УДК 004.056.5
Зайко Т.А.[1], Косенков.І.С[2]
[1]канд. техн. наук, доц. НУ «Запорізька Політехніка»
[2]студ. гр. КНТ-118 НУ «Запорізька Політехніка»

ЗАХИСТ ІНТЕРНЕТУ РЕЧЕЙ

Концепції IoT, такі як розумні пристрої, розумні машини, розумні міста та розумні будинки, охоплюють як статичні, так і динамічні об'єкти у фізичному світі та світі освіти, які можна ідентифікувати та інтегрувати в комунікаційні мережі. Важливо зазначити, що надані дані часто є конфіденційними. Вони можуть включати стан навколишнього середовища, стан наших будинків і міст або стан нашого особистого здоров'я та діяльності. З цієї причини механізми забезпечення та гарантування безпеки та конфіденційності даних в Інтернеті речей мають вирішальне значення. За своєю природою захист Інтернету речей є комплексним і складним завданням.

Завдяки своїй природі як різнорідної мережі, потенційні загрози для даних IoT мають майже нескінченні можливі вектори атак [1]. Ці вектори можна приблизно розділити за початковою ціллю атаки:

– атаки проти IoT-пристроїв: в першу чергу експлуатуються вразливості обладнання;

– атаки проти комунікацій: в основному експлуатується вразливості, пов'язані з перевіркою цілісності даних;

– атаки на рівень сприйняття: в основному використання вразливості безпеки в сенсорних мережах, як цілісність служб та доступність мережі;

– атаки на фізичний рівень: експлуатуються вразливості, пов'язані з фізичними каналами;

– атаки на мережевий рівень: експлуатуються вразливості каналів передачі.

Складні системи, такі як IoT та Cloud, не можуть бути захищені єдиним загальним протоколом. Кожен рівень мережі має свої вимоги [2]. Один із підходів полягає в тому, що взаємодія між користувачем та пристроєм

повинна обмежуватися підключенням до віртуального об’єкта за допомогою відповідного захисту. Кожен користувач у хмарі може навіть мати особисте уявлення про послуги та налаштування пристрою, що обмежує ймовірність витоку даних та крадіжки дозволів.

Часто дані IoT не є надійно засвідченими, а послуги репутації даних не доступні [4]. Застосування Blockchain вирішує проблему довіри, надаючи вузлам можливість перевіряти дані, розподілені мережею, щоб переконатись, що вони жодним чином не підроблені. Однак Blockchain сам по собі не гарантує, що дані не будуть підроблені до того, як дані з нього потраплять у мережу. Ці завдання повинна вирішувати система моніторингу. Необхідність збереження історії транзакцій може бути вирішена принаймні частково за допомогою частково розподіленим блок-ланцюгом, коли кожен вузол містить лише відповідні дані.

IoT інтегрує передові технології комунікацій, мереж, хмарних обчислень, зондування та спрацьовування, а також прокладе шлях для новаторських додатків у різних областях, що вплине на багато аспектів життя людей та принесе багато зручностей. Тим не менше, враховуючи величезну кількість підключених пристроїв, у питаннях безпеки, конфіденційності та управління в IoT виникають дуже значні ризики. Незважаючи на те, що жодне рішення "для всіх" неможливо створити найближчим часом, все ж є можливість значно підвищити безпеку мережі IoT за допомогою комбінації запропонованих способів та рішень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Choudhury T. Privacy and Security of Cloud-Based Internet of Things (IoT) 2017 3rd International Conference on Computational Intelligence and Networks (CINE), 2017 – pp. 40-45

2. Kakanakov N. Adaptive models for security and data protection in IoT with Cloud technologies / N. Kakanakov, M. Shopov // 2017 40th International Convention on Information and Communication Technology 2017. – pp.1001-1004.

3. Oh S. Development of IoT security component for interoperability / S. Oh and Y. Kim // 2017 13th International Computer Engineering Conference (ICENCO), 2017. – pp. 41-44

4. Rodrigo R. On the features and challenges of security and privacy in distributed internet of things / R.Rodrigo, Z. Jianying, J. Lopez // Computer Networks 57.10, 2013 – pp. 2266- 2279

5. Liu C. A Novel Approach to IoT Security Based on Immunology / C. Liu, Y. Zhang and H. Zhang // 2013 Ninth International Conference on Computational Intelligence and Security, 2013, – pp. 771-775

6. Соколов М.Н., Смолянинова К.А., Якушина Н.А. Проблемы безопасности интернета вещей: обзор. – Вопросы кибербезопасности : журнал. – 2015. – № 5(13). – 34с.

7. Исаков В.Б., Сарьян В.А., Фокина А.А. Правовые аспекты внедрения Интернета вещей // ИТ-Стандарт. – 2015. – № 4-1 (5). – С. 9-16.