ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1577

# PhiNex: An ARM-FPGA Hybrid Security Gateway for Real-Time Phishing Detection Using PYNQ-Z2

Brent Warren M. Morta[1]; Carl Christian Jarque[2]; Rafael Nickolai Pugay[3]; Jan Tristan Buenviaje[4]; Robert Perido[5]; Paolo Roberto Lozada[6]

[1,2,3,4,5,6]College of Engineering, San Sebastian College – Recoletos de Cavite, Cavite City, Philippines

Publication Date: 2026/06/01

**Abstract: Phishing attacks constitute a persistent and escalating cybersecurity threat, disproportionately affecting households and small businesses in the Philippines due to limited access to affordable protective infrastructure. This study developed the PhiNex an Advanced RISC Machine and Field-Programmable Gate Array (ARM-FPGA) Hybrid Security Gateway for Real-Time Phishing Detection and Domain Name System (DNS)-Level Threat Mitigation using the PYNQ-Z2 development board. The system integrates hardware-accelerated threat pre-filtering through reprogrammable FPGA logic with XGBoost-based machine learning classification on an ARM Cortex-A9 processor, enabling real-time phishing detection across multiple networked devices simultaneously. Functional testing against five verified DNS-resolvable phishing and legitimate URLs demonstrated 100% threat detection accuracy with an average response time of 68.8 milliseconds. Live operational testing over 8.15 hours across 450 DNS queries confirmed a 47.33% overall threat detection rate across three heterogeneous device platforms, with the FPGA pre-filtering mechanism reducing machine learning inference workload by 44.89%. User satisfaction evaluation yielded an overall mean score of 3.48 out of 4.0, while expert effectiveness assessment by three IT security professionals produced a mean rating of 3.62 out of 4.0, both confirming strong practical deployability for non-technical users from diverse socioeconomic backgrounds.**

***Keywords:*** *Phishing Detection; ARM-FPGA; DNS-Level Security; Hardware Acceleration; Real-Time Threat Detection; Machine Learning.*

**How to Cite:** Brent Warren M. Morta; Carl Christian Jarque; Rafael Nickolai Pugay; Jan Tristan Buenviaje; Robert Perido; Paolo Roberto Lozada (2026) PhiNex: An ARM-FPGA Hybrid Security Gateway for Real-Time Phishing Detection Using PYNQ-Z2. *International Journal of Innovative Science and Research Technology*, 11(5), 2562-2567. https://doi.org/10.38124/ijisrt/26may1577

## I. INTRODUCTION

The global cybersecurity threat landscape has undergone unprecedented escalation, with phishing attacks emerging as one of the most pervasive and consequential forms of cybercrime. Non-malware activity, including phishing and social engineering, accounted for 75% of all identity-based cyberattacks identified in 2023 [1]. Financial losses attributed to online fraud exceed $10 billion annually, with households, small businesses, and the hospitality sector increasingly targeted through fraudulent booking scams and credential harvesting [2].

The Philippines is disproportionately exposed to these threats, recording a fourfold increase in malicious cyber activity during the first quarter of 2024, reaching a record 5 billion attacks per day [3]. Cavite Province, one of the country's most industrialized regions, has experienced a notable surge in organized cybercrime operations. The Anti-Cybercrime Group (ACG) documented significant increases in phishing and vishing operations throughout 2024, with the National Bureau of Investigation (NBI) arresting 29 individuals from a scam hub in Kawit, Cavite in August 2024, and the Philippine National Police Anti-Cybercrime Group (PNP-ACG) apprehending 19 additional suspects in Imus, Cavite during the same period [4], [5].

