

УДК 004

DOI <https://doi.org/10.32782/2663-5941/2024.2/22>

Сокульський О.Є.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Топольськов Є.О.

Національний транспортний університет

Жданова Ю.Д.

Київський столичний університет імені Бориса Грінченка

АНАЛІЗ МОЖЛИВОСТЕЙ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ З ВИКОРИСТАННЯМ МІЖМАШИННОГО ЗВ'ЯЗКУ «M2M» ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

Метою цього дослідження є аналіз можливостей машинно-машинних (M2M) та систем Інтернету речей (IoT) для побудови інтегрованої архітектури розумного будинку.

Для аналізу використано теоретичні та статистичні методи дослідження. Статистичні методи дозволяють визначити загальний зв'язок вхідних і вихідних параметрів між M2M та IoT, а також проаналізувати параметри інтеграції двох систем для побудови інтеграційної моделі.

У статті на основі теоретичних та емпіричних методів дослідження проаналізовано можливість інтеграції технологій M2M та IoT з порівнянням призначення кожної технології. Було виявлено, що при інтеграції комунікаційних систем M2M з пристроями IoT інтеграція складається з основних, таких як провайдери, Інтернет-сервіси, платформи та сервіси. Однак для інтеграції важливо враховувати основні аспекти, які складаються з протоколів і стандартів, хмарних технологій, аналітики даних, безпеки та безпеки, інтеграції з існуючими системами, моніторингу та управління. Крім того, також аналізується, що інтеграція M2M з IoT поєднує фактори для її забезпечення, що включає наступне: забезпечення зв'язку; аналітика, збір та обробка даних; ефективно управління ресурсами, безпека та шифрування; масштабованість і гнучкість; енергоефективність та оптимізація.

Дослідження аналізує можливість інтеграції M2M з IoT для побудови архітектури розумного будинку за допомогою дротових і бездротових мереж. Проаналізовано основні характеристики та відмінності між M2M та IoT, на основі яких побудовано архітектуру розумного будинку на прикладі двокімнатної квартири.

На основі архітектури M2M з використанням дротових і бездротових технологій в технології Smart Home проаналізовано алгоритм послідовності зв'язку обладнання M2M з пристроями IoT за допомогою бездротових і дротових мереж. Програми та додатки, що використовують інтеграцію M2M з IoT, забезпечують керування сполученими пристроями за допомогою смартфона, де здійснюється моніторинг та управління освітленням, побутовою технікою тощо.

Ключові слова: машина-машин, Інтернет речей, інтеграція, шлюз, бездротові мережі, розумний будинок.

Постановка проблеми. Інтернет речей (IoT) завдяки своїм можливостям відіграє важливу роль в наступному революційному рівні розвитку інформаційних технологій після комп'ютерів, Інтернету та мобільного телефонного зв'язку. Незважаючи на те, що IoT активно розвивався протягом останніх 20 років його можливості дозволяють поєднувати всі можливі сфери діяльності повсякденного життя [1]. Розвиток Інтернету речей обумовлений тим, що завдяки збільшенню чисельності користувачів Інтернету та модифі-

кації технологій роботи в Інтернеті дозволило об'єднати в одну мережу повсякденні об'єкти та системи. З іншого боку Інтернет речей відноситься до інноваційної технології, яка фокусується на взаємозв'язку між гаджетами та людьми або клієнтами для досягнення поставлених цілей та задач в залежності від потреб користувачів [1-2].

Сучасні технології розширили можливості передачі та обробки даних, що обумовлено розвитком та появою розумних систем, які працю-

ють без участі людського фактору. Міжмашинний зв'язок (M2M) та IoT є суттєвими аспектами сучасних технологій, де за допомогою M2M здійснюється обмін даними між пристроями, тоді як IoT розширює це поняття, з'єднуючи різні пристрої в інтернет для обміну інформацією та автоматизації процесів [1, 3].

Розвиток IoT посприяло виникненню промислового IoT (який спочатку був запропонований для розмежування промислових та споживчих додатків з метою об'єднання виробництва і IoT), що складається з інтелектуальних та взаємопов'язаних мереж з різними промисловими компонентами, які досягають вищої продуктивності та нижчих операційних витрат завдяки моніторингу в режимі реального часу, де важливу роль відіграють машини, які можуть обмінюватися даними між собою та підтримувати стабільний зв'язок. На відміну від IoT промисловий IoT потребує більш вищої стабільності, доступності та безпеки, однак за останні роки промисловий IoT широко застосовується для «розумних» міст та технологій, наприклад, для нафтогазової та газопереробної промисловості, аграрної промисловості, машинобудівній та літакобудівній промисловості тощо [4]. Велика кількість додатків, таких як «розумна» нафтогазова промисловість, «розумний» транспорт, «розумні» електромережі засновані на основі використання концепції інтелектуальних пристроїв IoT, які мають можливості зондування, активації, зберігання та обробки даних, що в свою чергу створює складні проблеми в мережі [5].

На відміну від машин, пристрої IoT мають можливість взаємодіяти через мережу за допомогою різних мережевих протоколів, наприклад, WiFi (802.11), ZigBee (802.16), Bluetooth (802.15), або за допомогою інтеграції з сумісними датчиками і виконавчими пристроями [6, 7]. Використання інтелектуальних (розумних) технологій Інтернет речей дозволяють інтегрувати та контролювати розумними пристроями, послугами та сервісами, а також об'єднувати фізичний світ з цифровим [7]. Однак поширення та розвиток технологій Інтернету речей призвело до появи нових викликів та проблем, які пов'язані з вразливістю в системі безпеки [8, 9].

Аналіз останніх досліджень і публікацій. IoT залишається основною частиною, яка відіграє важливе значення для пристроїв та комунікаційних систем майбутнього покоління, які забезпечують не тільки отримання та обробку даних, але й керування ними за допомогою машинного

взаємозв'язку M2M [10]. Інтенсивне зростання комунікаційних пристроїв, обчислювальної та вимірювальної техніки посприяло розвитку та виникненню глибокої технології, відомої як зв'язок між машинами (M2M), яка розроблена на основі крос-платформної інтеграції. З цією метою у дослідженні [11] наведено порівняльний аналіз різних протоколів та архітектури M2M (де для оцінки протоколів використовувалися Raspberry-Pi та ОС Raspbian), що надає уявлення про важливість технології, яка необхідна для взаємодії між машинами з використанням технології Інтернету речей.

