3. Самостійно купити не найдешевші тести [1] та сподіватися, що тест покаже дійсний стан здоров'я.

Як можна побачити, усі шляхи вирішення проблеми не надають 100 % безпеки чи гарантії. Чому ж не інтегрувати дистанційний прийом до лікаря? Не все так легко, тут й приходять на допомогу сучасні ІТ розробки, а саме технологія машинного навчання.

Чому машинне навчання обов'язково має бути присутнє в додатку?

По-перше, це економія людських ресурсів – лікарів завжди недостатньо, та, крім цього, вони повинні вислуховувати кожного, на це йде багато часу. Через це, в деяких хворих, хвороба може загостритися, оскільки в належний час лікар був занятий іншим пацієнтом, який навіть може бути здоровим. Як це буде вирішувати додаток? Наданням пріоритету хворим та залишанням «екстра-вікон» у черзі, для хворих з високим пріоритетом. Пріоритет буде надаватися відповідно до симптомів, їх інтенсивності та минулих діагнозів.

По-друге, усі лікарі – люди, вони також можуть мати погане самопочуття відчувати втому та інше, що може впливати на працездатність. Натомість машини залишені від цих побічних ваг. Машини можуть працювати і по святам, і по вихідним, і навіть вночі. Але відповідальність за похибку в діагнозі падає і на машини рівнозначно як і на лікарів.

Саме для розподілення пріоритетів між пацієнтами та зменшення можливої похибки і буде використовуватися машинне навчання, а саме метод «випадковий ліс» (random forest) [2]. Метод «випадковий ліс» складається з декількох «дерев рішень» (decision trees) [3], кожне з яких виносить свою пропозицію, а остаточне рішення отримується за більшістю голосів, що зменшує ймовірність похибки в N разів (N – кількість «дерев» у «лісі»). Кожне «дерево рішень» складається з «гілок» – ребер, на яких записані атрибути, від яких залежить цільова функція, та з «листів» – блоків, де записані значення цільової функції. В нашому випадку, «гілки» відповідають запитанням лікарів, або проханням до пацієнта виміряти температуру чи здати певний аналіз. Отримані відповіді надходять до «листів», де приймається рішення про можливий діагноз чи, якщо інформації недостатньо, про наступне запитання.

Після встановлення можливого діагнозу машиною, лікар має підтвердити діагноз, для цього потрібно лише прочитати, надані пацієнтом, скарги та результати аналізів, або ж, якщо рішення про діагноз непрозоре, назначити голосовий/відеодзвінок чи особистий прийом, відповідно до пріоритету. При підтверджені діагнозу, додаток може надати корисні поради аби полегшити симптоми чи пришвидшити одужання.

Таким чином, за допомогою машинного навчання, зменшуються черги, будь-які контакти з іншими хворими, навантаження на лікарів та прискорюється постанова діагнозу, відповідно і лікування.

Література

1. Де у Вінниці роблять тест на COVID-19 і скільки це коштує. URL: https://vezha.ua/de-u-vinnytsi-roblyat-test-na-covid-19-i-skilky-tse-koshtuye/ (дата звернення: 24.04.2021)
2. Random Forest. URL: https://en.wikipedia.org/wiki/Random_forest (дата звернення: 24.04.2021)
3. Decision Tree. URL: https://en.wikipedia.org/wiki/Decision_tree (дата звернення: 24.04.2021)

УДК 004.82:004:85

ДЕТЕКТУВАННЯ ФІШИНГОВИХ ПОСИЛАНЬ

Т. В. Нескородєва, В. Ю. Грущенко

Фішинг – це форма шахрайства, при якій зловмисник намагається дізнатись конфіденційну інформацію, таку як дані для входу в обліковий запис або дані облікового запису.

Зазвичай жертва отримує повідомлення, яке, здається, було надіслане відомим контактом або організацією. Повідомлення містить шкідливе програмне забезпечення, орієнтоване на комп'ютер користувача, або має посилання на шкідливі веб-сайти, щоб обдурити їх на розголошення особистої та фінансової інформації, таких як паролі, ідентифікатори рахунків або дані кредитної картки.

