

Д. С. Положий, О. О. Орехов

Національний аерокосмічний університет імені М. Є. Жуковського «ХАІ», Харків, Україна

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ АВТОМОБІЛЬНОЇ БЕЗПЕКИ НА ОСНОВІ ХМАРНИХ АРХІТЕКТУР

Анотація. У роботі досліджено інтелектуальні системи автомобільної безпеки на основі хмарних архітектур. Показано взаємозв'язок сучасних систем автомобільної безпеки з технологією Інтернету речей. Охарактеризовано сучасні інтелектуальні системи автомобільної безпеки. Розкрито принципи формування основних функціональних складових систем. Доведено, що безсерверні обчислення є значним зрушенням у способах створення та розгортання додатків розробниками. Наголошено, що абстрагуючи базову інфраструктуру, безсерверні обчислення дозволяють розробникам зосередитись на написанні коду та створенні функціональних можливостей. Незважаючи на деякі обмеження, переваги безсерверних обчислень, включаючи масштабованість, економічність та гнучкість, роблять їх привабливим варіантом для багатьох випадків використання у сфері автомобільної безпеки. Охарактеризовано категорії користувачів системи, це користувачі системи, постачальники послуг з оцінки відповідності, адміністратори системної платформи. Описано принципи формування мікросервісів, зазначається, що у системі автомобільної безпеки результати обмеженого контексту безпосередньо інформують підрозділ мікросервісів. Остаточна конфігурація мікросервісів складається з трьох основних доменів: домен користувача, домен реалізації та домен правила. Сформовано комплексну архітектуру платформи, яку представлено графічно з відокремленням двох основних складових фронтенду та бекенду, описано структуру багаторівневої логіки надання послуг та потік даних у системі. Зазначається, що враховуючи масштабність сучасних інтелектуальних систем автомобільної безпеки запропонована архітектура може бути інтегрована під різні системи такі як виявлення несправності в роботі автомобіля, аварійне керування авто, система підтримки швидкості, тощо. Детально описано процес інтеграції системи та принцип роботи із застосуванням датчиків різного напрямлення.

Ключові слова: хмара, мікросервіс, безсерверна архітектура, розподілена програма, безпека, дорога, автомобіль, інтелектуальна система.

Вступ

Постановка проблеми. Враховуючи сучасний розвиток логістичної системи та посилення глобалізації спостерігається прогрес у цифровізації та автоматизації всіх сфер людської діяльності. Поява технології Інтернету речей (IoT) призвела до поширення взаємозв'язаних пристроїв і систем, що охоплюють широкий спектр датчиків, інтелектуальних пристроїв і систем управління автомобільним транспортом. Значний обсяг даних, створених цими пристроями та системами, забезпечує ефективну взаємодію та обмін інформацією через Інтернет, значно прискорюючи розвиток автомобільної інформації.

З повсюдною інтеграцією технології IoT загальною та інтелектуальною автомобільною технікою зокрема, питання безпеки IoT набуло підвищеної уваги. Взаємозв'язок пристроїв і систем в рамках IoT вимагає підключення через Інтернет, за допомогою якого запити від розподілених пристроїв централізовано обробляються та відповідають на них. Однак цей централізований підхід створює вразливі місця в безпеці, включаючи мережеві атаки, витік даних, порушення конфіденційності та вразливість системи безпеки. Примітно, що у сфері інтелектуальної автомобільної техніки необхідність інформаційної безпеки та захисту стає ще більш критичною та складною через залучення зовнішніх факторів.

Аналіз останніх досліджень і публікацій. Формування наукової думки в окресі автомобільної безпеки та впровадження технології IoT у автомобільну сферу є різноманітним та масштабним. У сучасній науковій площині з'являються роботи присвячені дослідженням хмарних сервісів та алгоритмів їх впровадження у інтелектуальні автомобільні системи.

