http://www.moderntechno.de/index.php/meit/article/view/meit35-00-043
DOI: 10.30890/2567-5273.2024-35-00-043

УДК 004.056.53(045)

MULTIFACTOR AUTHENTICATION USING IN INTERNET OF THINGS NETWORKS MANAGEMENT SYSTEMS

ВИКОРИСТАННЯ БАГАТОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ В СИСТЕМАХ УПРАВЛІННЯ МЕРЕЖАМИ ІНТЕРНЕТУ РЕЧЕЙ

Gulak N.K. / Гулак Н.К.
c.t.s./ к.т.н.
ORCID: 0000-0001-8524-8635
Dubchak E.V. / Дубчак О.В.
ORCID: 000-0001-9739-3960
National Aviation University, Kyiv, Guzara 1,03058
Національний авіаційний університет, м. Київ, Л. Гузара 1, 03058

Анотація. *Розглянуто ключові блоки IoT, на основі яких можна розробити ефективну багаторівневу архітектуру IoT; наведено аналіз загроз щодо безпеки IoT; визначено необхідність забезпечити захист даних ще на етапі проєктування мереж; проаналізовано фактори управління IoT – пристроями, які сприяють підвищенню їхньої вразливості; обґрунтовано використання багатофакторної автентифікації для захисту управління IoT – пристроями; розроблено алгоритм модуля багатофакторної автентифікації, що ґрунтується на біометричних методах за голосом та відбитком пальця; математично підтверджено доцільність застосування обраних методів автентифікації як комплексного засобу захисту інформації в IoT.*

Ключові слова. *IoT, архітектура IoT, загрози IoT, методи захисту IoT, багатофакторна автентифікація, біометричні методи автентифікації, оцінювання рівня захищеності IoT.*

Вступ.

IoT (Internet of Things, Інтернет речей) — це система фізичних об’єктів («речей»), які пов’язані між собою за допомогою вбудованих датчиків, програмного забезпечення (ПЗ) та/або інших технологій. Прогрес у технічних можливостях IoT відкрив доступ до дешевих енергоефективних технологій. А наявність і надійність новітніх датчиків зробили IoT сучасним рішенням для широкого кола виробників і підприємств.

За прогнозами експертів, кількість IoT-пристроїв за поточне десятиліття зросте майже вдвічі і до 2030 р. становитиме понад 29 млрд. [1]

Управління пристроями таких систем доволі часто виконується за допомогою голосу, що, враховуючи велику кількість програм щодо імітації голосу, може зробити систему управління IoT дуже вразливою. Використання багатофакторної автентифікації пропонується в якості одного з методів щодо підвищення захисту від стороннього втручання в управління IoT.

Основний текст

1. Вплив кібератак на IoT. Для усвідомлення уразливості IoT розглянемо архітектуру, що містить типові блоки, а саме:

- «розумні» речі;
- мережі та міжмережеві пристрої, які дозволяють малопотужним IoT-пристроям отримувати доступ до Інтернету;
- проміжне ПЗ або IoT- платформи, що надають можливість зберігати дані,

та сучасні обчислювальні механізми, які здатні до аналітичних дій;

- програми, які дозволяють кінцевим користувачам отримувати зиск від IoT і керувати фізичним середовищем. [2]

Указані блоки визначають архітектурне рішення для будь-якої системи IoT, базуючись на якому можна розробити ефективну багаторівневу структуру, що найчастіше містить:

- рівень сприйняття, який складається з «розумних» речей;
- рівень підключення, який передає дані з фізичного рівня в хмару і навпаки через мережі та міжмережеві пристрої;
- рівень опрацювання, який використовує IoT- платформи для збирання та керування всіма потоками даних;
- прикладний рівень, який надає рішення для кінцевого користувача щодо аналітики, звітності та управління пристроями. [2]

Розглянемо функції та склад стандартизованої архітектурної моделі IoT. [2]

1. Рівень сприйняття

Основою будь-якої системи IoT є широкий спектр «речей» або кінцевих пристроїв. Залежно від функцій IoT-речі можна розділити на такі групи: датчики, лічильники; виконавчі механізми; машини та пристрої, що або підключені до датчиків і приводів, або мають їх як вбудовані частини.

Важливо відзначити, що архітектура не накладає обмежень на розмір своїх компонентів або їх розташування.

