УДК 004.056.5:004.738.5

РОЗРОБКА СИСТЕМИ ВІДДАЛЕНОГО ВИДАЛЕННЯ ДАНИХ НА ANDROID-ПРИСТРОЯХ ЯК ЕЛЕМЕНТА МОБІЛЬНОЇ БЕЗПЕКИ

Аліна Хмілевська, Леся Булатецька

DEVELOPMENT OF A REMOTE DATA DELETION SYSTEM ON ANDROID DEVICES AS A MOBILE SECURITY ELEMENT

Alina Khmilevska, Lesia Bulatetska

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *This paper explores the development of a remote data deletion system for Android devices, focusing on data protection in case of device loss, theft, or compromise. Built using Flutter for cross-platform development, Firebase for cloud synchronization, and Android's native APIs, the proposed solution enables secure and selective removal of personal content, contacts, messages, and application data. The system is designed to function under limited connectivity and enforces proper permission handling and user authentication to minimize risks of abuse. The architecture allows future integration of anomaly detection and AI-enhanced decision-making for proactive mobile security.*

У сучасному цифровому середовищі мобільні пристрої відіграють важливу роль у повсякденному житті, забезпечуючи не лише зв'язок, а й постійний доступ до конфіденційної інформації – особистої, ділової, медичної, фінансової. Втрата фізичного контролю над пристроєм або його компрометація може мати серйозні наслідки для безпеки даних. Тому важливим напрямом у сфері мобільної безпеки є створення технологій, які дозволяють надійно й оперативно знищувати інформацію на віддалених пристроях.

У межах цієї роботи було спроєктовано та реалізовано систему віддаленого видалення даних для пристроїв на базі Android, яка поєднує сучасні підходи до мобільного програмування, хмарні обчислення й нативні API операційної системи.

Ключовим інструментом, який забезпечує взаємодію між серверною частиною й мобільним застосунком, виступає Firebase Cloud Messaging. За його допомогою здійснюється передача команд на видалення, які отримуються клієнтським застосунком і виконуються в реальному часі. Важливою особливістю реалізованої системи є можливість обробки команд навіть при тимчасовій відсутності підключення до мережі – команди зберігаються та виконуються при першій можливості, що критично важливо для забезпечення надійності в умовах нестабільного зв'язку, характерних для кризових ситуацій.

Архітектура системи побудована з використанням Flutter як інструменту кросплатформної розробки, що забезпечує сумісність між різними версіями Android, а також дозволяє реалізувати адаптивний інтерфейс для майбутніх iOS-рішень. Такий підхід значно розширює потенційну аудиторію користувачів та спрощує подальшу підтримку і розвиток системи. Для зберігання метаданих, журналу операцій і стану пристрою використовується Firebase Firestore, що забезпечує надійність і масштабованість без необхідності ручного адміністрування серверів.

Застосунок виконує знищення даних через низку взаємодоповнюючих механізмів. На системному рівні використовується DevicePolicyManager – стандартний інструмент керування пристроєм у корпоративному середовищі. Він дозволяє реалізувати як повне скидання налаштувань пристрою, так і вибіркове очищення локальних даних. Для більш гнучкого підходу до видалення специфічних типів даних розроблено власні алгоритми, які працюють

через ContentResolver та безпосередню взаємодію з файловою системою при наявності відповідних дозволів.

У рамках проєкту реалізовано можливість вибіркового видалення медіафайлів, контактів, SMS-повідомлень, історії дзвінків, а також даних застосунків, які не зберігають інформацію в захищених розділах. Така гранулярність забезпечує гнучкість у налаштуванні системи під конкретні потреби користувача або організації. Для кожного типу даних розроблено оптимальний алгоритм видалення, який враховує особливості їх зберігання та обробки в системі Android.

У процесі реалізації було враховано політику обмежень, запроваджену в Android 10+ щодо роботи з файловою системою (Scoped Storage). Щоб уникнути винятків і помилок доступу, система при першому запуску запитує всі необхідні дозволи та зберігає їхній стан для подальшого використання без втручання користувача. Для пристроїв з новішими версіями Android реалізовано спеціальні механізми обробки RecoverableSecurityException та використання MediaStore.createDeleteRequest для отримання тимчасових дозволів на видалення медіафайлів.

Захист системи від несанкціонованого доступу реалізовано на основі Firebase Authentication. Особлива увага приділена безпеці комунікацій між компонентами системи. Всі передачі даних відбуваються через захищені канали з використанням HTTPS, а критично важлива інформація додатково шифрується на рівні додатку. Push-сповіщення, які містять команди на видалення даних, підписуються цифровим підписом для забезпечення їх автентичності та захисту від підробки.

Інтерфейс системи адаптований під користувача без технічної освіти: інтуїтивна панель керування, чітка візуалізація статусу пристрою, історія дій та можливість перегляду технічних деталей для адміністратора. Для зручності використання реалізовано систему сповіщень, яка інформує користувача про хід та результати виконання операцій видалення даних, що підвищує прозорість роботи системи та довіру користувачів.

Розроблена система була протестована на різних моделях пристроїв та версіях Android (від 6.0 Marshmallow до 14.0), що підтвердило її надійність та ефективність у різних умовах. Особлива увага приділялася тестуванню в умовах обмеженого доступу до мережі та при різних сценаріях використання, включаючи екстрені ситуації, коли швидке реагування є критично важливим.

Результатом проведених досліджень стала працездатна, масштабована система, здатна працювати в реальному часі та забезпечувати високий рівень захисту даних у мобільному середовищі. Практична значимість розробки полягає в створенні реального інструменту для захисту конфіденційної інформації, який може бути використаний як індивідуальними користувачами, так і організаціями для забезпечення безпеки своїх даних.

У перспективі розглядається інтеграція алгоритмів машинного навчання для автоматичного виявлення загроз на основі поведінкових патернів пристрою, що дозволить ще до моменту втрати або крадіжки пристрою ініціювати профілактичне блокування або видалення даних. Також планується розробка механізмів автоматичного реагування на основі аналізу географічного положення, мережевої активності та інших параметрів, які можуть вказувати на компрометацію пристрою.

Таким чином, розроблена система поєднує технічну ефективність, простоту користування та високу гнучкість. Вона може бути адаптована для корпоративного використання, впроваджена в середовища з підвищеним рівнем безпеки (банківські установи, державні служби) або використовуватися індивідуальними користувачами для захисту особистої інформації.

Бібліографія

1. Device administration overview | Android Enterprise | Android Developers. Android Developers. URL: https://developer.android.com/guide/topics/admin/device-admin.
2. Firebase Cloud Messaging. Firebase. URL: https://firebase.google.com/docs/cloud-messaging.
3. Flutter documentation. Docs | Flutter. URL: https://docs.flutter.dev.