Огляд методів безперервної автентифікації на смартфонах за динамікою натискання клавіш

Для автентифікації користувача треба зробити:

* 1. збір даних, їх обробку
  2. вилучення особливостей
  3. генерацію шаблону, класифікацію даних, їх адаптацію

Використовуються такі методи безперервної автентифікації на смартфонах:

1. Імовірнісне моделювання

Основною ідеєю імовірнісної техніки моделювання є прогнозування ймовірності даного тестового зразка, що належить конкретному предмету, використовуючи попередню ймовірність, обчислену з навчальних зразків. Одним із широко застосовуваних методів імовірнісного моделювання є мережа Байєса. Він використовує ациклічну модель графіка для пошуку ймовірнісних взаємозв’язків між батьківським та дочірнім вузлом. Наприклад, дані про елементи із довідкового шаблону будуть використовуватися як батьківський вузол та асоційований предмет ідентифікується як дочірній вузол. Потім, отримавши тестовий зразок (дані динаміки дотику, отримані на етапі аутентифікації користувача), можна знайти вірогідний звязок між батьківським та дочірнім вузлом.

2. Методика кластерного аналізу. Вона передбачає, що зразки, що належать одному і тому ж предмету, мають подібні властивості. Мета полягає в групуванні зразка з подібними властивостями для формування однорідного кластера. Тоді мітка тестового зразка визначається ступенем близькості до кластера. Зразки з різних кластерів сильно відрізняються, але дуже схожі серед зразків у тому самому кластері. Існують варіанти техніки кластерного аналізу, включаючи K-засоби та k-Найближчі сусіди.

3. Техніка дерева рішень. Вона популярна і використовується у багатьох сферах. Добре відома своєю низькою обчислювальною складністю. Цей метод особливо підходить для задач класифікації, які включають невелику кількість вихідних міток. Основна мета цих методів - створити деревоподібну модель, яка передбачає мітку класу даного тестового зразка на основі раніше відомих навчальних зразків. Дерево рішень будується шляхом безперервного розподілу даних об’єктів на підмножини, щоб коефіцієнт посилення інформації на кожному вузлі дерева був максимізованим. Цей ітераційний процес зупиняється, коли вузол має лише одну мітку або коли подальше розбиття деревного вузла більше не забезпечує додатковий приріст інформації.

4. Машина опорного вектора - ще одна техніка, яка зазвичай використовується у багатьох дослідженнях біометрії. Основна концепція цієї методики полягає в тому, щоб спочатку визначити, як два класи даних ознак відрізняються один від одного, а потім створити межу, яка найкраще їх відокремлює. Маючи цю межу, наступні тестові зразки можуть бути класифіковані як законні або нелегітимні відповідно до того, на якій стороні межі вони розташовані.

5. Техніка нейронної мережі імітує структуру обробки інформації біологічних нейронів. Як правило, архітектура нейронної мережі складається з трьох взаємопов'язаних шарів. Для початку дані об’єктів від усіх суб’єктів подаються на вхідний рівень мережі як набір нейронів. Функція активації використовується для присвоєння ваги кожному нейрону. Потім інформація про активовані нейрони передається від одного до іншого в межах прихованого шару. Цей процес повторюється, поки не буде отримано вихідні дані.

6. Вимірювання відстані. Метод вимірювання відстані обчислює оцінку несхожості або подібності між тестовим зразком та навчальним зразком даного суб'єкта. Потім оцінка порівнюється з пороговим значенням, щоб визначити, чи належить тестовий зразок до цільового суб'єкта.

7. Статистичні. Існує кілька статистичних методів, які використовувались у біометричних дослідженнях. Ці методи включають середнє та стандартне відхилення та толерантність до відхилень. З цими техніками пов’язаний ряд переваг. Наприклад, у порівнянні з обговореними вище методами, вони менш складні та легкі у реалізації, коштують менше обчислювального часу та споживають менше ресурсів, таких як заряд акумулятора. Ці переваги важливі для мобільних пристроїв з обмеженими ресурсами.

Список літератури:

Pin Shen The et al. A survey on touch dynamics authentication in mobile devices. Computers and Security. Volume 59, Issue C, June 2016, pp. 210-235.