Для того, щоб машини могли взаємодіяти між собою використовується технологія бездротового зв'язку, наприклад, в роботі [12] авторами наведений огляд сучасних викликів та досягнень в галузі бездротового зв'язку для M2M-з'єднання в IoT. Це підкреслює важливість бездротового зв'язку з метою забезпечення безперебійного підключення та обміну даними між машинами в різних галузях та сферах застосування. Однак бездротовий зв'язок вказує на необхідність застосування ефективних та надійних протоколів для підтримки зростаючої кількості взаємопов'язаних пристроїв та систем в IoT.

Останнім часом «розумні» технології найчастіше згадуються в дослідженнях, які зосереджені на прагненні автоматизувати всі процеси отримання, обробки та зберігання даних до Інтернету речей, проте, існують також сучасні виклики та проблеми. Наприклад, в роботі [13] наведено огляд досліджень, які пов'язані з проблемами безпеки, комунікації та оптимізації з якими стикається зв'язок між IoT та M2M. Окрім того, потрібно розуміти, що також існують проблеми підключення мережевих пристроїв до M2M-мережі, як описано в роботі [14].

Для підвищення безпеки даних в роботі [15] авторами запропонований інтелектуальний механізм, який автоматично виявляє атаки на пристрої IoT за допомогою фреймворку «машина-машина» (M2M), який розроблений за допомогою різних інструментів криміналістичного аналізу та машинного навчання. В дослідженні [16] проаналізованого бізнес-моделі промислового Інтернету-речей в контексті міжмашинної взаємодії в контексті «машина-машина», на основі чого розроблено концептуальну основу з метою проведення класифікації різних типів інноваційних бізнес-моделей для компаній, що працюють у бізнес-просторі M2M. Одночасно з цим, авторами в роботі [17] з'ясовано, що технологія «машина-

машина» є специфічним дискурсивним середовищем Інтернету речей для підключення інтелектуальних пристроїв, підтримка якого вимагає базової концептуальної схеми, де авторами пропонується оцінка різних онтологічних моделей, які розглядають M2M та IoT одночасно, визначаючи синтаксичний та семантичний потенціал таких пристроїв.

Окрім того, використання комбінованої технології систем M2M та IoT вимагає стандартизації архітектури, яка дозволить проводити розпізнавання ідентифікаційних даних, мережевого зв'язку та інших питань в системі IoT. Наприклад, в роботі [18] автори зосередилися на дослідженні бездротового зв'язку між машинами, що працює трьома способами, а саме: машина-машина, машина-мобільний телефон та мобільний телефон-машина.

До основних проблем використання M2M та IoT відноситься: безпека (збільшення кількості підключених пристроїв створює ризики щодо безпеки даних та конфіденційності, вимагаючи ефективних заходів захисту); стандартизація (відсутність єдиної стандартної архітектури та протоколів може ускладнювати взаємодію між різнорідними пристроями та системами); масштабованість (з приростом кількості підключених пристроїв виникають виклики управління та обробки великої кількості даних); енергоефективність (багато пристроїв IoT працюють від батареї, тому ефективне використання енергії є критичним); конфіденційність даних (збір та обробка даних великої кількості особистих даних може породжувати етичні питання та вимагати суворих правил) [19-21].

Постановка завдання. Метою даного дослідження є проведення аналізу можливостей систем міжмашинного зв'язку (M2M) та Інтернет речей (IoT) для побудови інтегрованої архітектури «розумного» будинку. Завданням цього дослідження є дослідити ключову залежність використання шлюзу та пристроїв IoT за допомогою бездротової мережі Wi-Fi з метою визначення параметрів відстані та кількості між пристроями та шлюзом для «розумної» технології управління будинком.

Для проведення аналізу використовувалися теоретичні та статистичні методи дослідження. Зокрема, аналіз та синтез наукової та спеціальної літератури з технічних спеціальностей та програмування з метою визначення сутності використання M2M в поєднанні з IoT, де порівнюються між собою призначення кожної з технологій,

а також визначаються особливості цих інформаційних систем. Статистичні методи дозволяють визначити спільний взаємозв'язок вхідних та вихідних параметрів між M2M та IoT, а також дозволяють проаналізувати параметри інтеграції двох систем для побудови інтеграційної моделі. На основі проаналізованих літературних джерел та статистичних результатів розглянемо інтеграцію систем M2M та IoT для побудови архітектури розумної технології управління будинком.

Виклад основного матеріалу

Інтеграція систем M2M та IoT для архітектури розумної технології

Інтеграція систем M2M з IoT включає об'єднання пристроїв, сенсорів, мереж для забезпечення ефективного обміну даними та автоматизації процесів. Це дозволяє збирати, аналізувати та використовувати дані для оптимізації функціоналу та прийняття рішень в реальному часі.

Мережа M2M містить безліч різних вузлів зв'язку, в яких основним об'єктом є машина (пристрій), однак енергоефективність є основною проблемою, оскільки декілька пристроїв можуть працювати від батареї одночасно. Декілька пристроїв здатні виробляти великі масиви даних з різним форматом, розміром та періодом. Комунікація відбувається без втручання людини, що вимагає безперебійної та стабільної мережі.

Телекомунікації передбачають собою те, що вся необхідна інформація про віддалене середовище по суті надається оператором, а основне з'єднання створюється в режимі зв'язку ведучого і веденого, що називається M2M-зв'язком за допомогою Інтернет. Протяжність вузлів один від одного величезна, затримка передачі даних може порушити роботу системи, що в результаті впливає на продуктивність роботи, а якість зв'язку та показники продуктивності є важливими аспектами будь-якої комунікації. В іншому випадку продуктивність мережі знижується, якщо в ній присутній зловмисний вузол, де відбувається некоректна поведінка вузла, що призводить до зловмисних атак та втрату пакетів, які порушують правила маршрутизації й впливають на спотворення передачі даних, а також на скидання та втрату даних [22].

