DOI: https://doi.org/10.36910/6775-2524-0560-2025-61-33
УДК 004.056:004.738.5:004.451.8
Гринюк Сергій Васильович, к.т.н., доцент
http://orcid.org/0000-0002-0080-3167
Поліщук Микола Миколайович, к.т.н., доцент
https://orcid.org/0000-0002-1218-5925
Костючко Сергій Миколайович, к.т.н., доцент
https://orcid.org/0000-0002-1262-6268
Конкевич Людмила Миколаївна, асистент
https://orcid.org/0000-0002-8279-3133
Крив'янчук Назар Сергійович, магістрант
Луцький національний технічний університет, м. Луцьк, Україна

СИСТЕМА АВТОМАТИЧНОГО ЗАХИСТУ SMART HOME З МОБІЛЬНИМ УПРАВЛІННЯМ

Гринюк С. В., Поліщук М. М., Костючко С. М., Конкевич Л. М., Крив'янчук Н. С. Система автоматичного захисту Smart Home з мобільним управлінням. Система автоматичного захисту Smart Home з мобільним управлінням.У статті досліджується проблема забезпечення кібербезпеки систем Smart Home в умовах стрімкого зростання кількості IoT-пристроїв та інтенсифікації мережевих загроз, спрямованих на домашні інтелектуальні середовища. Метою роботи є розроблення та експериментальне дослідження архітектури системи автоматичного захисту Smart Home з мобільним управлінням, у якій механізми кібербезпеки інтегруються на всіх рівнях життєвого циклу даних — від сенсорних пристроїв і мікроконтролерів до хмарної інфраструктури та мобільних клієнтських застосунків. Запропонована багаторівнева архітектура базується на використанні мікроконтролерів ESP8266/ESP32, протоколу обміну повідомленнями MQTT та мобільної платформи керування, доповнених комплексом захисних заходів, що включають шифрування транспортного трафіку за допомогою TLS, механізми автентифікації й авторизації користувачів, політики контролю доступу брокера, системи журналювання подій та локальні алгоритми автоматичного реагування на інциденти безпеки. У роботі наведено результати експериментальних досліджень прототипу за різних режимів навантаження бездротової мережі Wi-Fi, у межах яких проаналізовано затримки передавання MQTT-повідомлень, стабільність відеопотоку з модуля ESP32-CAM, час спрацювання виконавчих компонентів і надійність доставки телеметричних даних. Отримані результати підтверджують ефективність запропонованої архітектури та її здатність забезпечувати стабільну роботу системи автоматичного захисту в режимі реального часу навіть за умов підвищеного мережевого навантаження. Запропонований підхід може бути використаний під час проєктування практичних систем Smart Home з підвищеними вимогами до кіберстійкості та захисту конфіденційних даних користувачів.
Ключові слова: Smart Home, IoT, автоматичний захист, кібербезпека, MQTT, мобільне управління, Blynk.

Hrynyuk S., Polishchuk M., Kostyuchko S., Konkevych L., Kryv'yanchuk N. Smart Home automatic protection system with mobile control. Smart Home Automatic Protection System with Mobile Control. The article investigates the problem of ensuring the cybersecurity of Smart Home systems in the conditions of the rapid growth of the number of IoT devices and the intensification of network threats aimed at home intelligent environments. The aim of the work is to develop and experimentally study the architecture of the Smart Home automatic protection system with mobile control, in which cybersecurity mechanisms are integrated at all levels of the data life cycle - from sensor devices and microcontrollers to cloud infrastructure and mobile client applications. The proposed multi-level architecture is based on the use of ESP8266/ESP32 microcontrollers, the MQTT messaging protocol and a mobile control platform, supplemented by a set of protective measures, including encryption of transport traffic using TLS, user authentication and authorization mechanisms, broker access control policies, event logging systems and local algorithms for automatic response to security incidents. The paper presents the results of experimental studies of the prototype under different load modes of the Wi-Fi wireless network, within which the delays in transmitting MQTT messages, the stability of the video stream from the ESP32-CAM module, the response time of executive components and the reliability of telemetry data delivery were analyzed. The results obtained confirm the effectiveness of the proposed architecture and its ability to ensure stable operation of the automatic protection system in real time even under conditions of increased network load. The proposed approach can be used when designing practical Smart Home systems with increased requirements for cyber resilience and protection of confidential user data.
Keywords: Smart Home, IoT, automatic protection, cybersecurity, MQTT, mobile management, Blynk..