Дослідження активних систем безпеки для автотранспортних засобів здійснили М. В. Коростельов та А. В. Гнатов [1]. Авторами проведено дослідження активних систем безпеки автомобілів на дорозі з метою вжиття заходів для підвищення безпеки учасників дорожнього руху, проаналізовано основні системи допомоги водію в активній системі безпеки автомобіля і розглянуто різні елементи для підвищення безпеки людей в автомобілі в пасивній системі безпеки. О.П. Алексієв, В.О. Алексієв, С.М. Неронов та А.Е. Дьяков [2] розглянули принципи побудови інтелектуальної транспортної системи міста. Науковці зазначають, що міста, які бажають стати розумним містом, найчастіше починають із розбудови інтелектуальної транспортної інфраструктури у формі Інтелектуальної транспортної мережі (ITN). У [3] досліджено бортові системи інтелектуального автомобіля. Авторами доведено, що для керування автомобілем потрібен обмін інформацією між окремими електронними блоками керування, тобто, роботою в мережі у тісному взаємозв'язку одного з одним. Застосовувана на автомобілях система CAN дає можливість об'єднати в локальну мережу блоки керування або складні датчики.

Із зарубіжних авторів варто відмітити роботи таких науковців як: Лінь Дяньчао, Лі Лі [4] який запропонував ефективну орієнтовану на безпеку модель слідування автомобіля для САУ з урахуванням впливу дискретних сигналів; Ван Юй, У Цзе, Хе Ханьфу [5] провели тематичне дослідження попереджувальних знаків чотирьох основних марок автомобілів у цьому сценарії та дослідили метод розробки сигналу в сценарії попередження про виїзд зі смуги руху; Сун Дунцзянь, Чжу Бінь, Чжао Цзянь, Хан Цзяї, Чень Чжичен [6] запропонували стратегію контролю за автомобілем на основі гібриду навчання з підкріпленням (RL) і

навчання під наглядом (SL); Лю Ян, Фань Інці, Хуан Дарун, Мі Бо, Хуан Ліюань [7] представили практичне дослідження інтелектуального автомобіля, змодельованого стохастичними мережами Петрі та Z. Результати показують, що це може підвищити безпеку та ефективність інтелектуальної системи водіння автомобіля; Ельсамадісі Омар, Ші Тяньюй, Смирнов Ілля, Абдулхай Бахер [8] запропонували SECRM (Безпечна, ефективна та комфортна модель слідування за автомобілем на основі RL) для автономного слідування за автомобілем, яка врівноважує максимізацію ефективності трафіку та мінімізацію ривків, підпорядковуючись жорстким аналітичним обмеженням безпеки щодо прискорення; Чень Сінюй, Бай Хайцзянь, Дін Хен, Гао Цзяньше, Хуан Веньцзюань [9] на основі інтелектуальної моделі LSTM у поєднанні з моделлю безпечного уникнення зіткнень Gipps побудували нову модель Gipps-LSTM, яка може не лише вивчати розумну поведінку людей, але й забезпечувати безпеку транспортних засобів. Ідея комбінації моделей Gipps-LSTM полягає в наступному: вводиться концепція потенційної точки зіткнення (PCP), а модель LSTM або модель Gipps контролюється та запускається за допомогою алгоритму оцінки ризику; Лі Маошен, Фань Цзін, Лі Джейон [10] розширили модель CF для адаптації поведінки ручного водіння на стані різних рівнів безпеки та проаналізували потік дорожнього руху в середовищі від ручного водіння до інтелектуального водіння високого рівня з різними затримками; Ван Шуфен, Ван Сінькай, Ван Шіхао [11] розробили покращену модель еліпса автомобіля та застосували її до мінімальної безпечної відстані для вільної зміни смуги руху інтелектуальних транспортних засобів; Пен Ліцзюнь, Хуан Цзюй, Чжоу Туцянь, Сюй Шуцай [12] досліджують продуктивність транспортного потоку в широко поширеному середовищі V2V, розгорнутому для всіх типів HDV та IV, рівнях від L0 до L5. Виходячи з цього припущення, переміщення та операції транспортного засобу збираються в набір даних V2X BSM, і для будь-якого транспортного засобу в парку послідовні рухи та поведінку автомобіля попереду можна передбачити в короткостроковій перспективі та розглядати як вхідні дані для моделі кооперативного адаптивного круїз-контролю (CACC) керованого автомобіля; Кападія Рія, Мехта Куш [13] розглянули зміну парадигми, яка можлива завдяки методам глибокого навчання для отримання стабільного та надійного автономного керування для безпілотних автомобілів та інших.

