AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

CYBERRECON - A CYBERSECURITY FRAMEWORK FOR RECONNAISSANCE ANALYSIS AND SECURITY RISK ASSESSMENT

[1]Dr.B Ravi Kumar, [2]V Mythri, [3]G Jyoshna, [4]Yaseen
[1]Associate Professor, [234]Students
Department of Computer Science and Engineering,
Siddhartha Institute of Technology and Sciences, Narapally, Korremula Road,
Ghatkesar, Medchal-Malkajgiri, Hyderabad, Telangana - 500088. INDIA
dr.brkou@siddhartha.org.in, 23TQ1A6209@siddhartha.co.in,
23TQ1A6218@siddhartha.co.in, 23TQ1A6217@siddhartha.co.in

Abstract

CyberRecon is a cybersecurity framework designed to support reconnaissance analysis and security risk assessment in a structured and controlled environment. Reconnaissance is an important phase of cybersecurity because it helps identify publicly available information, exposed services, technologies, and potential security weaknesses associated with an authorized target. The proposed framework organizes these activities into a unified workflow rather than requiring security analysts to depend on multiple disconnected tools.

The system collects and analyzes authorized reconnaissance information such as domain details, DNS records, subdomains, IP addresses, open service information, technology indicators, and other publicly available security-relevant metadata. The collected information is processed and categorized to make the results easier to understand. CyberRecon focuses on passive and controlled reconnaissance so that security assessment activities can be performed without unnecessarily affecting the target environment.

A risk assessment component evaluates discovered assets and observations using predefined security criteria. Potentially important findings can be classified according to their severity and relevance, allowing analysts to prioritize areas that require further investigation. The framework can also maintain assessment records and generate structured reports containing discovered assets, observations, risk classifications, and recommended defensive actions.

The primary objective of CyberRecon is to improve the efficiency, consistency, and visibility of reconnaissance-based security assessment. By combining information gathering, analysis, risk classification, visualization, and reporting within a single framework, the system can help security teams understand their external attack surface more effectively. The framework is intended for legitimate security testing, vulnerability assessment, academic research, and authorized organizational security monitoring.

I. Introduction

Cybersecurity has become an essential requirement for organizations that depend on websites, cloud services, networks, applications, and digital infrastructure. As organizations expand their online presence, the number of publicly exposed assets

also increases. Attackers may use information available from public sources to understand an organization's infrastructure before attempting further attacks. Therefore, identifying and analyzing externally visible information is an important part of proactive security assessment.

Reconnaissance refers to the process of collecting information about a target environment before conducting a security assessment. It may involve discovering domains and subdomains, examining DNS information, identifying network addresses, observing exposed services, and determining technologies used by publicly accessible applications. When performed with proper authorization, reconnaissance helps security professionals understand what information an organization unintentionally exposes to the internet.

Traditional security assessment workflows often require analysts to use several specialized tools independently. The output from these tools may appear in different formats, making it difficult to correlate related findings. Analysts may also need to manually organize results, identify important assets, classify risks, and prepare reports. Such fragmented processes can consume significant time and may lead to inconsistent analysis.

CyberRecon addresses these challenges by providing a structured framework for reconnaissance analysis and security risk assessment. The framework can collect authorized reconnaissance information, normalize the collected data, organize assets, analyze security observations, and present findings through a centralized interface. It can also provide risk prioritization and reporting capabilities to help security teams make informed defensive decisions.

The proposed system is designed primarily as a defensive cybersecurity solution. It emphasizes authorized information gathering, controlled assessment, data organization, and risk awareness rather than exploitation. By providing a systematic approach to reconnaissance and assessment, CyberRecon can assist security analysts, students, researchers, and organizations in understanding their external security posture and identifying areas that deserve defensive attention.

II. Literature Survey

Reconnaissance has traditionally been considered an important stage of penetration testing and security assessment. Security researchers have developed numerous approaches for discovering information about network infrastructure, domains, applications, and services. These approaches generally involve passive information collection followed by controlled active assessment. The literature demonstrates that early identification of exposed assets can improve the overall effectiveness of security testing because analysts can better understand the environment before evaluating its security.

Research on attack-surface management has emphasized the importance of continuously identifying internet-facing assets. Modern organizations may operate multiple domains, cloud resources, APIs, applications, and third-party services. Some of these assets may not be adequately documented internally. External attack-surface discovery techniques attempt to provide visibility into such assets by correlating

publicly available information and identifying relationships between domains, addresses, services, and technologies.

