https://www.sworldjournal.com/index.php/swj/article/view/swj19-01-020
DOI: 10.30888/2663-5712.2023-19-01-020

УДК 004.056

SECURE IoT TECHNOLOGY STACK
БЕЗПЕКОВИЙ ТЕХНОЛОГІЧНИЙ СТЕК IoT

Korobeinikova T.I. / Коробейнікова Т.І.
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0003-2487-8742
Iskovych T.V. / Іськович Т.В.
студент / student
Lviv Polytechnic National University, S. Bandera St. 12, Lviv, 79013
Національний університет «Львівська політехніка», Львів, Бандери, 12, 79013

Анотація. *Робота присвячена аналізу існуючих рішень для побудови безпекового технологічного стеку для системи Інтернету речей (IoT). Як результат, було створене припасування обраних відомих технологій відповідно безпековому підходу до організації IoT. Тут запропоноване приведення моделі до стандартів моделей OSI та TCP/IP із урахуванням принципів SOA для збільшення гнучкості системи. Проілюстровано співвідношення компонентів системи IoT до елементів безпеки, з деталізацією кожного з них. Здійснено аналіз та відповідний розподіл потенційних загроз для системи безпеки для кожного з рівнів IoT. Для виконання задач дослідження створено безпекову модель IoT з описом компонентів та функцій кожного та відображенням потенційних атак, та методами їх подолання. Питання забезпечення безпечного середовища для функціонування екосистеми IoT є важливим завданням під час проектуванні та впровадженні відповідних рішень.*

Ключові слова: *IoT, архітектура IoT, протокольний стек, безпека даних, безпекова модель IoT.*

Вступ.

Популяризація Інтернету речей (Internet of Things, скорочено IoT) та його активне використання у побутових, корпоративних, управлінських та інших сферах життя породжують питання безпеки стосовно IoT [1–3]. Пристрої IoT (розумні дверні дзвінки, гаражні двері, термостати, спортивні відстежувачі, кардіостимулятори, світлофори, спеціально облаштовані місця для паркування тощо) взаємодіють людьми та з іншими пристроями, обмінюються даними, аналізують зібрані дані та здатні приймати на цій основі рішення. Всі такі комунікації здійснюються по мережі і за допомогою протоколів, що прошити і протокольні стеки та керуються відкритими моделями [4]. Нині більшість безпекових прикладних задач можна вирішувати на рівні побудови безпекових технологічних стеків.

Стек технологій – це типовий набір технологій, які допомагають в досягненні поставлених цілей [4]. У даній роботі під поняттям «стек технологій» ми будемо розуміти спільне використання необхідних технологічних рішень для вирішення проблеми проектування та реалізації [5] системи IoT. Такий підхід дає можливість уніфікувати та об’єднати певні технології в одне ціле, з певною метою та призначенням. Створення та використання безпекового стеку технологій для IoT, дозволяє нам отримати розуміння потрібних технологічних та програмних рішень для вирішення безпекової цілі без проведення великих та об’ємних наукових та технічних досліджень для всіх майбутніх учасників цих процесів. Також це виступає основою для подальших перспективних досліджень

технологій та програм для можливого удосконалення стеку чи створення нових технічних та/або технологічних рішень.

В цій роботі здійснено аналітичне припасування технологічного стеку IoT до відомих протокольних та технологічних стеків, зокрема TCP/IP та відомих моделей, зокрема, OSI [6–7]. Це дало можливість спроектувати систему IoT на основі вже проведених досліджень та набутого раніше досвіду щодо релевантності тієї чи іншої технології чи способу реалізації у відповідності до поставлених завдань.

1. Технологічний стек рівнів Інтернету речей.

Відповідно до моделі сервіс-орієнтованої архітектури (Service-oriented architecture, SOA) технологічний стек рівнів Інтернету речей буде містити 4 рівні (рис. 1). SOA-архітектура забезпечує взаємодію між великою кількістю різних пристроїв. Кожен з цих рівнів має такі функції:

– сенсорний рівень взаємодіє з обраними апаратними об'єктами для визначення стану речей та збору даних (рівень 1);
– рівень інтерфейсів надає різні методи користувачам та додаткам для можливості взаємодії між ними (рівень 2);
– мережевий рівень надає повноцінну інфраструктуру, яка необхідна для стабільної підтримки провідних і бездротових з'єднань у мережі (у т.ч., в корпоративній) (рівень 3);
– службовий рівень дає можливість створювати і управляти сервісами, які необхідні користувачам або додаткам (рівень 4);

Відобразимо модель OSI, протокольний стек TCP/IP та модель технологічного стеку IoT за принципами сервіс-орієнтованої архітектури SOA рівнозначно їх рівням.

