Digital Asset Discovery for Organizations

Mrs.P.Elakkiya[1], CVignesh[2], A Raj Mohamed[3], S Suryananthan[4], K Thilak[5]
[1]Assist prof, Dept of Computer Science and Engineering
[2, 3, 4, 5] Dept of Computer Science and Engineering
[1, 2, 3, 4, 5] Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tamil Nadu, India

Abstract- *The rapid expansion of cloud computing, APIs, and third-party services has significantly increased the digital attack surface of modern organizations. Many cyber incidents occur due to unmanaged or forgotten assets such as test servers, misconfigured cloud storage, and undocumented APIs. Existing security tools often lack continuous external visibility and centralized asset mapping.*

This paper presents a Digital Asset Discovery framework that automatically identifies and monitors organizational digital assets from an attacker's perspective. The system performs automated enumeration of domains, subdomains, IP addresses, cloud resources, APIs, and certificates. Discovered assets are enriched with exposure and hosting information, followed by risk classification and prioritization. Continuous monitoring mechanisms detect newly exposed assets in real time.

The proposed approach improves asset visibility, reduces security blind spots, and supports proactive security management through dashboards and reports.

Keywords: Attack Surface Management, API Security, Continuous Monitoring, Digital Asset Discovery, OSINT, Shadow IT, Web Security

I. INTRODUCTION

The rapid adoption of cloud computing, SaaS platforms, APIs, and third-party integrations has significantly expanded the digital attack surface of modern organizations. Digital assets such as domains, subdomains, IP addresses, cloud storage, APIs, and exposed services are continuously increasing, often without centralized visibility. Attackers leverage OSINT-based reconnaissance techniques and internet-wide scanning tools to identify and exploit these exposed assets [5], [6].

Recent studies highlight that incomplete asset inventories significantly increase cyber risk [1], [3]. Misconfigured cloud storage, exposed APIs, and leaked credentials in public repositories remain common causes of data breaches [12], [19]. Traditional security solutions primarily focus on internal infrastructure and lack external visibility into unknown or shadow IT assets.

Attack Surface Management (ASM) has emerged as a proactive approach to continuously discover, classify, and monitor internet-facing assets from an attacker's perspective [2]. However, many existing ASM solutions are enterprise-centric and lack integration of OSINT, cloud enumeration, API discovery, and continuous monitoring within a unified framework.

This paper proposes Digital Asset Discovery for Organizations (DADO), an automated framework that integrates digital asset discovery, risk scoring, cloud misconfiguration detection, API exposure analysis, and continuous monitoring to improve organizational security posture.

II. RELATED WORK

Attack surface management and digital asset discovery have gained significant attention in recent years. Everson [1] and Ashley [2] examined network attack surface mapping and emphasized automated enumeration of internet-facing components. Large-scale scanning techniques such as ZMap and Censys demonstrate the feasibility of internet-wide asset discovery [5], [6].

Cloud security research highlights misconfigured storage buckets and exposed cloud services as major sources of breaches [12], [13]. Studies on SaaS and multi-cloud environments further emphasize the need for continuous monitoring and configuration validation [14].

API security has also emerged as a critical concern. Alrawi et al. [15] conducted a large-scale study of web API exposures, demonstrating widespread authentication weaknesses. SSL/TLS validation flaws and web application vulnerabilities remain prevalent attack vectors [16], [18].

In addition, OSINT and public repository analysis reveal significant risks associated with credential leakage and exposed secrets [19], [20]. These findings highlight the

importance of integrating reconnaissance-based detection mechanisms within attack surface discovery systems.

Despite these advances, most existing approaches address discovery, vulnerability analysis, or monitoring independently. There remains a need for an integrated framework that combines OSINT-based reconnaissance, cloud asset enumeration, API discovery, risk prioritization, and continuous monitoring into a unified system.

III. PROPOSED ATTACK SURFACE DISCOVERY FRAMEWORK

The framework follows an attacker-centric reconnaissance model in which asset discovery is performed externally without requiring internal network access. The system operates in iterative phases consisting of seed expansion, asset enumeration, enrichment, risk evaluation, and continuous validation. Each phase is modular, allowing extensibility and integration with additional reconnaissance tools.The overall workflow begins with seed input collection from organizational profiling. These seeds are expanded using DNS resolution, certificate transparency logs, OSINT sources, and internet-wide scanning databases. Newly discovered assets are recursively enumerated to ensure comprehensive coverage of the external attack surface.To improve scalability, the framework adopts asynchronous task scheduling and parallel scanning mechanisms. This enables efficient enumeration of large domain sets and IP ranges while maintaining performance and reducing scan latency. The modular backend architecture ensures that new discovery plugins (e.g., cloud APIs, SaaS services, API gateways) can be integrated without redesigning the core system.