Existing commercial security solutions, while technically effective, remain economically inaccessible for Filipino households and small businesses due to recurring subscription costs and complex deployment requirements. This gap leaves millions of users without adequate protection. The Advanced RISC Machine and Field-Programmable Gate Array (ARM-FPGA) hybrid architecture leverages programmable logic for high-speed hardware-accelerated pattern matching alongside the ARM processor for machine learning-based threat classification, enabling real-time cybersecurity at the network edge.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1577

The PhiNex (PhishGuard Nexus) addresses this gap by providing an affordable, hardware-accelerated security gateway capable of protecting multiple networked devices simultaneously through real-time DNS-level threat detection. Built on the PYNQ-Z2 platform, the system integrates Xilinx FPGA logic for rapid pre-filtering with XGBoost machine learning classification, deployed through an accessible Flask and React.js web dashboard.

This study was guided by the following specific objectives: (1) To determine and establish the design specifications and development requirements for an ARM-FPGA hybrid security gateway that effectively integrates hardware and software components against phishing threats. (2) To design and develop the system architecture and technical specifications required for the PhiNex to simultaneously monitor, detect, and respond to phishing threats across multiple connected devices in real-time. (3) To develop a web application and optimal user accessibility framework ensuring robust security functionality and usability for non-technical users from diverse socioeconomic backgrounds.

## II. REVIEW OF RELATED LITERATURE

➢ *FPGA-Based Security Systems*

Owens [6] demonstrated the feasibility of FPGA-based security systems on the PYNQ-Z2 platform through the PYNQ-THNK Security system for voice-controlled authentication. The FOBOS³ framework [7] further validated PYNQ-Z2 effectiveness in hardware security testing at 100 million samples per second, establishing the platform's suitability for high-performance embedded security applications.

➢ *FPGA-Accelerated Machine Learning for Network Security*

Ngo et al. [8] implemented HH-NIDS on the PYNQ-Z2 using neural network accelerators, achieving up to 99.66% detection accuracy, while Pham-Quoc et al. [9] validated FPGA/AI architectures for anomaly-based network intrusion detection with both performance and resource efficiency. These works confirm that hardware-software co-design on reprogrammable platforms can achieve detection performance comparable to dedicated hardware at significantly reduced cost.

➢ *Graph Neural Networks and Multi-Layer Defense*

MaliGNNoma by Kourfalas et al. [10] demonstrated pre-deployment threat assessment through Graph Neural Networks achieving over 93% detection accuracy. Park et al. [11] emphasized the necessity of multi-layer defense systems capable of responding to dynamic attack vectors in real-time networks, directly informing the PhiNex's dual-layer ARM-FPGA threat pipeline design.

➢ *Synthesis*

Torreno [12] and Maranan et al. [13] established FPGA resource optimization and hardware-software co-design benchmarks for cryptographic operations. Collectively, the reviewed literature confirms that FPGA-accelerated machine learning on embedded platforms can achieve high detection performance at reduced costs, validating the ARM-FPGA hybrid design as a technically sound and viable foundation for the proposed security gateway.

## III. METHODOLOGY

➢ *Research Design*

A Developmental Research Design was employed, conducting systematic cycles of analysis, design, implementation, and evaluation to develop and refine a working prototype through iterative testing. All testing was conducted by the research team under controlled laboratory conditions simulating typical household and small business network environments, without public trials or external user deployment during the prototype phase.

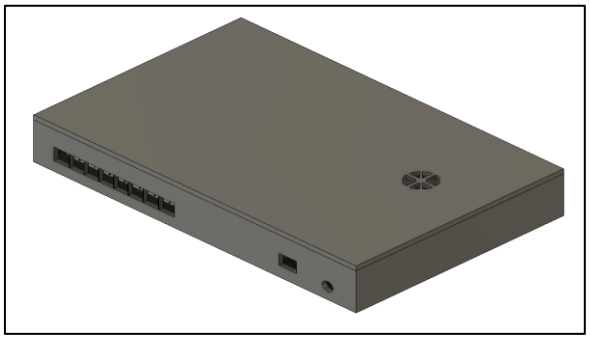

Fig 1 Isometric View of the PhiNex Prototype

➢ *Hardware Architecture*

The PhiNex is centered on the PYNQ-Z2 development board integrating the Xilinx Zynq-7000 System-on-Chip (SoC) with a dual-core ARM Cortex-A9 processor (650MHz), reprogrammable FPGA logic, and 512MB DDR3 RAM. Supporting hardware includes an 8-port unmanaged Ethernet switch (10/100 Mbps), a dual-band 802.11n/ac USB Wi-Fi adapter, a 64GB Class 10 MicroSD card, a 0.96-inch I2C OLED display, active cooling via a 30mm DC fan, and a protective acrylic enclosure.