Інтеграція екосистеми M2M-комунікацій у поєднанні з IoT зображена на рис. 1, де показано архітектуру, яка складається з екосистеми M2M та окремих типів провайдерів, таких як пристрій, інтернет-сервіси, платформи, сервіси та користувачі, а також з мережевого стеку IoT. Мережевий стек IoT складається з наступного:

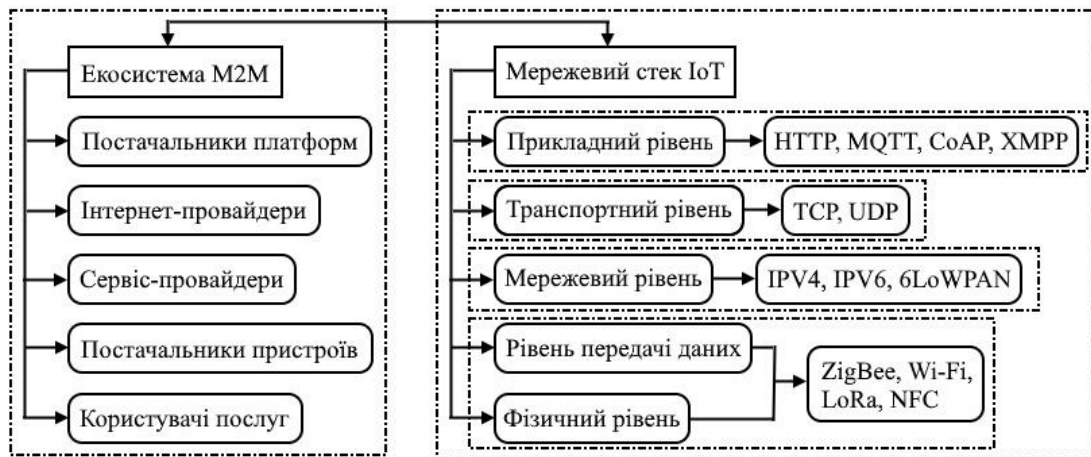


Рис. 1. Інтеграція систем M2M-комунікацій у поєднанні з пристроями IoT

Сформовано авторами на основі [7]

– прикладний рівень, який містить протоколи HTTP (HyperText Transfer Protocol), MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), XMPP (eXtensible Messaging and Presence Protocol);

– транспортний рівень, який містить протоколи TCP (Transmission Control Protocol), UDP (User Datagram Protocol);

– мережевий рівень, який складається з протоколів IPV4, IPV6 (Internet Protocol 4 версії та 6), де стандарт 6LoWPAN взаємодіє по протоколу IPV6, який дає можливість малопотужним пристроям обмінюватися інформацією один з одним;

– рівень передачі даних та фізичний рівень об'єднують в собі використання бездротових мереж, таких як Wi-Fi, ZigBee (специфікація мережевих протоколів верхнього рівня), LoRa (Long Range) та NFC (Near Field Communication).

Сфера застосування класифікується на транспорт, бізнес, послуги в реальному часі, дистанційне управління та моніторинг тощо. Важливим компонентом M2M комунікації є внутрішній сервер. Для всіх пристроїв створюється інтегрована точка збору даних, де M2M-пристроїв можуть бути стаціонарними, наприклад, мобільні гаджети, периферійні пристрої, побутова техніка та інше, що пов'язане та об'єднує в собі розумні технології.

Інтеграція технології M2M та IoT є ключовим етапом для створення ефективних та сучасних систем. Основні аспекти цієї інтеграції включають:

– протоколи та стандарти, де використовуються спільні протоколи, наприклад, MQTT (Message Queuing Telemetry Transport) або CoAP (Constrained Application Protocol), які дозволяють

різним пристроям спілкуватися та обмінюватися даними;

– хмарні технології, де використовуються хмарні платформи для збору, зберігання та обробки даних з пристроїв IoT та машин з метою покращення доступності та аналізу даних (наприклад Microsoft Azure IoT);

– аналітика даних, де впровадження аналітики даних дозволяє отримувати цінну інформацію та аналізувати процеси збору інформації на кожному етапі, що полегшує прийняття рішень та оптимізацію процесів;

– безпека та захист, де забезпечується безпека даних та захист пристроїв за допомогою шифрування та механізмів аутентифікації (SIEM – система, яка допомагає аналізувати та проводити моніторинг подій з питань безпеки з різних джерел, наприклад, файли журналів, сенсори та системи виявлення вторгнень IDS/IPS);

– інтеграція з існуючими системами, що дозволяє інтегрувати нові пристрої та технології вже існуючих систем, що полегшує розвиток та модернізацію;

– моніторинг та управління, де системи моніторингу та управління дозволяють в режимі реального часу відстежувати стан пристроїв, які підключені до мережі.

На основі інтеграції M2M-комунікації у поєднанні з IoT можливе створення інтелектуальних та підтримуючих інноваційних рішень в різних галузях. Розглянемо основні фактори для забезпечення інтеграції M2M з IoT, що складається з наступного: забезпечення зв'язку та надійність мережі (де технології M2M можуть забезпечити стійкий та надійний зв'язок між різними пристроями, що є критичним для оптимальної роботи

IoT); дані, аналітика, збір та обробка даних (де M2M дозволяє збирати великі обсяги даних з підключених пристроїв, що створює базу для аналізу та прийняття рішень); ефективне управління ресурсами та автоматизація (можливість автоматизації через M2M сприяє ефективнішому використанню ресурсів та оптимізації бізнес-процесів); безпека, ідентифікація, аутентифікація та шифрування (технології M2M дозволяють впроваджувати ефективні механізми шифрування та аутентифікації для захисту даних); масштабованість та гнучкість мережі (M2M може пристосуватися до зростаючого обсягу підключених пристроїв, забезпечуючи масштабованість мережі); енергоефективність та оптимізація витрат енергії (технології M2M можуть допомогти в розробці енергоефективних рішень для пристроїв IoT, що працюють від батарей) [24].

Інтеграція систем з використанням архітектури M2M та бездротових мереж у поєднанні з IoT

Інтеграція систем M2M з IoT обумовлює в собі об'єднання компонентів міжмашинної комунікації з пристроями IoT для збору даних за допомогою бездротової та локальної мережі (Wi-Fi), а також персональної мережі (Bluetooth). В якості інтеграції необхідно розглянути та проаналізувати архітектуру M2M з використанням дротових та бездротових мереж з пристроями IoT, а також проаналізувати основні характеристики та відмінності технологій, щоб побудувати в якості дослідження архітектуру M2M з використанням бездротової мережі для технології «розумного» будинку на прикладі двокімнатної квартири.

