УДК 004.056.55:004.738.5

І. О. Бучацький
О. В. Салієва

ПІДВИЩЕНЯ БЕЗПЕКИ IoT-СИСТЕМ НА ОСНОВІ ПОВЕДІНКОВОЇ АУТЕНТИФІКАЦІЇ ПРИСТРОЇВ У ПРОТОКОЛІ gRPC

Вінницький національний технічний університет

Анотація

У роботі розглядається проблема забезпечення безпеки систем Інтернету речей (IoT), що функціонують у середовищах із великою кількістю взаємопов'язаних пристроїв, де ключовими вимогами є надійність передачі даних, стійкість до кіберзагроз та забезпечення безперервності функціонування мережевої інфраструктури. Проаналізовано особливості використання протоколу gRPC для організації взаємодії між IoT-пристроями та серверними компонентами. Запропоновано підхід до підвищення рівня захисту шляхом впровадження поведінкової аутентифікації пристроїв, яка базується на аналізі параметрів їхньої мережевої активності та характеристик функціонування. Такий підхід дозволяє виявляти аномальну поведінку та ознаки компрометації навіть у випадках успішного проходження традиційної аутентифікації. Розглянуто можливість інтеграції механізмів динамічного контролю доступу, які забезпечують адаптивне коригування прав пристроїв залежно від рівня довіри до їхньої поведінки. Запропоноване рішення спрямоване на підвищення стійкості IoT-систем до кібератак, несанкціонованого доступу та компрометації вузлів мережі.

Ключові слова: Інтернет речей, інформаційна безпека, кібербезпека, gRPC, поведінкова аутентифікація, контроль доступу, аномалії поведінки, захист даних, мережеві протоколи.

Abstract

The paper addresses the problem of ensuring the security of Internet of Things (IoT) systems operating in environments with a large number of interconnected devices, where the key requirements include reliable data transmission, resilience to cyber threats, and the continuous operation of the network infrastructure. The features of using the gRPC protocol to organize interaction between IoT devices and server components are analyzed. An approach to increasing the level of protection is proposed by implementing behavioral authentication of devices, which is based on the analysis of the parameters of their network activity and operating characteristics. This approach allows detecting anomalous behavior and signs of compromise even in cases of successful completion of traditional authentication. The possibility of intefrating dynamic access control mechanisms that provide adaptive adjustment of device rights depending on the level of trust in their behavior is considered. The proposed solution is aimed at increasing the resilience of IoT systems to cyberattacks, unauthorized aaccess and compromise of network nodes.

Keywords: Internet of Things, information security, cybersecurity, gRPC, behavioral authentication, access control, behavioral anomalies, data protection, network protocols.

Вступ

Інтернет речей є однією з найдинамічніших технологічних концепцій сучасності, що забезпечує інтеграцію великої кількості пристроїв у єдиний інформаційний простір. IoT-системи активно впроваджуються в промислову автоматизацію, транспортну інфраструктуру, охорону здоров'я, енергетику та побутові сервіси. Водночас зростання кількості підключених пристроїв і обсягів переданих даних супроводжується збільшенням кількості кіберзагроз, серед яких особливу небезпеку становлять компрометація пристроїв, несанкціонований доступ до ресурсів мережі та атаки, спрямовані на порушення доступності сервісів.

Для забезпечення взаємодії між компонентами IoT-систем дедалі частіше використовується протокол gRPC, який характеризується високою продуктивністю, низькими затримками передачі даних та підтримкою сучасних механізмів захищеного обміну інформацією. Проте традиційні засоби автентифікації, що використовуються в таких системах, переважно базуються на статичних облікових даних або цифрових сертифікатах, які не дозволяють своєчасно виявляти скомпрометовані пристрої після їх успішного підключення до мережі.

