КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (6), 2019
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2019.6.618
УДК 004.77

Белей Олександр Ігорович
к.е.н., доцент, доцент кафедри САП
місце роботи: Національний університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0003-4150-7425
Oleksandr.I.Belei@lpnu.ua

Логутова Тамара Григорівна
д.е.н., професор, завідувач кафедри інноватики та правління
місце роботи: Державний вищий навчальний заклад «Приазовський державний технічний університет», Маріуполь, Україна
ORCID ID: 0000-0001-5664-2908
Logutova_t_g@pstu.edu

БЕЗПЕКА ПЕРЕДАЧІ ДАНИХ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

Анотація. У статті обговорюється протокол MQTT для Інтернету речей та сенсорних безпровідних мереж, його особливості, варіанти застосування та конкретні процедури. Проаналізовано інформаційні елементи та принципи власника повідомлення. Ця стаття охоплює такі теми, як безпечне зберігання даних Інтернету речей, передачу цих даних через захищений інтерфейс мобільних пристроїв та веб-додатків. Також розглядаються всі ключові інструменти, передбачені протоколом MQTT для захисту інформації. Запропонована у цій статті ідентифікація користувачів здійснюється щляхом їх визначення із бази даних Cloudant. Таке застосування працює на сервері сервера Node.js в середовищі IBM Bluemix і надає інтерфейс API або RESTful, для яких потрібен мобільний клієнтський доступ аутентифікації користувачів. Послуга доступу до мобільного клієнта призначена для виклику цих двох API у будь-якому застосуванні аутентифікації. Запропоновано використовувати окремі підходи до аутентифікації: для веб-додатку - на Cloud Directory, а для мобільного додатку - MobileFirst Client Access. Однак і веб, і мобільні додатки використовують один і той же рівень захисту додатків, щоб дозволити користувачеві доступ до даних пристрою. Для покращення безпеки повідомлень запропоновано використовувати протокол транспортного рівня безпеки, які використовує різні криптографічні методи. Нам пропонується гомоморфне шифрування цих протоколів. Протокол транспортного рівня безпеки збільшує продуктивність протоколу і зменшує обчислювальні витрати, однак він не застосовується при початковому підключенні до сервера або у випадках, коли попередній сеанс вже минув. У статті представлено алгоритм виявлення порушення слабкої симетрії для аналізу випадковості відновленого електронного повідомлення. Запропоновано метод гомоморфного шифрування та аутентифікації користувачів і їхніх електронних повідомлень в безпровідних сенсорних мережах Інтернету речей.

Ключові слова: дані IoT; безпека; інтерфейс програмних застосувань; протокол MQTT; хмарна база даних; сценарій; протокол TLS; шифрування даних; сигнал передачі; хаотичні сигнали.

1. ВСТУП

Безпека Інтернету речей стає ключовим аспектом побудови таких безпровідних сенсорних мереж. Отримавши доступ до одного пристрою, зловмисник може проникнути в мережу, і тоді будь-яка інформація перестає бути конфіденційною. Це

ISSN 2663 - 4023

передбачає актуальність питань захисту інформації в таких мережах, де необхідно враховувати обмеження підключених до них пристроїв.

Основною перевагою, відмінною особливістю хмарних сховищ даних, будь-якої моделі розгортання, є можливість доступу до даних з будь-якого пристрою, що має доступ в Інтернет. Користувачі мають можливість опубліковувати свої файли, ділитися ними, редагувати їх, переглядати в браузері. Хмарний сервіс також зберігає історію змін файлів. Є у них і можливість синхронізації папок між пристроями - персональним комп'ютером, смартфоном, планшетом. Хмарні сховища дозволяють організовувати спільний доступ до файлу для його перегляду або редагування шляхом встановлення користувачем певного кола осіб. Збереження даних гарантується завдяки використанню провайдером «хмарних» послуг резервних дисків з копіями файлів. Для захисту даних користувача від перегляду сторонніми особами використовується шифрування цих даних. Залежно від сервісу, ключ може зберігатися на стороні сервера або на стороні користувача. У першому випадку система забезпечує конфіденційність ключа і даних, розшифровуючи їх для користувача. У другому випадку захищені дані розшифрувати зможе лише сам користувач або той, кому користувач особисто передасть ключ. Однак при втраті цього ключа сам користувач виявиться без можливості їх розшифровки.

Для забезпечення належного рівня безпеки інфраструктури IoT необхідна комплексна стратегія захисту. Вона забезпечує захист даних у хмарі, захист цілісності даних під час передачі через Інтернет, а також безпечний зв'язок між пристроями. Зараз існує безліч хмарних сховищ даних [1], кожне з яких пропонує певний набір функцій, і, звичайно, має свої переваги та недоліки. У статті [2] розглянуто приклад аналізу відповідності DSS Cloud PCI і обговорено хмарну безпеку з врахуванням можливих інцидентів.