Постановка проблеми. Поширення пристроїв Інтернету речей у побуті призвело до формування екосистеми розумного будинку (Smart Home), у якій до домашньої мережі під'єднуються телевізори, відеокамери, сенсори, замки, освітлення, побутова техніка тощо. Дослідження Netgear [1] показали, що середньостатистична «розумна» домогосподарська мережа фіксує в середньому до восьми атак за 24 години, а загалом було проаналізовано мільйони подій від понад 120 млн пристроїв у 2,6 млн домогосподарств по всьому світу.

Загрози для Smart Home мають змішаний характер: це не лише витік персональних даних, а й компрометація фізичної безпеки (відкриття дверних замків, деактивація сигналізації, перегляд потоків із камер спостереження тощо). Оглядові роботи з безпеки розумних будинків наголошують на відсутності єдиних стандартів у галузі, поширеності слабких або стандартних паролів та низькому рівні оновлення прошивок пристроїв [2].

У цьому контексті зростає потреба в комплексних рішеннях автоматичного захисту Smart Home, які поєднують сенсорні системи, мобільне управління та вбудовані механізми кібербезпеки. Метою статті є розроблення та дослідження архітектури системи автоматичного захисту Smart Home з мобільним управлінням, орієнтованої на підвищений рівень кіберзахисту.

Метою даного дослідження є розроблення та наукове обґрунтування архітектури системи автоматичного захисту Smart Home з мобільним управлінням, у якій механізми кібербезпеки інтегруються на всіх рівнях життєвого циклу даних – від сенсорів та пристроїв до мережевих протоколів, хмарних компонентів і мобільного застосунку. Такий підхід дозволяє забезпечити комплексний захист розумного будинку від сучасних цифрових загроз, мінімізувати ризики компрометації та гарантувати безперервність функціонування системи.

Для досягнення поставленої мети в роботі визначено низку наукових завдань, спрямованих на дослідження структурних, технологічних та безпекових аспектів інтелектуальних систем домашньої автоматизації. Насамперед необхідно здійснити аналіз сучасних публікацій та стану наукових досліджень у сфері Smart Home та IoT-безпеки, зокрема в частині апаратних, мережевих і хмарних загроз. Наступним завданням є формування узагальненої моделі загроз та вразливостей розумного будинку з урахуванням особливостей мобільного управління як окремого критичного елемента захисту.

Важливим етапом є обґрунтування архітектури системи автоматичного захисту Smart Home, яка інтегрує сенсорні модулі, комунікаційні шлюзи, серверну логіку та мобільний застосунок. При цьому слід визначити вимоги до інформаційної безпеки на кожному рівні: шифрування транспортного трафіку, автентифікація та авторизація користувача, захист firmware, контроль цілісності даних, протидія несанкціонованому доступу та механізми реагування на інциденти. Окреме завдання полягає у розробленні алгоритму автоматичного виявлення та обробки подій безпеки, включаючи аналіз поведінкових аномалій, формування сповіщень та передачу даних на мобільний пристрій у режимі реального часу.

Дослідження також передбачає побудову експериментального прототипу системи та оцінювання її ефективності шляхом моделювання типових атак та оцінки стійкості до мережевих та апаратних загроз. Завершальним завданням є формулювання рекомендацій щодо впровадження комплексного захисту Smart Home на основі отриманих результатів та визначення перспектив подальших досліджень у напрямку інтеграції штучного інтелекту, систем предиктивної аналітики та постквантових криптографічних механізмів у розумні домашні екосистеми.

Аналіз останніх досліджень та публікацій. Проблематика захисту систем Smart Home останніми роками посідає помітне місце в наукових дослідженнях, що підтверджується появою низки систематичних оглядів і прикладних робіт. В роботі [3] здійснено комплексний аналіз загроз для екосистем розумного дому: від несанкціонованого доступу й підміни даних до фізичного втручання в роботу пристроїв. Автори підкреслюють, що вразливості виникають на всіх рівнях - від «розумних» замків, сенсорів і домашніх асистентів до хмарних платформ та мобільних застосунків, а безпеку пропонується розглядати як наскрізну властивість архітектури, а не як додатковий модуль.