Для того, щоб побудувати архітектуру технології «розумного» будинку за допомогою M2M та IoT необхідно спочатку проаналізувати можливості доменів на рис. 2, де домен M2M з'єднує декілька вузлів і шлюз (gateway), що

дозволяє надавати різноманітні автоматизовані послуги [23]. Кожен вузол включає в себе різноманітні функції, наприклад, попередня обробка даних, збір даних, комунікаційні інтерфейси, унікальні адреси, зберігання даних та джерела живлення тощо.

Вони можуть приймати інтелектуальні рішення і передавати дані до шлюзу в режимі одного або декількох стрибків. Вбудовані вузли збирають пакети і можуть інтелектуально управляти пакетами, а також забезпечувати ефективні способи відправки пакетів на віддалений сервер через мережу. Мережа складається з різноманітних точок приєднання. Тут конвергентна гетерогенна мережа забезпечує оптимальне зондування пакетів для ефективної та надійної передачі каналів в M2M областях застосування M2M. Пристрої підключаються до основної мережі, а дротове рішення забезпечує найвищу швидкість передачі даних, надійність, безпеку та низьку затримку, але всі M2M-з'єднання в результаті цього можуть бути втрачені. Однак низька швидкість передачі даних, слабка захищеність і серйозні перешкоди згадані в універсальній інфраструктурі, які створюють обмеження в використанні M2M.

Для того, щоб проаналізувати можливості «розумної» технології на основі використання технології M2M та IoT розглянемо в якості прикладу двокімнатну квартиру, яку показано на рис. 3, де показано основні місця розташування «розумних» пристроїв, які можуть з'єднуватися між собою за допомогою технології безпроводної локальної мережі WiFi та наявності смартфона. Квартира містить дві спальні кімнати, вітальню з кухнею, дві ванні кімнати та лоджію.

Технологія M2M в поєднанні з IoT є ефективним рішенням для створення та оцифрування робочих процесів з метою ефективного використання ресурсів та ефективності. Технологія

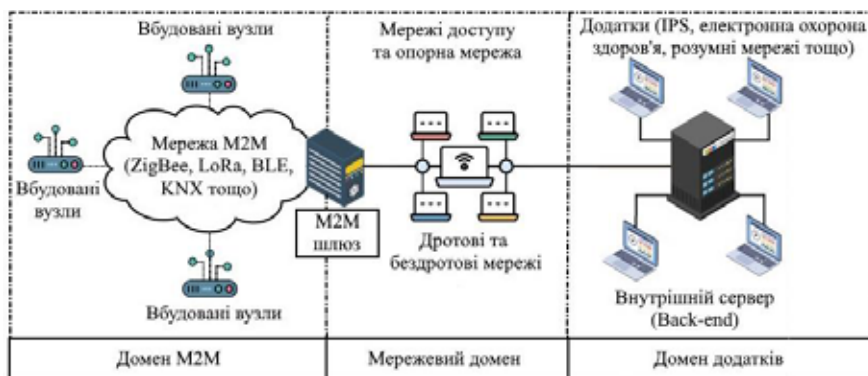


Рис. 2. Архітектура M2M з використанням дротових та бездротових мереж у поєднанні з Інтернет речей
Сформовано авторами на основі [3, 25]

Характеристика та відмінності технологій IoT та M2M

Технологія	Характеристики	Відмінності
Міжмашинний зв'язок (M2M)	<ol style="list-style-type: none"> Підвищення ефективності, що дозволяє пристроям автоматично обмінюватися даними та взаємодіяти між собою з метою оптимізації процесів, зменшення витрат та підвищення продуктивності. Моніторинг та діагностика проводиться за допомогою віддаленого спостереження різних параметрів (температура, вологість тощо), що дозволяє операторам вчасно реагувати на проблеми та здійснювати планове обслуговування. Покращення сервісу для клієнтів, де M2M дозволяє збирати дані про використання продуктів або послуг (наприклад, автоматичне вивчення звичок споживачів та надання персоналізованих пропозицій). Управління мережею, що дозволяє ефективно керувати мережею за допомогою підключених пристроїв, забезпечуючи оптимальне використання ресурсів та мінімізацію витрат. Вдосконалення та розвиток нових послуг, де відкривається шлях для створення нових продуктів та послуг, які базуються на автоматизації та взаємодії між пристроями (системи дистанційного контролю, системи «розумного» будівництва чи системи управління транспортними потоками). Безпека і збереження даних, де M2M вимагає великої уваги до захисту даних, оскільки обмін даними відбувається без участі людини, що включає в собі захист від зламу, шифрування даних та правильне керування доступом. 	<ol style="list-style-type: none"> З'єднання "точка-точка" часто включає в себе обладнання на території клієнта; Багато пристроїв підключаються до мережі через стільникові або кабельні з'єднання; Призначений для невеликих проектів; Пристрої M2M не завжди повинні бути підключені до інтернету; Оскільки пристрої повинні дотримуватися однакових протоколів зв'язку, вибір інтеграції обмежений
Інтернет речей (IoT)	<ol style="list-style-type: none"> Моніторинг і управління дозволяє в реальному часі проводити спостереження за станом різних пристроїв та систем, включаючи обладнання, транспортні засоби, будівлі тощо, що забезпечує підприємствам виявляти проблеми. Оптимізація процесів, де IoT може оптимізувати різні процеси, включаючи виробництво, логістику, енергетику тощо (наприклад, за допомогою сенсорів та аналітики даних можна зменшити втрати енергії, оптимізувати маршрути, автоматизувати виробничі процеси тощо). Покращення сервісу для клієнтів, де IoT дозволяє компаніям збирати дані про використання своїх продуктів або послуг з наданням рекомендацій. Розробка нових продуктів та послуг, де IoT відкриває двері для розробки нових продуктів та послуг, які базуються на підключених пристроях (розумні пристрої для дому, медичні пристрої для моніторингу здоров'я, системи безпеки тощо). Збільшення продуктивності та зменшення витрат, де IoT може сприяти збільшенню продуктивності за рахунок автоматизації процесів і зменшення витрат, що пояснюється ефективним використанням ресурсів. Покращення якості життя, де IoT може забезпечувати зручність та комфорт у повсякденному житті (наприклад, за допомогою розумних систем управління будинком підвищується безпека та зменшуються витрати на комунальні послуги). 	<ol style="list-style-type: none"> Мережа складається з віддалених та локальних пристроїв, які передають інформацію через IP; Дані передаються через хмарний проміжний рівень Зазвичай можна масштабувати для великих проектів У більшості випадків пристрої потребують безперервного доступу до інтернету