Постановка проблеми. Враховуючи численні вимоги до безпеки, конфіденційності, прозорості та дотримання вимог, вибір постачальника послуг IoT стає дуже важким завданням. Надійний постачальник програмного забезпечення та послуг IoT повинен мати великий досвід розробки таких послуг, які охоплюють різні рівні інфраструктури, враховують географічне розташування та надають інструменти для безпечного та прозорого горизонтального масштабування. Великою перевагою для вибраного постачальника буде також багаторічний досвід розробки захищеного програмного забезпечення, встановленого на мільйонах комп'ютерів по всьому світу, а також можливість швидко та професійно оцінити та усунути загрози, пов'язані із впровадженням IoT.

Аналіз останніх досліджень і публікацій. Використання традиційних методів захисту пристроїв IoT, таких як шифрування та введення заходів фізичної безпеки, вимагає значної реінжинірингу та адаптації, оскільки пристрої мають багато обмежень. Наприклад, для зберігання шкідливих підписів та чорних списків може знадобитися багато місця на диску, що не завжди можливо. IoT зазвичай складається з портативних пристроїв з низьким енергоспоживанням, малим форм-фактором та обмеженими можливостями. Часто пристрої працюють без участі оператора, який міг би ввести облікові дані або вирішити, наскільки довірена команді чи додатку, тому пристрої повинні приймати такі рішення самостійно. Архітектура систем IoT вимагає безпровідних мереж та хмарної бази даних для зв'язку.

Сенсорна мережа контролює дані про навколишнє середовище за допомогою електронних датчиків малої потужності та формує мережу за допомогою безлічі бездротових модулів XBee. Система сенсорної мережі та запропоновані методи збирання енергії в [3] налаштовані для досягнення безперервного джерела енергії для сенсорної

мережі. Бездротова система WBAN використовує медичні діапазони для отримання фізіологічних даних із сенсорних вузлів [4]. Медичні смуги вибираються для зменшення перешкод і, таким чином, збільшення співіснування пристроїв сенсорних вузлів з іншими мережевими пристроями, наявними в медичних центрах.

Вузол датчика передає кілька імпульсів на біт для збільшення середньої потужності переданого сигналу з метою поліпшення продуктивності швидкості передачі бітів (BER) [5]. Техніка множинного імпульсу на біт також використовується як схема кодування для ідентифікації окремих вузлів датчиків, коли більше ніж один датчик утворює мережу. Інший дає вичерпний огляд останніх систем, технологій та застосувань WBAN [6]. Різні фахівці, які є експертами у своїх областях досліджень та практики, написали глави книги.

До 2020 року через радіозв'язок буде підключено понад 50 мільярдів пристроїв [7]. У поєднанні зі швидким зростанням ринку Інтернету речей (IoT), широкосмугові мережі з низькою потужністю (LPWAN) стали популярною низькошвидкісною технологією радіозв'язку на великій відстані. Для задоволення вимог дальньої дальності, невеликого обсягу передачі даних, малої потужності та низької вартості Інтернету речей (IoT) у фактичних додатках застосовується підхід для моніторингу інформації з широкополосною мережею малої потужності на базі NB-IoT a LoRa пропонується в [8]. Цей підхід використовує режим зв'язку, який містить основний вузол та декілька підвузлів для адаптації до потреб широкомасштабного моніторингу інформації.

Постійний моніторинг стану здоров'я немовлят досягається розвитком та злиттям носячих чутливих технологій, бездротових технологій зв'язку та мікропроцесором з низьким споживанням енергії з високоефективними алгоритмами обробки даних [9].

Мета статті. Основна метою захисту хмарного додатку IoT є унеможливлення отримання доступу несанкціонованим користувачам до конфіденційних та приватних даних із пристроїв. Крім того, необхідно не допустити, щоб програма надсилала несанкціоновані команди на пристрої. Актуальність дослідження обумовлена стрімким розвитком архітектури користувачів Інтернету Речей, для якої цей протокол є найбільш характерним.

2. ПРОТОКОЛ ПЕРЕДАЧІ ДАНИХ ДЛЯ ЗАСТОСУВАНЬ ІНТЕРНЕТУ РЕЧЕЙ

Для зв'язку між собою пристрої використовують різні промислові протоколи і один з найпопулярніших протоколів для цього є MQTT. Повідомлення в протоколі MQTT обмінюються між клієнтом, який може бути власником або отримувачем повідомлень, та повідомленнями брокера.

Протокол MQTT вимагає обов'язкової наявності брокера даних. Це центральна ідея технології. Всі пристрої посилають дані тільки брокеру і приймають дані теж тільки від нього. Отримавши пакет, брокер надсилає його усім пристроям в мережі згідно їх підписці. Щоб пристрій щось отримав від брокера потрібно, щоб він «підписався» на топік. Топіки виникають динамічно за фактом передплати або за фактом приходу пакету з даними топіком. Топіки є зручним механізмом організації зв'язків різних видів: один до багатьох, багато до одного і багато до багатьох.

Видавець надсилає дані брокеру MQTT, вказуючи в повідомленні певну тему та тему. Абоненти можуть отримувати різні дані від декількох видавців, залежно від підписки на відповідні теми. На рис. 1 показаний загальний формат MQTT повідомлень.

ISSN 2663 - 4023

Повідомлення складається із заголовків: фіксованої довжини; змінна довжина; поля змінної довжини корисного навантаження.

У цій статті описано заголовок фіксованої довжини, оскільки основні особливості протоколу MQTT реалізовані з використанням полів цього заголовка. Перший байт заголовка включає чотири поля, три з яких - спеціальні прапори, четверте вказує на тип повідомлення. Другий байт використовується для позначення залишкової довжини повідомлення, яка є сумою розміру заголовка змінної довжини та величини корисного навантаження.

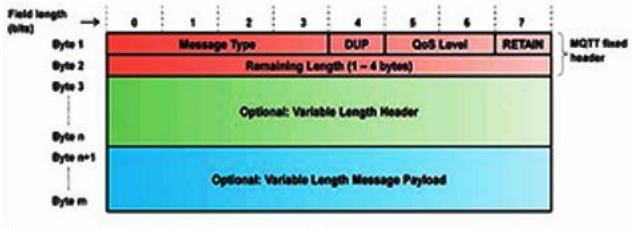

Рис. 1. Формат повідомлення для протоколу MQTT

До головних особливостей протоколу MQTT можна віднести можливість використовувати різні рівні обслуговування, які визначаються значенням цього прапора. Це робить протокол MQTT більш гнучким, на відміну від протоколу протоколу обмежених застосувань (CoAP), повідомлення якого можуть бути підтверджені або оброблені без підтвердження.

Видавець публікує повідомлення про брокера, а брокер публікує його передплатнику. Однак видавець не вимагає, щоб це повідомлення було гарантією передплатнику. Іншими словами, абонент може не отримувати це повідомлення, але видавець цього не відстежує. Описаний сценарій (рис. 3) використовується для тих випадків, коли втрата даних не є критичною. При постійному моніторингу температури, коли втрата одного вимірювання не відіграє значної ролі в загальній картині.

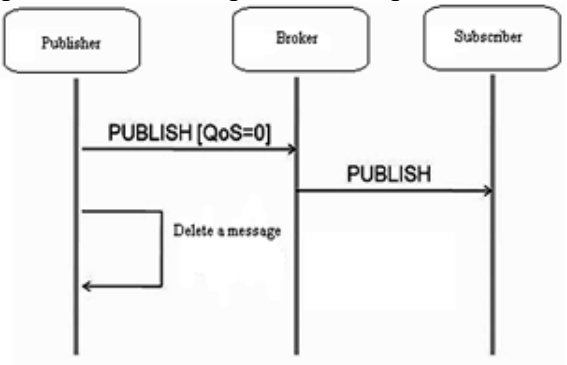

Рис. 2. Сценарій "Не більше одного"

Клієнт публікує повідомлення на брокері (ПУБЛІКАЦІЯ). Брокер зберігає це повідомлення і публікує його передплатнику. Лише після публікації повідомлення для абонента, брокер надсилає підтвердження публікації видавцю. Сценарій такої взаємодії показаний на рис. 3. Тобто, поки видавець не отримає передплатником підтвердження публікації; ця публікація буде надіслана брокеру та далі абоненту. Таким чином, абонент повинен отримати це повідомлення хоча б один раз.

ISSN 2663 - 4023

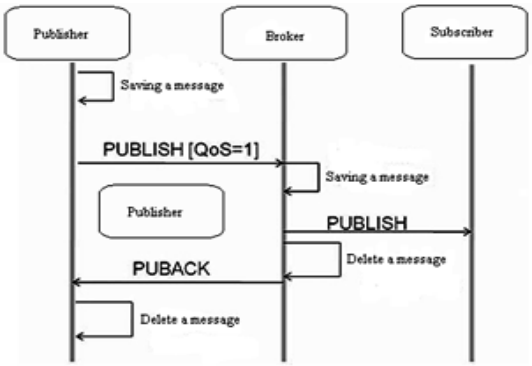

Рис. 3. Сценарій "Принаймні один"

Рівень QoS забезпечує найвищу гарантію доставки повідомлень з використанням додаткових процедур підтвердження та завершення публікації. Сценарій присутній на рис. 4 і підходить для ситуацій, коли потрібно усунути будь-які втрати та дублювання даних з датчиків.

