری به‌عنوان یک رویکرد یکپارچه مورد توجه قرار گرفته است. این رویکرد می‌تواند با کاهش هشدارهای کاذب و افزایش دقت تشخیص، کارایی سامانه‌های ضدسرقت را در شرایط واقعی بهبود بخشد [۱۰،۱۳].

شکل۱- دیاگرام معماری سامانه ضدسرقت هوشمند مبتنی بر تحلیل داده‌های سنسوری



جدول۱ـ مقایسه رویکردهای فناورانه به‌کاررفته در سامانه‌های ضدسرقت خودرو[۶،۱۰،۱۲،]

رویکرد فناورانه	کارکرد اصلی	مزایا	محدودیت ها
سامانه مبتنی بر GPS/GSM	ردیابی موقعیت و ارسال هشدار	سادگی پیاده سازی و پوشش ارتباطی مناسب	ماهیت واکنشی و وابستگی به شبکه محابراتی
روش احراز هویت هوشمند	جلوگیری از دسترسی غیر مجاز	افزایش امنیت در سطح	هزینه پیاده سازی و محدودیت
سنسور های داخلی خودرو	تشخیص رفتار های غیر عادی	قابلیت پیش دستانه و کاهش هشدار های کاذب	نیاز به تحلیل داده های پیچیده
رویکرد یکپارچه پیشنهادی	تلفیق چند فناوری	دقت تشخیص بالا و کاهش زمان واکنش	پیچیدگی طراحی و اجرا

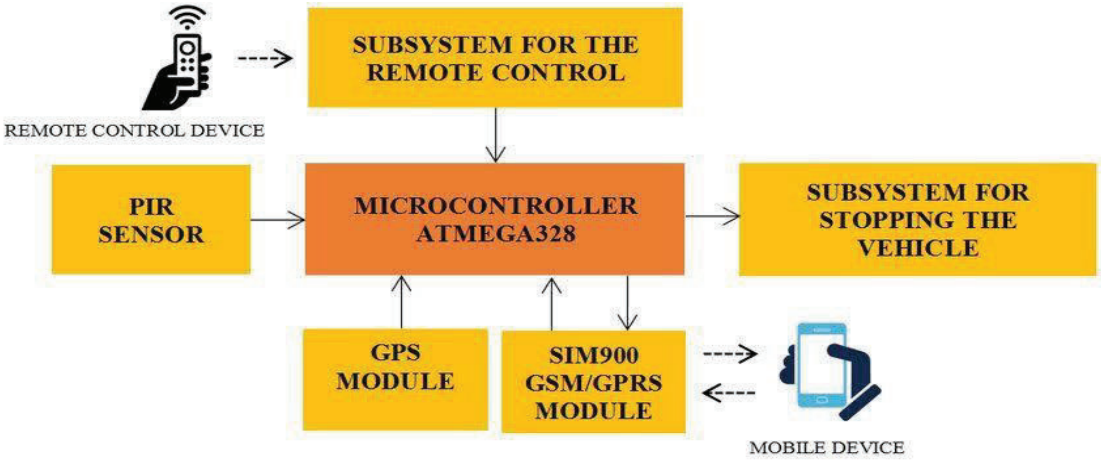
۴-تحلیل الگوی سرقت خودرو

تحلیل الگوهای سرقت خودرو نشان می‌دهد که این پدیده ماهیتی تصادفی نداشته و از الگوهای نسبتاً مشخصی از نظر زمان، مکان و شیوه ارتکاب تبعیت می‌کند. مطالعات جرم‌شناختی بیانگر آن است که بخش قابل‌توجهی از سرقت‌های خودرو در ساعات خاصی از شبانه‌روز و در مکان‌هایی با نظارت کمتر، نظیر معابر فرعی و پارکینگ‌های عمومی، رخ می‌دهد [۴،۵]. همچنین نوع خودرو، تجهیزات ایمنی موجود و سهولت دسترسی به قطعات از عوامل مؤثر در انتخاب هدف توسط سارقین محسوب می‌شوند. از منظر شیوه ارتکاب، سرقت کامل خودرو، سرقت قطعات و استفاده غیرمجاز هر یک ویژگی‌ها و نشانه‌های متفاوتی دارند که می‌توانند در طراحی سامانه‌های ضدسرقت مورد توجه قرار گیرند. برای مثال، سرقت قطعات معمولاً با الگوهای لرزشی خاص و تغییرات غیرعادی در وضعیت خودرو همراه است، در حالی که سرقت کامل خودرو اغلب با جابه‌جایی غیرمجاز و تغییر ناگهانی موقعیت مکانی مشخص می‌شود [۳]. نادیده گرفتن این تفاوت‌ها در سامانه‌های امنیتی می‌تواند منجر به افزایش هشدارهای کاذب یا کاهش دقت تشخیص شود. بر این اساس، بهره‌گیری از یافته‌های جرم‌شناختی در کنار تحلیل داده‌های سنسوری می‌تواند نقش مهمی در افزایش کارایی سامانه‌های ضدسرقت ایفا کند. تلفیق الگوهای زمانی و مکانی سرقت با داده‌های بلادرنگ سنسورها این امکان را فراهم می‌سازد که سامانه، رفتارهای مشکوک را با دقت بیشتری شناسایی کرده و واکنشی متناسب با نوع تهدید ارائه دهد. این رویکرد زمینه‌ساز طراحی سامانه‌هایی با قابلیت پیش‌بینی و پیشگیری مؤثرتر در برابر سرقت خودرو است [۴،۵].

۵-چارچوب پیشنهادی سیستم

چارچوب پیشنهادی این پژوهش با هدف پیشگیری و تشخیص هوشمند سرقت خودرو، به‌صورت یک ساختار یکپارچه و چندلایه طراحی شده است که قابلیت پایش مداوم وضعیت خودرو و واکنش متناسب با نوع تهدید را فراهم می‌کند. این چارچوب با تلفیق داده‌های سنسورهای داخلی خودرو، فناوری‌های ارتباطی و تحلیل الگوهای رفتاری، تلاش دارد محدودیت‌های سامانه‌های واکنشی متداول را برطرف کند.

شکل۲-فلوچارت عملکرد سیستم ضدسرقت پیشنهادی



در این چارچوب، داده‌های جمع‌آوری‌شده از سنسورهای مختلف به‌صورت بلادرنگ به واحد پردازش مرکزی ارسال می‌شوند. این داده‌ها پس از پردازش اولیه، با الگوهای رفتاری از پیش‌تعریف‌شده و سناریوهای رایج سرقت مقایسه می‌شوند. در صورت شناسایی رفتار مشکوک، سامانه بسته به نوع و شدت تهدید، تصمیم مناسب را اتخاذ می‌کند؛ این تصمیم می‌تواند شامل ارسال هشدار به مالک، ارائه اطلاعات مکانی خودرو یا فعال‌سازی مکانیزم‌های کنترلی نظیر قفل‌کردن موتور باشد [۱،۷].

منطق عملکرد سیستم به‌گونه‌ای طراحی شده است که از صدور هشدارهای غیرضروری جلوگیری کرده و تنها در شرایطی که احتمال وقوع سرقت وجود دارد، واکنش فعال نشان دهد. این ویژگی با استفاده از تحلیل هم‌زمان داده‌های سنسوری و در نظر گرفتن الگوهای زمانی و مکانی سرقت حاصل می‌شود [۴،۵]. چنین رویکردی امکان تشخیص پیش‌دستانه تهدید را فراهم کرده و زمان واکنش سامانه را به‌طور قابل‌توجهی کاهش می‌دهد.

در مجموع، چارچوب پیشنهادی با ایجاد تعامل مؤثر میان لایه حسگری، لایه تحلیل و لایه تصمیم‌گیری، بستری مناسب برای توسعه سامانه‌های ضدسرقت هوشمند و مقیاس‌پذیر فراهم می‌سازد و می‌تواند به‌عنوان مبنایی برای پیاده‌سازی‌های عملی و پژوهش‌های آینده مورد استفاده قرار گیرد.

۶-بحث و بررسی

نتایج تحلیلی این پژوهش نشان می‌دهد که رویکرد یکپارچه پیشنهادی می‌تواند محدودیت‌های سامانه‌های ضدسرقت متداول را تا حد زیادی برطرف کند. برخلاف بسیاری از مطالعات پیشین که بر یک فناوری خاص تمرکز داشته‌اند، چارچوب ارائه‌شده با تلفیق داده‌های سنسوری، قابلیت‌های ارتباطی و تحلیل الگوهای جرم‌شناختی، امکان تشخیص پیش‌دستانه تهدید را فراهم می‌سازد. این ویژگی نقش مهمی در کاهش زمان واکنش سامانه و افزایش کارایی آن در شرایط واقعی ایفا می‌کند. همچنین، استفاده از تحلیل رفتارهای مشکوک به‌جای اتکای صرف به تحریک‌های ساده سنسورها می‌تواند به کاهش هشدارهای کاذب منجر شود؛ موضوعی که یکی از چالش‌های اصلی سامانه‌های ضدسرقت محسوب می‌شود [۸،۱۳]. با این حال، پیاده‌سازی عملی چنین چارچوبی مستلزم دسترسی به داده‌های دقیق سنسوری و تنظیم مناسب آستانه‌های تصمیم‌گیری است. از جمله محدودیت‌های پژوهش حاضر می‌توان به عدم ارزیابی تجربی سامانه

در محیط واقعی و نبود داده‌های کمی برای مقایسه عملکرد اشاره کرد. با وجود این، چارچوب ارائه‌شده می‌تواند به‌عنوان مبنایی مفهومی برای توسعه سامانه‌های ضدسرقت هوشمند و انجام مطالعات کاربردی آینده مورد استفاده قرار گیرد.