Одним із перспективних напрямів підвищення рівня безпеки є застосування поведінкової аутентифікації, яка ґрунтується на аналізі характерних параметрів роботи пристрою, зокрема особливостей мережевого трафіку, частоти запитів, типових сценаріїв взаємодії та інших поведінкових характеристик. Використання такого підходу дозволяє сформувати високий рівень

довіри до пристрою в режимі реального часу та своєчасно реагувати на відхилення від нормальної поведінки.

У зв’язку з цим актуальним є дослідження можливостей підвищення безпеки IoT-систем шляхом інтеграції механізмів поведінкової аутентифікації в протокол gRPC, що сприятиме своєчасному виявленню потенційних загроз і підвищенню стійкості системи до сучасних кібернетичних атак.

Результати досліджень

Сучасний розвиток концепції Інтернету речей сприяє активному впровадженню інтелектуальних пристроїв у промислові, транспортні, медичні та побутові системи. За оцінками міжнародних аналітичних компаній, кількість підключених IoT-пристроїв щороку зростає, що призводить до збільшення обсягів мережевого трафіку та розширення площини потенційних кібератак [1]. Більшість IoT-пристроїв характеризується обмеженими обчислювальними ресурсами, що ускладнює використання складних криптографічних механізмів захисту та створює додаткові виклики для забезпечення інформаційної безпеки.

Для організації ефективної взаємодії між компонентами IoT-систем дедалі частіше використовується протокол gRPC, який базується на технології віддаленого виклику процедур та використовує HTTP/2 як транспортний рівень. Перевагами gRPC є висока швидкість передачі даних, підтримка двостороннього потокового обміну повідомленнями, компактне представлення даних за допомогою Protocol Buffers та можливість роботи в гетерогенних середовищах [2]. Завдяки цим особливостям протокол активно застосовується при побудові розподілених систем, мікросервісних архітектур та платформ Інтернету речей.

Незважаючи на наявність вбудованих механізмів захисту, зокрема TLS-шифрування та сертифікатної автентифікації, сучасні IoT-системи залишаються вразливими до атак, пов'язаних із компрометацією кінцевих пристроїв. У багатьох випадках зловмисник, отримавши доступ до легітимних облікових даних або цифрових сертифікатів, може здійснювати взаємодію із системою від імені довіреного пристрою. Традиційні механізми автентифікації перевіряють пристрій лише на етапі підключення до мережі, однак не враховують зміни його поведінки під час подальшої експлуатації [3].

Для усунення цього недоліку запропоновано використання поведінкової аутентифікації, що базується на безперервному моніторингу характеристик роботи IoT-пристроїв. Основною ідеєю такого підходу є формування індивідуального поведінкового профілю для кожного вузла мережі. Під час функціонування системи здійснюється аналіз частоти звернень до сервісів gRPC, типів викликів віддалених процедур, середнього часу відповіді, інтенсивності мережевого трафіку, обсягів переданих даних, послідовності виконання операцій та інших характеристик мережевої активності [4]. Відхилення від встановленого профілю може свідчити про компрометацію пристрою, спробу несанкціонованого доступу або виконання шкідливого програмного коду.

Особливістю запропонованого підходу є інтеграція поведінкової аутентифікації безпосередньо у процес взаємодії між сервісами gRPC. Для кожного пристрою формується динамічний коефіцієнт довіри, який розраховується на основі аналізу поточної поведінки [5]. У разі виявлення аномальної активності система автоматично змінює рівень доступу пристрою до ресурсів мережі. На відміну від традиційних моделей контролю доступу, де права визначаються лише під час початкової автентифікації, запропонований механізм забезпечує їх адаптивне коригування протягом усього життєвого циклу взаємодії пристрою із системою [6].

У роботі розроблено концепцію вдосконаленого захищеного протоколу взаємодії на основі gRPC, який поєднує механізми поведінкової аутентифікації та динамічного управління правами доступу. Запропонований підхід дозволяє здійснювати безперервну перевірку рівня довіри до пристрою після його підключення до мережі, а також автоматично реагувати на зміни його поведінки шляхом обмеження доступу до критичних сервісів або переведення пристрою до ізольованого сегмента мережі. На відміну від існуючих рішень, запропонована модель орієнтована на використання саме в IoT-середовищах із великою кількістю вузлів та високою інтенсивністю обміну даними.