Рисунок 1 – Приведення до стандартів технологічного стеку IoT

Авторська розробка

Під час використання такої моделі технологічного стеку, вся система ділиться на підсистеми, які не є строго залежними від інших і, які, при необхідності можуть бути повторно використані для забезпечення підтримки функціонування всієї системи. Такий підхід дозволяє створити безперебійне функціонування систем, адже якщо один елемент стане недоступним, то решта продовжить свою роботу. В тих системах, де надійність та доступність є головними пріоритетами при проектування, така модель є найкращим вибором.

Так простіше взаємодіяти з протоколами передачі даних та різними рівнями системи, бо така архітектура сприяє підвищенню взаємодії між об'єктами, а отже полегшує процес керування.

Така модель технологічного стеку IoT, організована за принципами SOA, дає можливість системі Інтернету речей розкритись повністю та показати усі свої переваги. Вона забезпечує можливість створення комплексних сервісів, де на виконання різного типу завдань, можна виділити різні типу об’єкти системи.

2. Розробка безпекової архітектури IoT.

Кожна система має свій тип структури, або іншими словами архітектури, тобто, як саме побудована ієрархія взаємодії всіх елементів [8]. Система Інтернету речей не виняток.

В сучасному світі, який все більше цифровізується в усіх своїх аспектах, питання повноцінного функціонування програмного чи апаратного продукту набуває все більшого масштабу та більшої пріоритетності. Завадити повноцінній роботі таких пристроїв чи програм може несанкціоноване втручання різного типу і на різних рівнях згадуваних тут об’єктів. Тож під час проектування системи будь-якого програмного чи апаратного продукту, в тому числі і нашої цільової системи Інтернету речей, надзвичайно важливо враховувати забезпечення питань безпеки [4]. Проаналізувавши джерела, було прийнято рішення проілюструвати співвідношення компонентів системи IoT до елементу безпеки, з деталізацією по кожному з них. Це зображено на рисунку 2. Така структура, яка є цілісною системою, повинна гарантувати бездоганну роботу власних компонентів (де головним фактором під час проектування є надійність) та пов'язувати фізичну і віртуальні складові.

Головною вимогою для досягнення цілісної системи є ретельний підхід під час проектування до процесу відновлення системи після її збоїв та її масштаби, враховуючи те, що це вагомий фактор в контексті забезпечення безпечного середовища. Враховуючи чим раз більшу мобільність у цьому світі, сучасна архітектура системи повинна прагнути до високого рівня адаптованості для правильної обробки різних динамічних взаємодій у всій своїй структурі. Надання рівня абстракції на більш високому рівні, який може приховувати деякі деталі реалізації, безсумнівно можна вважати перевагою еталонних архітектур і моделей.

На рисунку 3 зображено відповідність рівнів стеку системи IoT тим проблемам безпеки, що притаманні цим рівням.

