УДК 004.89:004.7:005.934

ВИКОРИСТАННЯ ЛОКАЛЬНИХ ШІ-МОДЕЛЕЙ ДЛЯ ПІДВИЩЕННЯ КОНФІДЕНЦІЙНОСТІ В СИСТЕМАХ «РОЗУМНОГО ДОМУ»

Перехрест Д. О.
perekhrestdmytro07@gmail.com
Черкаський державний фаховий бізнес коледж
Ратайчук П. Є.
м.Черкаси, Україна

Сьогодні технології IoT фактично стали стандартом для сучасного житла, а системи «Розумного дому» зустрічаються все частіше. Величезна кількість датчиків та мікроконтролерів генерує постійний потік даних, який потребує розумної обробки. Зазвичай для цього використовують хмарні сервіси, але у них є три суттєві недоліки: залежність від стабільного інтернету, помітні затримки у реакції та питання конфіденційності.

Саме тому зараз стає популярним підхід Edge Computing, коли штучний інтелект працює не десь на віддаленому сервері, а безпосередньо в мережі будинку. Локальний запуск ШІ-моделей дозволяє зробити систему повністю автономною та швидкою, а головне – гарантує, що особисті дані не покинуть межі квартири.

Головною перевагою розгортання локальних великих мовних моделей (LLM) є абсолютна приватність. Жодна аудіокоманда чи телеметрія з датчиків не залишає меж фізичної мережі будинку. Крім того, локальні моделі забезпечують мінімальний час відгуку, що є критично важливим для систем реального часу, де затримка у ввімкненні освітлення чи спрацюванні сигналізації викликає дискомфорт або небезпеку.

Ефективність роботи інтелектуальних моделей безпосередньо залежить від технічних характеристик сервера. На відміну від хмарних сервісів, де обчислювальні ресурси практично необмежені, локальний запуск LLM потребує значного обсягу відеопам'яті (VRAM). Використання методів оптимізації, як-от квантування моделей до 4 або 8 біт, дозволяє успішно застосовувати споживчі графічні адаптери. Зокрема, відеокарта рівня NVIDIA RTX 3060 з 12 ГБ

відеопам'яті є оптимальним рішенням для розгортання моделей із кількістю параметрів 7–8 мільярдів. Це робить побудову інтелектуальної системи керування доступною, оскільки зникає потреба у дорогому професійному обладнанні.

Щоб адаптувати базову мовну модель до умов конкретної IoT-мережі, доцільно використовувати методи ефективного донавчання, зокрема технологію LoRA (Low-Rank Adaptation). Це дозволяє моделі «вивчити» унікальну топологію будинку, назви окремих пристроїв та логіку роботи мікроконтролерів (наприклад, на базі ESP32). У результаті ШІ перестає бути просто текстовим помічником: він починає генерувати точні структуровані команди у форматі JSON або передавати інструкції через протокол MQTT безпосередньо на виконавчі пристрої.

Можливості локального штучного інтелекту в межах розумного дому значно ширші за звичайне голосове керування. Система може виступати аналітичним центром, що здійснює предиктивний аналіз на основі даних із датчиків температури та присутності. Це дозволяє автоматично оптимізувати роботу кліматичної техніки, враховуючи історію енергоспоживання.

Окрім комфорту, локальна модель стає ключовим елементом безпеки. Вона здатна розпізнавати аномалії в поведінці системи – наприклад, зафіксувати нетиповий рух або вчасно попередити про залишені ввімкненими електроприлади. Важливо, що такий глибокий аналіз патернів життя мешканців відбувається повністю автономно, що виключає будь-яку можливість витоку конфіденційної інформації за межі домашнього сервера.

Окрему увагу в межах розробки системи моніторингу слід приділити архітектурі взаємодії між локальним інтелектуальним ядром та периферійними вузлами мережі. На відміну від стандартних комерційних рішень, пропонована система базується на використанні відкритих протоколів передачі даних. Використання мікроконтролерів сімейства ESP32 як кінцевих вузлів дозволяє реалізувати гнучку мережу датчиків, що обмінюються даними через протокол MQTT. Це забезпечує високу швидкість реакції та стійкість до втрати пакетів.