Organization Profiling

The Organization Profiling module defines the initial scope of attack surface discovery. Seed inputs include primary domains, IP ranges (CIDR blocks), cloud tenant identifiers, and known SaaS integrations. These inputs act as anchor points for recursive enumeration. The module validates input consistency, removes duplicates, and structures seed data for downstream processing. Proper scoping ensures targeted scanning while minimizing false positives and unauthorized enumeration.

Asset Discovery Engine

The Asset Discovery Engine performs automated reconnaissance using multiple enumeration strategies. Domain expansion is conducted through DNS brute-forcing, certificate transparency analysis, passive DNS records, and OSINT sources. IP-based discovery includes port scanning, service fingerprinting, and exposure identification. Cloud resource discovery inspects publicly accessible storage, APIs, and serverless endpoints. The engine continuously expands the asset graph by identifying relationships between domains, IPs, and hosting providers. This attacker-perspective approach ensures visibility into both known and shadow IT assets..

Asset Enrichment and Analysis

Discovered assets undergo enrichment to provide contextual intelligence. The system collects metadata including hosting provider information, ASN details, geolocation, SSL/TLS certificate data, and service banners. Exposure analysis identifies open ports, weak configurations, and publicly accessible services. Cloud assets are evaluated for misconfigurations such as publicly exposed storage or unsecured endpoints. Enrichment enhances raw discovery results and enables informed risk assessment..

Risk Scoring and Visualization

The Risk Scoring module classifies assets based on exposure severity, configuration weaknesses, and contextual criticality. A rule-based scoring model inspired by standardized vulnerability scoring principles assigns risk levels (Low, Medium, High, Critical). Factors include internet exposure, authentication absence, service type, and certificate validity. The Visualization component represents assets as interconnected nodes within an interactive graph, enabling security teams to identify high-risk entry points and lateral exposure paths within the attack surface..

TABLE I. RISK CLASSIFICATION CRITERIA

Risk Level	Exposure Characteristics
Low	Internal assets with restricted access
Medium	Internet-facing assets with standard configurations
High	Public services with open ports or weak configurations
Critical	Exposed storage, sensitive APIs, or misconfigured cloud resources

Monitoring and Alerts

The Monitoring and Alerts module enables continuous attack surface validation. Scheduled scans periodically reassess previously discovered assets to detect DNS changes, certificate updates, newly opened ports, and cloud configuration modifications. Delta analysis identifies deviations from baseline states. When high-risk exposures are detected, automated alerts are generated through the dashboard interface. Continuous monitoring transforms the

system from a static inventory tool into a proactive security management platform.

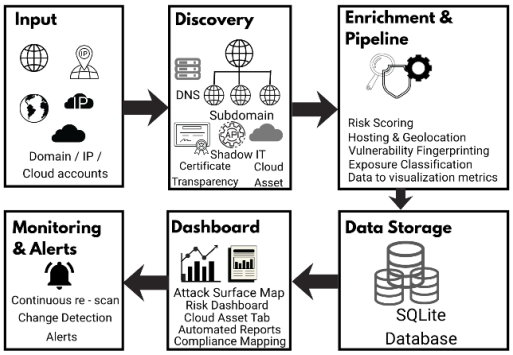

Fig. 1. Architecture of Asset Discovery System

IV. RESULTS AND DISCUSSION

The framework was implemented using Python-based backend services and open-source reconnaissance tools, with a web-based dashboard for visualization. Testing showed

A comparison between the proposed system and existing approaches is presented in Table II.

TABLE II. COMPARISON WITH EXISTING APPROACHES

Feature	Existing Tools	Proposed System
Automated Asset Discovery:	Partial	Full
Shadow IT Detection	Limited	Supported
Risk Prioinuous Monitoring	Exposure-based	Basic Yes
Visualization	Limited	Graph-based

effective discovery of unknown subdomains, cloud assets, and exposed services.

Risk-based prioritization enabled faster remediation of critical assets. Continuous monitoring ensured timely detection of new exposures, improving overall security awareness.