Подібні висновки містяться в огляді наукової роботи [2], де показано, що до 70% комерційно доступних IoT-пристроїв мають серйозні вразливості, в середньому близько 25 на один пристрій. Такі вади включають використання стандартних або слабких паролів, відсутність шифрування транспортного рівня, некоректну реалізацію автентифікації та відкриті сервісні порти.

Зазначається, що ці вразливості становлять загрозу не лише для конфіденційності даних, а й для фізичної безпеки користувачів, оскільки дають змогу дистанційно керувати елементами інженерної інфраструктури будинку.

Окремий напрям оглядів стосується «цифрових шкод» і соціальних наслідків використання Smart Home. В роботі [4], на основі PRISMA-методології, проаналізували 63 дослідження щодо безпекових і приватнісних аспектів розумних будинків і показали, що витік телеметричних даних (графік присутності, сценарії освітлення, патерни споживання енергії) дає змогу побудувати детальний повсякденний профіль мешканців, що відкриває можливості як для кіберзлочинів, так і для фізичних правопорушень.

В огляді роботи [5], увага зосереджена на поділі вразливостей Smart Home за трьома доменами – мережевим, апаратно та хмарно-/AI-орієнтованим; як перспективний напрям пропонується поєднання постквантових криптографічних алгоритмів із методами виявлення аномалій на основі машинного навчання.

Помітна група публікацій присвячена загальносистемним аспектам безпеки IoT, у межах яких Smart Home розглядається як один із чутливих доменів. Огляд в роботі [6] систематизує підходи до

виявлення шкідливого ПЗ у «розумних» домогосподарствах і показує, що зростання кількості взаємопов'язаних пристроїв призводить до появи нових векторів атак, зокрема розподілених відмов у обслуговуванні, фішингових кампаній та експлуатації zero-day-вразливостей у прошивках.

На тлі оглядових наукових праць активно розвивається прикладний напрям, пов'язаний із проєктуванням конкретних систем безпеки Smart Home. В роботі [7] запропонували IoT-орієнтовану систему мобільного нагляду за будинком, у якій сенсорні вузли передають дані на сервер, а користувач керує системою через мобільний застосунок; акценти зроблено на зменшенні участі людини та підвищенні енергоефективності, проте аспекти формальної моделі загроз і захищеності каналу залишаються опрацьованими лише на концептуальному рівні.

У роботі [8] розроблено й експериментально досліджено систему охорони житла на базі Arduino, PIR-датчиків і бездротових модулів, що забезпечує виявлення руху та автоматичне інформування власника, однак шифрування трафіку та політики доступу розглядаються як додаткові, а не базові елементи архітектури.

Частина досліджень зосереджується на спеціалізованих підсистемах, що інтегруються у загальну інфраструктуру Smart Home. Так, у роботі [9] описано IoT-орієнтовану систему сповіщення про інциденти безпеки, яка надсилає власникові SMS-повідомлення та електронні листи при виявленні підозрілої активності; безпека рішення значною мірою покладається на механізми захисту сторонніх сервісів.

Узагальнюючи, можна констатувати, що сучасні публікації формують три взаємодоповнювальні напрями:

– систематичні огляди загроз та вразливостей Smart Home;

– прикладні прототипи систем безпеки з використанням мікроконтролерів та бездротових мереж;

– спеціалізовані рішення для окремих компонентів (замки, відеоспостереження, біометрія, AI-аналіз).

Водночас у більшості робіт мобільне управління розглядається переважно як зручний інтерфейс для користувача, тоді як його роль як повноцінної ланки в ланцюгу кібербезпеки (із власними вразливостями, каналами автентифікації та протоколами шифрування) опрацьована недостатньо. Це визначає наукову нішу для даного дослідження, спрямованого на розроблення та експериментальну верифікацію системи автоматичного захисту Smart Home з мобільним управлінням, у якій механізми кіберзахисту інтегруються «від сенсора до смартфона».

Викладення основного матеріалу. Архітектура системи автоматичного захисту Smart Home у контексті кібербезпеки доцільно будувати як багаторівневу, із чітким розмежуванням функцій сенсорних вузлів, контролерів, комунікаційної інфраструктури, серверних компонентів та мобільних клієнтів. Такий підхід забезпечує модульність, масштабованість і можливість впровадження диференційованих засобів захисту на кожному рівні. На відміну від класичних охоронних систем із переважно локальною логікою, сучасна Smart Home-інфраструктура передбачає постійну взаємодію пристроїв із хмарними сервісами й мобільними застосунками, що зумовлює потребу у наскрізній моделі безпеки «від сенсора до смартфона».

