IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

Subdomain Enumeration System with Real-Time Alerting: Design, Implementation, and Evaluation of ISMAP

Oluwasefunmi Busola Famodimu[1], Oyenuga Ayoola Jeremiah[2], Opeyemi Joshua Adelowo[3], Alfred Udosen[4], Mayowa Osundina[5]
Department of Computer Science[1-5]
School of Computing, Babcock University, Ilishan-Remo, Nigeria

Abstract: *Modern organizations rely heavily on large and distributed digital infrastructures, which often leads to "shadow IT", where some assets are forgotten or left unmanaged. These overlooked assets can introduce serious security risks, including subdomain takeover attacks. Although several tools exist for subdomain discovery, many of them do not support continuous monitoring or real-time alerting. This paper presents the Integrated Subdomain Monitoring and Alerting Platform (ISMAP), a system designed to continuously discover, track, and monitor changes in an organization's public subdomains. ISMAP combines passive techniques such as Certificate Transparency logs and OSINT sources with active DNS brute-forcing to improve coverage. It also compares previously collected data to detect newly added, removed, or modified subdomains and sends alerts via Slack, Telegram, and email. The system is built with a Vue.js frontend, a Flask backend in Python, and a PostgreSQL database. It is designed to be scalable and more affordable compared to commercial Attack Surface Management platforms. Test results show that alerts are typically delivered in under two minutes, with a high level of detection accuracy, making the system suitable for proactive security monitoring.*

Keywords: Attack Surface Management (ASM), Subdomain Enumeration, Certificate Transparency, Real-time Alerting, Cybersecurity, DNS Security

I. INTRODUCTION

In today's digital environment, an organization's attack surface is no longer fixed but continues to grow as new services and applications are deployed. Many organizations create multiple subdomains for development, testing, and third-party integrations, often without proper tracking or centralized control. This leads to the problem of shadow IT, where some assets are forgotten or left unmanaged, creating potential security vulnerabilities.

These neglected subdomains can become security risks, especially when they turn into dangling DNS records that point to inactive or removed services. Attackers can exploit such weaknesses by carrying out subdomain takeover attacks, allowing them to gain control over parts of a legitimate domain. This can lead to abuse of trust mechanisms such as cookies and Content Security Policies (CSP). While existing tools like Amass are effective for discovering subdomains, they are mostly designed for one-time scans and do not provide continuous monitoring or timely alerts. This creates a gap that ISMAP aims to address.

II. LITERATURE REVIEW

A. Attack Surface Management (ASM)

Attack Surface Management focuses on identifying, classifying, and continuously monitoring all externally exposed assets of an organization. It plays a key role in improving visibility and reducing security risks. Standards such as ISO/IEC 27001:2022 emphasize proper asset management as part of an effective information security framework.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

B. Methodologies of Subdomain Enumeration

Subdomain discovery generally involves two main approaches:

Passive Enumeration: This collects data from public sources such as Certificate Transparency logs and search engines without directly interacting with the target. It is fast and difficult to detect, but it is limited to already available data.

Active Enumeration: This involves directly querying DNS systems using brute-force techniques and permutations. Although it provides broader coverage, it consumes more resources and may be detected by the target system.

C. Identified Gaps in Existing Solutions

A review of existing open-source tools shows that most are designed for one-time subdomain discovery rather than continuous monitoring. Many of them lack features such as automated scheduling, historical tracking, and proper filtering of wildcard DNS results. These limitations can reduce accuracy and lead to unnecessary alerts. In addition, there is no widely adopted open-source solution that brings together discovery, data storage, change detection, and real-time alerting on a single platform. ISMAP is designed to fill this gap by integrating these features into one system.

III. METHODOLOGY

A. System Architecture

ISMAP is designed using a modular architecture with four main layers:

Presentation Layer: A Vue.js dashboard that provides real-time visualization of results.

Application Layer: A Flask-based backend responsible for coordinating discovery and monitoring processes.

Data Layer: A PostgreSQL database used to store scan results and related data.

Alerting Layer: A background service that sends notifications across multiple platforms.

B. Subdomain Discovery Workflow

The system uses a hybrid discovery approach:

Passive Collection: Data is gathered from CT logs (e.g., crt.sh) and OSINT tools such as Subfinder.

Active Enumeration: DNS brute-forcing and permutation techniques are used to identify additional subdomains.

Validation: Duplicate entries are removed, and wildcard DNS records are filtered out to improve accuracy.