Однак незважаючи на масштабність наукових досліджень питання дослідження інтелектуальних систем автомобільної безпеки на основі хмарних архітектур з подальшою розробкою адаптивної архітектури системи не викликає сумнівів.

Постановка завдання. Метою роботи є дослідження інтелектуальних систем автомобільної безпеки на основі хмарних архітектур з подальшою розробкою адаптивної архітектури системи.

Викладення основного матеріалу дослідження

Одним із важливих напрямків розвитку інтелектуальних автомобільних систем є системи безпеки

автомобіля. Основним призначенням систем безпеки є запобігання аварійній ситуації, при виникненні якої система самостійно (без участі водія) оцінює ймовірну небезпеку та за необхідності запобігає їй шляхом активного втручання у процес управління. Застосування систем безпеки дозволяє зберегти керованість та курсову стійкість автомобіля у критичних ситуаціях.

В умовах сьогодення широкого застосування знайшли інтелектуальні системи автомобільної безпеки наведені у табл. 1.

В основі роботи інтелектуальних систем автомобільної безпеки лежить принцип IoT. Децентралізовані характеристики сценаріїв IoT ефективно гармонують з архітектурою розподілених додатків. Дві відомі парадигми проектування архітектури програмного забезпечення, а саме архітектура мікросервісів і архітектура без серверів, набули широкого поширення в різних областях як невід'ємні компоненти архітектури розподілених програм. Архітектура мікросервісів полегшує створення дуже гнучких і масштабованих систем, перевершуючи складні централізовані методології обробки з точки зору масштабованості, зручності обслуговування та розширення. Отже, мікросервіс пропонує чудову адаптивність до змінних вимог, підвищуючи надійність і продуктивність системи. З іншого боку, безсерверна архітектура представляє більш гнучкий і універсальний підхід до розробки, який прискорює розгортання нових програм, одночасно зменшуючи витрати на розробку та експлуатацію.

Архітектура мікросервісів і безсерверна архітектура стикаються з певними проблемами, пов'язаними з цілісністю системи та інформаційною безпекою, включаючи ризики порушення конфіденційності інформації, викриття інтерфейсу та неадекватні заходи безпеки та конфіденційності в різних мікросервісах і функціях.

Завдяки широкому впровадженню технології зв'язку 5G IoT зазнав значного прогресу. Ефективний розподіл ресурсів в епоху 5G і 6G став вирішальним, враховуючи експоненціальне зростання даних у різних галузях, що вимагає інтелектуальних рішень для підвищення продуктивності мережі та надання високоякісних послуг користувачам. Різні сценарії додатків IoT вимагають різних підходів до архітектури системи, щоб відповідати вимогам до комунікаційних, обчислювальних ресурсів і ресурсів зберігання. У наступному еру 6G обчислювальна потужність поширюватиметься по всій мережі. Розвиток хмарних обчислень і периферійних обчислень полегшив міграцію звичайних програм до хмарних і периферійних середовищ, дозволяючи їм обслуговувати більшу базу користувачів. Переносючи значну кількість завдань хмарних обчислень на сервер, можна значно зменшити навантаження на мережеву хмару, тим самим прискорюючи швидкість обробки даних. Враховуючи наявні ресурси хмарних обчислень, туманних обчислень і периферійних обчислень, важливо гнучко використовувати ці ресурси та оптимізувати планування ресурсів, щоб задовольнити вимоги багаторівневого розгортання та гнучкого планування обчислювальних сховищ і мережевих ресурсів для майбутніх послуг 6G.