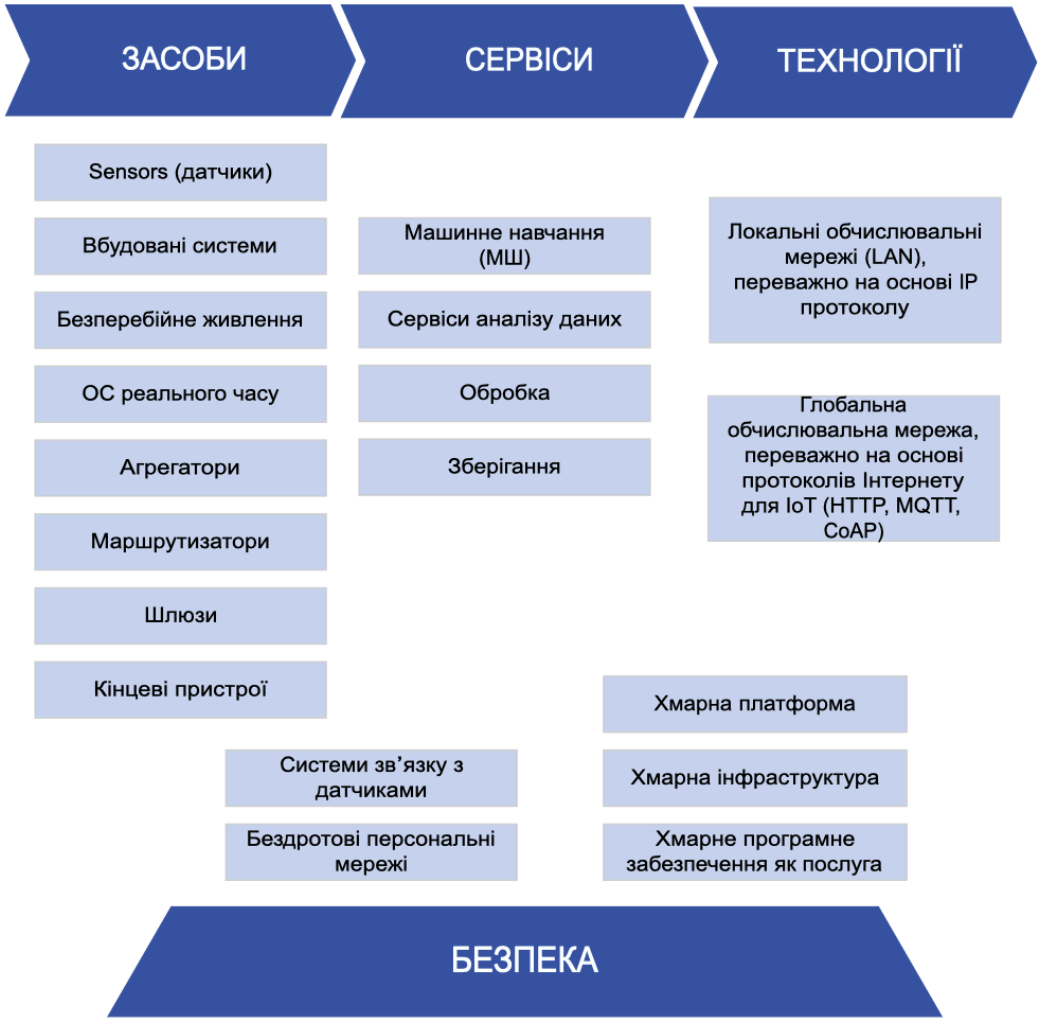

Рисунок 2 – Безпекова архітектура IoT

Авторська розробка

Рисунок 3 – Розподіл загроз безпеці по рівням моделі архітектури IoT

Авторська розробка

3. Безпекова модель IoT.

Якщо можемо орієнтуватися на відкриті стандарти, запропонуймо вирішення питань безпеки на кожному з рівнів технологічного стеку Інтернету речей [8].

Таблиця 1 – Безпекова модель IoT

<table>
<tr><th>OSI</th><th>TCP/IP</th><th>IoT</th><th>Об’єкт захисту (протокол, технологія, тощо)</th><th>Метод захисту</th><th>Опис</th></tr>
<tr><td>Додатків</td><td rowspan="3">Додатків</td><td rowspan="3">Службовий рівень</td><td rowspan="3">DHCP, SSH, CoAP, AMQP, XMPP, masquerad</td><td rowspan="3">DHCP snooping, RSA, ACL, IPS, брандмауер, шифрування,</td><td rowspan="3">Хмарні послуги, сервіси аналізу даних, машинне навчання (МШ), зв’язок з пристроями (частково), безпека</td></tr>
<tr><td>Предста-влення</td></tr>
<tr><td>Сесії</td></tr>
<tr><td>Транспорт-ний</td><td>Транспортний</td><td rowspan="2">Мережевий рівень</td><td rowspan="2">DDoS, DoS, IPv4, IPv6, MQTT та DDS, TLS / SSL, MITM, TCP, UDP</td><td rowspan="2">SYN protection, 6LowPAN,</td><td rowspan="2">Зв’язок з пристроями, провідні та безпровідні мережі, протоколи передачі даних (частково), мережні пристрої (частково)</td></tr>
<tr><td>Мережевий</td><td>Інтернету</td></tr>
<tr><td>Канальний</td><td rowspan="2">Мережевого доступу</td><td>Рівень інтерфейсів</td><td>MAC, DHCP, MIM, DNS, ARP, Адресні spoofing, STP, RFID, WSN, PKI, VLAN</td><td>PortSecurity, DHCP Snooping, DAI, IPSG, PortFast та BPDU Guard</td><td>Мережні пристрої (частково), протоколи передачі даних (частково), міжплатформне ПЗ</td></tr>
<tr><td>Фізичний</td><td>Сенсорний рівень</td><td>selfish загроза, фізична безпека, порушення цілісності даних, зловмисне ПЗ</td><td>IPsec, IEEE 802.11 AH</td><td>Датчики, безперебійне живлення, ОС реального часу, безпека, GPS, Bluetooth</td></tr>
</table>

Авторська розробка

З метою підвищення загального рівня захищеності системи IoT кожен рівень стеку забезпечує безпеку за допомогою різних протоколів безпеки, послуг та механізмів безпеки. Таким чином, кожен рівень намагається досягти окремо і в цілому основних цілей безпечної роботи, а саме: інформаційної безпеки, фізичної та стабільного функціонування системи управління безпекою.