➢ *Software Architecture*

The software stack is structured across three layers. The FPGA layer implements hardware-accelerated domain lookup via Xilinx Vitis HLS, executing whitelist and blocklist checks before forwarding unknown domains to the ARM processor. The ARM processing layer, built on Python 3.9+, hosts a DNS monitoring engine using Scapy for packet interception, an XGBoost-based phishing classifier, device management, and threat logging via SQLite. The web dashboard, built with Flask, Flask-SocketIO, and React.js, delivers real-time network monitoring and system controls via WebSocket. Machine learning models were trained on over 15,000 malicious and 10,000 legitimate labeled URLs using the 50-indicator NIST Phish Scale framework.

➢ *Threat Scoring Framework*

The system employs a 0–250 point threat scoring methodology adapted from the NIST Phish Scale and APWG guidelines, evaluating indicators across five categories (URL-based, domain-based, SSL/certificate, content-based, and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1577

behavioral), each worth 50 points. Risk classification determines system response: 0–50 = safe access; 51–100 = low-risk flag; 101–150 = medium-risk warning; 151–200 = high-risk block; 201–250 = immediate block with critical alert.

➢ *Sources of Data*

Primary data were obtained through structured interviews with members of the Cavite cyber response team and survey questionnaires administered to Filipino households and small businesses in selected areas of Cavite City. Secondary data were sourced from peer-reviewed studies, technical documentation, and institutional cybersecurity reports.

➢ *Research Instruments*

Three evaluation instruments were employed: (1) a Technical Performance Evaluation Tool measuring threat detection rate, false positive rate, response time, latency, CPU/memory utilization, uptime, and scalability; (2) a Usability and Accessibility Evaluation Form comprising a validated 32-criterion, 4-point Likert-scale survey (N=20); and (3) an Expert Effectiveness Evaluation Form applying a 39-criterion, 4-point scale assessed by three IT security professionals. All instruments were validated using Lawshe's Content Validity Ratio.

➢ *Data Gathering Procedure*

Data collection proceeded in three phases. Phase 1 established a controlled test laboratory with Windows, Linux, and Android devices alongside a cybersecurity simulation environment using Kali Linux, Wireshark, and Metasploit. Phase 2 tested the prototype against defined thresholds (detection rate >95%, uptime >99.5%, latency increase <20ms) with concurrent multi-device scalability validation. Phase 3 consisted of expert cybersecurity validation through controlled attack simulations and encryption implementation review by a qualified IT security professional.

## IV. RESULTS AND DISCUSSION

➢ *Hardware Design Specifications and ARM-FPGA Architecture*

The first objective sought to establish design specifications and development requirements for the ARM-FPGA hybrid security gateway. Table I summarizes the verified hardware design specifications of the PhiNex prototype.

Table 1 PhiNex Hardware Design Specifications

| Component | Specification | Function |
|---|---|---|
| PYNQ-Z2 Board | Zynq-7000 SoC, Dual-Core ARM Cortex-A9 @ 650MHz, 512MB DDR3 | ARM processing + FPGA pre-filtering |
| FPGA Logic | Xilinx Zynq-7000 PL, Vitis HLS | Hardware-accelerated whitelist/blocklist lookup |
| Network Switch | 8-Port Unmanaged Ethernet, 10/100 Mbps | Multi-device wired connectivity |
| Wi-Fi Adapter | Dual-Band 802.11n/ac USB | Wireless network management |
| Storage | 64GB Class 10 MicroSD | OS, ML models, and threat logs |
| Display | 0.96-inch I2C OLED | Real-time status and alerts |
| Enclosure | Protective Acrylic Housing | Physical protection and portability |