Таблиця 1 – Інтелектуальні системи автомобільної безпеки

| № | Назва | | Активний датчик / прилад | Фірма виробник |
|---|---|------------------------------------|---|---|
| 1 | Система стеження за дорогою | Road tracking system | інфрачервоний лазерний промінь; сенсор LIDAR (Light Detection And Ranging) | Advanced Pedestrian Detection System компанії TRW і EyeSight фірми Subaru, BMW Night Vision, Honda Sensing, Ford Pre-Collision Assist, Toyota Night View, PRE-SAFE від Mercedes |
| 2 | Система нічного бачення для виявлення пішоходів у небезпечній близькості до проїжджої частини | Dynamic Light Spot | датчик серцебиття | BMW |
| 3 | Система стеження за розміткою на дорозі | LDW (Lane Departure Warning) | датчик відстані | BMW Night Vision, Honda Sensing, Ford Pre-Collision Assist |
| 4 | Система автоматичного перемикання ближнього та далекого світла фар | HBA (High Beam Assist) | камери стеження | BMW, Honda, Ford |
| 5 | Контроль втоми водія | DAS (Driver Attention Support) | <ul style="list-style-type: none"> – біометричні датчики; – інфрачервоний датчик за кермовим колесом, що контролює температуру обличчя. – п'єзоелектричний датчик у ремені безпеки для моніторингу частоти дихання; – провідні накладки на обід рульового колеса для вимірювання пульсу; – інфрачервоні датчики на обід рульового колеса для вимірювання температури долонь. | Ford, Toyota |
| 6 | Система підтримки швидкості | SAS (Speed Assistance Systems) | датчик швидкості, датчик відстані | Ford, Toyota, Mercedes |
| 7 | Автоматичне аварійне кермо | AES (Automatic Emergency Steering) | датчик вимірювання рівня системи після-аварійного моніторингу, датчик швидкості, датчик осей, датчик повороту керма | BMW, Honda, Ford, Toyota, Mercedes |

Традиційна монолітна архітектура програми, яка об'єднує всі програмні модулі в єдину програму, створює проблеми з точки зору розробки, обслуговування та розмежування завдань. Що потребує підвищених вимог до модульності та масштабованості програмного забезпечення. Щоб задовольнити ці вимоги, архітектура служби додатків еволюціонувала від початкової монолітної архітектури до сервісно-орієнтованої архітектури, а згодом до архітектури мікросервісів, яка краще узгоджується з вимогами Інтернету. Концепція архітектури мікросервісів була вперше представлена Мартіном Фаулером і Джеймсом Льюїсом у 2014 році. В останні роки зі швидким зростанням Інтернету монолітна архітектура додатків стала недостатньою для задоволення вимог, що призвело до широкого впровадження архітектури мікросервісів у різних галузях. У відповідності до концепцій розподіленої архітектури та відображення віртуальної мережі, архітектура мікросервісів інкапсулює відносно незалежні програми в різні служби, ізольовує бізнес-логіку та розгортає кожну службу окремо на різних серверах. Управління контейнерами використовується для контролю кожної

служби, забезпечуючи ефективне управління та розгортання компонентів системи.

Щоб звільнити розробників від обтяжливих завдань керування сервером, безсерверна технологія вводить концепцію хмарних сервісів у обчислювальну модель. Ця модель фактично відокремлює розробників додатків від серверів, звільняючи їх від обов'язків, пов'язаних із керуванням і безпекою серверів. Крім того, постачальники хмарних послуг розміщують базу інфраструктуру, усуваючи вплив відмінностей пристроїв на програми верхнього рівня. Порівняно з традиційними обчислювальними моделями, безсерверна технологія демонструє максимальну продуктивність з точки зору високого паралелізму, низької затримки та інших аспектів. Отже, функції планування та управління ресурсами, а також практики розподілених додатків є життєво важливими областями досліджень у сфері безсерверних технологій.

Загалом інтелектуальна система автомобільної безпеки націлена на три різні категорії користувачів: користувачі системи, постачальники послуг з оцінки відповідності, адміністратори системної платформи.

