УДК 621.396.1

ОСНОВНІ ХАРАКТЕРИСТИКИ СИСТЕМ INTERNET OF THINGS

Новогрудська Р. Л., Миніч М. А.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: rinan@ukr.net, marinka43753@gmail.com

MAIN CHARACTERISTICS OF SYSTEMS INTERNET OF THINGS

The research devotes to the review of systems Internet of things. The main characteristics and features of IoT systems, potential areas of use of such systems are presented, as well as a list of problems associated with their implementation.

Наведене дослідження присвячено огляду систем Internet of Things. Наведено основні характеристики та особливості систем IoT, потенційні сфери використання таких систем, а також перелік проблем, пов’язаних з їх впровадженням.

На сьогоднішній день Internet of Things (IoT) широко використовується в різних сферах. Наприклад, транспортування, охорона здоров'я, комунальні послуги, логістика, фармацевтика та інші. У майбутньому, майже всі активні пристрої матимуть інтернет-інтерфейс. Компанії і вчені звертають увагу на забезпечення рішення для двох проблем: опрацювання великих об'ємів інформації, що надходить з пристроїв і розпізнавання необроблених даних. Парадигма IoT охоплює величезну кількість різних областей і здатна атакувати різні існуючі і майбутні проблеми, пов’язані з апаратним забезпеченням, потужністю, безпекою, надійністю, сумісністю та проблеми обміну даними [1]. Тому, на даний момент ці проблеми є актуальними, так як технологія IoT застосовуватиметься в найближчому майбутньому.

IoT поєднує всі види речей, пов’язаних з інтернетом. Ці «речі» включають все, починаючи від сенсорів руху, пристроїв, що вимірюють температуру та закінчуючи різними типами смарт речей, таких як, смартфони, автономні автомобілі, будівлі та ін. Всі ці пристрої в майбутньому будуть збирати дані, ділитися інформацією і функціонувати раціональним шляхом, тому наше життя стане легшим і гармонійним.

Для кращого розуміння технологій IoT досліджено пов’язані сфери, такі як всепроникаючий комп’ютинг, інтегрований інтелект, розумні будинки та міста, зв’язок від машини до машини (M2M), бездротові сенсорні мережі, семантичні сенсорні мережі, семантика та великі дані, машинне навчання.

Потенційні домени додатків IoT. IoT має величезний ринковий потенціал в останні роки. У 2014 році було 1,5 мільярди інтернет-ком’ютерів і 1 мільярд мобільних телефонів з підтримкою інтернету. До 2020 року кількість IoT пристроїв, підключених до інтернету, становитиме близько 50-100 мільярдів [2]. IoT використовується в найрізноманітніших доменах додатків. Для прикладу: авіація, навчання, енергія, розваги і спорт, екологія, фінанси, влада, розумні будинки, логістика, важка індустрія та багато інших.

Характеристики та особливості IoT. У світі IoT існує мільярди пристроїв. Деякі з них мають високорівневі архітектури з великими

можливостями пам'яті, високою швидкістю процесора (наприклад, мобільними телефонами). Тим часом деякі з них, навпаки, мають архітектуру низького рівня, обмежену пам'ять та обчислювальні можливості (наприклад, датчики температури). Взаємозв'язок між цими пристроями робить IoT дуже складною системою взагалі.

Хмарні обчислення грають важливу роль в екосистемі IoT. За допомогою хмарних обчислень можуть бути збільшені обчислювальні ємності і обсяги для зберігання. Крім того, датчики можуть використовуватися скрізь, і дані з них можуть опрацьовуватись через служби хмарних обчислень.

Питання безпеки і конфіденційності піднімаються через велику кількість пристроїв і відсутність уніфікованої стандартизації вивчення безпеки IoT. Кожен пристрій, що підключений до інтернету може викликати проблеми з безпекою. Тому, такі дослідження не повинні ігноруватись. Дослідження і реалізація безпеки IoT в останні роки стає передовим питанням через атаки DoS (відмова в обслуговуванні). Згідно з опитуванням Мохамеда [3] щодо різних загроз, пов’язаних з IoT, визначено такі категорії: відмова в обслуговуванні, фізичні атаки, підслуховування та пасивний моніторинг, аналіз трафіку та виведення даних. Також розглянуті питання безпеки та конфіденційності в IoT належать до конфіденційності користувачів та захисту даних, аутентифікація та управління ідентифікацією, політика інтеграції, авторизації та контролю доступу, надійні рішення для атак.