Крім того, реалізація механізмів поведінкового аналізу на стороні серверних компонентів або шлюзів IoT дозволяє мінімізувати навантаження на пристрої та водночас забезпечити своєчасне виявлення аномалій. Це особливо важливо для критично важливих інфраструктур, систем промислового Інтернету речей, медичних інформаційних систем та платформ розумного міста, де

наслідки компрометації окремого вузла можуть призвести до значних фінансових збитків або порушення функціонування сервісів.

Таким чином, використання поведінкової аутентифікації у поєднанні з механізмами динамічного контролю доступу в протоколі gRPC створює передумови для побудови більш стійких до кіберзагроз IoT-систем, здатних адаптуватися до змін середовища функціонування та ефективно протидіяти сучасним атакам.

Висновки

У роботі проаналізовано особливості забезпечення інформаційної безпеки сучасних IoT-систем та визначено основні недоліки традиційних механізмів автентифікації, які не враховують поведінку пристрою після його підключення до мережі. Встановлено, що використання лише сертифікатної автентифікації та TLS-шифрування не гарантує захисту від загроз, пов'язаних із компрометацією легітимних пристроїв та викраденням їх облікових даних.

У результаті запропоновано підхід до підвищення безпеки IoT-систем на основі інтеграції механізмів поведінкової аутентифікації в протокол gRPC. Запропоноване рішення передбачає формування поведінкового профілю пристрою, безперервний моніторинг його мережевої активності та розрахунок динамічного коефіцієнта довіри. На основі отриманих даних реалізується адаптивне управління правами доступу, що дозволяє автоматично обмежувати можливості пристроїв у разі виявлення аномальної поведінки.

Отримані результати свідчать про перспективність поєднання поведінкової аутентифікації та динамічного контролю доступу для побудови більш захищених IoT-середовищ. Запропонований підхід забезпечує своєчасне виявлення потенційно скомпрометованих вузлів, знижує ризик несанкціонованого доступу до ресурсів мережі та підвищує загальну стійкість системи до сучасних кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Security, Privacy and Trust in Internet of Things: The Road Ahead. Computer Networks URL **:** https://www.researchgate.net/publication/270107935_Security_privacy_and_trust_in_Internet_of_Things_The_road_ahead html (дата звернення: 02.06.2026)
2. On the Features and Challenges of Security and Privacy in Distributed Internet of Things. Computer Networks URL: https://www.researchgate.net/publication/257582417_On_the_features_and_challenges_of_security_and_privacy_in_distributed_Internet_of_things (дата звернення: 02.06.2026)
3. Google. gRPC Documentation URL: https://docs.cloud.google.com/api-gateway/docs/grpc-overview (дата звернення: 02.06.2026)
4. Enhancing Security and Real-Time Resilience in Microservices: Automated Self-Healing Controls for Secure gRPC over HTTP/3 with AES-256-GCM URL: https://www.researchgate.net/publication/396154226 _Enhancing_Security_and_Real-Time_Resilience_in_Microservices_Automated_Self-Healing_ Controls_ for_Secure_gRPC_over_HTTP3_with_AES-256-GCM (дата звернення: 02.06.2026)
5. Security of IoT Systems: Design Challenges and Opportunities URL: https://www.researchgate.net/publication/308195507_Security_of_IoT_Systems_Design_Challenges_and_Opportunities (дата звернення: 02.06.2026)
6. Fog Computing for the Internet of Things: Security and Privacy Issues URL: https://ieeexplore.ieee.org/document/7867732 (дата звернення: 02.06.2026)

Бучацький Ілля Олександрович – студент групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: illiabu2005@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD), доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Buchatskyi Illia O. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: illiabu2005@gmail.com

Supervisor*:* ***Saliieva Olha V.*** – Doctor of Philosophy (PhD), Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, email: salieva8257@vntu.edu.ua