Розподілимо рівні моделі IoT (згідно рис. 1) відповідно функціональним елементам та розпишемо протокольний стек IoT згідно архітектури IoT та з погляду безпеки та аналізу літературних джерел та відобразимо у вигляді Таблиці 1 безпекову модель IoT

У таблиці 1 наведені компоненти та функції кожного рівня безпеки IoT із відображенням атак, проблем та вимоги безпеки, які необхідні для кожного рівня. Крім того, таблиця 2.1 ілюструє перелік методів для вирішення проблем безпеки в системі IoT.

Для того, щоб продемонструвати вимоги до безпеки в системі Інтернету речей на прикладі, згадаємо зазначену нами раніше чотирирівневу IOT архітектуру, яка складається з сенсорного, інтерфейсного, службового та мережевого рівнів.

Кожен з цих рівнів має забезпечити сприяння чіткому процесу управління безпекою, зокрема забезпеченню контролю доступу, автентифікації, цілісності даних та їх конфіденційності, а також наявності інструментів для захисту системи IOT від вірусів та атак. Тож створювана система безпеки повинна мати можливість відстежувати кожен пристрій окремо, контролювати трафік та бути спроможною захистити чи тимчасово відімкнути пристрій/-ої щоб унеможливити критичні наслідки для цілої екосистеми IoT. Тепер коротко розглянемо кожен рівень архітектури в контексті безпекових загроз.

Безпека на сенсорному рівні. Даний рівень архітектури системи IoT можна охарактеризувати як сполучення трьох ланок, які забезпечують дані: пристрої збору інформації, їх місцерозташування та безпосередньо люди. Для повноцінної реалізації функції безпеки необхідно передбачене виробником виконання елементів безпеки в пристроях, тобто можливість аутентифікації, шифрування даних та обмеження в локальному збереженні зібраної інформації. Проблемними питаннями безпеки на сенсорному рівні архітектури IoT є:

1) Фізична безпека пристроїв збору інформації. Це ускладнений або неможливий доступ до пристрою. Рішенням є конструкції пристрою, що дасть можливість доступу авторизованим особам (наприклад обслуговуючому персоналу) та його блокування для сторонніх.
2) Недостатня модернізація. Часто в пристроях немає передбаченої можливості для їх оновлення чи переналаштування. Нові вразливості розкриваються постійно, тож якщо пристрій не буде спроможний для оновлення своїх налаштувань, це може послабити безпеку системи.

Безпека на рівні інтерфейсів. Цей рівень є посередником між IoT системою і різними додатками. Він надає підтвердження того що процес взаємодії між додатками і системою є легальним. Потенційними проблемами на цьому рівні є:

1) Необхідність подібних налаштувань конфігурації на всіх пристроях для

досягнення сумісності.

2) Забезпечення безпеки даних на цьому рівні архітектури.
3) Створення ефективних рішень безпеки задля оптимізації процесу.

Рекомендаціями для вирішення проблем безпеки даного рівня є дотримання конфіденційності, цілісності та доступності, регулярне оновлення ПЗ, аутентифікація та авторизація користувачів та адміністратора.

Безпека на мережевому рівні. Мережевий рівень є надважливою частиною архітектури системи, так як виступає каналом передачі даних між іншими рівнями (сенсорним та службовим наприклад). Зважаючи на те, що екосистема IOT складається з великої кількості побічних гібридних систем, фактор проблеми масштабованості мережі, її складності та безпеки передачі даних є значним. Серед проблем, які виникають на даному етапі є:

1) Забезпечення базових вимог інформаційної безпеки - конфіденційності, цілісності та доступності.
2) Фізична безпека (стосується не лише сенсорного рівня), в випадку коли пристрої які забезпечують передачу даних можуть бути в вільному доступі.
3) Надмірність підключень в мережі, що створює додаткові складнощі в обслуговуванні, надмірні витрати мережевого ресурсу та збільшення вразливості до зловмисного впливу.
4) Можливість запобіганню зловмисного роду атак, як-от атака типу «Man-In-The-Middle» щоб перехопити інформацію, яка передається між двома об’єктами.

Основними викликами для безпеки на мережевому рівні в системі Інтернету речей є мінімізація можливості впливу зловмисників на систему та збільшення ефективності її роботи для покращення якості обслуговування.