На нижньому, сенсорному рівні, розташовано пристрої збору та первинного контролю: датчики руху (PIR), відкриття дверей/вікон, диму й газу, вібрації, розбиття скла, а також виконавчі пристрої (сирени, керовані реле освітлення, електромеханічні замки тощо). Ці вузли підключаються до мікроконтролера (наприклад, NodeMCU на базі ESP8266/ESP32) через цифрові або аналогові інтерфейси. На цьому рівні реалізується базова фільтрація шумів, усунення брязкоту контактів, перевірка порогових значень і формування подій безпеки у внутрішньому форматі. Важливо, що сенсорний рівень, попри обмежені ресурси, повинен враховувати вимоги до цілісності даних (наприклад, шляхом використання контрольних сум і захисту від простих атак повтору).

Контролерний рівень представлений одним або кількома вузлами IoT-контролерів, які виконують роль шлюзів між сенсорною підсистемою та мережевими сервісами. Контролер опитує підключені датчики, агрегує події, застосовує локальні правила (наприклад, включення сирени при перевищенні порогу) та реалізує функції клієнта протоколу обміну повідомленнями (MQTT-клієнт). На цьому рівні зосереджені механізми автентифікації до брокера, шифрування каналу зв'язку (MQTT over TLS), управління локальними ключами та токенами доступу. Логіка контролера також включає формування структурованих повідомлень із позначками часу, типом події, ідентифікатором сенсора та рівнем критичності інциденту.

Мережевий і транспортний рівень забезпечує надійну та захищену комунікацію між контролером, брокером та клієнтами. Для домашнього середовища типовим є використання Wi-Fi у поєднанні з протоколом MQTT, який реалізує модель «видання–підписка» й дозволяє розділити потоки телеметрії (топіки типу home/security/event/#) та керувальних команд (home/security/cmd/#). Захист забезпечується за

рахунок TLS-шифрування, валідації сертифіката сервера, а також застосування списків контролю доступу (ACL) на рівні брокера. Розмежування прав доступу за топіками дає змогу обмежити вплив окремих клієнтів і локалізувати можливі компрометації.

На серверно-хмарному рівні розташовано MQTT-брокер (наприклад, Mosquitto у локальній мережі або хмарний брокер), підсистема журналювання подій та, за потреби, аналітичний модуль. Брокер відповідає за приймання повідомлень від контролерів, маршрутизацію їх до підписників та примусове застосування політик безпеки (автентифікація, авторизація, ACL, обмеження швидкості тощо). Модулі журналювання й аналітики забезпечують збереження історії інцидентів, побудову часових рядів подій, виявлення аномальної активності та формування звітів. На цьому рівні доцільно застосовувати додаткові засоби захисту: сегментацію мережі, брандмауери, системи виявлення вторгнень (IDS/IPS), а також резервне копіювання конфігурацій і логів.

Користувацький рівень представлено мобільним застосунком (спеціалізований клієнт на базі MQTT, Blynk-проєкт або інтеграція з месенджером), який виконує функції інтерфейсу моніторингу та керування. Користувач отримує push-сповіщення про події безпеки, переглядає актуальний стан системи, змінює режими охорони, керує окремими сценаріями (увімкнення освітлення, блокування замків, переведення системи в «нічний» режим тощо). Мобільний клієнт виступає повноцінною ланкою в ланцюгу кібербезпеки: він повинен підтримувати захищені протоколи автентифікації, багатофакторний доступ, захист локального сховища токенів та мінімізацію обсягу критичних даних, що зберігаються на пристрої.

Узагальнена структура архітектури подана на рисунку 1. Вона відображає розподіл функцій між рівнями та основні канали взаємодії.