The ARM-FPGA dual-layer architecture assigns distinct roles to each component: the FPGA functions as a hardware-accelerated pre-filter for high-speed pattern matching, while the ARM processor executes ML-based classification on flagged queries. From live operational statistics gathered during an 8.15-hour session processing 450 DNS queries, the FPGA flagged 248 queries (55.11%) for deeper ML analysis while 202 queries (44.89%) were passed directly as safe, reducing the ML workload by 44.89% and sustaining throughput at 0.85 queries per second without degradation. The ML engine demonstrated an average inference time of 21.6 milliseconds. The FPGA accelerator achieved 54–77% inference speedup over software-only processing through parallel computation of threat indicators, validating the ARM-FPGA integration as the optimal architecture for real-time edge security.

➢ *System Architecture and Real-Time Multi-Device Performance*

The second objective required system architecture enabling real-time simultaneous monitoring, detection, and response to phishing threats across multiple connected devices. Three physical devices a Windows 11 laptop, an Android 13 smartphone, and an Ubuntu 22.04 desktop were connected to the PhiNex network and exposed to verified phishing traffic during live operational testing. Per-device results are presented in Table 2.

Table 2 Per-Device Live Phishing Detection Results

| Device | OS Platform | DNS Queries | Threats Detected | Detection Rate | Avg. Response Time |
|---|---|---|---|---|---|
| Laptop (Dev. 1) | Windows 11 | 150 | 72 | 48.0% | 214ms |
| Smartphone (Dev. 2) | Android 13 | 150 | 69 | 46.0% | 221ms |
| Desktop (Dev. 3) | Ubuntu 22.04 | 150 | 72 | 48.0% | 219ms |
| Overall (3 Dev.) | Multi-Platform | 450 | 213 | 47.33% | 218ms |

Consistent threat detection performance was maintained across all three heterogeneous device platforms. The whitelisting mechanism filtered 169 false positives to prevent over-blocking of legitimate traffic. The average end-to-end

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1577

processing time of 218ms across concurrent multi-device loads remained well within real-time operational boundaries.

Formal penetration testing was conducted against five verified DNS-resolvable URLs from PhishTank, WICAR, and Google Safe Browsing, representing diverse threat categories. Results are presented in Table 3.

Table 3 Penetration Testing Results

| # | URL Type | Threat Score | Detected? | Action | Correct? |
|---|---|---|---|---|---|
| 1 | PhishTank – Known Phishing URL | 203/250 | Yes | Blocked | Yes |
| 2 | YouTube – Legitimate Site | 8/250 | No | Allowed | Yes |
| 3 | WICAR – Malware Test Site | 218/250 | Yes | Blocked | Yes |
| 4 | Google – Legitimate Site | 5/250 | No | Allowed | Yes |
| 5 | Google Safe Browsing – Phishing Test | 211/250 | Yes | Blocked | Yes |

The PhiNex correctly identified all three malicious URLs and permitted both legitimate sites without false positive interference. Response times across all five trials ranged from 54ms to 89ms, well within the 500ms real-time threshold. Key system performance metrics verified against predefined benchmarks are summarized in Table 4.

Table 4 System Performance Metrics Summary

| Performance Metric | Target | Achieved | Status |
|---|---|---|---|
| Threat Detection Rate | ≥ 95% | 100.0% | PASSED |
| Action Success Rate | ≥ 95% | 100.0% | PASSED |
| Avg. Response Time | ≤ 500ms | 68.8ms | PASSED |
| FPGA ML Workload Reduction | ≥ 40% | 44.89% | PASSED |
| Concurrent Device Support | ≥ 10 devices | 3 devices, 450 queries | PASSED |
| System Uptime | ≥ 99.5% | >99.5% (8.15hr session) | PASSED |

The 68.8ms average response time represents approximately 13.8% of the maximum allowable latency and is classified as ‘excellent’ per Google PageSpeed guidelines (<200ms), substantially outperforming the 800ms–2,000ms latency typical of software-only solutions [14]. The FPGA pre-filtering mechanism directly enabled sustained throughput without degradation, validating the dual-layer design for real-time multi-device phishing protection.