Проблеми впровадження IoT. Зрозуміло, що у наступні роки буде проведено багато розробок IoT, але також необхідне проведення досліджень та аналізів у майбутньому. Нижче наведені основні напрями розвитку IoT та проблеми його впровадження.

1. Підвищення IoT стандартів

За підтримки компаній та дослідницьких груп за останні роки прикладено багато зусиль для стандартизації IoT. Хоча, все ще не вистачає стандартизації в реалізації машинного навчання і у великих структурах обробки даних. Зрозуміло, що при впровадженні нової технології формування загальноприйнятої стандартизації займає деякий час. Протягом процесу стандартизації, різні вендори та компанії лише з декількох спроб реалізують свої системи.

2. Приватність та безпека IoT

Зростає турбота про проблеми безпеки та конфіденційності, які потребують розділеного доступу, високошвидкісний потік даних, автономне прийняття рішень тощо. Зі зростанням складності таких мереж, стає набагато складніше підтримувати загальну безпеку та конфіденційність. Кібербезпека стала однією з найважливіших областей завдяки вищезгаданим проблемам у світі IoT. Збільшення заходів безпеки може погіршити продуктивність обробки даних IoT. Мабуть, це одне з головних відкритих питань.

3. Використання семантики в світі IoT

Семантичний веб використовується в нижніх шарах розробки IoT, наприклад, онтологія SSN, опис датчиків і датчики даних. Оскільки, неоднорідність і розмір світового IoT розширюється, то сумісність між

пристроями, фреймфорками та системами стане ще важчою. M2M стандарт намагається подолати це, використовуючи семантичні технології абстракції і сумісність.

4. Розробка систем навчання для IoT

Декілька років тому були розроблені навчальні системи та рішення з особливостями контекстної обізнаності. Вони в основному розроблені логічно, правильно і з використанням різноманітних алгоритмів. Нейронні мережі можуть використовуватись більш широко з великими даними IoT, що швидко накопичуються, а отже рішення побудови IoT систем можуть вдосконалитися. Нові навчальні фреймворки для більших IoT розробок зі значно більшим трафіком даних можуть бути розроблені з новими великими аналітичними даними та рішеннями.

5. Впровадження та розробка методів глибокого навчання

Однією з основних характеристик глибокого навчання є використання низькорівневих функцій (або навіть самих вихідних даних) і перетворення їх у змістовні, висококласні функції в межах моделі шляхом застосування неконтрольованого та контрольованого навчання за допомогою каскадних шарів. Для успішної реалізації глибокого навчання загалом потрібні великі набори даних, де модель вивчає приховані функції високого рівня. Це добре підходить для великих даних та концепції IoT.

6. Підвищення автономії та впровадження самоорганізованого IoT

Структури програм IoT можуть бути розширені та розроблені з повністю автоматизованим зв'язком M2M, автоматичними міркуваннями та системами навчання. Не надаючи інформацію та повідомлення людям для взаємодії та прийняття рішень, пристрої зможуть сприймати, навчитися, взаємодіяти та вирішувати різні питання, використовуючи системи та рішення IoT. Цифрові персональні помічники, які керують усіма навколишніми пристроями, і спілкуються з іншими рішеннями з особистої допомоги, можуть бути додатково розроблені. Розроблені знання структур IoT можуть бути вдосконалені. Розумні міста, які керують усіма пристроями IoT та спілкуються з іншими розумними містами, автономними транспортними засобами, розумними дорожними системами, інтелектуальними мережами та системами виробництва енергії, а також більш розумною планетою, можуть бути майбутніми проектами та ініціативами з використанням рішень IoT.

Проаналізувавши інформацію щодо IoT, впевнено можна сказати, що проблем і невирішених питань досить багато і вони потребують зусиль для вирішення. Тому дослідження і розробки передових компаній та розробників спрямовані на покращення функціонування цієї передової технології IoT.

Література

1. Internet of Things Global Standards Initiative. Internet of Things Global Standards Initiative. 2015. URL: www.itu.int.
2. Charith Perera et al. “Semantic-Driven Configuration of Internet of Things Middleware”. In: 9th International Conference on Semantics, Knowledge and Grids. IEEE, 2013, pp. 66–73.
3. Mohamed Abomhara and Geir M. Koien. “Security and privacy in the Internet of Things: Current status and open issues”. In: 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS). IEEE, May 2014, pp. 1–8.