Єдиний локатор ресурсів (URL) створюється для адресування веб-сторінок. На малюнку нижче показано відповідні частини в структурі типової URL-адреси.

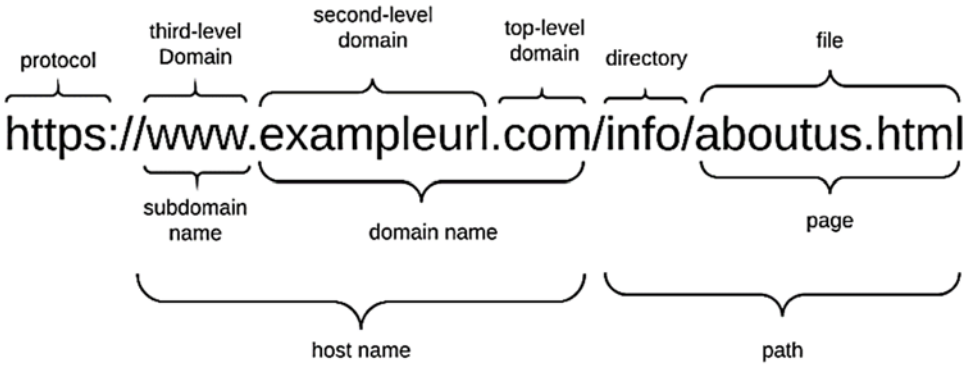

Рис.1. Структура URL

Зловмисник може зареєструвати будь-яке доменне ім'я, яке раніше не було зареєстровано. Цю частину URL можна встановити лише один раз. Фішер може змінити FreeURL у будь-який час, щоб створити нову URL-адресу. Причина, через яку захисники безпеки намагаються виявити фішингові домени, полягає в унікальній частині домену веб-сайту (FreeURL). Коли домен виявляється як шахрайський, легко запобігти цьому домену, перш ніж користувач отримає до нього доступ.

KNN – це непараметричний алгоритм, що використовується як для класифікації, так і для регресії. Його класифікація працює на невідомих даних, найближчих до k у просторі навчальних ознак. Найближчі точки вибираються за допомогою функцій відстані, таких як хеммінгова. KNN працює повільно, якщо обсяг даних великий.

Завдяки успіху обробки (NLP), досягнутим методами глибокого навчання, деякі з них нещодавно були використані для виявлення фішингу, наприклад, CNN, рекурентні нейронні мережі (RNN), періодичні згорткові нейронні мережі (RCNN) та глибокі нейронні мережі (DNN). Незважаючи на те, що методи глибокого навчання мало використовуються для виявлення фішингу через великий час навчання, вони часто забезпечують більшу точність і автоматично витягують функції з необроблених даних без будь-яких попередніх знань.

Запропонований підхід використовує згорткові нейронні мережі (CNN) для класифікації з високою точністю, щоб відрізнити справжні сайти від фішинг-сайтів.

Оцінити моделі, використовуючи набір даних, отриманий із 157 справжніх та 4898 фішингових веб-сайтів. На основі результатів великих експериментів моделі на базі CNN можуть виявитись високоефективними у виявленні невідомих фішингових сайтів. Крім того, підхід, заснований на CNN, працював краще, ніж традиційні класифікатори машинного навчання, оцінені на тому самому наборі даних, досягнувши 98,2 % рівня виявлення фішингу.

Прогнозування фішингових веб-сайтів є важливим і це можна зробити за допомогою нейронних мереж.

Таким чином продуктивність можна покращити, враховуючи нейронні мережі, оскільки це зменшує помилки і дає кращий результат.

Література

1. Detecting Phishing Sites – An Overview P.Kalaharshaa,b , B. M. Mehtrea, Department of Computer Science, Department of Statistics, Stanford University

2. A Framework for Predicting Phishing Websites Using Neural Networks A.Martin1, Na.Ba.Anutthamaa2, M.Sathyavathy3, Marie Manjari Saint Francois4, Dr.Prasanna Venkatesan5

3. Phishing Site Detection Analysis Using Artificial Neural Network M E Pratiwi1, T A Lorosae2 and F W Wibowo3