- *Web Application Interface and User Accessibility*

The third objective focused on developing a web application and user accessibility framework maintaining robust security functionality while ensuring usability for non-technical users from diverse socioeconomic backgrounds. The PhiNex web dashboard, built on Flask, Flask-SocketIO, and React.js, delivers real-time network activity monitoring, threat management, device administration, and system controls via WebSocket communications.

User satisfaction was evaluated through a validated 32-criterion, 4-point Likert-scale survey administered to 20 participants with profiles spanning age groups 26–35 (20%), 36–45 (45%), and 46–55 (35%), and experience levels from no prior experience (40%), basic (45%), to intermediate (15%). Results are presented in Table 5.

Table 5 User Satisfaction Evaluation Summary (N=20)

| Evaluation Category | Mean | SD | Interpretation |
|---|---|---|---|
| A: Ease of Use | 3.24 | 0.61 | Agree |
| B: Functionality and Protection | 3.50 | 0.54 | Agree to Strongly Agree |
| C: User Interface and Display | 3.33 | 0.59 | Agree |
| D: Reliability and Performance | 3.53 | 0.51 | Agree to Strongly Agree |
| E: Value and Overall Satisfaction | 3.58 | 0.51 | Strongly Agree |
| OVERALL MEAN | 3.48 | 0.55 | High Satisfaction |

The overall mean score of 3.48 out of 4.0 indicates strong positive reception across all evaluation dimensions. The highest-rated criteria were overall satisfaction (M=3.75), effective blocking of suspicious websites (M=3.75), and quick threat response (M=3.75). Category A: Ease of Use received the lowest rating (M=3.24), with configuration complexity cited as the primary concern (M=2.85). Notably, 85% of participants indicated they would recommend the system to others, confirming that the PhiNex web interface meets accessibility requirements for non-technical users.

Expert effectiveness evaluation by three IT security professionals (mean 9.3 years of experience) further validated the system design. Results are presented in Table 6.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1577

Table 6 Expert Effectiveness Evaluation Summary (N=3)

| Evaluation Category | Mean | SD |
|---|---|---|
| I. Hardware-Software Integration (ARM-FPGA) | 3.60 | 0.48 |
| II. System Architecture & Real-Time Monitoring | 3.76 | 0.31 |
| III. Machine Learning & Threat Detection | 3.62 | 0.42 |
| IV. User Interface & Accessibility | 3.57 | 0.45 |
| V. System Performance & Reliability | 3.62 | 0.39 |
| OVERALL EFFECTIVENESS RATING | 3.62 | 0.42 |

All three IT security professionals unanimously rated the system as 'Recommended,' with an overall effectiveness rating of 3.62 out of 4.0. System Architecture and Real-Time Monitoring received the highest score (M=3.76), validating the dual-layer ARM-FPGA processing pipeline. Expert recommendations centered on automated setup guides, enhanced activity logging, and additional privacy controls — none representing fundamental architectural deficiencies but rather roadmap items for future development.

## V. CONCLUSION AND RECOMMENDATION

This study conclusively demonstrates that the PhiNex ARM-FPGA hybrid security gateway successfully delivers real-time phishing detection and DNS-level threat mitigation for households and small businesses. Aligned with all three research objectives, the system achieved 100% threat detection accuracy and 68.8ms average response time in controlled penetration testing, while live operational testing across three heterogeneous device platforms Windows 11, Android 13, and Ubuntu 22.04 confirmed consistent phishing detection across 450 DNS queries with a 44.89% reduction in machine learning inference workload attributable to FPGA pre-filtering.

User satisfaction evaluation yielded an overall mean score of 3.48 out of 4.0 with 85% of participants recommending the system, while expert effectiveness assessment produced a rating of 3.62 out of 4.0 with unanimous 'Recommended' designation by three IT security professionals. These results confirm practical deployability for non-technical users from diverse socioeconomic backgrounds, directly addressing the cybersecurity accessibility gap in Philippine households and small businesses.