۷-نتیجه‌گیری و پیشنهادات آینده

در این پژوهش، یک چارچوب هوشمند و یکپارچه برای پیشگیری و تشخیص سرقت خودرو ارائه شد که بر مبنای تحلیل داده‌های سنسوری داخلی خودرو، فناوری‌های موقعیت‌یابی و رویکردهای نوین تحلیل رفتار طراحی شده است. مرور ادبیات پژوهش نشان داد که بخش قابل‌توجهی از سامانه‌های ضدسرقت موجود، ماهیتی واکنشی دارند و عمدتاً پس از وقوع سرقت فعال می‌شوند، در حالی که چارچوب پیشنهادی این پژوهش با تمرکز بر شناسایی رفتارهای مشکوک، رویکردی پیش‌دستانه را دنبال می‌کند [۱]. نتایج تحلیل‌ها حاکی از آن است که تلفیق داده‌های سنسوری با الگوهای شناخته‌شده سرقت می‌تواند موجب افزایش دقت تشخیص، کاهش هشدارهای کاذب و بهبود زمان واکنش سیستم شود. همچنین، ساختار چندلایه پیشنهادی این چارچوب، امکان توسعه‌پذیری و انطباق با شرایط مختلف محیطی و الگوهای متنوع سرقت را فراهم می‌کند. با این حال، پژوهش حاضر دارای محدودیت‌هایی از جمله عدم پیاده‌سازی عملی سامانه و نبود داده‌های میدانی واقعی برای ارزیابی کمی عملکرد است. ازاین‌رو، پیشنهاد می‌شود در تحقیقات آینده، چارچوب ارائه‌شده در قالب یک نمونه عملی پیاده‌سازی شده و با استفاده از داده‌های واقعی خودروها، دقت، قابلیت اطمینان و کارایی آن به‌صورت تجربی مورد سنجش قرار گیرد. همچنین، به‌کارگیری روش‌های یادگیری ماشین و هوش مصنوعی پیشرفته می‌تواند به بهبود عملکرد سیستم در شناسایی الگوهای پیچیده‌تر سرقت منجر شود.

مراجع

[1] Murkomen, T., Wakoli, L., & Omolo, R. (2025). Security and Privacy Issues in the Internet of Vehicles (IoV). International Journal of Research Publication and Reviews, 6(8), 4463–4469

[2] Studnia, I., Nicomette, V., Alata, E., Laarouchi, Y., Kaaniche, M., & Kaâniche, M. (2013). A survey of security threats to automotive networks. IEEE Communications Surveys & Tutorials, 15(3), 1014–1033.

[3] Petit, J., & Shladover, S. E. (2015). Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems, 16(2), 546–556.

[4] Checkoway, S., McCoy, D., Kantor, B., et al. (2011). Comprehensive experimental analyses of automotive attack surfaces. USENIX Security Symposium.

[5] Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. Black Hat USA

[6] Thing, V. L. L., & Wu, J. (2016). Autonomous vehicle security: A taxonomy of attacks and defenses. IEEE Internet of Things Journal, 3(6), 1135–1145.

[7] Hussain, R., Zeadally, S., & Baig, Z. (2020). Security and privacy in connected autonomous vehicles. IEEE Communications Magazine, 58(10), 58–63.

[8] Lin, Y., Wang, L., & Zhang, H. (2019). Vehicle behavior analysis using onboard sensor data. IEEE Transactions on Intelligent Transportation Systems, 20(10), 3853–3864.

[9] Wang, J., Liu, X., & Chen, Z. (2017). Biometric-based vehicle access control systems. Sensors, 17(8), 1854.

[10] Al-Khateeb, H., & Al-Muhtadi, J. (2020). Smart vehicle security framework based on IoT and cloud computing. Journal of King Saud University – Computer and Information Sciences, 32(10), 1183–

[11] Koscher, K., Czeskis, A., Roesner, F., et al. (2010). Experimental security analysis of a modern automobile. IEEE Symposium on Security and Privacy.

[12] Woo, S., Jo, H. J., & Lee, D. H. (2015). A practical wireless attack on the connected car. Black Hat Europe.

[13] Enev, M., Takakuwa, A., Koscher, K., & Kohno, T. (2016). Automobile driver fingerprinting. Proceedings on Privacy Enhancing Technologies, 2016(1), 34–50.