Сформовано авторами на основі [7, 24, 25]

M2M та IoT з'єднує пристрої через IP-мережі з метою моніторингу та контролю, що дозволяє отримувати інформацію з взаємопов'язаних при-

строїв. Окрім того, шлюз IoT (NXP Modular IoT) є мережевим з'єднувальним пристроєм, який використовується для з'єднання двох пристроїв



Рис. 3. Зразок двокімнатної квартири для проведення аналізу дослідження

Сформовано авторами

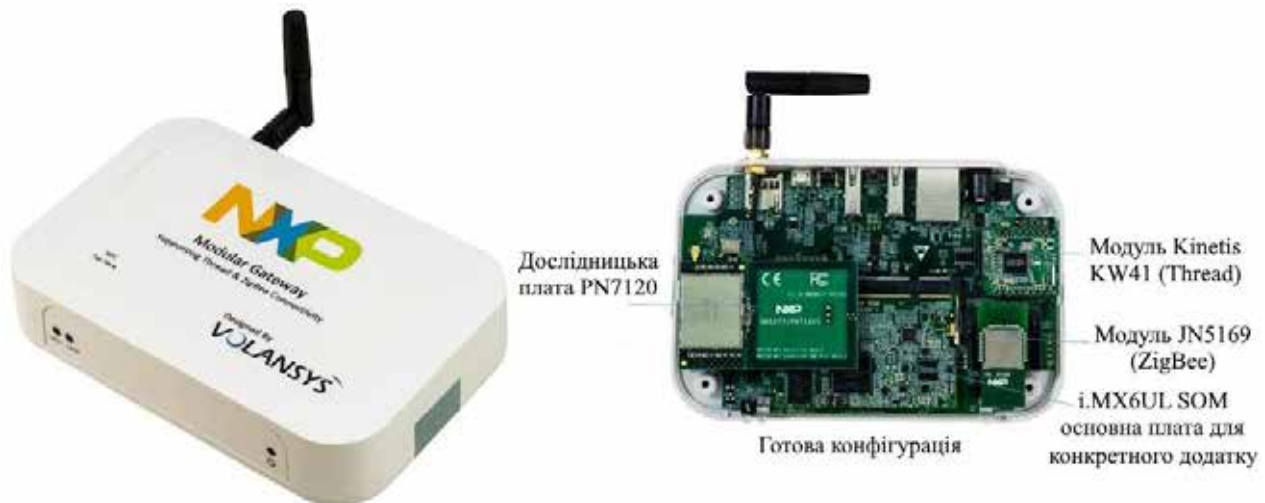


Рис. 4. IoT Modular Gateway Solution від компанії «NXP»

Сформовано авторами

в двох рівних мережах. Шлюз NXP Modular IoT використовується для крупних вузлів мережі на основі системи з модулем Volansys і MX6UL з підтримкою протоколів безпроводного зв'язку, таких як ZigBee, NFC, а також містить допоміжні модулі Wi-Fi та Bluetooth. Основна функція шлюзу полягає в тому, що слугує «дверима» між двома мережами, що може бути сервером, брандмауером, маршрутизатором або будь-яким іншим пристроєм, який використовує трафік для проходження через мережу. Шлюзи слугують точками входу і виходу мережі, так як всі данні повинні проходити через комунікаційний шлюз, перш ніж вони дійдуть до маршрутизатора. На рис. 4 показано шлюз Modular IoT від компанії «NXP», який

містить в собі безліч модулів для підтримки бездротового зв'язку, наприклад, Wi-Fi, Bluetooth, ZigBee, Thread, NFC для використання пристроями IoT.

Далі розглянемо архітектуру M2M з використанням дротових та бездротових технологій в технології Smart Home. На рис. 5 показано алгоритм послідовності прив'язки обладнання M2M з пристроями IoT за допомогою бездротових та дротових мереж. Застосунки та додатки за допомогою інтеграції M2M з IoT забезпечується контроль спарених пристроїв за допомогою смартфона, де здійснюється контроль та керування освітленням, побутовою технікою тощо. Окрім того, на рис. 5 показано шлюз M2M, взаємодію з мере-

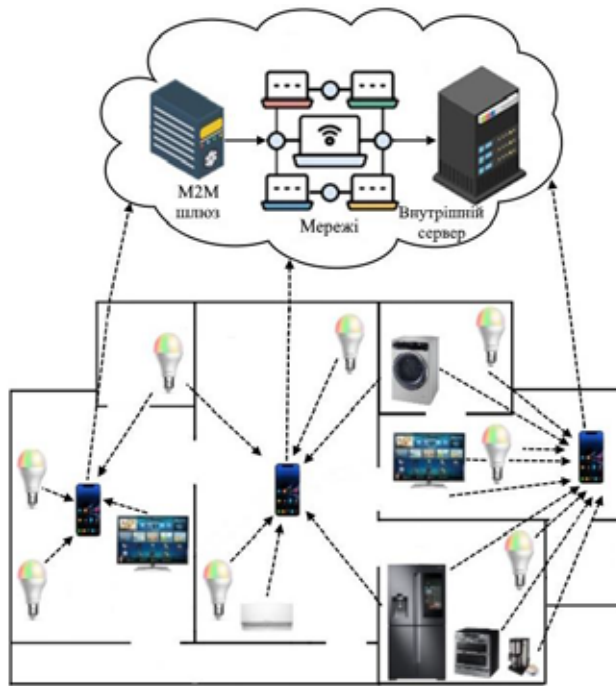


Рис. 5. Архітектура M2M з використанням дротових та бездротових технологій в технології Smart Home

Сформовано авторами

жами та внутрішній сервер, що дозволяє взаємодіяти машинам з IoT за допомогою смартфона. Також на рисунку показано основну побутову техніку та прилади, які мають взаємодіяти з технологією M2M. Наприклад, за допомогою смартфона (POCO X3 PRO) відбувалася взаємодія з технологією «розумного» будинку, яка дозволяє керувати освітленням в приміщенні, побутовими приладами, сантехнікою, а також системами мультимедіа.

