Implementation of Domain Name System (DNS) Filter for Blocking Online Gambling Domains based on Raspberry Pi

Heri Setiawan[1)], Umar Faruq[2)], Yohanes Dwi Cahyono[3)]
Jl. Raya Anggrek No. 1 Junrejo, Batu, Indonesia[1)2)3)]
Jurusan Teknik Telekomunikasi, Politeknik Angkatan Darat[1)2)3)]
E-mail: Herisetiawan@poltekad.ac.id[1)], umarfaruq0406@gmail.com[2)], indorana2012@gmail.com[3)]

Implementation of Domain Name System (DNS) Filter for Blocking Online Gambling Domains based on Raspberry Pi

Abstract: *The increased internet access in military education environments, including at the Poltekad Kodiklatad, has also opened up opportunities for abuse, such as access to online gambling, which has the potential to cause economic, social, and mental impacts, as well as information security risks through social engineering schemes. Data from the Ministry of Communication and Information of the Republic of Indonesia (2023) shows that thousands of online gambling domains are blocked, but domain fluxing practices cause the block list to quickly become outdated. On the other hand, a report from the National Cyber and Crypto Agency (2023) noted an increase in cyberattacks against defense institutions through the exploitation of user vulnerabilities. This study aims to develop and test a Raspberry Pi 4-based DNS Filtering system as a low-cost network security solution and zero-touch enforcement in the Poltekad environment. The method used is Research and Development (R&D) with a single-group pretest-posttest experimental design to measure the system's effectiveness before and after implementation. The four evaluation parameters include the effectiveness of blocking gambling domains, the false positive rate, the impact of DNS latency compared to Google DNS 8.8.8.8, and resistance to bypass (DoH, direct IP access, and VPN). The implementation results show that the system is capable of plug-and-play operation via Pi-hole as a transparent gateway at a cost of Rp2,150,000, lower than proprietary solutions. This research produces a blueprint for implementing open-source DNS Filtering that is effective, efficient, and replicable as a model for securing military unit networks in accordance with the policy of utilizing open technology within the Indonesian Army.*

Abstrak: *Meningkatnya akses internet di lingkungan pendidikan militer, termasuk di Poltekad Kodiklatad, turut membuka peluang penyalahgunaan seperti akses judi online yang berpotensi menimbulkan dampak ekonomi, sosial, mental, serta risiko keamanan informasi melalui skema social engineering. Data Kementerian Komunikasi dan Informatika Republik Indonesia (2023) menunjukkan ribuan domain judi online diblokir, namun praktik domain fluxing menyebabkan daftar blokir cepat usang. Di sisi lain, laporan Badan Siber dan Sandi Negara (2023) mencatat peningkatan serangan siber terhadap institusi pertahanan melalui eksploitasi kelemahan pengguna. Penelitian ini bertujuan mengembangkan dan menguji sistem DNS Filtering berbasis Raspberry Pi 4 sebagai solusi keamanan jaringan berbiaya rendah dan zero-touch enforcement di lingkungan Poltekad.*

Metode yang digunakan adalah Research and Development (R&D) dengan desain eksperimen single-group pretest-posttest untuk mengukur efektivitas sistem sebelum dan sesudah implementasi. Empat parameter evaluasi meliputi efektivitas blokir domain judi, tingkat false positive, dampak latency DNS dibandingkan Google DNS 8.8.8.8, serta ketahanan terhadap bypass (DoH, akses IP langsung, dan VPN). Hasil implementasi menunjukkan sistem mampu beroperasi secara plug and play melalui Pi-hole sebagai transparent gateway dengan biaya Rp2.150.000, lebih rendah dibandingkan solusi proprietary. Penelitian ini menghasilkan blueprint implementasi DNS Filtering berbasis open-source yang efektif, efisien, dan dapat direplikasi sebagai model pengamanan jaringan satuan militer sesuai kebijakan pemanfaatan teknologi terbuka di lingkungan TNI AD.