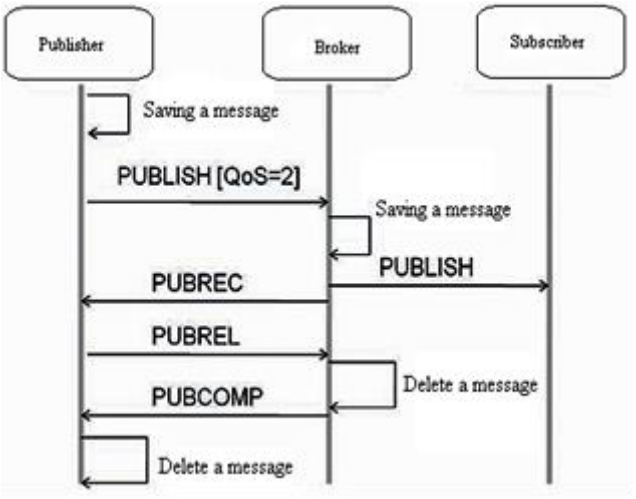

Рис. 4. Сценарій "Гарантований один"

Спеціальний параметр RETAIN використовується для позначення збереження останнього повідомлення, отриманого брокером. Тобто параметр "QoS=1" у повідомленні PUBLISH від видавця інформує брокера, що повідомлення на цю тему слід зберегти, а коли новий користувач приєднається до теми, надіслати йому це повідомлення.

Встановлення з'єднання з повідомленням про з'єднання починає надсилатися від клієнта до брокера. Він вказав: унікальний ідентифікатор для кожного клієнта, який підключається до брокера; прапор для видалення збережених повідомлень з попередніх сеансів для цього клієнта; ім'я користувача та пароль для ідентифікації та авторизації клієнта; інтервал часу, що регулює передачу запитів ping та відповідей ping для контролю відключення однієї із сторін.

ISSN 2663 - 4023

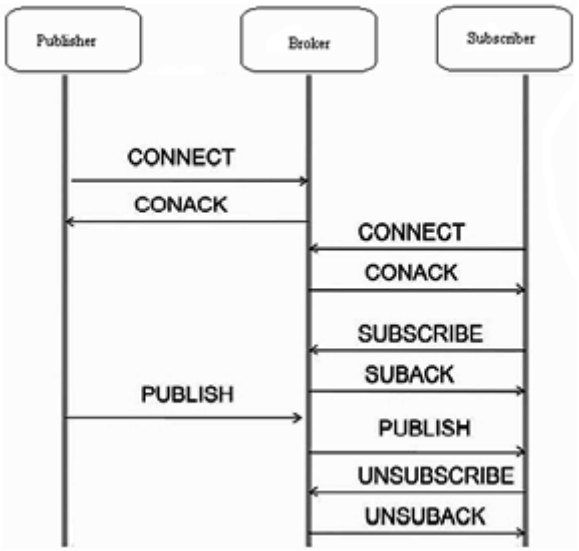

Рис. 5. Встановлений сценарій з'єднання та обміну повідомленнями

У відповідь брокер надсилає клієнту повідомлення CONACK, що складається з: вказує, чи існують сеанси для клієнта з попередніх з'єднань; повідомляє клієнта про успішне з'єднання або будь-які помилки.

Після того, як клієнт MQTT підключиться до брокера, він може розміщувати повідомлення. Публікація відбувається шляхом надсилання повідомлення брокеру від клієнта із зазначенням: назви теми, на яку повідомлення стосується. Це поле є обов'язковим, оскільки брокер MQTT вирішує, чи надсилати повідомлення клієнту, виходячи з того, на який клієнт підписаний; QoS, DUP та RITEIN; корисне навантаження, куди передаються самі дані. Отримавши повідомлення PUBLISH, брокер надсилає підтвердження про публікацію та передає отримане повідомлення всім клієнтам, які підписалися на цю тему.

3. МЕТОДИКА ЗАХИСТУ ДАНИХ В ЗАСТОСУВАННЯХ IoT

Серверна програма для демонстрації безпеки IoT, яка розглядається в цій статті, функціонує на основі Watson IoT і передає отримані дані в базу даних Cloudant для зберігання. Щоб продемонструвати безпеку IoT, програма шифрує деякі конфіденційні атрибути збережених даних під час передачі даних у сховище - корисне навантаження, яке отримане від пристроїв IoT. Корисне навантаження надходить у форматі JSON та зберігається у зашифрованому форматі AES сховища даних Cloudant. Воно розшифровується для авторизованих користувачів. Воно є прозорим для користувача.

До даних IoT, що зберігаються в базі даних Cloudant, можна отримати прямий доступ одним із двох способів: через сторонній додаток, який надає ключ API Cloudant; через розроблені API, що захищені службою безпеки Bluemix.

Коли ми додаємо службу DB Cloudant до Bluemix, для нашої програми формуються облікові дані доступу, щоб дозволяє програмно отримати доступ до сховища даних Cloudant. Ім'я користувача та пароль можна використовувати для створення ключів Cloudant API. Після створення ключ API можна використовувати так само, як і звичайний обліковий запис користувача.

ISSN 2663 - 4023

Пари ключів та паролів API використовуються так само, як і будь-який інший обліковий запис користувача. Можна передати ключ API іншим користувачам, щоб поділитися з ним базою даних та призначити відповідні дозволи. Пари ключі і паролі API можуть використовуватись у будь-якій ситуації, коли вихідний код має облікові дані для доступу і ми хочемо запрограмувати створення декількох облікових записів користувачів з різними дозволами.

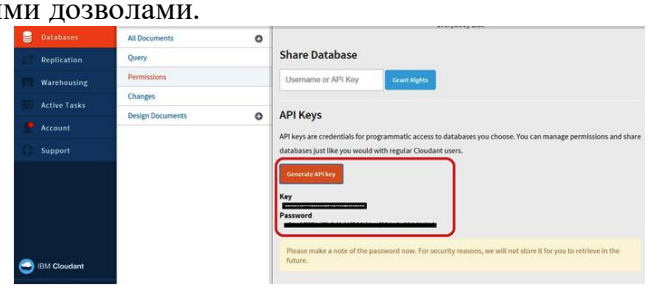

Рис. 6. Створення ключа API на інформаційній панелі Cloudant

Забезпечення прямого доступу до бази даних Cloudant робить інтеграцію із стороннім доступом нестабільною та дорогою в технічній підтримці. У цьому випадку ми використовуємо архітектуру, яка за допомогою спеціальних інтерфейсів API забезпечує шар інкапсуляції поверх бази даних. Спеціальні API приховують деталі, що стосуються бази даних, і повертають інформацію про пристрій від конкретного користувач.

Після того, як дані захищені та передані за допомогою спеціальних API, наступним кроком є захист цих API за допомогою аутентифікації та авторизації. Для виклику цих API, веб-додатки та мобільні додатки повинні надати необхідні облікові дані для аутентифікації для доступу до даних лише тих пристроїв, на які вони мають дозвіл. Для демонстрації захисту конкретних API нами використано мобільний клієнтський доступ на платформі IBM Bluemix.

На рис. 7 показаний підхід з уніфікованою аутентифікацією та авторизацією на основі послуги мобільного клієнтського доступу. Якщо використовується уніфікований підхід аутентифікації, і мобільні програми, і веб-додатки використовують один і той же постачальник аутентифікації та авторизацію на основі Cloudant для захисту даних пристрою та обмеження джерел, які можуть надсилати команди на пристрій.

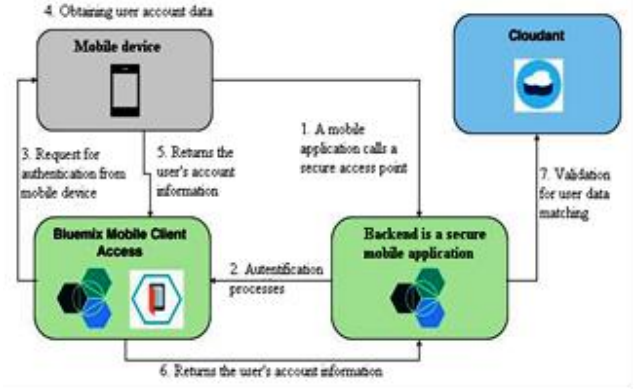

Рис. 7. Така сама аутентифікація, однаковий захист програми

У нашому веб-додатку для демонстрації SSO та авторизації в IoT використано Cloud Cloud Directory для підтримки спеціальної аутентифікації для веб-програми. Під

ISSN 2663 - 4023

час використання цієї опції наш зразок веб-програми повинен підтримувати необхідні облікові дані для виклику резервного API.

Веб-додатки, які надають доступ до даних пристроїв IoT, повинні бути захищені за допомогою комбінації імені користувача та пароля для користувачів програми. У нашому веб-додатку резервний реєстр користувачів використовує для зберігання всієї інформації про користувачів. Крім того, додаток реалізує функцію єдиного входу за допомогою сервісу SSO, який підтримує три джерела ідентичності, які можуть зберігати облікові дані користувачів: реєстр користувачів, який використовує обмін топіками SAML для аутентифікації; реєстр користувачів, розміщений у середовищі IBM Cloud.