DNS and domain enumeration have also received considerable attention in cybersecurity research. DNS records can provide useful information about an organization's internet infrastructure, including domain relationships, mail services, name servers, and address mappings. Subdomain discovery can further reveal application endpoints or services that may otherwise be overlooked during manual assessment. However, discovered information must be validated carefully because DNS data can change frequently and may contain inactive or third-party resources.

Another area of research focuses on technology fingerprinting and service identification. Understanding the technologies associated with an application can help security analysts determine which components require closer defensive review. Web servers, frameworks, content management systems, programming technologies, and other infrastructure indicators can provide useful context during security assessments. Nevertheless, technology identification is not always completely accurate, so automated results should be treated as assessment indicators rather than definitive evidence.

Security risk assessment methodologies provide another important foundation for CyberRecon. Risk assessment generally considers factors such as asset importance, exposure, likelihood, and potential impact. Prioritization allows organizations to focus resources on findings that present greater potential risk. A structured risk model can therefore transform large quantities of reconnaissance data into actionable security information instead of simply presenting raw technical observations.

Existing research and cybersecurity tools demonstrate the usefulness of automated reconnaissance, asset discovery, vulnerability assessment, and reporting. However, many solutions concentrate on individual stages of the security workflow or require users to combine several tools manually. CyberRecon builds on these concepts by integrating reconnaissance data management, analysis, risk classification, visualization, and reporting into a single defensive framework. The goal is not to replace specialized security tools but to provide a structured layer for organizing and interpreting authorized assessment results.

III. System Analysis

System analysis for CyberRecon focuses on understanding the requirements involved in reconnaissance analysis and security risk assessment. The system must accept an authorized target such as a domain or organization-owned asset for assessment. It should collect relevant passive and controlled reconnaissance information from permitted sources. The collected information may include domains, subdomains, DNS records, IP addresses, services, and technology indicators. The framework should normalize different types of information into a consistent internal data structure. It must distinguish individual assets and observations so that related information can be correlated. A risk assessment module should evaluate findings using predefined security criteria. The system should classify findings into meaningful priority levels to assist analysts. A dashboard should present assets, observations, and risk information in an understandable format. The framework should maintain assessment history so

that analysts can review previous results. Reporting functionality should summarize important findings and recommended defensive actions. Security, authorization, data validation, and responsible use must be considered throughout the system design.

Existing System

Existing reconnaissance and security assessment processes commonly depend on multiple independent cybersecurity tools. Analysts may use separate utilities for domain discovery, DNS analysis, network information gathering, technology identification, and security assessment. Each tool can generate results using its own output format and terminology. Analysts therefore frequently need to manually collect and organize information from different sources. Correlating assets and observations across multiple tools can be time-consuming. Raw reconnaissance results may also contain duplicate, outdated, or low-value information. Many basic reconnaissance utilities focus primarily on information collection rather than risk prioritization. Risk evaluation may consequently be performed manually using separate spreadsheets or assessment documents. Report preparation can require additional manual effort after the technical assessment is completed. Historical comparisons between assessments may also be difficult when results are stored in unrelated locations. This fragmented workflow can reduce efficiency and make consistent security analysis more difficult. CyberRecon proposes an integrated framework to address these organizational and analytical limitations.

Disadvantages of Existing System

- Requires multiple independent cybersecurity tools.
- Produces results in different formats.
- Requires considerable manual data organization.
- Difficult to correlate related assets and findings.
- Duplicate or outdated reconnaissance information may appear.
- Limited centralized risk prioritization.
- Manual risk assessment can lead to inconsistent classification.
- Report generation may require additional effort.
- Historical assessment comparison can be difficult.
- Limited centralized visualization of the external attack surface.
- Analysts may need to switch between several interfaces.
- Difficult to maintain a unified assessment workflow.

Proposed System

CyberRecon is proposed as an integrated framework for authorized reconnaissance analysis and security risk assessment. The system provides a centralized environment for collecting and organizing security-relevant reconnaissance information. It can accept an authorized domain or asset as the assessment scope. The reconnaissance layer gathers permitted information such as domain details, DNS records, subdomains, IP addresses, services, and technology indicators. A processing layer validates, normalizes, and correlates the collected information. The system stores structured assessment data in a centralized database for future analysis. A risk assessment engine evaluates observations using configurable criteria and assigns appropriate priority levels. A dashboard provides visual summaries of assets, findings, and overall risk

conditions. Analysts can review individual findings and examine the information associated with each asset. The reporting module generates structured assessment reports containing findings and recommended defensive actions. Historical records can support comparison between different assessments. The framework therefore provides a systematic and centralized approach to reconnaissance-driven security assessment.