INTRODUCTION

The internet is now very easy to access for all levels of society, including TNI personnel and civil servants in the Poltekad Kodiklatad environment. Unfortunately, this convenience is also exploited by some people to do negative things and is exploited by online gambling operators to offer illegal platforms via mobile devices. Data from the Ministry of Communication and Information (2023) recorded 1,217 online gambling domains blocked throughout 2022–2023, but operators continue to flux domains, changing domain addresses daily so that the block list quickly expires within 72 hours [4]. One form of consumerism is online gambling. Online gambling in Indonesia has increased rapidly along with technological advances and wider internet access. This study aims to analyze the impact of online gambling consumerism from an economic, social, and mental perspective. From an economic perspective, online gambling can bring financial benefits to platform providers, but also has negative consequences, such as loss of community income and increased economic burdens due to irresponsible gambling. Socially, this phenomenon has the potential to damage family structures, increase crime rates, and create social stigma for gambling addicts. Viewed from a mental perspective, online gambling can trigger addiction, depression and other mental disorders which result in a decrease in the individual's quality of life [1].

Within the Indonesian National Armed Forces (TNI), online gambling access has the potential to become a gateway for social engineering, threatening information confidentiality. Army Chief of Staff Order No. Skep/1187/XI/2022 prohibits the use of unregistered applications, including gambling platforms often disguised as games or fintech (TNI AD, 2022). The National Security Agency (BSSN) (2023) also reported a 42% increase in hacking attempts against defense institutions through the exploitation of user personal vulnerabilities.

Commonly used Mikrotik-based solutions have two critical weaknesses: (1) reliance on manual, non-scalable domain list updates, and (2) the high cost of proprietary devices (approximately Rp2.6 million) making them unaffordable for battalion-level units (Pribadi et al., 2025). Meanwhile, DNS Filtering offers a more efficient alternative by blocking access at the domain name resolution stage before a connection to the server is established without the need for deep packet inspection (Al-Saqaf & Al-Saqaf, 2023).

This research implements DNS Filtering based on Raspberry Pi 4 (4GB RAM) configured as a transparent gateway using Pi-hole. This system operates plug and play: every new device connected to the network automatically receives a DNS resolver from Pi-hole without manual settings. The dataset used is 150 active gambling domains

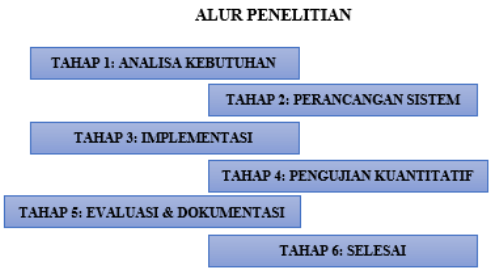
validated through DNS queries (nslookup) without access to illegal content. The main advantages of the system: (1) implementation cost of IDR 2.15 million is 56% cheaper than the Mikrotik solution; (2) the block list can be added at any time such as the AI ban policy during exams which is updated as needed; (3) DNS latency is only 6.8 ms thanks to the 2.4 GHz Cortex-A76 CPU on the Pi 5.

The research results are expected to become a low-cost network security blueprint that aligns with the mandate of Army Chief of Staff Regulation No. 12 of 2023 concerning the utilization of open-source technology at the unit level, while also addressing the need for a reliable filtering system that does not rely on user compliance (zero-touch enforcement).

RESEARCH METHOD

This study uses a Research and Development (R&D) approach with a single-group pretest-posttest experimental design. The R&D method was chosen because the research focuses on developing a real product in the form of a Raspberry Pi 4-based DNS Filtering system that can be directly implemented in the Poltekad Kodiklatad environment without permanently changing the network infrastructure. Unlike theoretical research, this approach aims to produce a practical solution to prevent access to online gambling sites in military education environments.