2. Рівень підключення

Цей рівень відповідає за всі комунікації між пристроями, мережами та хмаровими сервісами, які складають інфраструктуру IoT. Зв'язок між пристроями та хмаровими службами або шлюзами передбачає різні мережеві технології, зокрема: Ethernet, Wi-Fi, NFC (Near Field Communication), Bluetooth, LPWAN (Low-power Wide-area Network), ZigBee.

3. Рівень опрацювання

Рівень опрацювання збирає, зберігає та опрацьовує дані з попереднього рівня. Усі ці завдання зазвичай вирішуються за допомогою IoT- платформ і містять два основні кроки - накопичення даних і абстракції даних.

4. Рівень застосування

На цьому рівні інформація аналізується ПЗ для відповіді на ключові питання бізнесу. Існують сотні таких додатків IoT, що відрізняються за складністю та функціональністю, використовують різні стеки технологій та операційні системи.

Слід зауважити, що потенційна вразливість IoT— це загальна кількість точок входу для несанкціонованого доступу до мережі. Безпека IoT- пристроїв включає той факт, що суб’єкти загроз можуть пошкодити мережу та ПЗ, яке підтримує IoT-пристрої, а також й самі пристрої.

Оскільки Іот-пристроями є комп’ютеризовані під’єднані до Інтернету об’єкти, такі як мережеві камери безпеки, розумні холодильники та автомобілі з підтримкою Wi-Fi тощо, то безпека IoT являє собою процес захисту цих пристроїв і забезпечення того, щоб вони не створювали загрози для мережі.

Найрозповсюдженішими загрозами щодо безпеки незахищених IoT-пристроїв технічні експерти, зазвичай, вважають несанкціонований доступ, атаки між пристроями, витік даних та DDoS-атаки. [3]

Крім того, існують і інші загрози, до яких чутливий IoT, і в рамках тематики дослідження доцільно їх розглянути.

1.Синтез мовлення (TTS, Text-to-Speech). Це метод створення мовлення з вхідних даних, яке звучить максимально природно та зрозуміло. Метод має широкий спектр застосувань, включаючи системи розмовного діалогу, переклади з однієї мови на іншу, допомогу людям із розладами голосу та автоматичне читання електронних книг. Двома основними компонентами типової системи TTS є аналіз тексту та генерація мовлення. Перший компонент аналізує вхідний текст і генерує послідовність фонем, які визначають специфікацію мовлення тексту. Використовуючи ці фонеми, спеціальний модуль генерує «мовну хвилю». Однак у наскрізних системах глибокого навчання шаблони мовлення генеруються безпосередньо з вхідного тексту. [4]

2. Перетворення голосу (VC, Voice Changer) спрямоване на перетворення голосу одного мовця на голос іншого. Типові системи VC працюють безпосередньо з мовними сигналами зловмисника та цільового мовця, за допомогою яких функція перетворення змінює акустичні параметри зловмисника на параметри цільового мовця. Застосування технології VC включає створення природних звуків для людей з вадами мови та дублювання голосу в індустрії розваг. [5]

Із швидким зростанням популярності та функціональності голосових IoT-пристроїв потенційні голосові атаки стають серйозним ризиком для безпеки, оскільки відрізняються простотою здійснення. Часто їх важко або навіть неможливо виявити людям через прихованість таких атак іншими звуками, вбудованими в аудіо- та відеозаписи. Більше того, неважко масштабувати такий тип атак, наприклад, прихований зловмисний зразок аудіо у відео на YouTube може націлитися на мільйони пристроїв одночасно.

Хоча реалізації існуючих методів атаки можуть суттєво відрізнятися, їхні цілі однакові: згенерувати сигнал, що змусить систему голосового керування виконати певну шкідливу команду, яку користувач не зможе виявити чи розпізнати.

Як приклад атак на основі реалізації - базова атака відтворення голосу, яку легко виявити, проте вона становить підґрунтя іншим, більш просунутим і небезпечним атакам, таким як A11Y (замість слова «Accessibility» використовується нумероним).

Відсутність в багатьох IoT-пристроях вбудованого інструментарію безпеки може створювати особливі проблеми та розширювати поверхню атаки. Кількість і географічний розподіл активних IoT - пристроїв підвищує ймовірність того, що команда безпеки може вчасно не врахувати нові пристрої, додані до мережі. Дані з периферійних датчиків надсилаються через мережу на шлюзи, централізовані сервери або хмару, надаючи зловмисникам більше точок доступу. Обмеження систем зберігання даних і їхніх ємностей - причини ще більшого ускладнення надання оновлень по бездротових мережах для усунення

вразливостей безпеки.