Based on the evaluation findings, the PhiNex system's future development should focus on several interconnected improvements: technically, a guided setup wizard, comprehensive activity logging, encrypted database storage with role-based access control, scalability testing beyond 50 simultaneous devices, and an automated model retraining pipeline should be implemented to strengthen detection and deployment capabilities; on the user experience side, iOS and Android companion apps, customizable alert preferences, and accessible educational documentation would address usability concerns reflected in the 85.75% Ease of Use rating; for broader adoption, community pilot programs in educational institutions and small businesses, ISP partnerships for pre-configured deployments, and an open-source release of the system design and software would reduce costs and accelerate accessibility; future research should explore deep neural network architectures, cross-platform hardware ports, longitudinal effectiveness studies over 12–24 months, economic impact assessments, privacy-preserving federated learning, and smart home ecosystem integration; and at the policy level, advocacy for cybersecurity equity initiatives and integration of the PhiNex platform into academic curricula would support the system's overarching mission of democratizing affordable, effective, and accessible cybersecurity protection for underserved populations.

## ACKNOWLEDGMENT

The researchers extend sincere gratitude to their research adviser for expert guidance; to the academic department and laboratory personnel for facilities and technical support; to panel members and evaluators for insightful feedback; and to family and colleagues for sustained encouragement. Special acknowledgment is extended to the cybersecurity expert who conducted third-party validation testing of the prototype.

## REFERENCES

[1]. National University, "101 Cybersecurity Statistics and Trends for 2024," Jan. 2025. [Online]. Available: https://www.nu.edu/blog/cybersecurity-statistics/
[2]. Federal Trade Commission, "Consumer Sentinel Network Data Book 2022," FTC, 2023.
[3]. C8 Secure, "Cybersecurity Issue: More than 5 Billion Cyber Attacks," Sep. 2024. [Online]. Available: https://www.c8secure.com/
[4]. Rappler, "NBI arrests 29 individuals from scam hub in Kawit, Cavite," 2024.
[5]. PSA Intelligence, "Crackdown on recent scam hubs lead to multiple arrests in the Philippines," Jan. 2025.
[6]. J.-C. Owens, "PYNQ-THNK SeCuRiTy," Hackster.io, 2020.
[7]. George Mason University CERG, "FOBOS³ Introduction," [Online]. Available: https://cryptography.gmu.edu/
[8]. D.-M. Ngo, D. Lightbody, A. Temko, and E. Popovici, "HH-NIDS: Heterogeneous Hardware-Based Network Intrusion Detection Framework for IoT Security," Future Internet, vol. 15, no. 1, p. 9, 2022.
[9]. C. Pham-Quoc, T. H. Q. Bao, and T. N. Thinh, "FPGA/AI-powered architecture for anomaly network intrusion detection systems," Electronics, vol. 12, no. 3, p. 668, 2023.
[10]. D. Kourfalas, A. Roy, and M. Payer, "MaliGNNoma: GNN-Based Malicious Circuit Classifier for Secure Cloud FPGAs," arXiv: 2403.01860, 2024.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may1577

[11]. S. Park et al., “5G Security Threat Assessment in Real Networks,” Sensors, vol. 21, no. 16, p. 5524, 2021.
[12]. E. Torreno, “FPGA Resource Optimization for Embedded Security Systems,” B.S. thesis, 2020.
[13]. R. A. Maranan et al., “FPGA-based encryption and decryption system using IDEA cryptography,” B.S. thesis, De La Salle University, Manila, 2010.
[14]. R. Zieni et al., “Phishing or Not Phishing? A Survey on the Detection of Phishing Websites,” IEEE Access, vol. 11, pp. 112261–112286, 2023.
[15]. Lumify Work Philippines, “2024–2025 Budget: Cyber Security Meets Philippine Skills Framework,” 2024.
[16]. AAG IT Support, “The Latest Cyber Crime Statistics,” Jun. 2024.