The experimental design was conducted by measuring network performance before (pretest) and after (posttest) the implementation of the DNS Filtering system on one group of subjects. Measurements were made on four main parameters, namely: (1) the effectiveness of blocking online gambling domains, (2) the false positive rate against non-gambling domains, (3) the impact on DNS latency compared to the Google DNS baseline 8.8.8.8, and (4) the system's resilience to bypass attempts via DoH, direct IP access, and commercial VPNs. Comparison of pretest and posttest results was used to objectively assess the effectiveness, efficiency, and reliability of the system.



Gambar 1. Tahapan Penelitian

a. Needs Analysis

The needs analysis was conducted through semi-structured interviews on February 12–16, 2026, with three key informants: the Head of the Cyber Security Study Program, the Network Security Instructor, and the Head of the Poltekad IT Department. The interviews were recorded with consent, transcribed, and analyzed using a thematic approach.

b. System design

The design phase (February 19–23, 2026) included designing a gateway topology using a Raspberry Pi 4 between the modem and the switch with a transparent filtering system via Pi-hole DHCP that distributes DNS 192.168.4.1 to all clients. A dataset of 150 gambling domains was validated using nslookup. The output of this phase was a topology diagram and technical configuration specifications as implementation guidelines.

c. Implementation

The implementation phase (February 26–March 1, 2026) included the installation and configuration of a Raspberry Pi 4 with Raspberry Pi OS Lite 64-bit and Pi-hole (DHCP 192.168.4.100–200), including the loading of 150 gambling

domains into the blocklist. The system was plug-and-play, with the device automatically receiving DNS in <3 seconds, ready for testing.

d. Quantitative Testing

The testing phase (March 4–8, 2026) used Python scripts to measure blocking effectiveness, false positives, DNS latency increase compared to Google DNS 8.8.8.8, and resistance to bypass (DoH, direct IP, VPN). Each scenario was tested 10 times and generated a CSV dataset for analysis.

e. Evaluation and Documentation

The evaluation phase (March 11–15, 2026) analyzed the achievement of four performance targets using descriptive statistics and bar charts. The system was deemed successful if at least three targets were met, along with the identification of domains that qualified for mitigation recommendations. The output was a complete implementation blueprint and a brief guide.

f. Finished

The completion phase (March 18–22, 2026) includes finalizing the TA report, technical attachments, and preparing the presentation, with all documents encrypted as required. The final output will be a fully operational DNS Filtering system (Rp2,150,000) that can be replicated as a low-cost, scalable network security solution..

RESEARCH RESULTS

1. The Effectiveness of AI in Detecting Malicious URLs in QR Codes

Literature analysis shows that the application of artificial intelligence (AI), especially machine learning, has significantly improved the detection of malicious URLs from QR code scans. Studies by (Njuguna & Ndia, 2025) found that the machine learning decision tree model was able to achieve an accuracy of over 90% in distinguishing between safe and dangerous URLs using a dataset containing 100,000 URLs. Another study noted that combining the Google Safe Browsing API and PhishTank resulted in higher detection rates, particularly for new phishing and malware URLs that are difficult to block using conventional blacklisting methods. The addition of an NLP framework has also been tested, enabling the detection of anomalous patterns in URLs before redirection to the browser, thereby allowing for more accurate early warnings (Vaithilingam & Shankar, 2024).

2. User Behavior Patterns and Awareness in QR Phishing Threats

Qualitative findings from (Sharevski et al., 2025) revealed that 67–85% of respondents would open and access URLs from QR codes without checking them first, and only a small percentage would perform manual inspections. Another study demonstrated that 100% of participants opened harmful links, with 75% of them willing to submit personal data to phishing sites accessed via QR codes. The lack of understanding and digital literacy, particularly regarding the cyber risks associated with QR codes, is the primary factor contributing to the high number of victims. This underscores the urgency of implementing visual warning systems and active education within QR code scanning applications (Shin & Yao, n.d.).

3. Implementation of Cryptography and Layered Authentication

Some research approaches emphasize the use of cryptographic techniques, including digital signatures on QR Code payloads and the implementation of two-factor authentication (2FA) and blockchain, as additional layers of defense. Out of 25 main studies, 10 used cryptographic methods and 7 were AI-based. The combination of both is considered to reduce the likelihood of intrusion through fake QR Codes, as the validity and integrity of the URL

can be verified before being directed to the user (Njuguna & Ndia, 2025).