На основі аналізу початкової функціональної складової системи мікросервісів можна розділити за функціями виконання дій. В принципі, кожен обмежений контекст відповідає одному мікросервісу; однак такі фактори, як відповідальність за обслуговування та неоднорідність команди, повинні враховуватися під час процесу впровадження. У системі результати обмеженого контексту безпосередньо інформують підрозділ мікросервісів. Остаточна конфігурація мікросервісів складається з трьох основних доменів: домен користувача, домен реалізації та домен правила. На додаток до цих основних доменів існує домен статистики, який полегшує пошук інформації адміністратора, а також загальний домен, який підтримує системні операції.

На основі дизайну мікросервісів і розділення формується комплексна архітектура платформи. Для підвищення якості впровадження та функціональності інтелектуальної системи автомобільної безпеки пропонується системна платформа, яка поєднує мікросервісну та безсерверну архітектури, розглядаючи різні аспекти, включаючи загальну діаграму архітектури, діаграму системних аспектів, подання процесу, режим зв'язку мікросервісу та механізм взаємодії мікросервісу. Проект архітектури системи забезпечує детальне уявлення про загальну технічну архітектуру системи, структуру багаторівневої логіки надання послуг та потік даних у системі. Дизайн безперервної інтеграції/безперервного розгортання окреслює методи розгортання як інтерфейсного, так і бекенд-компонентів, а також покрокових процедур. Крім того, режим зв'язку мікросервісу пояснює обґрунтування вибору технології реалізації та пропонує рішення шляху API.

У процесі проектування архітектури оцінка трафікового навантаження на систему виявляється складною через впровадження нового бізнес-сценарію. Розгортання додатків безпосередньо на хмарних серверах із використанням традиційних підходів вимагатиме горизонтального масштабування вручну для забезпечення недостатнього трафіку, що потенційно призведе до втрати ресурсів, якщо кілька серверів надано заздалегідь. Для вирішення цієї проблеми та відповідності бізнес-вимогам прийнято безсерверну архітектуру на основі AWS. Завдяки розгортанню мікросервісів на AWS Lambda та використанню периферійних обчислень програма може автоматично еластично масштабуватися залежно від обсягу трафіку, а витрати розраховуються відповідно до кількості запитів і часу обчислення.

Щоб оперативно реагувати на зміну вимог користувачів, підвищувати ефективність розробки та пришвидшувати доставку системи, впровадження безперервної інтеграції та безперервної доставки (CI/CD) має важливе значення для автоматизації всього процесу. Автоматизація таких завдань, як компіляція, збірка та розгортання коду, зводить до мінімуму потребу в ручному моніторингу кожної зміни та знижує системні ризики шляхом проактивного виявлення потенційних проблем. Цей процес автоматизації охоплює не тільки дії, пов'язані з кодом, але й динамічне створення, знищення та оновлення ресурсів,

необхідних для роботи системи, включаючи сервери та бази даних. Загальний дизайн безсерверної архітектури системи показаний на рис. 1.

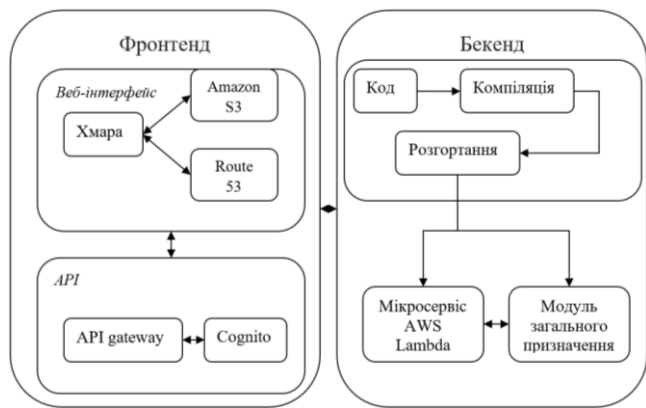


Рис. 1. Архітектура системи

Технічна архітектура системи в першу чергу складається з наступних компонентів:

- мікросервісний серверний модуль, що складається з Lambda. Сервер використовує AWS Lambda як обчислювальний блок для реалізації безсерверної системної архітектури, використовуючи її можливості автоматичного масштабування та економічну ефективність на основі принципів оплати за використання;
- інтерфейсний модуль, створений за допомогою React і розміщений у хмарних службах. Інтерфейсні функціональні модулі розробляються за допомогою React, а скомпільовані файли розгортаються на S3 і поширюються через CloudFront CDN, щоб покращити доступність глобальних користувачів і підвищити продуктивність;
- безсерверні загальні компонентні послуги, що надаються постачальниками хмарних послуг. Загальні безсерверні компоненти охоплюють бази даних DynamoDB NoSQL, черги повідомлень, служби електронної пошти та служби зберігання об'єктів. Хоча база даних спеціально призначена для мікросервісу, решта компонентів розроблено як загальні компоненти, доступні для обчислювального модуля мікросервісу (Lambda);
- конвеєри безперервної інтеграції та безперервного розгортання (CI/CD). Конвеєр CI/CD розділено на два автономні конвеєри для інтерфейсного та внутрішнього модулів. Кожен конвеєр включає в себе сховище коду, службу збірки та блок розгортання. Після виявлення змін у основній гілці сховища коду конвеєр ініціює виконання та, після затвердження, розганяє зміни у призначеному середовищі облікового запису. Впровадження CI/CD сприяє прискореній розробці та зменшенню часу доставки.

Враховуючи масштабність сучасних інтелектуальних систем автомобільної безпеки запропонована архітектура може бути інтегрована під різні системи такі як виявлення несправності в роботі автомобіля, аварійне керування авто, система підтримки швидкості, тощо.

Відбувається це за рахунок встановлення датчиків та їх зв'язку з мікропроцесором з підтримкою WiFi, який є доступним у сучасних мікроконтроллерах,

який, таким чином, може встановлювати бездротове з'єднання між різними мережами та Інтернетом і навіть передавати та приймати дані. Параметри руху та стану авто і дороги, зчитуються датчиками і використовуються пристроєм, а отримані дані зберігаються в хмарну базу даних.

Висновки

У роботі проаналізовано інтелектуальні системи автомобільної безпеки на основі хмарних архітектур. Доведено, що сучасна інтелектуальна система авто-

мобільної безпеки потребує розподіленої, гнучко конфігурованої та динамічно масштабованої архітектури мережевої програми. Ця архітектура має важливе значення, щоб задовольнити постійно зростаючі вимоги до розширюваної системи додатків IoT, підвищуючи при цьому гнучкість планування та масштабованість.

Перспективами подальших досліджень є розробка та впровадження інтелектуальної системи керування рухом автомобіля в складних умовах управління на базі запропонованої архітектури.