Важливим компонентом M2M-комунікації є внутрішній сервер. Для всіх пристроїв створюється інтегрована точка збору даних. M2M-пристрої можуть бути стаціонарними, такими як побутова техніка або мобільні пристрої. Пристрої підключаються до основної мережі за допомогою мережі Access. А дротове рішення забезпечує найвищу швидкість передачі даних, надійність, безпеку та низьку затримку, але всі M2M-з'єднання в результаті цього можуть бути втрачені. Однак низька швидкість передачі даних, слабка захищеність і серйозні перешкоди згадані в універсальній інфраструктурі, створюють обмеження на використання M2M [26].

Принципи вимірювання відстані та кількості підключених пристроїв з використанням шлюзу для пристроїв IoT

Використання шлюзу для IoT розглядається з використанням позиційного підходу з евклі-

довою відстанню, який заснований на позиціюванні, де відстань вимірюється за допомогою формули прямої відстані між двома точками. Для вимірювання евклідової відстані між пристроями та шлюзом використовується наступна формула [22, 26]:

$$ED = \sqrt{(q_2 - q_1)^2 + (p_2 - p_1)^2} \quad (1)$$

де ED – евклідова відстань; q_1, p_1 , – координати шлюзу та q_2, p_2 – координати пристрою IoT у прямокутній системі координат.

Цю залежність на основі рівняння можна зобразити графічно, де на рис. 6 показано відстань між двома точками згідно з теоремою Піфагора.

Окрім того, рівняння для вимірювання евклідової відстані між окремими пристроями та різними точками доступу до шлюзу враховує також розташування окремих вузлів, які можуть збігатися між собою, що дозволяє вимірювати відстань для компактних або ізольованих кластерів для бездротової мережі [22].

Наведемо розрахунки евклідової відстані, де координати шлюзу q_1, p_1 дорівнюють 3 і 5, а координати пристрою IoT q_2, p_2 дорівнюють 7 і 9. Підставляємо дані згідно з рівняння (1):

$$ED = \sqrt{(7 - 3)^2 + (9 - 5)^2}$$

$$ED = \sqrt{(4)^2 + (4)^2} = \sqrt{16 + 16} = \sqrt{32} \approx 5,65$$

Отже, евклідова відстань між шлюзом та пристроєм IoT складає приблизно 5,66 м.

До обмеження евклідової відстані відноситься те, що якщо значення атрибутів в двох векторах даних не є нормальним, то тоді відстань між цими двома векторами може бути меншою, ніж між парою інших векторів даних з ідентичними значеннями атрибутів.

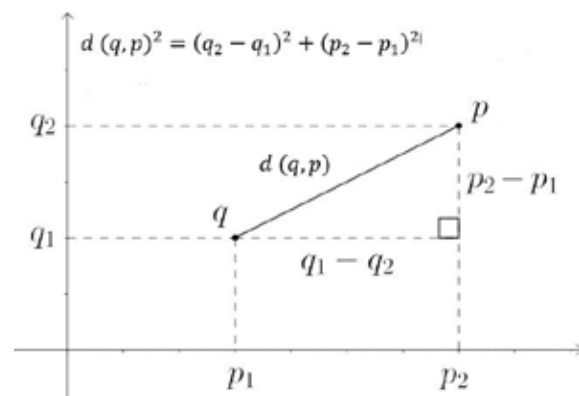


Рис. 6. Відстань двох точок у прямокутній системі координат на основі теореми Піфагора

Далі розглянемо приклад обчислення кількості підключених пристроїв IoT за допомогою формули (2). Ця формула може бути корисною для оцінки масштабу мережі IoT і розрахунку необхідних ресурсів для її підтримки [27]. Припустимо, що наші вихідні дані згідно рис. 5 складають:

- загальна кількість пристроїв, які необхідно підключити до мережі IoT $N = 15$;
- максимальна кількість пристроїв, яку може підтримувати шлюз $M = 20$.

Формула для обчислення кількості необхідних шлюзів:

$$W = \left\lceil \frac{N}{M} \right\rceil \quad (2)$$

Тоді $W = \left\lceil \frac{15}{20} \right\rceil = [0,75] = 0,75$ (1 шлюз)

Отже, для підключення 15 пристроїв IoT в двокімнатній квартирі достатньо одного шлюзу.

Припустимо, що під час дослідження необхідно проводити моніторинг мережі IoT протягом 24 годин ($t=24$), а середній інтервал між кожним підключеним пристроєм становить 30 хвилин ($\tau = 30$). Розрахуємо кількість підключених пристроїв:

$$k = \frac{t}{\tau} = \frac{24}{0,5} = 48$$

Таким чином, очікується, що за 24 години моніторингу матимемо приблизно 48 пристроїв IoT за умови, якщо середній інтервал між повторними підключеннями становитиме 30 хв.

В даній роботі на основі інтеграції систем з використанням архітектури M2M та бездротових технологій у поєднанні з пристроями IoT було досліджено та проаналізовано можливості технології «розумного» будинку. В якості аналізу розглядалися можливості технології «розумного» будинку згідно з принципами, які пов'язані з вимірюванням відстані та обчисленням кількості пристроїв для використання шлюзу Modular IoT від компанії «NXP», де для підключення 15 пристроїв через бездротову технологію Wi-Fi знадобився один шлюз, який на основі розрахунку евклідової відстані повинен забезпечувати підключення на відстані від 5,65 м і більше. Протягом 1 доби загальна кількість підключених пристроїв склала 48 одиниць з повторним підключенням до мережі.

Результати були отримані на основі теоретичних та статичних методів, а також проведеного літературного огляду, де розглядалися схожі за темою дослідження інших авторів. На основі отриманих результатів в нашому дослідженні

можна провести порівняння з іншими роботами, де замість принципів розглядаються алгоритми розгортання шлюзу, де в роботі [22] описується рішення розміщення шлюзів, що забезпечує підвищення загальної ефективності мережі IoT, оскільки великий обсяг даних створюється для підтримки різних додатків в розумних технологіях. Окрім того, автором також розглядається оптимізація енергоефективності системи на основі відстані для досягнення оптимальної пропускної здатності бездротової мережі. Проаналізувавши отримані результати нашого дослідження можна зробити припущення, що в роботі [22] автором наведений короткий опис використання формул (де згадуються формули евклідової відстані та позиційного підходу з Манхеттенською відстанню без наведення розрахунків) для вибору оптимального шлюзу та алгоритмів (вибір місця розташування шлюзу).