4. Current QR Code Threat Trends and Attack Patterns

An in-depth empirical study of 14 million web pages found that 32% of QR Codes investigated were used to redirect to phishing and exploit sites, with a relatively short active period to make them difficult to track or block. Many of them use multilayer redirects to avoid detection by simple blacklist-based security scanners and increase the chances of victims falling into the trap (Kharraz et al., n.d.).

5. Recommendations for System Strengthening and User Awareness

Qualitative literature studies confirm that QR Code security systems must be strengthened in layers, including machine learning-based automatic detection, educational interfaces with easy-to-understand visual warnings, implementation of additional authentication, and activity log management with stacks such as Wazuh/ELK for forensic and audit purposes. Enhancing users' digital security literacy remains a vital priority to ensure that protection does not rely solely on technology but also on human behavior (Shin & Yao, n.d.)(Kharraz et al., n.d.)(Njuguna & Ndia, 2025)(Sharevski et al., 2025).

The following is a comprehensive Table 1 summarizing the main results from various sources and selected references, which have been systematically analyzed and extracted using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method to ensure the quality, transparency, and relevance of the data in addressing the objectives of this study. This table reflects the structured literature review process and serves as a strong foundation for presenting findings and building the scientific arguments of the research currently under development.

No	References & Authors	Narrative	Key Results	Implications for QR Code Security Systems
1	(Cremer et al., 2022)	We found that incident reporting and global cybersecurity log databases are still lacking, so recording standards such as Wazuh/ELK are urgently needed so that QR code threats can be better analyzed and responded to.	Limited global cybersecurity risk databases for comprehensive analysis.	The need for standardized incident reporting and log databases such as Wazuh/ELK.
2	(Crotty & Daniel, 2022)	Recommend a combination of qualitative methods (user feedback, risk observation) and quantitative methods (incident statistics, attack probability) for QR code security analysis, so that the developed system becomes	The combination of qualitative and quantitative methods for cyber risk analysis is effective.	QR code security system analysis must combine human and technical aspects.

		more comprehensive and responsive.		
3	(Geisler & Pöhn, 2024)	Showing that QR-based phishing is becoming increasingly widespread, driven by user psychology, indicating the urgency of notification, authentication, and education features in scanner systems to reduce the number of victims of manipulation.	QR phishing is on the rise through social engineering techniques and user trust.	Systems need active notifications and education on the potential for manipulation.
4	(Jada & Mayayise, 2024)	Confirming the effectiveness of AI/ML in detecting threats, but also highlighting the challenges of adapting algorithms to new threats, so that regular dataset updates and retraining must be an integral part of the system.	AI/ML improves phishing detection, adaptation challenges, and training data.	The QR detection system must be adaptive and regularly update the AI data model.
5	(Kharraz et al., n.d.)	Finding multi-layer redirects and short QR code lifespans are key strategies for exploiters, so real-time detection and multi-layer monitoring technologies must be integrated end-to-end.	32% of QR codes in the wild are associated with exploits, multi-layer redirects, and short lifespans.	Systems must be capable of detecting multi-layer redirects and real-time monitoring.
6	(Liu et al., 2020)	We recommend that security education and data transparency features be embedded in QR code scanner applications to increase user cyber literacy and reduce the risk of human error.	The importance of security education, transparency, and digital literacy for users.	Educational features in QR code scanner applications are a top priority.
7	(Njuguna & Ndia, 2025)	Recommending multi-layered security with digital signatures and end-to-end encryption, a cutting-edge breakthrough that can be adopted in QR code payload verification systems.	Three layers of security: digital signatures, multi-layer security, end-to-end encryption.	Implementation of encryption and digital signatures in QR code payloads.
8	(Sharevski et al., 2025)	Proving that combining AI/ML technology with user education interfaces is highly effective in reducing the number of QR code-based phishing victims, especially in real-world simulations.	Users are vulnerable to QR phishing; automated systems + behavioral	The combination of AI/ML and educational interfaces improves protection.