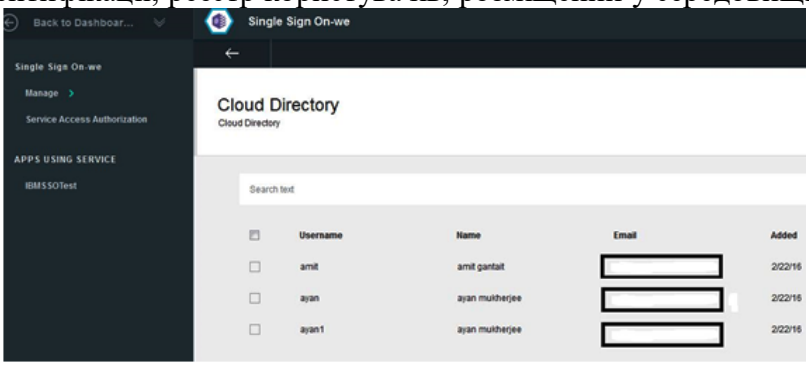

Рис. 8. Створення IBM Cloud Directory з каталогів зі створенням списку користувачів

Перш ніж розробник програми зможе вбудувати можливості SSO у свою програму, адміністратор повинен створити екземпляри відповідної служби та додати джерела ідентифікації. Виконайте наступні дії для впровадження можливостей SSO у нашому веб-додатку.

Щоб зробити ще швидше, була розроблена технологія TLS False Start, яка є додатковим розширенням протоколу, що дозволяє надсилати дані, коли TLS Handshake лише частково завершений. Детальна схема помилкового запуску TLS представлена на рис. 9:

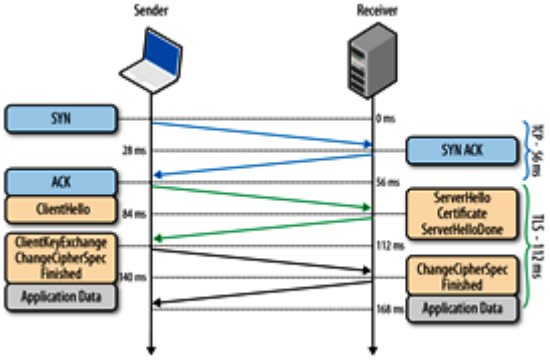

Рис. 9. Технологія TLS False Start для передачі даних клієнту MQTT

TLS False базується на припущенні, що коли клієнт і сервер вже знають про параметри підключення та симетричні ключі, дані програми вже можуть надсилатися, а будь-які необхідні перевірки можна проводити паралельно. В результаті з'єднання готово використовувати для однієї ітерації повідомлень раніше.

ISSN 2663 - 4023

4. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Шифрування та аутентифікація є невід'ємною частиною кожного TLS-з'єднання. Розглянемо найпростіший процес аутентифікації між Алісою та Боб: і Аліса, і Боб генерують власні публічні та приватні ключі; Еліс та Боб обмінюються відкритими ключами; Аліса генерує повідомлення, шифрує його своїм приватним ключем і надсилає його Бобу; Боб використовує ключ, отриманий від Аліси, для розшифровки повідомлення і тим самим перевіряє справжність отриманого повідомлення.

Очевидно, що ця схема побудована на довірі між Алісою та Бобом. Передбачається, що обмін відкритими ключами відбувся під час особистої зустрічі, і, таким чином, Аліса впевнена, що вона отримала ключ безпосередньо від Боба, а Боб, у свою чергу, впевнений, що отримав відкритий ключ Аліси.

Тепер нехай Аліса отримає повідомлення від Чарлі, з яким вона не знайома, але яка стверджує, що дружить з Бобом. Щоб довести це, Чарлі попросив заздалегідь підписати власний відкритий ключ приватним ключем Боба та додає цей підпис до повідомлення Аліси. Еліс спочатку перевіряє підпис Боба на ключі Чарлі (вона вміє це робити, оскільки вона вже знає публічний ключ Боба), переконує, що Чарлі справді є другом Боба, приймає його повідомлення та виконує відому перевірку цілісності, переконуючись, що повідомлення є від Чарлі:

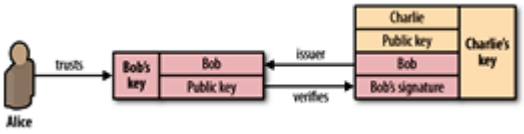

Рис. 10. Переадресація повідомлення у брокера за допомогою протоколу TLS

У протоколі TLS ці ланцюги довіри базуються на сертифікатах справжності, наданих спеціальними органами, які називаються органами з сертифікації. Органи сертифікації здійснюють перевірку, і якщо виданий сертифікат порушений, цей сертифікат відкликається.

З виданих сертифікатів додається вже розглянутий ланцюжок довіри. Його коренем є так званий сертифікат, підписаний великим центром, довіра до якого незаперечна. Загалом, ланцюжок довіри виглядає приблизно так:

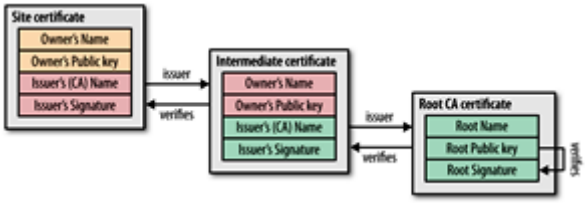

Рис. 11. Сертифікація повідомлень у брокера за протоколом TLS

Більшість алгоритмів даних шифрування, стійкість яких заснована на складності дискретних логарифмів у кінцевому полі, досить легко перенести на випадок еліптичних кривих. Криптосистеми на основі еліптичних кривих перевершують інші системи відкритого ключа за двома важливими параметрами: ступінь захисту обчислення для кожного ключового біта та швидкість реалізації програмного забезпечення.