СПИСОК ЛІТЕРАТУРИ

1. Коростельов М. В., Гнатов А. В. Дослідження активних систем безпеки для автотранспортних засобів / Автомобільний транспорт, 2020. вип. 46. С. 40-46. DOI: 10.30977/AT.2219-8342.2020.46.0.40
2. Інтелектуальна транспортна система міста. Адаптивне керування рухом / Алексієв О.П., Алексієв В.О., Неронов С.М., Дьяков А.Е. // Матеріали конференції КІТ-2022, Харків, ХНАДУ, 2022. С. 134-136.
3. Бортові системи інтелектуального автомобіля / Мигаль В.Д., Бажинова Т.О., Іванов А.А. // Матеріали Всеукраїнської науково-практичної конференції «Автомобільний транспорт в аграрному секторі: проектування, дизайн та технологічна експлуатація» – 2019. Харків, 2019. С. 95-96.
4. Lin Dianchao, Li Li. (2023). An Efficient Safety-Oriented Car-Following Model for Connected Automated Vehicles Considering Discrete Signals. *IEEE Transactions on Vehicular Technology*. PP. 1-13. 10.1109/TVT.2023.3257048.
5. Wang Yu, Wu Jie, He Hanfu. (2023). Research on Sound-Guided Design of Lane Departure Scenarios in Intelligent Car Cockpit. 10.1007/978-3-031-35678-0_13.
6. Song Dongjian, Zhu Bing, Zhao Jian, Han Jiayi, Chen Zhicheng. (2023). Personalized Car-Following Control Based on a Hybrid of Reinforcement Learning and Supervised Learning. *IEEE Transactions on Intelligent Transportation Systems*. PP. 1-16. 10.1109/TITS.2023.3245362.
7. Liu Yang, Fan Yingqi, Huang Darong, Mi Bo, Huang Liyuan. (2022). Formal Model and Analysis for the Random Event in the Intelligent Car with Stochastic Petri Nets and Z. *Security and Communication Networks*. 2022. 10.1155/2022/3288308.
8. Elsamadisy Omar, Shi Tianyu, Smirnov Iliia, Abdulhai Baher. (2023). Safe, Efficient, and Comfortable Reinforcement-Learning-Based Car-Following for AVs with an Analytic Safety Guarantee and Dynamic Target Speed. *Transportation Research Record Journal of the Transportation Research Board*. 10.1177/03611981231171899.
9. Chen Xingyu, Bai Haijian, Ding Heng, Gao Jianshe, Huang Wenjuan. (2023). A Safety Control Method of Car-Following Trajectory Planning Based on LSTM. *Promet - Traffic&Transportation*. 35. 380-394. 10.7307/ptt.v35i3.118.
10. Li Maosheng, Fan Jing, Lee Jaeyoung. (2023). Modeling Car-Following Behavior with Different Acceptable Safety Levels. *Sustainability*. 15. 6282. 10.3390/su15076282.
11. Wang Shufeng, Wang Xinkai, Wang Shihao. (2022). Lane Change Decision and Trajectory Planning for Intelligent Cars in Curved Road Scenarios. 10.3233/ATDE221112.
12. Peng Liqun, Huang Ju, Zhou Tuqiang, Xu Shucui. (2023). V2V-enabled cooperative adaptive cruise control strategy for improving driving safety and travel efficiency of semi-automated vehicle fleet. *IET Intelligent Transport Systems*. n/a-n/a. 10.1049/itr2.12402.
13. Kapadia Riya, Mehta Kush. (2023). Advancing Autonomous Navigation: Deep Learning Techniques for Self-Driving Cars. *International Journal for Research in Applied Science and Engineering Technology*. 11. 1863-1869. 10.22214/ijra-set.2023.55491.

Received (Надійшла) 24.08.2023

Accepted for publication (Прийнята до друку) 08.11.2023

Intelligent automotive security systems based on cloud architectures

Denys Polozhyi, Oleksandr Oriekhov

Abstract. Intelligent automotive security systems based on cloud architectures are investigated in the work. The relationship between modern car safety systems and Internet of Things technology is shown. Modern intelligent automobile safety systems are characterized. The principles of formation of the main functional component systems are disclosed. Serverless computing has proven to be a significant shift in the way developers build and deploy applications. It is emphasized that by abstracting the underlying infrastructure, serverless computing allows developers to focus on writing code and creating functionality. Despite some limitations, the advantages of serverless computing, including scalability, cost-effectiveness, and flexibility, make it an attractive option for many automotive safety use cases. The categories of system users are characterized, these are system users, conformity assessment service providers, and system platform administrators. The principles of formation of microservices are described, it is noted that in the car safety system, the results of the limited context directly inform the microservices unit. The final configuration of microservices consists of three main domains: the user domain, the implementation domain, and the rule domain. The complex architecture of the platform is formed, which is presented graphically with the separation of the two main components of the frontend and backend, the structure of the multi-level logic of service provision and the flow of data in the system are described. It is noted that, taking into account the scale of modern intelligent car safety systems, the proposed architecture can be integrated into various systems, such as detection of malfunctions in the operation of the car, emergency control of the car, speed support system, etc. The process of system integration and the principle of operation using sensors of various directions are described in detail.

Keywords: cloud, microservice, serverless architecture, distributed application, security, road, car, intelligent system.