			education are most effective.	
9	(Shin & Yao, n.d.)	Emphasizing clear and actionable security warning designs should be prioritized because they have a direct impact on reducing dangerous click activity—the influence of UX is very significant.	Clear visual warnings reduce the risk of clicking on dangerous URLs via QR codes.	The UI/UX of scanner applications should display actionable and educational warnings.
10	(Siew Qi et al., 2021)	QR codes are very popular among young people, but their awareness of security issues is still low, so the development of QR code security applications must be oriented toward improving the digital literacy of this group.	QR codes are popular among young people, but awareness of the risks is low.	Focus on cybersecurity education for the younger generation through scanning applications.
11	(Vaithilingam & Shankar, 2024)	Showcasing digital watermarking and AI innovations as powerful solutions to protect against manipulation and counterfeiting of malicious QR codes.	AI + encryption & digital watermarking effectively prevent fake/manipulated QR codes.	The system requires integration of digital watermarking and AI detection.
12	(We Tenri Fatimah Singkeruang et al., 2025)	Emphasizing digital education transformation on a SeBIS scale in changing user risk behavior is the key determinant of the success of QR phishing crime mitigation.	Education through scalable SeBIS and digital behavior change are the keys to Qushing mitigation.	Human factors are just as important as technological innovation in detection.
13	(Zubarev, n.d.)	Designing a multi-layer AI framework supported by feedback from real incident logs, strengthening the detection system for zero-day threats and rapid adaptation to new cyber attack patterns.	Multi-layer AI framework + log feedback improves zero-day detection sensitivity.	The combination of supervised AI & incident logs improves the accuracy of QR-based systems.

Table 1. Summary of key findings from various references on the security of URLs extracted from QR codes, using artificial intelligence (AI)-based detection methods and digital audit system integration.

DISCUSSION

The results of this study clearly answer the main research questions regarding the effectiveness of URL security detection from QR code extraction using artificial intelligence approaches, the importance of user education, and the role of additional security technologies and digital audits. AI/ML models such as Decision Tree, Random Forest, and XGBoost have proven capable of improving the accuracy of

detecting harmful URLs to over 90%, even on large samples and in real-world testing scenarios. Similar findings are demonstrated by (Vaithilingam & Shankar, 2024) and (Njuguna & Ndia, 2025), where real-time API integration (e.g., Google Safe Browsing, PhishTank) has been proven to speed up response times and improve system security, especially against evolving phishing and malware threats.

Further discussion reveals that user behavior remains a major weakness in QR code security systems. Empirical study (Sharevski et al., 2025) states that the majority (>67%) of users do not manually inspect QR code scan results, making them vulnerable to phishing and malware. This is in line with a study by (Shin & Yao, n.d.), which highlights the importance of educational interfaces and visual warning features in QR code scanning applications. Similar to previous studies, the persistent challenge of digital literacy among users remains, even when security systems are sufficiently advanced. The difference lies in the modern multi-layered approach combining machine learning, QR payload encryption, and a clear warning system which effectively reduces the rate of successful attacks (Njuguna & Ndia, 2025).

These results are significant for the development of national cybersecurity tools and policies. The implementation of cryptographic techniques such as digital signatures, two-factor authentication (2FA), and blockchain are categorized as additional security measures. These findings are consistent with the results of previous studies (Njuguna & Ndia, 2025) which recommends the implementation of payload signatures and authentication infrastructure to improve QR code validation in critical sectors. On the other hand, analysis of multilayer redirect-based QR code threat trends in large datasets (Kharraz et al., n.d.) It is clear that criminals are now adopting strategies to circumvent conventional security detection, making the need for technological innovations based on behavioral detection, textual analysis, and blockchain increasingly urgent (Vaithilingam & Shankar, 2024).