Для порівняльного аналізу криптосистеми, що використані нами для проведення експерименту, була реалізована матриця криптосистеми на матричних поліномах, в якій паралельно обчислювальна технологія CUDA використовувалася для множення матриць і поліномів разом з модифікованою системною бібліотекою HElib.

Було проведено ряд експериментів з різними параметрами стійкості криптовалюти. Ми оцінювали час, необхідний для проведення наступних операцій: шифрування; дешифрування; множення.

Таблиця 1

Оцінка функціонування криптосистеми протоколу TLS

Параметр стійкості	Шифрування	Дешифрування	Виконання шифротексту
16	4 мс	13 мс	8 мс
24	79 мс	13 мс	15 мс
32	1,5 с	14 мс	22 мс
64	2 хв	20 мс	1 с

Таблиця 2

Оцінка функціонування модифікованої криптосистеми Gentry

Параметр стійкості	Шифрування	Дешифрування	Виконання шифротексту
16	2 мс	6 мс	5 мс
24	40 мс	11 мс	12 мс
32	1 с	15 мс	50 мс
64	5 хв	200 мс	10 с

Виходячи з наших оцінок ефективності в Таблицях 1 і 2, зрозуміло, що на практиці криптосистема, заснована на матричних поліномах, не поступається вдосконаленій моделі шифрування Gentry і навіть отримує користь від використання паралельних обчислювальних технологій. Ми провели експеримент щодо максимального значення параметра і вже при цьому значенні ми отримали, що модель Gentry, яка вважається асимптотикою найбільш "швидкою", дає модель на матричних поліномах.

На підставі вищесказаного можна стверджувати, що на практиці криптосистеми, призначені для застосування гомоморфного шифрування, повинні задовольняти щонайменше таким вимогам: набір підтримуваних математичних функцій повинен охоплювати повсякденні потреби програмістів; точність та швидкість обчислень не повинні погіршуватися під час обчислень; стабільність алгоритму повинна виключати атаку шляхом повного перебору.

На відміну від легкої криптографії для гомоморфного шифрування, відповідні міжнародні стандарти ще не розроблені; однак ведеться робота зі створення прийнятних рішень, які можуть надійно обробляти чутливі дані у хмарі та для брокерів IoT.

5. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Інтернет речей є концепцією побудови розподілених мереж пристроїв, сенсорів, роботизованих систем та машин. Очевидно, що критичні системи вимагають від програмних додатків та пристроїв розробити рішення ситуації незалежно від якості підключення до Інтернету, а також у разі повного відключення.

Мінімальні накладні витрати, наявність класів обслуговування та ієрархічна структура тем є незаперечною перевагою протоколу MQTT, про що свідчить велика різноманітність як програмного забезпечення клієнта, так і сервера, включаючи

програмне забезпечення з відкритим кодом. Таким чином, ми спостерігаємо зрушення парадигми від маршрутизації на транспортному рівні до маршрутизації на рівні програми.

В подальших дослідженнях будете приділятися особлива увага шифруванню хаотичних електронних повідомлень на основі динамічних математичних моделей та хаотичних алгоритмів протоколів передачі даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1.] O. Beley, “Features of the management of data encryption keys in the cloud storage MS SQL Azure”, Informatyka, Automatyka, Pomiary w Gospodarce I Ochronie Środowiska, T. 8, № 4, pp. 12–15, 2018.
[2.] O. Belej, I. Artyshchuk, W. Sitek, “The Controlling of Transmission of Chaotic Signals in Communication Systems Based on Dynamic Models”, CEUR Workshop Proceedings, Vol. 2353, pp. 664-673, 2019.
[3.] F. Wu, C. Rüdiger, M.R. Yuce, “Real-Time Performance of a Self-Powered Environmental IoT Sensor Network System,” Sensors, 17:282, pp. 184-253, 2017.
[4.] M.R. Yuce, J. Khan, “Wireless Body Area Networks: Technology, Implementation, and Applications,” CRC Press; Boca Raton, FL, USA, pp. 67-79, 2011.
[5.] H. C. Keong, M. R. Yuce, “UWB-WBAN sensor node design,” *IEEE Trans., Boston, MA*, pp. 2176-2179, 2011.
[6.] E. Wilhelm, S. Siby, Y. Zhou, X.J.S. Ashok, M. Jayasuriya, S. Foong, J. Kee, K.L. Wood, N.O. Tippenhauer, “Wearable environmental sensors and infrastructure for mobile large-scale urban deployment,” *IEEE Sens. J.*, pp. 137-149, 2016.
[7.] K. Mekki, E. Bajic, F. Chapel, F. Meyer, “A comparative study of LPWAN technologies for large-scale IoT deployment,” *ICT Express*, pp. 276-279, 2018.
[8.] X. Zhang, M. Zhang, F. Meng, Y. Qiao, S. Xu, S.H. Hour, “A Low-Power Wide-Area Network Information Monitoring System by Combining NB-IoT and LoRa,” *IEEE Internet Things J.*, pp. 356-419, 2018.
[9.] Z. Zhu, T. Liu, G. Li, T. Li, Y. Inoue, “Wearable sensor systems for infants,” *Sensors*, pp. 3721–3749, 2015.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (6), 2019
ISSN 2663 - 4023

