

Аналіз проблеми захисту при обміні або передаванні даних між пристроями Інтернету речей

Вінницький національний технічний університет

Анотація

Розглянуто кіберзагрози в IoT, методи шифрування та захищені протоколи зв'язку. Описано ризики несанкціонованого доступу, атак на дані та DDoS-атак. Проаналізовано засоби безпеки, зокрема AES, RSA, TLS, 2FA. Визначено виклики та перспективи розвитку, включаючи квантове шифрування й штучний інтелект.

Ключові слова: Інтернет речей (IoT), кібербезпека, шифрування, автентифікація, протоколи зв'язку, DDoS-атаки, децентралізація, квантове шифрування, штучний інтелект.

Abstract

Cyber threats in IoT, encryption methods and secure communication protocols are reviewed. The risks of unauthorized access, data attacks and DDoS attacks are described. Security tools are analyzed, in particular AES, RSA, TLS, 2FA. Challenges and development prospects are identified, including quantum encryption and artificial intelligence.

Keywords: Internet of Things (IoT), cybersecurity, encryption, authentication, communication protocols, DDoS attacks, decentralization, quantum encryption, artificial intelligence.

Вступ

У сучасному цифровому просторі, що швидко розвивається, Інтернет речей (IoT) набуває все більшого значення, сприяючи тісному поєднанню фізичних та віртуальних середовищ. Сьогодні технологія IoT (Internet of Things, IoT) являє собою динамічну глобальну мережеву екосистему інформаційних пристроїв, яка забезпечує високий рівень доступності, цілісності та інтеграції між різними інтелектуальними пристроями і їх комунікацію через мережу Інтернет.

Дослідження

Інтернет речей (IoT) є однією з найбільш швидкозростаючих технологій сучасності, яка відкриває широкі можливості для автоматизації, підвищення ефективності та покращення якості життя. Проте зростання кількості IoT-пристроїв несе ризики, пов'язані з кібербезпекою при передаванні та обробленні даних, що робить необхідним розробку ефективних засобів захищеного обміну інформацією.

Важливо визначити основні кіберзагрози для безпеки обміну даними між IoT-пристроями: перехоплення та несанкціонований доступ – зловмисники можуть прослуховувати трафік або отримувати контроль над пристроями; атаки на цілісність даних – зміна або підробка переданих повідомлень; DDoS-атаки – велика кількість скомпрометованих пристроїв може використовуватись для перевантаження системи IoT; недостатня автентифікація – слабкі методи перевірки справжності пристроїв сприяють несанкціонованому підключенню.

Для безпечного обміну даними в IoT-мережах застосовується технологія шифрування, що є основним методом захисту інформації та передається між пристроями. Використовуються такі підходи:

- AES (Advanced Encryption Standard) – симетричне шифрування для швидкої та безпечної передачі даних;
- RSA та ECC (Elliptic Curve Cryptography) – асиметричні алгоритми, які забезпечують автентифікацію пристроїв;
- TLS (Transport Layer Security) – захищає дані під час їх передачі по мережі.
- DES (Data Encryption Standard) – застарілий симетричний алгоритм шифрування, який використовується для захисту даних, але поступово замінюється більш безпечними методами через недостатню довжину ключа (56 біт).

Із метою уникнення несанкціонованого доступу використовуються такі засоби як: сертифікати X.509 – перевіряють справжність пристроїв перед встановленням з'єднання; протоколи OAuth та

OpenID Connect (протоколи X.25, 802.1x/802.1q) – забезпечують безпечний доступ до сервісів IoT; двофакторна аутентифікація (2FA) – додає додатковий рівень захисту.

Для безпечного обміну даними використовуються для протоколи MQTT (Message Queuing Telemetry Transport) із TLS – популярний протокол для обміну повідомленнями між IoT-пристроями; CoAP (Constrained Application Protocol) з DTLS – ефективний протокол для обмежених пристроїв; HTTPS – забезпечує безпечну взаємодію IoT-пристроїв з веб-сервісами. Інші протоколи IoT: CoAP, Zigbee, LoRa, BLE, AMQR, DDS, Z-Wave, Bluetooth.

Зауважимо, технології Інтернету речей можуть бути використані для децентралізованого зберігання даних та забезпечення їхньої незмінності. Вони дозволяють: реєструвати та перевіряти автентичність пристроїв, відстежувати всі операції між IoT-пристроями, захищати мережу від зовнішніх атак завдяки децентралізованій архітектурі.

Попри значні досягнення у сфері безпеки IoT, існують певні виклики: обмежені обчислювальні ресурси IoT-пристроїв – складні алгоритми шифрування можуть сповільнювати роботу пристроїв; необхідність стандартизації – відсутність єдиного стандарту ускладнює інтеграцію різних рішень; захист від квантових атак – розвиток квантових комп'ютерів може зробити традиційні методи шифрування вразливими.

У майбутньому розвиток штучного інтелекту для автоматичного виявлення загроз в пристроях IoT, інтеграція квантового шифрування та вдосконалення стандартів безпеки допоможуть підвищити захищеність IoT-мереж.

Висновки

Отже, забезпечення безпечного обміну даними між пристроями Інтернету речей є критично важливим завданням. Використання сучасних методів шифрування, автентифікації, захищених протоколів зв'язку, технології у сфері Інтернету речей (IoT) дозволяє знизити ризики, пов'язані з кіберзагрозами. Але необхідні подальші дослідження та розробка нових захищених підходів та засобів, що сприятимуть безпечному впровадженню IoT пристроїв та систем у різні сфери повсякденного життя.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Asghari, P., Rahmani, A. M., & Javadi, H. H. S. Internet of Things applications: A systematic review. *Computer Networks*, 2019, № 148, 2, pp. 41-261.
2. Kabalci, Y., Kabalci, E., Padmanaban, S., Holm-Nielsen, J. B., Blaabjerg, F. Internet of things applications as energy internet in smart grids and smart environments. *Electronics*, 2019, № 8 (9), p. 972.
3. Soldatos, J., Gusmeroli, S., Malo, P., & Di Orio, G. Internet of things applications in future manufacturing. In *Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds*, 2022, pp. 153-183.

Платенков Дмитро Андрійович – студент групи БКС-216, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: dplatenkov@gmail.com

Науковий Керівник: **Малиновський Вадим Ігорович** – канд. техн. наук, доцент кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця

Platenkov Dmytro A. – Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: dplatenkov@gmail.com

Supervisor: **Malinovsky Vadym I.** – Cand. Sc. (Eng.), Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia