УДК 004.056:004.738.5

А. С. Мосєвніна

АРХІТЕКТУРНІ ПІДХОДИ ДО ПРОЄКТУВАННЯ ЗАХИЩЕНИХ СИСТЕМ ГОЛОСОВОГО ЗВ'ЯЗКУ В SMART-БУДИНКАХ

Вінницький національний технічний університет;

Анотація

У роботі розглянуто архітектурні підходи до проєктування захищених систем голосового зв'язку в Smart-будинках, що функціонують у середовищі Інтернету речей. Проаналізовано основні проблеми забезпечення безпеки голосового трафіку, зокрема ризики перехоплення даних, несанкціонованого доступу та затримок передачі. Досліджено централізовані, децентралізовані та гібридні підходи до побудови систем голосового зв'язку. Запропоновано архітектурний підхід, що поєднує використання edge-обчислень, криптографічних механізмів захисту та модулів автентифікації пристроїв, що дозволяє підвищити рівень конфіденційності, цілісності та доступності голосових даних у системах Smart-будинку.

Ключові слова: Smart-будинок; голосовий зв'язок; IoT; архітектура систем; інформаційна безпека; edge computing; захист даних; автентифікація.

Abstract

The paper examines architectural approaches to designing secure voice communication systems in smart home environments operating within the Internet of Things (IoT). Key security challenges of voice traffic transmission are analyzed, including risks of data interception, unauthorized access, and communication delays. Centralized, decentralized, and hybrid architectures for voice communication systems are considered. An architectural approach combining edge computing, cryptographic protection mechanisms, and device authentication modules is proposed, which enhances the confidentiality, integrity, and availability of voice data in smart home systems.

Keywords: smart home; voice communication; IoT; system architecture; information security; edge computing; data protection; authentication.

Вступ

Сучасний розвиток технологій Інтернету речей (IoT) сприяв активному впровадженню систем Smart-будинку, які об'єднують різноманітні пристрої для автоматизації побутових процесів та підвищення комфорту користувачів. Одним із ключових напрямів розвитку таких систем є використання голосового зв'язку та голосових інтерфейсів, що забезпечують природну взаємодію користувача з пристроями та дозволяють здійснювати обмін голосовими повідомленнями між компонентами системи [1].

Разом із розширенням функціональних можливостей голосових сервісів зростає і складність забезпечення їхньої безпеки. Передача голосових даних у мережах IoT супроводжується низкою загроз, серед яких перехоплення інформації, підміна повідомлень, несанкціонований доступ до пристроїв, а також вплив на доступність сервісів через перевантаження мережі або затримки передачі [2]. Традиційні підходи до захисту, що базуються виключно на використанні криптографічних алгоритмів, не завжди забезпечують необхідний рівень безпеки та продуктивності в умовах обмежених ресурсів IoT-пристроїв.

У зв'язку з цим особливої актуальності набуває питання проєктування архітектури систем голосового зв'язку, яка враховує як вимоги інформаційної безпеки, так і обмеження середовища функціонування. Раціонально обрана архітектура дозволяє підвищити рівень захищеності системи, зменшити затримки передачі даних та забезпечити надійну взаємодію між пристроями Smart-будинку.

Актуальність

Актуальність дослідження зумовлена стрімким розвитком технологій Інтернету речей та широким впровадженням систем Smart-будинку, які активно використовують голосові інтерфейси для взаємодії користувача з пристроями. Голосовий зв'язок стає важливим елементом таких систем, забезпечуючи зручність керування та обмін інформацією між компонентами середовища.

Водночас збільшення кількості IoT-пристроїв і обсягів переданих голосових даних призводить до зростання кількості загроз, пов'язаних із перехопленням інформації, підміною повідомлень, несанкціонованим доступом та порушенням доступності сервісів. Існуючі підходи до захисту голосового трафіку часто орієнтовані переважно на використання криптографічних методів, що не завжди враховують особливості архітектури систем і обмежені ресурси IoT-пристроїв.

У таких умовах важливим завданням є розробка ефективних архітектурних підходів до проєктування систем голосового зв'язку, які забезпечують комплексний захист інформації з урахуванням вимог до продуктивності, масштабованості та надійності. Саме архітектурні рішення дозволяють досягти балансу між безпекою та ефективністю функціонування систем Smart-будинку, що визначає актуальність даного дослідження [3].

Аналіз проблем побудови систем голосового зв'язку в Smart-будинках

Системи Smart-будинку, що використовують голосовий зв'язок, функціонують у розподіленому середовищі Інтернету речей, де велика кількість пристроїв взаємодіє через мережу. Така організація створює низку проблем, пов'язаних із забезпеченням безпеки та ефективності передачі голосових даних.

До основних проблем належать:

- наявність єдиної точки відмови у централізованих системах;
- підвищені затримки передачі через використання складних механізмів шифрування;
- обмежені обчислювальні ресурси IoT-пристроїв;
- складність забезпечення автентифікації великої кількості пристроїв;
- вразливість до атак типу «людина посередині» (MITM) та перехоплення трафіку.

Зазначені фактори свідчать про необхідність використання комплексного підходу до проєктування архітектури систем голосового зв'язку.

