Qrust: AI-powered Phishing Detection and Secure QR Generation

Kyoungmin Roh, Junhyeong Kim, Minseok Seong (Advisor: Prof. Taekyoung Yoon)
Dept. of Cyber Security, Dankook University, Republic of Korea

Vision

Research Question

"How can we maintain the convenience of QR codes while ensuring security against phishing attacks before the user scans them?"

Background & Problem Recognition

- **Explosive Growth of QR code** usage in daily transactions [1]
- **Invisible destination risk:** users cannot verify URLs before scanning
- **Qshing Attacks:** malicious overlay or replacement of legitimate codes [2]
- **Credential theft, data leakage, user deception**
- **Reactive defenses:** blacklist-based, limited generalization
- **Urgent need** for real-time, AI-driven, proactive detection

Limitation of Previous Approaches

- **Insufficient Qshing Detection:** focuses only on phishing URLs, not on-camera scanning or real-time analysis [3].
- **Low Usability:** complex verification steps undermine QR's convenience and instant access [4].
- **Weak User Engagement:** users rarely adopt phishing detection apps due to low perceived necessity [5].

Steps

1. **Problem Definition:** Analyzed overlay and replacement-based Qshing attacks
2. **System Design:** Proposed a dual-layer defense combining "Secure QR generation" and "AI-based phishing detection"
3. **Developing Secure QR Generation:** Implemented HMAC-based signature embedding to prevent forged or overlaid QR codes
4. **AI Model Training:** Trained a lightweight machine learning (ML) model on URL-level features for real-time phishing detection
5. **Inegration:** Built the Qrust mobile prototype

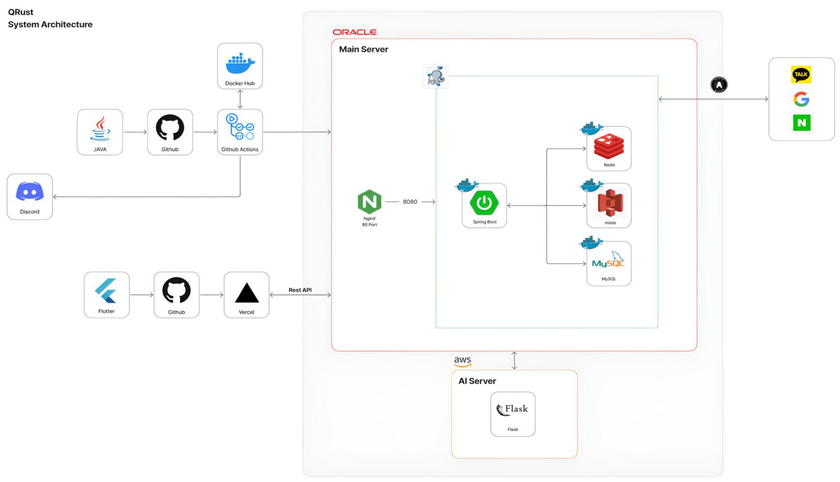

Figure 1. Overall Architecture of Qrust Application

News

- **AI Model Performace:** Achieved 96% F1-score
- **Secure QR Generation:** Implemented HMAC-based QR signature, enabling verification and rejection of forged or overlaid codes.
- **Dual Defense Deployment:** Integrated database-based filtering and AI-driven zero-day detection into a unified mobile system.
- **Prototype Completed:** Full Qrust mobile app developed
- **Trusted Ecosystem Vision:** Establishing a reliable QR environment

Core Idea 1: Secure QR Generation

- Uses HMAC (Hash-based Message Authentication Code) Signatures [6] to embed authenticity information such as URL, name, and password inside each QR code.
- The app validates each scanned code against its HMAC signature.
- It is used to prevent Overlay attacks, ensuring only QR codes generated by trusted sources are accepted.

$$\mathrm{HMAC}(K,m) = \mathrm{H}((K' \oplus opad \parallel \mathrm{H}((K' \oplus ipad) \parallel m))$$

$$K' = \begin{cases} \mathrm{H}(K), & K \text{ is larger than block size} \\ K, & \text{otherwise} \end{cases}$$

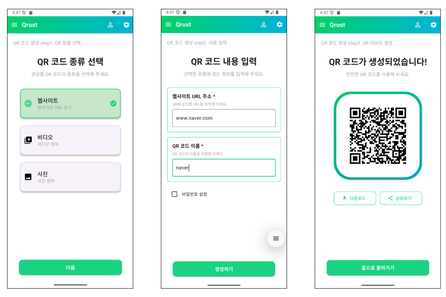

Figure 2. User Interface of Secure QR Code Generation

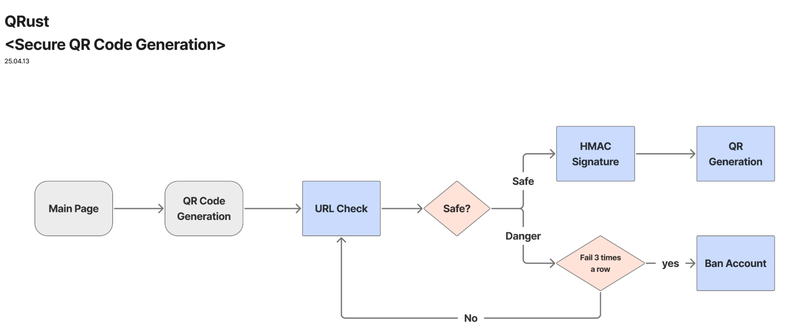

Figure 3. Secure QR Code Generation Pipeline

Core Idea 2: AI-based Qshing Detection

AI-based Qshing Detection implements five-stage verification pipeline:

1. Extract URL from QR code
2. Validate internal HMAC Signature
3. Check blacklist database using Google Safe Browsing API [7]
4. Check user-reported URL database
5. Run AI-based Qshing Detection

- Operates in real-time with a lightweight model optimized for mobile performance.
- Detects phishing URLs before redirection and alerts users instantly.
- Achieved 96% F1-score and 97% Accuracy.

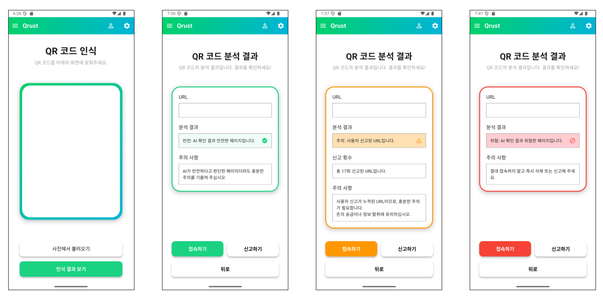

Figure 4. User Interface of AI-based Qshing Detection

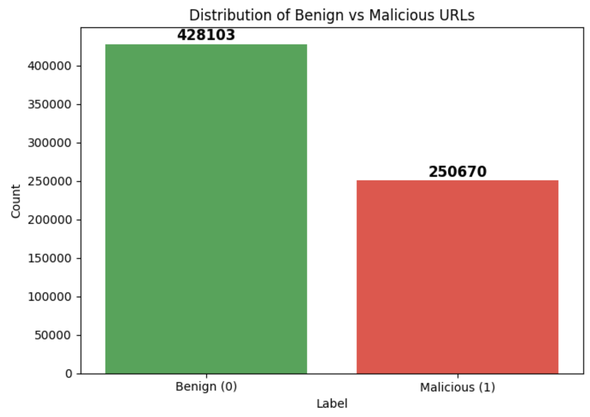

Figure 5. Distribution of Benign and Malicious URLs from training set

Contributions

In this project, we proposed a secure QR code system that prevents overlay attacks using HMAC-based signatures and detects phishing URLs through AI analysis. Our approach offers both robust security and user convenience, making it suitable for real-world deployment. Through our project, we achieved the following contributions:

- **Overlay Attack Prevention:** HMAC-based QR generation ensures authenticity; untrusted or overlaid QR codes are automatically rejected.
- **Zero-Day Qshing Defense:** Hybrid detection combines database-based phishing filtering with AI-driven zero-day attack identification.
- **Lightweight AI Architecture:** Optimized for mobile devices; compact model achieves high speed without compromising performance.
- **Balance of Security and Usability:** Provides strong protection while preserving the convenience and immediacy of QR use.

References

[1] QR Tiger, "61+ QR Code Statistics & Trends 2025 Full Report [Updated]," *QR Tiger*, Aug. 2025. [Online]. Available: https://www.qrcode-tiger.com/qr-code-statistics
[2] Secureworks, "QR Codes Abused for Qshing Attacks," *Secureworks Counter Threat Unit*, 2022. [Online]. Available: https://www.secureworks.com/blog/qr-codes-abused-for-qshing-attacks
[3] Dongwan Shin and Huiping Yao, "A User Study of Security Warnings for Detecting QR Code Based Attacks on Android Phone," in *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applicaitons*, vol. 4, pp. 49-64, 2013.
[4] Filipo Sharevski et. al., "Exploring Phishing Threats through QR Codes in Naturalistic Settings," in *Symposium on Usable Securiy and Privacy (USEC) 2024*, Feb, 2024.
[5] Sanghak Oh et. al., "Understanding and Improving User Adoption and Security Awareness in Passwork Checkup Services," in *CHI'25, Proceedings of the CHI Conference on Human Factors in Computing Systems*, no. 386, pp. 1-32, Apr, 2025.
[6] Mihir Bellare et. al., "Keying Hash Functions for Message Authentication," in *CRYPTO '96: Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, pp.1-15, Aug, 1996.
[7] Google Safe Browsing API, Google Developers, 2025. [Online]. Available: https://developers.google.com/safe-browsing/ [Accessed: Nov. 2025]