Центральний сервер, що базується на ОС Linux, виконує роль брокера та агрегатора даних, передаючи структуровану інформацію до локальної LLM для подальшого прийняття рішень.

Процес обробки інформації в такій системі можна розділити на три рівні: сенсорний рівень (збір первинних даних про температуру, вологість, освітлення та стан електромережі), рівень аналізу (обробка даних локальною моделлю штучного інтелекту) та виконавчий рівень (керування реле, освітленням чи побутовою технікою). Інтеграція голосового керування через локальні асистенти з відкритим кодом (наприклад, Jarvis) дозволяє реалізувати природний інтерфейс взаємодії без необхідності звернення до API зовнішніх сервісів. Це критично важливо для стабільної роботи системи в умовах можливих перебоїв з інтернет-зв'язком або при відключеннях електроенергії, коли локальна мережа продовжує функціонувати від джерел безперебійного живлення.

Додатковим фактором розширення функціональності є використання візуалізації даних моніторингу. Система передбачає побудову інтерактивних графіків споживання ресурсів, що дозволяє локальному ШІ надавати поради щодо енергоефективності. Наприклад, аналізуючи дані за певний період, модель може автоматично скоригувати графік роботи нагрівальних приладів, що призведе до значної економії коштів користувача без втрати рівня комфорту. Таким чином, система перетворюється з пасивного інструмента моніторингу на активного помічника.

Отже, впровадження локальних моделей штучного інтелекту в системи моніторингу та керування IoT-мережею «Розумний дім» є високоефективним рішенням, що дозволяє нівелювати ключові недоліки хмарних технологій. Розгортання таких систем забезпечує абсолютну конфіденційність користувацьких даних, мінімізує затримки при виконанні команд та гарантує автономну роботу навіть за відсутності підключення до мережі Інтернет. Практична розробка та тестування подібних IoT-мереж, зокрема інтеграція локальних голосових асистентів, підтверджує, що завдяки сучасним методам оптимізації та донавчання (LoRA, квантування) створення розумного та

безпечного житлового простору стає можливим на базі доступного комп'ютерного обладнання. Це відкриває нові перспективи для створення надійних та персоналізованих систем автоматизації.

Список використаних джерел:

1. Бакурова А. В., Терещенко О. В. Інтернет речей: технології та застосування : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2021. 245 с.
2. Олійник В. В. Периферійні обчислення (Edge Computing) в системах розумного дому: переваги та виклики // Сучасні інформаційні технології та комп'ютерна інженерія. 2024. Вип. 15. С. 112–118.
3. Коваленко О. М. Архітектура розподілених систем управління на базі мікроконтролерів ESP32 та протоколу MQTT // Вісник комп'ютерних систем та мереж. 2023. № 4. С. 45–52.
4. LoRA: Low-Rank Adaptation of Large Language Models / E. J. Hu, Y. Shen, P. Wallis [та ін.] // arXiv preprint. 2021. URL: https://arxiv.org/abs/2106.09685 (дата звернення: 16.03.2026).
5. Офіційна документація платформи Home Assistant. URL: https://www.home-assistant.io/docs/ (дата звернення: 16.03.2026).

УДК 004.056.53:004.8

МЕТОДИ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ У СИСТЕМАХ КІБЕРБЕЗПЕКИ

Олійник М.С.
maksres01@gmail.com
Черкаський державний фаховий бізнес-коледж
Медолиз М.М.
м. Черкаси, Україна

У сучасному середовищі інформаційних технологій динаміка розвитку кіберзагроз вимагає впровадження інтелектуальних засобів захисту. Традиційні системи виявлення вторгнень (IDS), що базуються на сигнатурному аналізі, демонструють обмежену ефективність проти атак нового типу, оскільки вони не