2. Необхідність розробки багатофакторної автентифікації для захисту IoT. Одним із методів захисту IoT є автентифікація. Розглянемо однофакторну автентифікацію. Найпоширенішою технологією є SSO (Single sign-on, єдиний вхід), яка дозволяє після автентифікації користувачам отримувати доступ до кількох програм за допомогою одного набору облікових даних, наприклад, імені користувача та пароля. Це означає, що після входу в систему користувачеві не потрібно знову входити в кожну програму, пов'язану з цією системою. [6] SSO — це, по суті, уніфікована угода про управління ідентифікацією між трьома суб'єктами: користувачами, постачальниками послуг (SP, Service Provider) та постачальниками ідентифікаційних даних (IdP, Identity Provider). Організації, які використовують SSO, часто вважають за доцільне посилити контроль автентифікації: збільшити кількість символів, необхідних у паролі; підвищити вимоги до складності паролів; застосувати політику блокування облікових записів і повторне використання пароля. Слід зауважити, що SSO потребує впровадження та налаштування, що може бути істотно дороговартісним. [6]

Уникнення перерахованих складнощів можливо за рахунок впровадження багатофакторної автентифікації. Як зазначалося вище, управління IoT - пристроями найчастіше виконується голосом, тобто біометричним параметром, на використанні якого ґрунтується відповідний метод. [7]

На рисунку 1 наведено оцінювання біометричних методів за універсальністю, унікальністю, стабільністю і зібраністю.

Слід зазначити, що лідером за всіма показниками є метод автентифікації за відбитком пальця, крім того, він не потребує дороговартісного обладнання, що робить цей метод популярним.

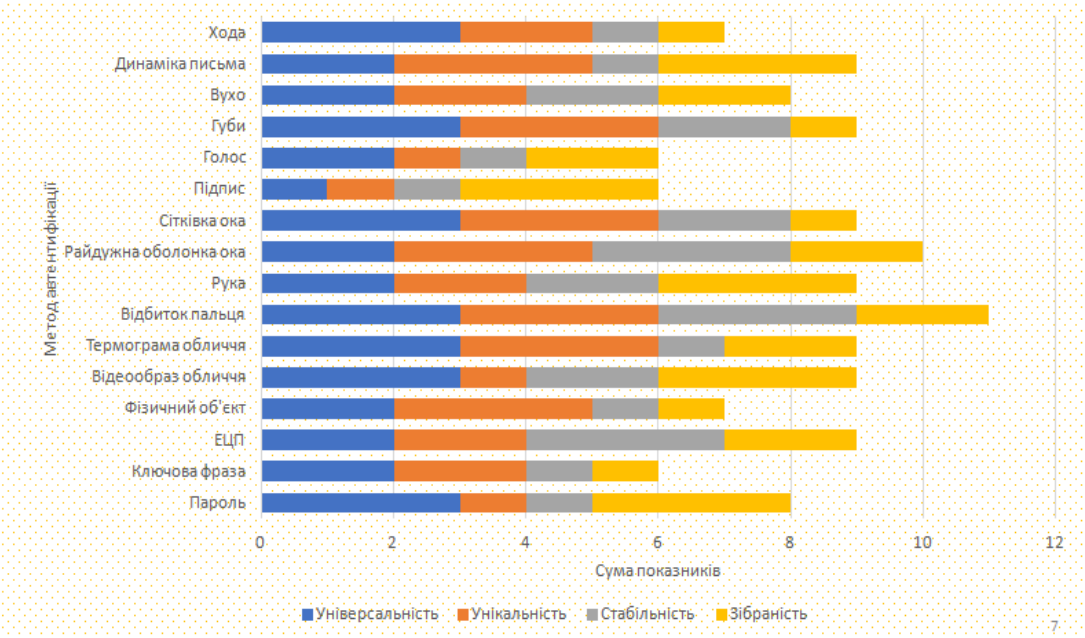

Рисунок – 1 Графічне порівняння методів автентифікації

IoT визначив нову еру в підвищенні автоматизації не тільки на робочих

місцях різноманітних виробництв, але й побутових приладів і функцій у домівках, особливо за допомогою електронних засобів, які підтримують дистанційне управління. Багато нових комунікаційних технологій, таких як мережі GSM/GPRS, бездротові сенсорні мережі, Bluetooth, оператори ліній електропередач та Інтернет використовуються в домашній автоматизації. Наприклад, бездротові сенсорні мережі на основі протоколу ZigBee широко використовуються в «розумних» будинках, що стало основним трендом у цій галузі.

