Г. В. Середюк
В. В. Гармаш

Підвищення безпеки QR-кодів у мобільних додатках через AI захист від шахрайства та фішингу

Вінницький національний технічний університет

Анотація

QR-коди стали важливим інструментом сучасних мобільних додатків, дозволяючи користувачам миттєво отримувати доступ до різноманітної інформації, здійснювати платежі, взаємодіяти з рекламними кампаніями та користуватися соціальними мережами. Така популярність QR-кодів сприяє їх швидкому поширенню, однак разом із тим підвищується ризик шахрайства та фішингових атак. Небезпечні QR-коди можуть містити посилання на фальшиві веб-сторінки, створені зловмисниками для збирання особистих даних користувачів або для перенаправлення на шкідливі ресурси, що загрожують безпеці даних та конфіденційності користувачів.

Ця робота зосереджена на дослідженні методів підвищення безпеки QR-кодів у мобільних додатках з використанням сучасних алгоритмів штучного інтелекту (AI), які здатні виявляти потенційно шкідливі QR-коди та захищати дані користувачів. Запропонований підхід передбачає використання кількох інструментів AI, таких як рекурентні нейронні мережі (RNN) для аналізу структури URL-адрес, алгоритми класифікації для верифікації легітимності доменів, а також автокодери для виявлення аномалій, що можуть свідчити про наявність шкідливих намірів. Розроблена система дозволяє вчасно виявляти та блокувати підозрілі QR-коди, запобігаючи можливим атакам на конфіденційність користувачів та зловживанню їхніми даними.

Додатково дослідження наголошує на важливості етапу збору та підготовки даних для навчання AI-моделей. Оскільки якість результатів залежить від повноти та якості навчальних даних, значна увага приділена розробці оптимальних методів збору та фільтрації інформації для забезпечення ефективності виявлення шкідливих елементів у QR-кодах. Використання штучного інтелекту для забезпечення безпеки QR-кодів є перспективним напрямком, який дозволяє розробникам мобільних додатків інтегрувати сучасні технології для захисту користувачів від шахрайства та фішингових атак. Цей підхід сприяє створенню безпечнішого цифрового середовища та підвищує довіру споживачів до мобільних технологій, підвищуючи загальну безпеку використання QR-кодів у повсякденному житті.

Ключові слова: *штучний інтелект, фішинг, безпека QR-кодів, аналіз URL, виявлення аномалій, нейронні мережі, мобільні додатки.*

Вступ

QR-коди (Quick Response Codes) за останні роки здобули величезну популярність, стаючи невід'ємною частиною сучасних технологій, зокрема в мобільних додатках. Вони пропонують швидкий та зручний доступ до інформації, що робить їх ідеальним інструментом для обслуговування клієнтів, рекламних кампаній та фінансових транзакцій. Наприклад, ресторани використовують QR-коди для надання доступу до меню, а фінансові установи впроваджують їх для проведення безконтактних платежів. Завдяки своїй універсальності, QR-коди дозволяють користувачам зекономити час, спростити процеси і забезпечити безконтактний доступ до послуг.

Однак разом з перевагами, що надають QR-коди, з’являються й серйозні ризики. За даними досліджень, зокрема, проведених компанією Malwarebytes, кількість фішингових атак за допомогою QR-кодів зросла на 300% у 2021-2023 роках. Це показує, що шахраї дедалі активніше використовують QR-коди для обману користувачів, підриваючи довіру до цього зручного інструмента. Вони можуть легко створювати шкідливі QR-коди, які ведуть на фальшиві веб-сайти, що призводить до викрадення особистих даних або фінансових втрат. Проблема ускладнюється тим, що багато користувачів не мають достатньої обізнаності про можливі загрози і зазвичай не перевіряють джерело QR-коду перед його скануванням. У цьому контексті стає зрозумілим, що потрібні нові рішення для забезпечення безпеки QR-кодів. Одним з найбільш перспективних підходів є використання штучного інтелекту (AI) для виявлення шкідливих QR-кодів. Алгоритми машинного навчання здатні аналізувати великі обсяги даних та виявляти аномалії, що робить їх ефективними в боротьбі з шахрайством. Наприклад, дослідження, проведене в Університеті Іллінойс, показало, що моделі глибокого навчання можуть досягати точності до 95% у виявленні

шахрайських QR-кодів. Це відкриває нові можливості для розробників мобільних додатків, які можуть інтегрувати технології AI в свої рішення, надаючи користувачам додатковий рівень захисту.

Основні методи підвищення безпеки QR-кодів

Одним з ключових підходів до підвищення безпеки QR-кодів є застосування алгоритмів машинного навчання для виявлення шкідливих кодів. Серед основних методів, які використовуються в цій галузі, можна виділити моделі глибокого навчання, які демонструють високу точність у виявленні шахрайських QR-кодів. Дослідження показують, що такі моделі здатні досягати точності до 95%, що забезпечує своєчасне попередження користувачів про потенційні загрози ще до моменту сканування коду. Використання машинного навчання дозволяє не лише автоматизувати процес виявлення, а й адаптуватися до нових методів шахрайства, забезпечуючи високий рівень безпеки для кінцевих користувачів. Нижче наведено методи захисту та розпізнавання шкідливих кодів, які можуть містити фішингові посилання.

1. Аналіз структури URL-адрес за допомогою Рекурентних нейронних мереж (RNN)

Рекурентні нейронні мережі (RNN) особливо ефективні для роботи з послідовними даними, такими як URL-адреси. Основною метою є аналіз послідовностей символів в адресах для виявлення підозрілих патернів.

Формула для обчислення стану RNN виглядає так:

$$h_t = \sigma(W_h h_{t-1} + W_x x_t + b)$$

де:

- h_t - поточний стан мережі,
- W_h та W_x - ваги, що відповідають за зв'язки між попереднім станом та вхідними даними,
- X_t - вхідний вектор, який представляє поточний символ URL,
- b - зсув,
- σ - активаційна функція, зазвичай використовують сигмоїдальну або tanh.

Для оцінки точності моделі на основі RNN можна використовувати метрики, такі як:

- **Accuracy** (Точність): визначає відсоток правильно класифікованих URL.
- **Precision** (Прецизійність): показує відсоток коректно виявлених шкідливих URL серед усіх виявлених.
- **Recall** (Відклик): відсоток правильних виявлень серед усіх фактично шкідливих URL.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

де:

- TP - кількість істинно позитивних (правильних класифікацій шкідливих URL).
- TNTNTN - кількість істинно негативних (правильних класифікацій безпечних URL).
- FPFPFP - кількість помилково позитивних (неправильних класифікацій безпечних URL як шкідливих).
- FNFNFN - кількість помилково негативних (неправильних класифікацій шкідливих URL як безпечних).

Таким чином, застосування RNN дозволяє не тільки виявляти шахрайські URL-адреси, але й проводити їхню класифікацію з високою точністю, якщо модель навчається на великій кількості легітимних і шкідливих прикладів.

Приклад: Розглянемо URL-адресу https://www.example.com. При обробці адреси RNN може виявити аномалії, наприклад, зміну літери "l" на цифру "1", створюючи схожу адресу, таку як https://www.examp1e.com. Мережа може навчитися розпізнавати патерни, які вказують на шахрайство, під час аналізу численних варіацій відомих адрес.

2. Виявлення аномалій за допомогою Автокодерів (Autoencoders)

Автокодери використовуються для виявлення аномалій у URL-адресах шляхом навчання відтворення "нормальних" адрес. Структура автокодера складається з двох частин: кодувальника та декодувальника.

Формули для автокодера:

Кодувальник:

$$z = f(x)$$

Декодувальник:

$$\hat{x} = g(z)$$

Середньоквадратична помилка (MSE) використовується для оцінки якості відтворення:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(x_i - \hat{x}_i)^2$$

Приклад**:** Припустимо, що ми маємо нормальну URL-адресу https://www.bank.com. Автокодер буде навчений на цій адресі. Якщо на вході ми отримаємо підозрілу адресу, таку як https://www.b4nk.com, автокодер визначить значну різницю між x та $x^{\wedge}$, що може призвести до високого значення MSE. У такому випадку система зможе сигналізувати про аномалію і запропонувати користувачу обережніше ставитися до URL.

3. Верифікація відомих доменів за допомогою алгоритмів класифікації

Для верифікації доменів можна використовувати різні алгоритми класифікації. Деякі з найпопулярніших включають:

1) **Деревоподібні моделі** (наприклад, Decision Trees, Random Forest):
   - Ці моделі можуть використовуватися для розпізнавання патернів на основі набору характеристик.
   - Приклад формули для дерева рішень може бути записаний як:

$$f(x) = \text{argmax}_j \sum_{i=1}^{N} I(y_i = j|x_i)$$

де:

- f(x) — функція прийняття рішення,
- y_i — клас (легітимний або шкідливий),
- I — індикатор, який приймає значення 1, якщо умова виконується, і 0, якщо ні.

2) Логістична регресія:

- Цей алгоритм дозволяє оцінити ймовірність того, що домен є легітимним, на основі набору незалежних характеристик.
- Модель може бути представлена як:

$$P(y = 1|X) = \frac{1}{1 + e^{-z}}$$

де

$$z = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + ... + \beta_n x_n.$$

3) CSupport Vector Machines (SVM):

- SVM може бути використаний для класифікації доменів на основі двох класів (легітимні/шкідливі) шляхом побудови гіперплощини в багатовимірному просторі.
- Формула для знаходження гіперплощини виглядає як:

$$w^T x + b = 0$$

де w - вектор ваг, b - зсув, а x - вектор характеристик.

Приклад**:** Розглянемо URL-адресу https://www.paypal.com. Класифікаційна модель може оцінити цю адресу, використовуючи різноманітні ознаки, такі як домен, наявність ключових слів, і порівняти її з відомими легітимними доменами. Якщо URL містить слова, пов'язані зі шахрайством, наприклад, "verify" чи "login", і має незвичну структуру, модель може сигналізувати про можливу загрозу.

Висновок

Було розглянуто основні методи підвищення безпеки QR-кодів за допомогою технологій машинного навчання, що спрямовані на захист користувачів від шахрайства та фішингу. У ході роботи були детально розглянуті підходи, пов'язані з аналізом закодованих URL-адрес, зокрема рекурентні нейронні мережі (RNN) для аналізу послідовностей символів, автокодери для виявлення аномалій та класифікаційні моделі для верифікації легітимності доменів. Кожен із методів має свої специфічні переваги та забезпечує ефективний захист на різних етапах аналізу даних.

RNN виявились ефективними для виявлення шахрайських змін у структурі URL, що робить їх корисними для аналізу патернів у послідовностях символів. Однак складність цього методу полягає у потребі навчання на великих наборах даних для досягнення високої точності.

Автокодери дозволяють виявляти аномалії, порівнюючи фактичні URL-адреси з тими, що вважаються "нормальними". Це дає змогу сигналізувати про можливі підробки або фішинг-атаки на основі відхилень у даних. Перевагою цього підходу є здатність ефективно працювати навіть без необхідності мати базу відомих шахрайських адрес.

Моделі класифікації дозволяють автоматично перевіряти легітимність доменів, надаючи швидку відповідь щодо безпеки адреси. Цей підхід є особливо корисним для виявлення доменів, що мають схожі на відомі адреси, але є шахрайськими.

Таким чином, застосування технологій машинного навчання, таких як RNN, автокодери та класифікаційні моделі, значно підвищує рівень безпеки при використанні QR-кодів у мобільних додатках. Вибір конкретного методу залежить від особливостей завдання та типу аналізованих даних, але в комплексі ці підходи забезпечують ефективний захист користувачів від потенційних загроз, що супроводжують використання QR-кодів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Nguyen, H., & Paparrizos, J. Detecting Malicious URLs using Machine Learning Techniques, 2020.
2. Zou, D., & Pan, L. ,Deep Learning for Malicious URL Detection, 2019.
3. Sakurada, M., & Yairi, T., Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction, 2018.
4. Dabrowski, A., et al., QR Inception: Barcode Redirects for Embedded Phishing Attacks, 2017.

Сердюк Гліб Володимирович – студент групи 174-23а, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, Вінниця, e-mail: glebserediuk@g,ail.com

Гармаш Володимир Володимирович – канд. техн. наук, доцент кафедри АІВТ, Вінницький національний технічний університет, Вінниця, e-mail: garmash.v.v@vntu.edu.ua

H. V. Serediuk
V. V. Garmash

Increase the security of QR codes in mobile applications through AI protection against fraud and phishing

Vinnytsia National Technical University

Abstract.

QR codes have become an important tool in modern mobile applications, allowing users to instantly access various information, make payments, interact with advertising campaigns, and use social networks. Such popularity of QR codes contributes to their rapid spread, but at the same time increases the risk of fraud and phishing attacks. Dangerous QR codes can contain links to fake web pages created by attackers to collect users' personal data or to redirect them to malicious resources that threaten data security and user privacy.

This paper focuses on the study of methods to improve the security of QR codes in mobile applications using modern artificial intelligence (AI) algorithms that can detect potentially malicious QR codes and protect user data. The proposed approach involves the use of several AI tools, such as recurrent neural networks (RNNs) for analyzing the structure of URLs, classification algorithms for verifying the legitimacy of domains, and autoencoders for detecting anomalies that may indicate malicious intent. The developed system allows timely detection and blocking of suspicious QR codes, preventing possible attacks on user privacy and misuse of their data.

Additionally, the study emphasizes the importance of the data collection and preparation stage for training AI models. Since the quality of the results depends on the completeness and quality of the training data, considerable attention is paid to the development of optimal methods for collecting and filtering information to ensure the effectiveness of detecting malicious elements in QR codes. The use of artificial intelligence to ensure the security of QR codes is a promising area that allows mobile application developers to integrate modern technologies to protect users from fraud and phishing attacks. This approach contributes to the creation of a safer digital environment and increases consumer confidence in mobile technologies, enhancing the overall security of using QR codes in everyday life.

Keywords: *artificial intelligence, phishing, QR code security, URL analysis, anomaly detection, neural networks, mobile applications.*

Serediuk Hlib V. – student of group 174-23a, faculty of intellectual information technologies and automation, Vinnytsia National Technical University, Vinnytsia, e-mail: glebserediuk@g,ail.com

Garmash Volodymyr V. – candidate technical of Sciences, associate professor of AIVT department, Vinnytsia National Technical University, Vinnytsia, e-mail: garmash.v.v@vntu.edu.ua