Advantages of Proposed System

- Centralized reconnaissance and assessment workflow.
- Organizes multiple reconnaissance data types in one platform.
- Reduces manual data organization.
- Supports asset discovery and classification.
- Correlates related reconnaissance information.
- Provides structured risk prioritization.
- Improves visibility of externally exposed assets.
- Provides centralized dashboard-based visualization.
- Supports assessment history and comparison.
- Simplifies security report generation.
- Helps analysts prioritize important findings.
- Encourages controlled and authorized security assessment.

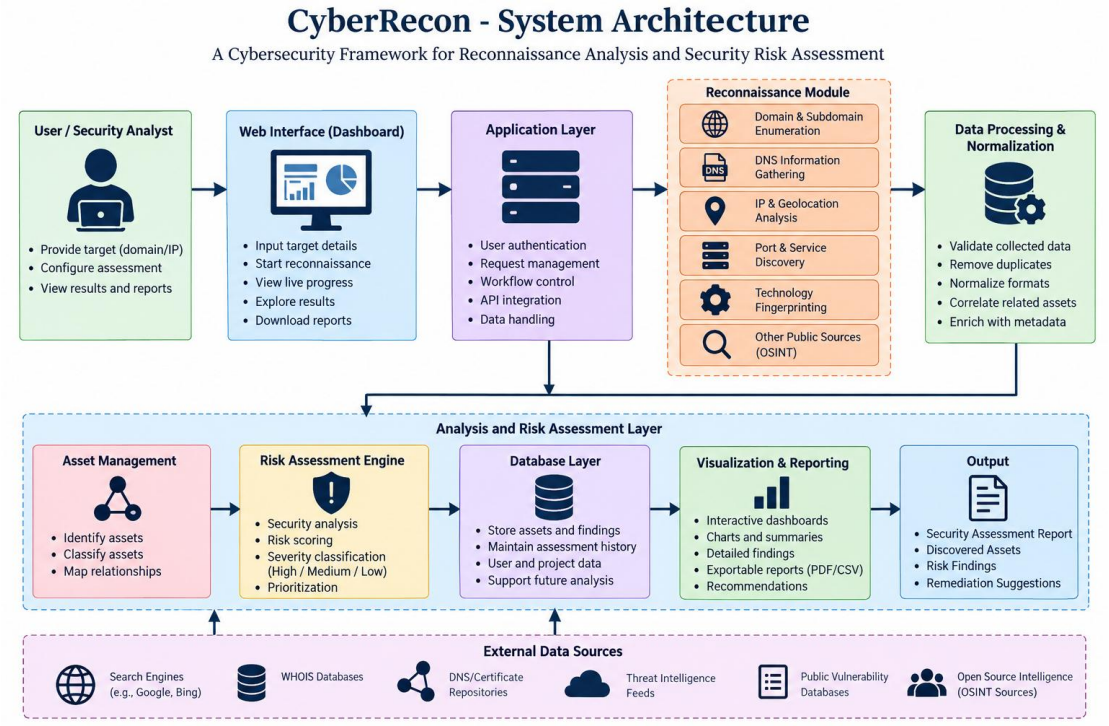
IV. Methodology

The CyberRecon methodology begins by defining the authorized scope of the security assessment. The analyst provides a permitted domain, asset, or organization-owned target for evaluation. The reconnaissance module then collects relevant information using passive and controlled discovery techniques. The collected data is validated to reduce inaccurate or irrelevant observations. Information from different sources is normalized into a common data structure. Related assets such as domains, subdomains, IP addresses, services, and technologies are correlated. The analysis module examines the collected information for security-relevant observations. The risk assessment component assigns priority based on predefined factors such as exposure, asset relevance, and potential impact. The results are stored in a centralized database for structured retrieval and historical analysis. A dashboard presents the discovered assets and risk findings using tables, indicators, and visual summaries. The reporting module converts assessment results into a structured security report. Finally, security teams can use the prioritized findings to guide authorized defensive investigation and remediation.