Архітектурні підходи до побудови систем голосового зв'язку

У сучасних дослідженнях виділяють кілька основних архітектурних підходів до побудови систем голосового зв'язку в Smart-будинках:

1. **Централізована архітектура**
   Передбачає використання центрального сервера для обробки та передачі голосових даних. Такий підхід є простим у реалізації та адмініструванні, проте має суттєві недоліки, зокрема наявність єдиної точки відмови та підвищену вразливість до атак [4].
2. **Децентралізована архітектура (peer-to-peer)**
   Забезпечує прямий обмін даними між пристроями без участі центрального вузла. Це підвищує рівень відмовостійкості та безпеки, однак ускладнює реалізацію механізмів керування та автентифікації.
3. **Архітектура з використанням edge/fog computing**
   Передбачає обробку даних на проміжних вузлах (локальних хабах або шлюзах), що розташовані ближче до джерел даних. Такий підхід дозволяє зменшити затримки передачі, знизити навантаження на мережу та підвищити рівень безпеки за рахунок локальної обробки інформації.

Порівняння зазначених підходів наведено у таблиці 1.

Таблиця 1. Порівняння архітектурних підходів

Архітектура	**Переваги**	**Недоліки**
Централізована	Простота реалізації, зручність управління	Єдина точка відмови, вразливість до атак
Децентралізована	Висока відмовостійкість, підвищена безпека	Складність реалізації та керування
Edge/Fog	Низькі затримки, зменшення навантаження, краща безпека	Потребує додаткових обчислювальних ресурсів

Запропонований архітектурний підхід

З метою підвищення рівня безпеки та ефективності систем голосового зв'язку пропонується використання гібридного архітектурного підходу, який поєднує переваги edge computing та децентралізованої взаємодії [5].

Основна ідея підходу полягає у використанні локального edge-вузла (хаба), який виконує функції обробки, контролю та захисту голосового трафіку, при цьому частина взаємодії між пристроями може здійснюватися безпосередньо.

Запропонована архітектура включає такі основні модулі:

- модуль автентифікації пристроїв, що забезпечує перевірку достовірності учасників зв'язку;
- модуль управління криптографічними ключами;
- модуль шифрування та дешифрування голосових даних;

- модуль моніторингу та аналізу трафіку;
- модуль адаптації якості обслуговування (QoS).

Використання такого підходу дозволяє:

- зменшити затримки передачі голосових даних;
- підвищити рівень захисту від атак;
- забезпечити масштабованість системи;
- ефективно використовувати ресурси IoT-пристроїв.

Висновки

У роботі розглянуто особливості проєктування систем голосового зв'язку в Smart-будинках, що функціонують у середовищі Інтернету речей. Проведений аналіз показав, що традиційні підходи до побудови таких систем не завжди забезпечують необхідний рівень безпеки та ефективності через наявність єдиних точок відмови, обмежені ресурси пристроїв та підвищені затримки передачі даних.

Досліджено основні архітектурні підходи до побудови систем голосового зв'язку, зокрема централізований, децентралізований та підхід із використанням edge/fog computing, а також визначено їх переваги та недоліки. На основі проведеного аналізу запропоновано гібридний архітектурний підхід, який поєднує локальну обробку даних із можливістю децентралізованої взаємодії між пристроями.

Запропонований підхід дозволяє підвищити рівень конфіденційності, цілісності та доступності голосових даних, зменшити затримки передачі та забезпечити більш ефективне використання ресурсів IoT-пристроїв. Отримані результати можуть бути використані при розробці програмних модулів захищеного голосового зв'язку в системах Smart-будинку та слугувати основою для подальших досліджень у цій галузі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Matthew B. Hoy. «Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants», 2018. URL: https://www.tandfonline.com/doi/abs/10.1080/02763869.2018.1404391

2. Abdullah Alfahaid., Easa Alalwany., Abdulqader Almars. «Machine Learning-Based Security Solutions for IoT Networks: A Comprehensive Survey», 2020. URL: https://www.researchgate.net/publication/392141464_Machine_Learning-Based_Security_Solutions_for_IoT_Networks_A_Comprehensive_Survey

3. Tinashe Magara., Yousheng Zhou. «Internet of Things (IoT) of Smart Homes: Privacy and Security», 2024. URL: https://www.researchgate.net/publication/379693713_Internet_of_Things_IoT_of_Smart_Homes_Privacy_and_Security

4. Roman R., Lopez J., Mambo M. «Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges», 2018. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167739X16305635

5. Falguni Suthar., Ms. Hiralben Patel. «Advanced Cryptographic Techniques for Securing AI-Driven IoT Systems», 2025. URL: https://www.researchgate.net/publication/394976019_Advanced_Cryptographic_Techniques_for_Securing_AI-Driven_IoT_Systems

Мосєвніна Аліна Сергіївна - студентка групи 1ПІ-25м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: mosievninaaa@gmail.com

Науковий керівник: Ракитянська Ганна Борисівна - *к.т.н., доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: rakit@vntu.edu.ua.*

Mosievnina Alina Sergiivna - student of group 1PI-25m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: mosievninaaa@gmail.com

Academic supervisor: Rakytianska Hanna Borysivna - *in Engineering, Associate Professor of the Department of, Vinnytsia National Technical University, Vinnytsia, e-mail: rakit@vntu.edu.ua.450*