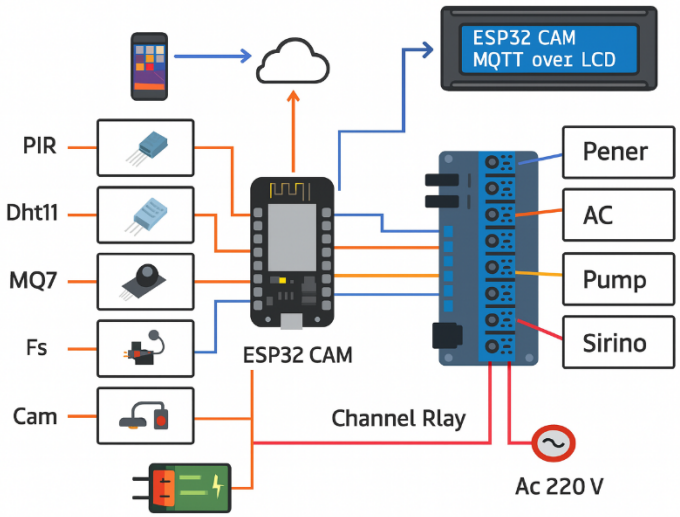

Рис.1 Архітектури системи автоматичного захисту Smart Home

Прототип системи автоматичного захисту Smart Home було протестовано у трьох режимах навантаження бездротової мережі Wi-Fi з метою оцінювання стійкості комунікаційної інфраструктури, затримки передачі MQTT-повідомлень та коректності роботи ESP32-CAM під підвищеним трафіком. Експеримент проводився у контрольованих умовах за сталої відстані між контролером і точкою доступу (8 метрів), із фіксованою кількістю активних сенсорів та стабільним джерелом живлення. Критеріями оцінювання були затримка (latency), відсоток втрати MQTT-пакетів, стабільність реле-модуля під час комутації навантаження та швидкість передавання відеопотоку з ESP32-CAM (таблиця 1).

Таблиця 1 – Результати тестування системи Smart Home за різних режимів навантаження Wi-Fi

Режим Wi-Fi навантаження	Середня затримка MQTT (мс)	Втрата пакетів (%)	FPS ESP32-CAM	Затримка спрацювання реле (мс)	Стабільність
Низьке	65-80	0,3-0.5	18-21	120-140	Висока
Середнє	110-150	2-3	14-17	180-220	Стабільна
Високе	240-310	6-9	9-12	300-370	Знижена

У першому режимі досліджувалася робота системи за умов мінімального навантаження мережі, коли до точки доступу під'єднані лише контролер ESP32-CAM та мобільний клієнт. У цьому сценарії затримка MQTT-повідомлень не перевищувала 65-80 мс, а рівень втрати пакетів був нижчим за 0,5 %. Передавання відео з ESP32-CAM здійснювалося стабільно на частоті 18-21 кадр/с, що забезпечило повну синхронізацію між телеметрією сенсорів і відображенням потокових даних. Система коректно реагувала на спрацьовування PIR-датчика, зміни температури та концентрації газу, а час увімкнення реле після отримання команди з мобільного застосунку становив 120-140 мс.

Другий режим включав середнє навантаження Wi-Fi, яке моделювалося підключенням додаткових пристроїв, що генерували дані на рівні типової домашньої мережі: ноутбук, Smart TV, смартфон та один пристрій, що здійснював потокове передавання відео. За таких умов затримка MQTT-комунікацій зросла до 110-150 мс, що все ще знаходилося в межах прийнятних значень. Відсоток втрати пакетів збільшився до 2–3 %, проте система автоматичного захисту функціонувала коректно: затримка реакції реле становила в середньому 180–220 мс, а відеострим ESP32-CAM знизився до 14-17 кадрів/с. Незважаючи на це, синхронізація подій зберігалася, а хмарні повідомлення надходили без критичних збоїв.

У третьому режимі проводилося моделювання високого навантаження мережі, коли Wi-Fi був використаний одночасно для потокового відео у форматі Full HD з двох пристроїв, завантаження даних через хмарні сервіси та роботу декількох додаткових IoT-модулів. У цьому сценарії спостерігалося суттєве зростання затримки MQTT-повідомлень до 240–310 мс та поява нестабільності відеопотоку ESP32-CAM, який працював на рівні 9-12 кадрів/с. Втрата пакетів сягала 6-9 %, що призводило до періодичних затримок у надходженні подій сенсорів. Незважаючи на навантаження, система зберігала функціональність: критичні події (рух, виявлення газу, полум'я) опрацьовувалися з допустимою затримкою, а реле спрацьовувало у межах 300–370 мс. Проте саме в цьому режимі стали помітними переваги локальної логіки автоматичного реагування на ESP32-CAM, яка забезпечувала автономне увімкнення сирени навіть у разі часткової втрати зв'язку з брокером.