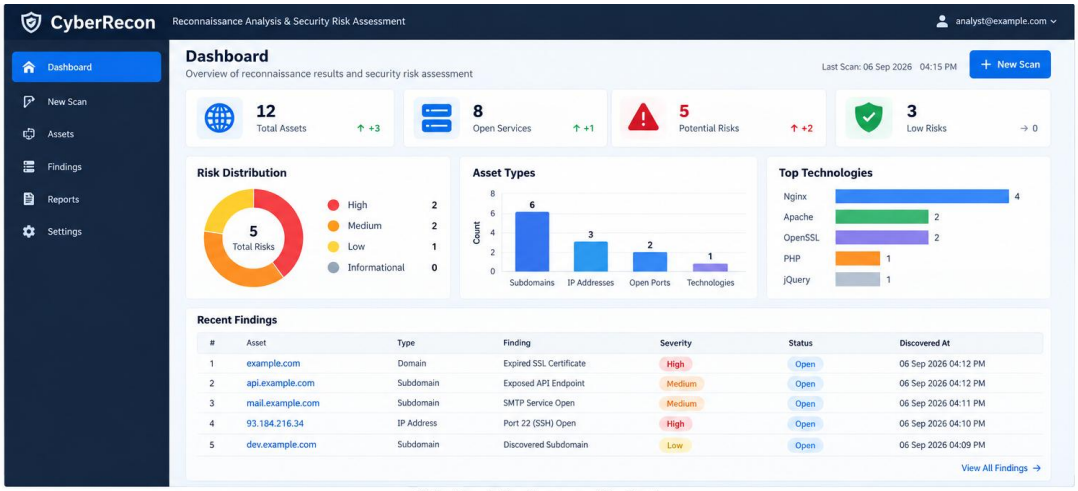
System Architecture

The CyberRecon architecture consists of several interconnected layers that work together to perform reconnaissance analysis and security risk assessment. The User Interface Layer provides a dashboard through which authorized analysts can define assessment scopes and review results. The Application Layer manages authentication, assessment requests, workflow control, and communication between system components. The Reconnaissance Layer gathers permitted information such as domains, subdomains, DNS records, IP addresses, services, and technology indicators. The Data Processing Layer validates, cleans, normalizes, and correlates the collected

information. The Risk Assessment Engine evaluates observations and assigns appropriate risk priorities using predefined assessment rules. The Database Layer stores assets, observations, assessment results, user information, and historical records. The Visualization Layer converts processed information into dashboards, charts, asset summaries, and risk indicators. The Reporting Module generates structured reports containing findings, priorities, and recommended defensive actions. Authentication and authorization controls restrict assessment activities to approved users and scopes. Logging mechanisms maintain records of important assessment activities for accountability. The overall architecture creates a controlled flow from authorized input through reconnaissance, processing, risk analysis, visualization, and reporting.



V. Result and Output



(a) Dashboard - Scan Summary and Key Results

(b) Scan Input (c) Scan Progress (d) Output - Generated Security Report

VI. Conclusion

CyberRecon provides a structured cybersecurity framework for reconnaissance analysis and security risk assessment in authorized environments. The system brings together asset discovery, reconnaissance data collection, information processing, risk classification, visualization, and reporting within a centralized platform. By organizing information such as domains, subdomains, IP addresses, services, DNS details, and technology indicators, CyberRecon helps security analysts obtain a clearer understanding of an organization's externally visible attack surface.

The proposed framework reduces the dependency on disconnected tools and manual analysis by providing a unified assessment workflow. Its risk assessment component helps classify and prioritize security observations so that analysts can focus on findings that require greater attention. The dashboard and reporting features further improve the presentation of assessment results and make the collected information easier to interpret and communicate.

Overall, CyberRecon can serve as a useful foundation for defensive security assessment, academic cybersecurity research, penetration-testing preparation, and authorized attack-surface analysis. Future enhancements can include continuous asset monitoring, improved risk-scoring models, integration with additional threat-intelligence sources, automated change detection, and advanced visualization. With appropriate authorization and responsible use, the framework can contribute to better security visibility and more proactive identification of potential risks.

References

[1] Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine

learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.
[2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.
[3] Sv satyakrishna, shirisha rangu ,bhargavi nalacheruve.(2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm
[4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.
[5] V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, "Real-Time Object Detection in Drone Surveillance Using YOLOv5," in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.
[6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, "Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks," in Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.
[7] R. D. Kumar, V. N. S.Manaswini, "Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology," in Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.
[8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.
[9] Ravi Kumar Banoth, Ramana Murthy B V, "Automatic crop recommendation system using LightGBM and decision tree machine learning models," Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.
[10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.
[11] Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.