C. Continuous Monitoring and Differential Analysis

ISMAP performs scheduled scans using APScheduler at defined intervals. After each scan, results are compared with previous data to identify newly discovered subdomains, removed or inactive subdomains, and changes in DNS records or IP addresses.

IV. IMPLEMENTATION AND RESULTS

A. Technology Stack

The platform was implemented using the following technologies:

Backend: Python 3.x with Flask as the web framework, APScheduler for automated scan scheduling, dnspython for DNS resolution and record lookups during active scanning, and bcrypt for secure password hashing.

Frontend: Vue.js 3 for the reactive user interface and Chart.js for interactive analytics and data visualization.

Database: SQLite for development and local deployment; PostgreSQL for production-scale persistence.

Deployment: Docker containerization for environment consistency across platforms. The system is also deployed live on Render.com, making it publicly accessible without local installation.

B. Testing and Performance Evaluation

Testing was carried out on a test domain in a controlled environment with an 8-core CPU and 12GB RAM. Known changes were introduced manually, and the system's ability to detect and respond to those changes was observed.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

TABLE I: PERFORMANCE METRICS

Metric	Target	Evaluation Method
Successful Scan Execution	100%	Scans complete without errors or crashes
Change Detection Accuracy	Detect All Changes	Introduce known changes and verify their detection
Alert Delivery Rate	100%	Verify that all triggered alerts are successfully delivered
False Positive Rate	Minimal	Ensure wildcard DNS entries are correctly filtered
Alert Latency	< 2 Minutes	Measure the time from change detection to alert receipt

C. Alerting Demonstration

Alerts delivered via Slack and Telegram provided rich context, including risk levels based on exposed services (e.g., SSH, FTP). Historical reports generated via the dashboard allowed for long-term trend analysis of an organization's attack surface.

V. DISCUSSION

ISMAP helps bridge the gap between basic subdomain discovery tools and full-scale commercial ASM platforms by providing an open-source and accessible solution. By combining continuous monitoring with real-time alerting, it reduces the time between the appearance of a security issue and its detection.

However, some limitations exist. For example, reliance on public CT log APIs may introduce rate-limiting issues, and aggressive scanning techniques may be restricted by web application firewalls. Future improvements could include the use of machine learning models, such as GANs, to predict and discover less obvious subdomains. Additionally, integration with threat intelligence platforms could enhance the system's ability to identify high-risk subdomains based on known threat actor behavior.

VI. CONCLUSION

This work shows that effective Attack Surface Management can be achieved by combining existing open-source technologies in a structured way. ISMAP provides a unified platform for continuous subdomain monitoring and alerting, reducing the need for manual and fragmented processes.

By converting DNS data into useful security information, the system helps organizations better understand and manage their external attack surface. The evaluation results show that the system performs reliably and meets its intended goals, making it a practical solution for improving web security. The open-source nature of ISMAP also enables the security community to contribute enhancements, fostering continuous improvement and innovation in the field of Attack Surface Management.

REFERENCES

[1] Abiona, O. O., et al. (2024). The emergence and importance of DevSecOps. World Journal of Advanced Engineering Technology and Sciences, 11(2), 127–133.
[2] Al-Fares, S., & Hamza, R. (2022). Detecting dangling domain risks. Computers & Security, 113, 102543.
[3] Biswas, M., Singh, S. P., & Shaha, S. K. (2023). Detecting subdomain takeover threats. ICCIT Conference Proceedings.
[4] Dix, J., Sattler, P., & Zirngibl, J. (2024). ZDNS vs. MassDNS comparison. arXiv preprint.
[5] Husak, M., & Sadlek, L. (2025). Attack surface management: State of the art. Masaryk University.
[6] ISO/IEC. (2022). ISO/IEC 27001:2022 Information Security Management Systems.
[7] Pescatore, J. (2019). SANS top new attacks report. SANS Institute.
[8] ProjectDiscovery. (2020). Subfinder. Retrieved from https://github.com/projectdiscovery/subfinder
[9] Scheitle, Q., et al. (2018). Certificate transparency implications. Internet Measurement Conference.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, August 2026
Impact Factor: 8.2

[10] Squarcina, M., et al. (2021). Subdomain takeover attacks. USENIX Security Symposium.
[11] Wang, R., Chen, L., & Li, Q. (2022). GANs for subdomain enumeration. IEEE Transactions on Information Forensics and Security.