З огляду на вищевказане, підвищення надійності захисту IoT від несанкціонованого доступу та перехоплення конфіденційної інформації за допомогою використання багатофакторної автентифікації на даний момент є актуальним.

3. Розробка модуля багатофакторної автентифікації для системи керування IoT. Алгоритм передбачає підтвердження особи користувача після отримання голосового повідомлення за допомогою відбитку пальцю, оскільки цей метод добре збалансовує недоліки автентифікації тільки за допомогою голосової команди. Схема алгоритму наведена на рисунку 2.

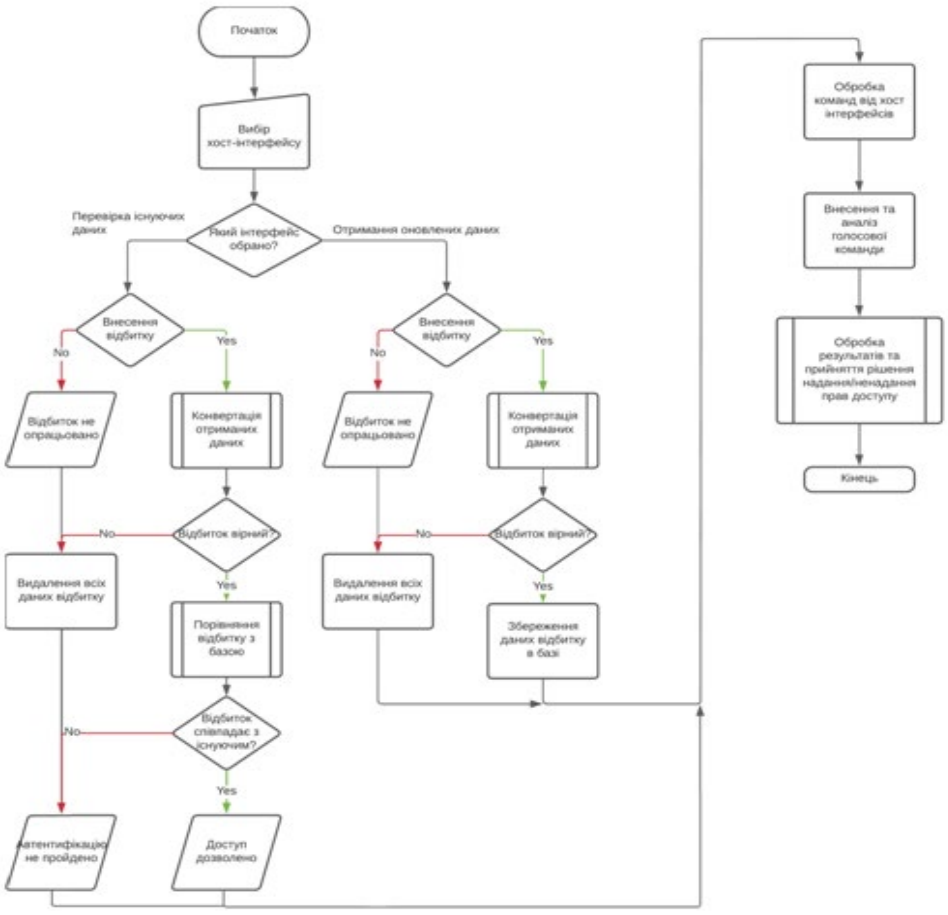

Рисунок – 2 Структурна схема алгоритму багатофакторної автентифікації

Наведемо оцінювання надійності алгоритму поєднання методів біометричної автентифікації за допомогою теореми множення ймовірностей.[8]

$$P_{нсд} = P_{в}^{нсд} \times P_{п}^{нсд} = (1 - P_{в}) \times (1 - P_{п}) \quad (1)$$

де: $P_{нсд}$ – ймовірність несанкціонованого доступу;

$P_{в}^{нсд}$ – ймовірність підроблення голосової команди;

$P_{п}^{нсд}$ – ймовірність підроблення відбитку пальцю;

$P_{в}$ – ймовірність правильного використання голосової команди;

$P_{п}$ – ймовірність правильного використання відбитку пальцю.

Ймовірність підроблення голосової команди становить 83%, відбитку пальцю – 85%.

Дані в коефіцієнтах: $P_{в} = 0,83$ та $P_{п} = 0,85$

$$P_{нсд} = (1 - 0,83) \times (1 - 0,85) = 0,0255 \quad (2)$$

Визначено, що вірогідність отримання несанкціонованого доступу при використанні запропонованого методу буде дорівнювати $P_{нсд} = 2,55\%$.