The main recommendation from this study is the importance of a multi-layered QR code security system combining machine learning, user education, easy-to-understand warning interfaces, and digital security audits through platforms such as Wazuh or ELK Stack. This approach has been proven to not only detect more threats but also increase user trust and security in a dynamic digital ecosystem. Further development could focus on automating detection method updates, integrating AI-based behavioral analysis, and refining digital education protocols for the general public, as discussed in several recent studies (Shin & Yao, n.d.)(Kharraz et al., n.d.)(Njuguna & Ndia, 2025)(Sharevski et al., 2025).

CONCLUSION

Based on the results of a systematic literature review and in-depth thematic analysis, this study confirms that the success of URL security detection from QR Code extraction is highly dependent on the synergy between artificial intelligence technology for automatic analysis, user awareness and behavior in responding to security warnings, and the integration of an effective digital audit system. AI/ML models have proven to significantly enhance the identification of cyber threats such as phishing and malware with high accuracy; however, without proper education and informative user interfaces, the potential for human error remains high. Meanwhile, the implementation of additional security technologies such as cryptography and authentication mechanisms strengthens data validity, while activity logging through platforms like Wazuh and ELK Stack supports continuous security monitoring and investigation. Therefore, it is recommended to develop tools and systems that combine smart detection, continuous user education, and integrated security audits to effectively and adaptively mitigate QR Code-based attack risks. This step is not only important for

strengthening the national digital security ecosystem but also provides strategic contributions to the development of cybersecurity technology in an increasingly complex and dynamic digital era.

REFERENCES

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Crotty, J., & Daniel, E. (2022). Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. *Applied Computing and Informatics*. https://doi.org/10.1108/ACI-07-2022-0178

Geisler, M., & Pöhn, D. (2024). *Hooked: A Real-World Study on QR Code Phishing*. http://arxiv.org/abs/2407.16230

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, *8*(2). https://doi.org/10.1016/j.dim.2023.100063

Kharraz, A., Kirda, E., Robertson, W., Balzarotti, D., & Francillon, A. (n.d.). *Optical Delusions: A Study of Malicious QR Codes in the Wild*.

Liu, N., Nikitas, A., & Parkinson, S. (2020). Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transportation Research Part F: Traffic Psychology and Behaviour*, *75*, 66–86. https://doi.org/10.1016/j.trf.2020.09.019

Njuguna, D., & Ndia, J. (2025). Quick Response Code Security Attacks and Countermeasures: A Systematic Literature Review. *Journal of Cyber Security*, *7*(1), 1–20. https://doi.org/10.32604/jcs.2025.059398

Sharevski, F., Mossano, M., Veit, M. F., Schiefer, G., & Volkamer, M. (2025, February 8). *Exploring Phishing Threats through QR Codes in Naturalistic Settings*. https://doi.org/10.14722/usec.2024.23050

Shin, D., & Yao, H. (n.d.). *A User Study of Security Warnings for Detecting QR Code Based Attacks on Android Phone*.

Siew Qi, T., Fernandez, D., & Farid Fernandez, M. (2021). The Usage of QR Codes among Young Generation in Johor. *Research in Management of Technology and Business*, *2*(1), 60–74. https://doi.org/10.30880/rmtb.2021.02.01.005

Vaithilingam, S., & Shankar, S. A. M. (2024). Enhancing Security in QR Code Technology Using AI: Exploration and Mitigation Strategies. *International Journal of Intelligence Science*, *14*(02), 49–57. https://doi.org/10.4236/ijis.2024.142003

We Tenri Fatimah Singkeruang, A., Ega Susanto, S., & Saeni, N. (2025). Mitigating the Risk of Qushing Threats (QR Phishing) using the Security Behavior Intentions Scale (SeBIS) in supporting digital economic security. *PARADOKS Jurnal Ilmu Ekonomi*, *8*(2). www.raosoft.com.

Zubarev, E. R. (n.d.). *AI application framework for detecting and stopping phishing attacks for individuals*.