Технологія «розумного» будинку враховує безліч факторів та пристроїв, які описуються використанням побутової техніки, освітлення, кондиціонерів та електроніки, що в загальному дозволяє обмінюватися даними дистанційно за допомогою безпроводних мереж та хмарних платформ. Тому наше дослідження спрямоване на вивчення системи домашньої автоматизації, яка дозволить автоматизувати всі важливо необхідні процеси для життєзабезпечення користувачів з метою задоволення власних потреб. В роботі [28] в якості такої системи пропонується Wireless Fidelity як комунікаційний інтерфейс, що дозволяє заощадити на розробці системи домашньої автоматизації, а також інтегрувати з комерційними продуктами.

Архітектура технології систем M2M в поєднанні з пристроями IoT містить певні характерні особливості, які розглядаються для сучасних досліджень, але якщо провести порівняння з іншими наявними дослідженнями, то тоді можна зробити наступний висновок. В роботі [29] авторами описується одна з задач нашого дослідження, що обумовлюється реалізацією архітектури, яка дасть змогу контролювати та допомагати користувачам розраховувати споживання енергії за допомогою технологій Інтернету речей, а також пропонує детальну інформацію про споживання та рекомендує засоби для покращення оптимізації.

Окрім використання бездротової технології Wi-Fi для передачі даних, також активно розвиваються та вдосконалюють вертикалі IoT, які працюють з підключенням до SIM-карт мобільного зв'язку, що спрямоване на масштабне дослідження

дження комерційно розгорнутих SIM-карт IoT для лічильників, в якості «розумних» пристроїв.

До обмежень нашого дослідження можна віднести наступне: обмежені літературні джерела для вимірювання відстані з використанням шлюзу M2M для пристроїв IoT; складне середовище розумного будинку, що пояснюється різною конфігурацією та стандартами зв'язку (стандартизація та сумісність); конфіденційність даних, де в роботі описується більше інтеграція, архітектура та масштабованість мережі, але менш значної ролі приділяється питанням безпеки та цілісності даних.

В якості перспективи для подальших досліджень необхідно буде в першу чергу акцентувати увагу на протоколи зв'язку з використанням стандартів, а також проаналізувати можливості використання «розумних» технологій для управління енергоефективністю будинком.

Практична цінність отриманих результатів дозволить іншим дослідникам звернути увагу на використання інтегрованої архітектури з використанням систем M2M та бездротових мереж в поєднанні з пристроями IoT, де автори зможуть використовувати принципи вимірювання відстані та кількості підключених пристроїв IoT з використанням різних видів шлюзу.

Висновки. В даній роботі згідно з поставленими задачами дослідження розглянуто та про-

аналізовано можливість інтеграції екосистеми M2M-комунікації у поєднанні з пристроями IoT, де досліджено основні аспекти інтеграції з існуючими інформаційними системами для побудови архітектури M2M з використанням бездротових мереж та пристроїв IoT. Досліджено характерні риси, характеристики та відмінності технологій M2M та IoT для побудови архітектури «розумної» технології управління будинком з використанням IoT Modular Gateway Solution від компанії «NXP».

В якості експериментальних досліджень використовувалися принципи для вимірювання відстані між пристроями IoT та шлюзом, а також наведені розрахунки кількості підключених пристроїв, де для підключення 15 пристроїв через бездротову технологію Wi-Fi знадобився один шлюз, який на основі розрахунку евклідової відстані повинен забезпечувати підключення на відстані від 5,65 м і більше. Протягом 1 доби загальна кількість підключених пристроїв склала 48 одиниць з повторним підключенням до мережі.

Практична цінність отриманих результатів полягає в вивченні комунікаційних процесів між шлюзом M2M та пристроями IoT за допомогою бездротового зв'язку, де з'ясовано, що кількість шлюзів суттєво впливає на відстань між пристроями та шлюзом, а також на кількість підключених пристроїв до шлюзу, де для одного шлюзу кількість пристроїв не повинна перевищувати 20 одиниць.

Список літератури:

1. Samy M.M., Anis W.R., Abdel-Hafez A.A., Eldemerdash H.D. An Optimized Protocol of M2M Authentication for Internet of Things (IoT). *International Journal of Computer Network & Information Security*, 2021. № 13(2).
2. Railkar P.N., Mahalle P.N., Shinde G.R. Scalable trust management model for machine to machine communication in Internet of Things using fuzzy approach. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 2021. № 12(6), P. 2483-2495.
3. Salama R., Altrjman C., Al-Turjman F. An overview of the Internet of Things (IoT) and Machine to Machine (M2M) Communications. *NEU Journal for Artificial Intelligence and Internet of Things*, 2023. № 2(3).
4. Pradhan D., Tun H.M. Security challenges: M2M communication in IoT. *Journal of Electrical Engineering and Automation*, 2022. № 4(3), P. 187-199.
5. Gong X., Feng T., Albettar M. PEASE: A PUF-Based Efficient Authentication and Session Establishment Protocol for Machine-to-Machine Communication in Industrial IoT. *Electronics*, 2022. № 11(23), 3920 p.
6. Conti M., Kaliyar P., Lal, C. Secure machine to machine communication in industrial Internet of Things. *Security and Privacy Trends in the Industrial Internet of Things*, 2019. P. 199-219.
7. Sudarmani R., Venusamy K., Sivaraman S., Jayaraman P., Suriyan K., Alagarsamy M. Machine to machine communication enabled internet of things: a review. *International Journal of Reconfigurable and Embedded Systems*, 2022. № 11(2), 126 p.
8. Djehaich R., Aidel, S., Sawalmeh A., Saeed N., Alenezi A.H. Adaptive Control of IoT/M2M Devices in Smart Buildings Using Heterogeneous Wireless Networks. *IEEE Sensors Journal*, 2023. № 23(7), P. 7836-7849.
9. Mazhar M.S., Saleem Y., Almogren A., Arshad J., Jaffery M.H., Rehman A.U., Hamam H. Forensic analysis on internet of things (IoT) device using machine-to-machine (M2M) framework. *Electronics*, 2022. № 11(7), p. 1126.
10. Lara E., Aguilar L., Sanchez M.A., García J.A. Lightweight authentication protocol for M2M communications of resource-constrained devices in industrial Internet of Things. *Sensors*, 2020. № 20(2), 501 p.