Ймовірність правильного використання представленого методу багатофакторної автентифікації – 97,45%.

Таким чином, запропонований метод багатофакторної автентифікації зможе збільшити надійність захисту від несанкціонованого доступу в 4,3 та 14 разів відносно методів сканування голосової команди та відбитку пальцю відповідно.

Підсумки та висновки

1. Розглянуто архітектуру IoT; проаналізовано найпоширеніші виклики щодо її безпеки, що дало можливість визначити слабкі місця IoT і відповідні методи убезпечення.

2. Обґрунтовано доцільність використання біометричних методів багатофакторної автентифікації для захисту управління в IoT, що склало основу для розроблення алгоритму багатофакторної автентифікації.

3. Проведено розрахунок, який підтвердив доцільність поєднання методів для багатофакторної автентифікації та дозволив підвищити надійність захисту мережі в 4,3 та 14 разів відносно методів сканування голосової команди та відбитку пальцю відповідно.

Література

1. Statista. Internet of things: statistics&facts [Електронний ресурс] - Режим доступу: https://www.statista.com/topics/2637/internet-of-things/

2. IoT Architectue: the Pathway from Physical Signals to Business Decisions [Електронний ресурс] - Режим доступу: https://www.altexsoft.com/blog/iot-architecture-layers-components/

3. Kinza Yasar. IoT Security (Internet of Things Security) [Електронний ресурс] - Режим доступу: https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security

4. Dutoit, Thierry. An Introduction to Text-to-Speech Synthesis. — Kluwer Academic Publishers, 1997. — 312 p.

5. Деркач М. Штучний інтелект який змінює голос: огляд популярних платформ [Електронний ресурс] - Режим доступу: https://psm7.com/uk/iskusstvennyj-intellekt/shtuchnij-intelekt-yakij-zminyuye-golos-

oglyad-populyarnih-platform.html

6. What is SSO? [Електронний ресурс] - Режим доступу: https://aws.amazon.com/ru/what-is/sso

7. Biometric Autentication [Електронний ресурс] - Режим доступу: https://www.logintc.com/types-of-authentication/biometric-authentication

8. Васильків І.М. Основи теорії ймовірностей та математичної статистики: навч. посібник/ І.М. Васильків - Львів:ЛНУ ім. Івана Франка, 2020 – 58 с. [Електронний ресурс] - Режим доступу https://new.mmf.lnu.edu.ua/wp-content/uploads/2020/04/Vasyl-kiv-I.M.-TIMS_CHASTYNA_1.pdf

Abstract. Introduction. *IoT is a system of physical objects. connected to each other using embedded sensors, software and other technologies. For experts predict, the IoT devices number will be more than 29 billion by 2030. IoT devices voice control can make the IoT management system vulnerable. Multifactor authentication, as one of increase protection methods to against outside interference in IoT management, is proposed.*

Impact of cyberattacks to IoT. *The functions and composition of IoT standardized architectural model are considered: perception level; connection level; processing level; application level. The total number of entry points for unauthorized access is defined as a potential IoT vulnerability. Unauthorized access, device-to-device attacks, data leak and DDoS attacks are threats of unprotected IoT devices security. Speech Synthesis and Voice Changer are analyzed. Voice attacks are defined as a serious security risk. The lack of built-in security tools in many IoT devices has been identified as IoT problems source.*

The need to develop multi-factor authentication to IoT protect. *Single-factor authentication as a method of IoT protecting is considered using the SSO technology example. Biombiomeetric methods assessment for versatility, uniqueness, stability and composure is given. The fingerprint authentication method is determined to be the most using. The increasing the reliability relevance of IoT protection from unauthorized access and interception of confidential information of multi-factor biometric authentication using is considered.*

Multifactor authentication module development for IoT management system. *The algorithm verifies the user's identity after receiving a voice message using a fingerprint. The method scheme is given. The algorithm reliability assessment, combining biometric authentication methods, using the probability multiplication theorem, is given.*

Results and conclusions. *1. The IoT architecture is considered; the most common security challenges are analyzed. 2. The expediency of multifactor authentication biometric methods using to protect management in IoT is considered; multifactor authentication algorithm is created. 3. The calculation, confirmed the correctness of multifactor authentication methods combination, is carried out. It makes possible to increase the IoT protection reliability.*

Key words: *IoT, IoT architecture, IoT threats, IoT protecting methods, multifactor authentication, biometric authentication methods, evaluation of IoT security level.*