Olexander I. Belej
PhD of ec.., ass. professor, ass. Professor of CAD department
Work place: Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0003-4150-7425
Oleksandr.I.Belei@lpnu.ua

Tamara G. Lohutova
D.e.n., professor, Head of department of innovations and management
Work place: State Higher Education Institution "Pryazovskyi State Technical University", Mariupol, Ukraine
ORCID ID: 0000-0001-5664-2908
Logutova_t_g@pstu.edu

SECURITY OF DATA TRANSFER TO THE INTERNET OF THINGS

Abstract. The article discusses the MQTT protocol for the Internet of Things and touch wireless networks, its features, applications, and specific procedures. The information elements and principles of the message owner are analyzed. This article covers topics such as secure storage of the Internet of Things, the transfer of that data through the secure interface of mobile devices and web applications. It also looks at all the key tools provided by MQTT for information security. The proposed identification of users in this article is to identify them from the Cloudant database. This application works on the Node.js server in IBM Bluemix and provides an API or RESTful that requires mobile client authentication. The mobile client access service is designed to call these two APIs in any authentication application. It is suggested to use separate authentication approaches: for the web application - on the Cloud Directory and for the mobile application - MobileFirst Client Access. However, both the web and mobile applications use the same level of application security to allow the user to access device data. To improve the security of messages, it is suggested to use a transport layer security protocol that uses different cryptographic methods. We are offered homomorphic encryption of these protocols. The transport layer security protocol increases the performance of the protocol and reduces the computational cost, but it does not apply when initially connecting to the server or when a previous session has already expired. The article presents an algorithm for the detection of weak symmetry breaking for the analysis of the chance of a recovered e-mail. A method of homomorphic encryption and authentication of users and their emails in wireless sensor networks of the Internet of Things is proposed.

Keywords: IoT data; security; application programming interface; massager queue telemetry transport protocol; cloud database; scenario; TLS protocol; encryption data.

REFERENCES

[1.]O. Beley, "Features of the management of data encryption keys in the cloud storage MS SQL Azure", Informatyka, Automatyka, Pomiary w Gospodarce I Ochronie Środowiska, T. 8, № 4, pp. 12–15, 2018.
[2.]O. Belej, I. Artyshchuk, W. Sitek, "The Controlling of Transmission of Chaotic Signals in Communication Systems Based on Dynamic Models", CEUR Workshop Proceedings, Vol. 2353, pp. 664-673, 2019.
[3.]F. Wu, C. Rüdiger, M.R. Yuce, "Real-Time Performance of a Self-Powered Environmental IoT Sensor Network System," Sensors, 17:282, pp. 184-253, 2017.
[4.]M.R. Yuce, J. Khan, "Wireless Body Area Networks: Technology, Implementation, and Applications," CRC Press; Boca Raton, FL, USA, pp. 67-79, 2011.
[5.]H. C. Keong, M. R. Yuce, "UWB-WBAN sensor node design," *IEEE Trans., Boston, MA*, pp. 2176-2179, 2011.
[6.]E. Wilhelm, S. Siby, Y. Zhou, X.J.S. Ashok, M. Jayasuriya, S. Foong, J. Kee, K.L. Wood, N.O. Tippenhauer, "Wearable environmental sensors and infrastructure for mobile large-scale urban deployment," *IEEE Sens. J.*, pp. 137-149, 2016.

[7.]K. Mekki, E. Bajic, F. Chapel, F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, pp. 276-279, 2018.

[8.]X. Zhang, M. Zhang, F. Meng, Y. Qiao, S. Xu, S.H. Hour, "A Low-Power Wide-Area Network Information Monitoring System by Combining NB-IoT and LoRa," *IEEE Internet Things J.*, pp. 356-419, 2018.

[9.]Z. Zhu, T. Liu, G. Li, T. Li, Y. Inoue, "Wearable sensor systems for infants," *Sensors*, pp. 3721–3749, 2015.