A. Experimental Setup

The DADO framework was implemented using Python-based backend services with modular discovery engines for domain enumeration, cloud asset identification, API discovery, and secret detection. Testing was conducted using sample organizational domains and publicly available infrastructure data.

B. Asset Discovery Performance

The system successfully identified previously unknown subdomains, exposed services, and publicly accessible cloud resources. OSINT-based enumeration improved detection coverage compared to basic DNS-only scanning techniques.

C. Monitoring Evaluation

Continuous monitoring mechanisms enabled detection of newly exposed assets and configuration changes over time. Risk scoring and exposure classification assisted in prioritizing critical assets for remediation.

V. CONCLUSION

This paper presented DADO, a Digital Asset Discovery framework designed to enhance organizational security visibility. By integrating OSINT-based reconnaissance, cloud asset enumeration, API exposure detection, and continuous monitoring, the system provides a comprehensive view of external digital assets. Risk-based prioritization further enables efficient remediation of high-severity exposures. Future work includes multi-cloud expansion, threat intelligence integration, and AI-based anomaly detection.

REFERENCES

[1] D. Everson, “A Survey on Network Attack Surface Mapping,” ACM Digital Library, 2024.
[2] T. Ashley, “Aggregate Attack Surface Management for Networked Systems,” Journal of Cyber Security, 2022.
[3] J. Amann et al., “No Attack Necessary: The Surprising Dynamics of SSL/TLS Certificate Revocation,” in Proc. USENIX Security Symposium, 2017.
[4] S. Frei et al., “Large-Scale Vulnerability Analysis,” ACM CCS Workshop, 2006.
[5] Z. Durumeric et al., “ZMap: Fast Internet-Wide Scanning and Its Security Applications,” USENIX Security, 2013.
[6] Z. Durumeric et al., “Censys: Internet-Wide Scanning and Security Analysis,” ACM CCS, 2015.
[7] M. Antonakakis et al., “Understanding the Mirai Botnet,” USENIX Security, 2017.
[8] J. Matherly, “Shodan: The Computer Search Engine,” DEFCON, 2013.
[9] H. Holm, “A Large-Scale Study of Reconnaissance Activity,” IEEE Security & Privacy, 2014.
[10] C. Sabottke et al., “Vulnerability Disclosure in the Age of Social Media,” USENIX Security, 2015.

[11] B. Krebs, "OSINT in Cyber Threat Intelligence," IEEE Security & Privacy, 2018.
[12] M. Almorsy et al., "An Analysis of the Cloud Computing Security Problem," Asia-Pacific Software Engineering Conf., 2011.
[13] S. Khandelwal et al., "Understanding Security Misconfigurations in Cloud Storage Services," IEEE Cloud Computing Conf., 2020.
[14] S. Subashini and V. Kavitha, "A Survey on Security Issues in Cloud Computing," J. Network Computer Applications, 2011.
[15] O. Alrawi et al., "The Security of Web APIs: A Large-Scale Study," IEEE EuroS&P, 2019.
[16] N. Georgiev et al., "The Most Dangerous Code in the World," ACM CCS, 2012.
[17] B. R. Bhimireddy et al., "Web Security and Web Application Security: Attacks and Prevention," ICACCS, 2023.
[18] OWASP Foundation, "OWASP Top 10 Web Application Security Risks," 2021.
[19] Y. Wang et al., "How Bad Can It Git? Characterizing Secret Leakage in Public Repositories," IEEE S&P, 2019.
[20] A. Saha et al., "Secrets in Source Code: Detecting Credential Leaks in GitHub Repositories," ACM Asia CCS, 2020.
[21] R. Bozorgi et al., "Beyond Heuristics: Learning to Classify Vulnerabilities," ACM SIGKDD, 2010.
[22] FIRST.org, "Common Vulnerability Scoring System v3.1 Specification," 2019.
[23] C. Grier et al., "Manufacturing Compromise: The Emergence of Exploit-as-a-Service," in Proc. ACM CCS, 2012.
[24] M. Zhang et al., "An Empirical Study of Public Cloud Storage Misconfigurations," in Proc. IEEE International Conference on Cloud Computing, 2021.
[25] S. Frolov and E. Wustrow, "The Broken Shield: Measuring Revocation Effectiveness in the Web PKI," in Proc. USENIX Security Symposium, 2017.