Безпека на службовому рівні. Службовий рівень забезпечує цій архітектурі ефективну взаємодію з точки зору використання апаратних та програмних ресурсів, в тому числі і можливість повторного використання цих ресурсів. На цьому рівні відбувається аналіз отриманих даних від сенсорного рівня, тож тут присутні служби обробки подій, служби інтеграції і аналітики та інші, які дозволяють обмін інформацією між службами, а також забезпечують виконання необхідних дій. Щодо проблем, які притаманні цьому рівню, то вони такі:

1) Забезпечення конфіденційності, цілісності та доступності.
2) Можливість недобросовісних маніпуляцій службами та службовою інформацією цього рівня.
3) Створення захисту від атак різного плану, в тому числі і DoS та DDoS-атак.
4) Забезпечення аналізу трафіку задля недопущення жодних маніпуляцій з даними.

Одним із варіантів для вирішення проблем на службовому рівні є слідування стандартам та різним протоколам при проектування та впровадженні системи, у відповідності до ваших потреб та можливих загроз.

Висновки.

У цій роботі було здійснено аналіз існуючих програмних та/або протокольних рішень для побудови технологічного стеку системи Інтернету речей. Як результат, було створене припасування обраних нами технологій відповідних стеків до 4-рівневого стеку рівнів IoT.

Було описано кожен з рівнів 4-рівневого стеку IoT, та запропоноване приведення даної моделі до стандартів моделей OSI та TCP/IP з врахуванням принципів сервіс-орієнтованої архітектури, яка сприяє гнучкості та більшій ефективності системи. Проілюстровано співвідношення компонентів системи Інтернету речей до елементів безпеки, з деталізацією кожного з них. Здійснений аналіз та відповідний розподіл потенційних загроз для системи безпеки для кожного з рівнів IoT.

Також було створено безпекову модель IoT з наведенням компонентів та функцій кожного рівня безпеки Інтернету речей та відображенням потенційних атак, проблем та вимог безпеки. Крім того були запропоновані варіанти вирішення цих проблем. Питання забезпечення безпечного середовища для функціонування екосистеми Інтернету речей є надзвичайно важливим завданням при проектуванні та впровадженні відповідних рішень.

Література:

1. Cheng, X., Zhou, J., Zhao, X., Wang, H., & Li, Y. (2023). A presentation attack detection network based on dynamic convolution and multi-level feature fusion with security and reliability. Future Generation Computer Systems, 146, 114-121. doi:10.1016/j.future.2023.04.012

2. Sharma, R., & Arya, R. (2023). Secured mobile IOT ecosystem using enhanced multi-level intelligent trust scheme. Computers and Electrical Engineering, 108 doi:10.1016/j.compeleceng.2023.108715

3. Chauhan, P., & Atulkar, M. (2023). An efficient centralized DDoS attack detection approach for software defined internet of things. Journal of Supercomputing, 79(9), 10386-10422. doi:10.1007/s11227-023-05072-y

4. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5Мбайт). – Київ: КПІім. Ігоря Сікорського, 2021. – 271 с.

5. Ma, W., Liu, R., Li, K., Yan, S., & Guo, J. (2023). An adversarial domain adaptation approach combining dual domain pairing strategy for IoT intrusion detection under few-shot samples. Information Sciences, 629, 719-745. doi:10.1016/j.ins.2023.02.031

6. Комп'ютерні мережі: навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2022. – 228 с.

7. Трояновська Т. І. Побудова захищених мереж на базі обладнання компанії Cisco. // Захарченко С.М., Трояновська Т. І., Бойко О.В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.

9. Kumar, M., Singh, P. K., Maurya, M. K., & Shivhare, A. (2023). A survey on

event detection approaches for sensor based IoT. Internet of Things (Netherlands), 22 doi:10.1016/j.iot.2023.100720

Abstract. *This paper is devoted to existing solutions analysis of building a secure technological stack for the Internet of Things (IoT). As a result, a matching of selected known technologies was created according to the security approach to the IoT organization. It is proposed to bring the novel model to the standards of the OSI and TCP/IP models, considering the SOA principles to increase the system flexibility. The ratio of IoT system components to security elements is illustrated, detailing each of them. The analysis and appropriate potential threats distribution to the security system for each of the IoT levels was carried out. To fulfill the research objectives, an IoT security model was created with a description of the components and functions of each and a display of potential attacks and methods of overcoming them. The issue of providing a secure environment for the functioning of the IoT ecosystem is an important task during the design and implementation of relevant solutions.*

Key words: *IoT, IoT architecture, protocol stack, data security, IoT security model.*

Науковий керівник: *к.т.н., доц. Коробейнікова Т.І.*
Стаття надіслана: 13.05.2023 р.