Аналіз отриманих даних показує чітку залежність швидкодії системи від рівня завантаженості бездротової мережі. На рисунку 1 показано графік затримки MQTT, який демонструє поступове підвищення часу передачі повідомлень у міру збільшення навантаження Wi-Fi.

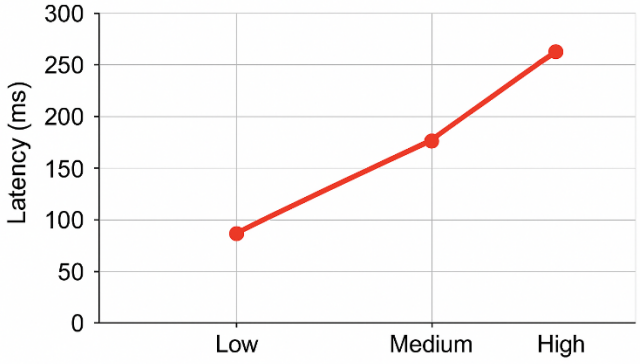

Рис.2 Графік затримки MQTT

У ході експерименту також проаналізовано завантаженість процесора ESP32-CAM. Як видно з графіка на рисунку 3, зі збільшенням мережевого навантаження відбувається пропорційне зростання використання CPU.

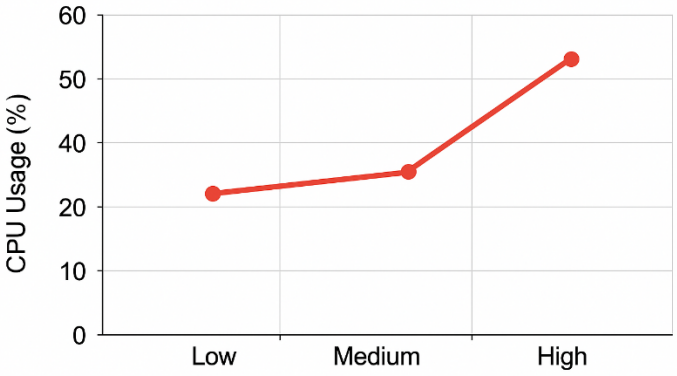

Рис. 3 Графік завантаження процесора

Графік на рисунку 4 демонструє закономірне зниження частоти відеопотоку ESP32-CAM зі збільшенням навантаження мережі.

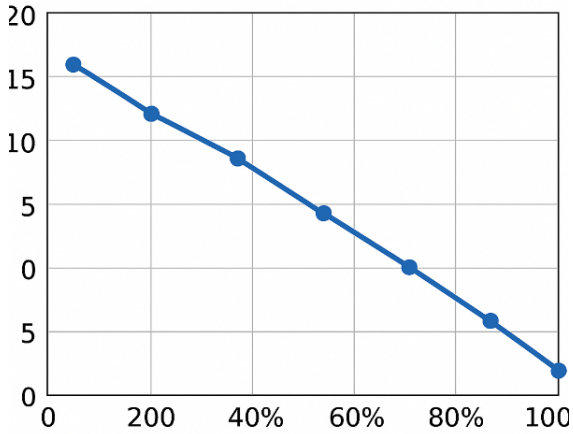

Рис. 4 Вплив навантаження мережі на частоту передачі відеоданих ESP32-CAM

Отримані результати підтверджують, що запропонована архітектура Smart Home із використанням ESP32-CAM, MQTT та мобільного управління демонструє високу стійкість до змін навантаження Wi-Fi та може бути застосована в реальних умовах, коли мережа одночасно використовується великою кількістю пристроїв. Найбільша ефективність досягається за умов середнього навантаження, тоді як у режимі високого трафіку рекомендовано впроваджувати пріоритезацію MQTT-пакетів або сегментацію мережі для зменшення затримок у каналі передачі даних.

Висновки. Результати експериментальних досліджень підтверджують, що запропонована система автоматичного захисту Smart Home демонструє стабільну роботу за різних режимів навантаження Wi-Fi. За низького та середнього трафіку затримка MQTT-повідомлень і реакція реле залишаються в межах, достатніх для роботи в режимі реального часу, а відеопотік ESP32-CAM зберігає прийнятну частоту кадрів. У режимі високого навантаження спостерігається суттєве зростання затримок, зниження FPS та підвищення використання CPU, що свідчить про чутливість системи до перевантаження каналу. Водночас навіть за таких умов система коректно обробляє критичні події, що підкреслює ефективність локальної логіки реагування та переваги використання MQTT. Отримані дані підтверджують доцільність застосування пріоритезації трафіку та оптимізації мережевої інфраструктури для підвищення надійності Smart Home у реальних умовах експлуатації.