11. Thota P., Kim Y. Implementation and comparison of M2M protocols for Internet of Things. In *2016 4th Intl Conf on Applied Computing and Information Technology/3rd Intl Conf on Computational Science/Intelligence and Applied Informatics/1st Intl Conf on Big Data, Cloud Computing, Data Science & Engineering (ACIT-CSII-BCD) 2016*. pp. 43-48. IEEE.
12. Rajendrakumar J.S., Thakur M. Wireless Communication for Machine-to-Machine (M2M) Connectivity in the Internet of Things (IoT). *NeuroQuantology*, 2022. № 20(17), 2273 p.
13. Pradhan D., Tun H.M. Security challenges: M2M communication in IoT. *Journal of Electrical Engineering and Automation*, 2022. № 4(3), p. 187-199.
14. Tsai W. C., Tsai T. H., Xiao G. H., Wang T. J., Lian Y. R., Huang S. H. An automatic key-update mechanism for M2M communication and IoT security enhancement. In *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)* 2020. pp. 354-355. IEEE.
15. Mazhar M.S., Saleem Y., Almogren A., Arshad J., Jaffery M.H., Rehman A.U., Hamam H. Forensic analysis on internet of things (IoT) device using machine-to-machine (M2M) framework. *Electronics*, 2022. № 11(7), 1126 p.
16. Leminen S., Rajahonka M., Wendelin R., Westerlund M. Industrial internet of things business models in the machine-to-machine context. *Industrial marketing management*, 2020. № 84, p. 298-311.
17. Amaya M.O.B., Parra O.J.S., Miranda J P.R. Ontological base models machine-to-machine M2M applied to the internet of things IOT. *Revista Boletín Redipe*, 2021. № 10(12), p. 148-161.
18. Yang Y., Xie W. Composition and Communication Analysis of M2M System in Internet of Things. In *2021 International Conference on Artificial Intelligence and Electromechanical Automation (AIEA)*, 2021. pp. 113-116. IEEE.
19. Raza M.S., Zongsheng T., Muslim M.M.A. A review of human-to-machine and machine-to-machine approaches for internet of things. In *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, 2021. pp. 1-5. IEEE.
20. Kanakamedala P., Harika Y., Krishnaveni M., Nallani, B. Internet of Things (IoT) Device Investigative Analysis Using Machine-to-Machine (M2M) Framework. *International Research Journal on Advanced Science Hub*, 2023. Vol. 05, Issue 05S. p. 2582-4376. 10.47392/IRJASH.2023.S007
21. Pradhan D., Tun H.M. Security challenges: M2M communication in IoT. *J. Electr. Eng. Autom*, 2022. № 4(3), p. 187-199.
22. Patil S. Distance aware gateway placement optimization for machine-to-machine (m2m) communication in iot network. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 2021. № 12(2), p. 1995-2005.
23. Patil S. Distance aware gateway placement optimization for machine-to-machine (m2m) communication in iot network. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 2021. № 12(2), p. 1995-2005.
24. Gupt B.B., Quamara M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience*, 2020. 32(21), 4946 p.
25. Lokhande M.P., Patil, D.D. Device classification for machine to machine communication in internet of things for tele-robotic surgery: a review. p. 618-628.
26. Itmamunafi A., Wibowo S.A., Vendyansyah N. Design and Build the LabM2M Platform as an IoT (Internet Of Things) Gateway Using Web Services. *International Journal of Computer Science and Information Technology*, 2024. № 1(1), p. 15-22.
27. Djehaiche R., Aidel S., Benhamimid K. A Smart Home Management based on M2M/IoT Technologies, 2022. p. 1-10.
28. Djehaiche R., Aidel S., Benziouche N. Design and implementation of M2M-Smart home based on Arduino-UNO. In *Artificial Intelligence and Renewables Towards an Energy Transition 4*, 2021. pp. 697-706. Springer International Publishing.
29. Ejigu MW., Santhosh J. IoT based comprehensive autonomous home automation and security system using M2M communication. *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, 2021. № 14(7), p. 2234-2246.
30. Thirumaran J., Kathirvelkumaran L. Internet of Things (IoT) and Machine-to-Machine (M2M) communications. *Research Journal of Science & IT Management*, 2015. № 5(01), p. 5-10.

Sokulskyi O.Ye., Topolskov Ye.O., Zhdanova Yu.D. ANALYSIS OF INFORMATION TECHNOLOGY CAPABILITIES USING MACHINE-TO-MACHINE COMMUNICATION (M2M) FOR THE INTERNET OF THINGS

The purpose of this study is to analyse the capabilities of machine-to-machine (M2M) and Internet of Things (IoT) systems for building an integrated smart home architecture.

Theoretical and statistical research methods were used for the analysis. Statistical methods allow to determine the common relationship of input and output parameters between M2M and IoT, as well as to analyse the integration parameters of the two systems to build an integration model.

On the basis of theoretical and empirical research methods, the article analyses the possibility of integration of M2M and IoT technologies with a comparison of the purpose of each technology. It has been found that by integrating M2M communication systems with IoT devices, the integration consists of the basic ones, such as providers, Internet services, platforms and services. However, for integration, it is important to consider the underlying aspects, which consist of protocols and standards, cloud technologies, data analytics, security and safety, integration with existing systems, monitoring and management. In addition, it is also analysed that the integration of M2M with IoT combines factors to ensure it, which includes the following: ensuring communication; analytics, data collection and processing; effective resource management, security and encryption; scalability and flexibility; energy efficiency and optimisation.

The study analyses the possibility of integrating M2M with IoT to build a smart home architecture using wired and wireless networks. The main characteristics and differences between M2M and IoT are analysed, on the basis of which the architecture of a smart home was built on the example of a two-room apartment.

Based on the M2M architecture using wired and wireless technologies in Smart Home technology, the algorithm of the sequence of linking M2M equipment with IoT devices using wireless and wired networks is analysed. Applications and applications using the integration of M2M with IoT provide control of paired devices using a smartphone, where lighting, household appliances, etc. are monitored and controlled.

Key words: *machine-to-machine, Internet of Things, integration, gateway, wireless networks, smart home.*