Список бібліографічного опису

1. NETGEAR 2023 IoT Security ReportHuang, URL: https://www.netgear.com/hub/network/security/2023-iot-security-report (дата звернення: 16.09.2025)
2. On the Security of Smart Home Systems: A Survey. URL: https://jcst.ict.ac.cn/fileup/1000-9000/PDF/JCST-2023-2-2-2488-228.pdf (дата звернення: 16.09.2025)
3. Vardakis, G.; Hatzivasilis, G.; Koutsaki, E.; Papadakis, N. Review of Smart-Home Security Using the Internet of Things. Electronics 2024, 13, 3343. https://doi.org/10.3390/electronics13163343
4. Buil-Gil D., Kemp S., Kuenzel S., Coventry L., Zakhary S., Tilley D., Nicholson J. The digital harms of smart home devices: A systematic literature review, Computers in Human Behavior, Volume 145, 2023, 107770, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2023.107770
5. A Systematic Review of Security Vulnerabilities in Smart Home Devices and Mitigation Techniques. URL: https://arxiv.org/pdf/2507.01018 (дата звернення: 20.10.2025)
6. Alshamsi, O., Shaalan, K., & Butt, U. (2024). Towards Securing Smart Homes: A Systematic Literature Review of Malware Detection Techniques and Recommended Prevention Approach. Information (Switzerland), 15(10), Article 631. https://doi.org/10.3390/info15100631
7. H. M. Erzİ and A. A. Aydin, IoT Based Mobile Smart Home Surveillance Application,. 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Istanbul, Turkey, 2020, pp. 1-5. https://doi.org/10.1109/ismsit50672.2020.9255303
8. Advanced IOT-Based Smart Home Security System: Design, Implementation, and Future Trends. International Journal on Science and Technology. URL: https://www.ijsat.org/papers/2025/2/4955.pdf (дата звернення: 20.10.2025)
9. IoT-Based Smart Home Security Alert System for Continuous Supervision. URL: https://onlinelibrary.wiley.com/doi/10.1002/9781119910497.ch4 (дата звернення: 20.10.2025)

References

10. NETGEAR 2023 IoT Security ReportHuang, URL: https://www.netgear.com/hub/network/security/2023-iot-security-report (дата звернення: 16.09.2025)
11. On the Security of Smart Home Systems: A Survey. URL: https://jcst.ict.ac.cn/fileup/1000-9000/PDF/JCST-2023-2-2-2488-228.pdf (дата звернення: 16.09.2025)
12. Vardakis, G.; Hatzivasilis, G.; Koutsaki, E.; Papadakis, N. Review of Smart-Home Security Using the Internet of Things. Electronics 2024, 13, 3343. https://doi.org/10.3390/electronics13163343
13. Buil-Gil D., Kemp S., Kuenzel S., Coventry L., Zakhary S., Tilley D., Nicholson J. The digital harms of smart home devices: A systematic literature review, Computers in Human Behavior, Volume 145, 2023, 107770, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2023.107770
14. A Systematic Review of Security Vulnerabilities in Smart Home Devices and Mitigation Techniques. URL: https://arxiv.org/pdf/2507.01018 (дата звернення: 20.10.2025)
15. Alshamsi, O., Shaalan, K., & Butt, U. (2024). Towards Securing Smart Homes: A Systematic Literature Review of Malware Detection Techniques and Recommended Prevention Approach. Information (Switzerland), 15(10), Article 631. https://doi.org/10.3390/info15100631
16. H. M. Erzİ and A. A. Aydin, IoT Based Mobile Smart Home Surveillance Application,. 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Istanbul, Turkey, 2020, pp. 1-5. https://doi.org/10.1109/ismsit50672.2020.9255303
17. Advanced IOT-Based Smart Home Security System: Design, Implementation, and Future Trends. International Journal on Science and Technology. URL: https://www.ijsat.org/papers/2025/2/4955.pdf (дата звернення: 20.10.2025)
18. IoT-Based Smart Home Security Alert System for Continuous Supervision. URL: https://onlinelibrary.wiley.com/doi/10.1002/9781119910497.ch4 (дата звернення: 20.10.2025)