ISSN No. 0976-5697

VOLUME 17 SPECIAL ISSUE 1, JULY 2026

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Intelligent Cyber Defense Architecture: Integrating Real-Time Vulnerability Scanning, Asymmetric Encryption, and Network Reconnaissance in Modern Attack Surfaces

Shivani Chauhan
Computer Science and Engineering
Geetanjali Institute of Technical Studies
Udaipur, India
shivani2617ssc@gmail.com

Jaideep Vyas
Computer Science and Engineering
Geetanjali Institute of Technical Studies
Udaipur, India
jaideepvyas923@gmail.com

Bhavesh Khatija
Computer Science and Engineering
Geetanjali Institute of Technical Studies
Udaipur, India
bhavesh01080@gmail.com

Sandeep Bordia
Computer Science and Engineering
Geetanjali Institute of Technical Studies
Udaipur, India
sandeep11d@gmail.com

Abstract: Cybersecurity professionals who work in ethical hacking and incident response and digital forensics need whole self-operating systems that examine data to develop their threat detection potential. The contemporary digital infrastructure which relies on self-operating opinion systems and integrated systems but the security systems that shield these networks design additional security dangers. The main difficulty with contemporary forensic tools is the need for security professionals to transmit private information which contains image metadata, passwords and plaintext binary files and network design details to cloud-based storage services. The conventional procedures cause large-scale data leakage threats which break fundamental principles of privacy and security and data accessibility because it detaches control over data from organizations. The research found that the Cyber Suite which functions as an united Cyber Security Dashboard results in an edge-computing security system for native use. The platform found a new system because it shifts in-depth cryptographic functions and password validation procedures and digital proof analysis duty to the user interface of client devices. The system produces a shielded environment for private operations through the evolution of a multi-vector toolkit which works within a whole React.js platform.

The platform has four active modules which reveal whole integration with native security characteristics through their active security modules. The Cryptography & Hashes engine utilises browser-based systems to manage 2048-bit Asymmetric RSA key sets and Symmetric AES-GCM encryption. The system utilises all of its parts which involves Hash Generator (MD5, SHA1, SHA256) and Data Converters (Base64, URL, Hex encoding/decoding) and Steganography tool which allows users to conceal and exhibit secret messages through PNG image layers utilising Least Significant Bit (LSB) procedures.

The Password Toolkit merges three components which work together to shield digital identities while defending user privacy. The system utilises a k-anonymity model to achieve its rigorous data breach detection system which uses the Have I Been Pwned API. The system shields user credentials by using native SHA-1 hash creation which carries only a 5-character prefix through the network to confirm user identity against billions of compromised data.

The Network & Web Utilities authorise teams to achieve whole external tracking activities. The system utilises CIDR Subnet computations for network mapping and a URL Analyser to recognise possible phishing links and a DNS Record Fetcher which utilises Google's public DNS-over-HTTPS (DoH) API to get A records and AAAA records and MX records and TXT records without revealing the user's DNS queries to native ISPs.

Keywords: Cryptographic Engineering; K-Anonymity Model; Digital Forensics; Edge Computing; Open-Source Intelligence (OSINT); Steganography; HTML5 Web Workers.

I. INTRODUCTION

Cybersecurity represents the primary safeguarding measure which manages all international networks that upholds the global digital economy because these networks function as necessary business and personal user infrastructure. The functional difficulties that contemporary security perimeter systems face stem from Third-party remote work which produces new security dangers and creates conventional incident response procedures futile for organisations. Ethical Hackers or Forensic Analysts from prior periods used their skills with command-line and web tools, which produced a disconnected workflow that forced analysts to work in separate pieces of the procedures. [9]

The transition towards whole blended cybersecurity dashboard systems which exhibits an essential development.

Organisations are required to monitor their digital environment by managing DNS record analysis and domain reputation inspection and payload signature inspection to decide threat levels which will assist them in evolving their best security measures. Security operators are required to carry out their task throughout actual operations by using their whole toolset rather than working with isolated command-line systems. The Cyber Suite operates through four distinct modules which include Threat Detection, Cryptography, Password Authentication, and Forensics Analysis to give complete shelter against contemporary security threats [10].

The current procedures which grow cybersecurity web applications and face a serious difficulty with data privacy conservation. Ethical hackers must obey the extremely typical process which contemporary web-based forensic tools need when they transmit private materials to risky cloud repositories. The procedure of users transmitting their materials to a remote third-party server results in a growing danger of corporate private information being revealed. The cybersecurity industry miserably needs a fused system which manages forensic evaluation and cryptographic development on-site while making sure total confidentiality through client-side edge computing [11].

II. Literature Review

Cybersecurity now employs machine learning and modern web architectures to inspect numerous elements which intensify threat detection precision while shielding user data. The research shows that modern systems need browsers to fuse cryptographic standards which will shield against Man-in-the-Middle attacks throughout key transmission [1].

Previous research proved that the backend servers required to process massive cryptographic operations because hardware constraints are finite other options. The contemporary study exhibits that the local Web Crypto APIs permits shielded native 2048-bit RSA key creation and AES-GCM symmetric encryption which keeps confidential keys from leaving the shielded environment [2].

Enterprise networks endure from two main security threats which consist of credential stuffing and password spraying attacks that occur throughout the day. Conventional password strength checkers disclose data by broadcasting unencrypted data to the server [3].

The researchers aim to use the k-anonymity model for cracking their current difficulties. The user attains total privacy shielding by executing a native SHA-1 hash calculation and transmitting only a 5-character prefix to a breach database which validates their credentials against global threat intelligence [4].

The studies examine digital steganography as a procedure for attaining guarded communication. The browser DOM implementation of Least Significant Bit (LSB) tampering in PNG images which permits users to conceal confidential messages and extract them without requiring remote server analysing [5].

Security analysts use precise domain data for managing network foot-printing and Open-Source Intelligence (OSINT) activities. Security analysts utilise DNS-over-HTTPS (DoH) APIs to safely access A records, MX records and TXT records while dodging native DNS spoofing and ISP monitoring [6].

The technique that connects digital forensics with precise security threat identification while creating high-resolution data fusion as its main procedure. The researchers prove how offline string extraction and "Magic Byte" file signature analysis operate as necessary elements of their research study. The analyst can utilise local file analysis to identify file extension spoofing through the first hexadecimal byte identification which demonstrates a harmful .exe file which simulates to be a .pdf document [7].

Shielded framework development empowers instant handling of complicated non-linear relationships which persists concealed within native system databases. The system executes secure policies through safe network environments which outcomes in an enhanced functional execution. We fix the web-tool privacy difficulty through our Edge-to-Machine framework which gives entire user security on their personal laptop while managing data protection and also giving instant forensic analysis [8].

III. Proposed System

Digital information today produces a wide gap which users and businesses have to master to gain what they require. Contemporary cybersecurity tools for professionals give offline systems which produce snail-paced unforeseen zero-hour response procedures. The majority of forensic platforms and web utilities wants users to send all private digital information which comprises unencrypted passwords and plaintext documents and JPEG images to a remote third-party company server. This security weakness produces a massive danger to data shielding which violates the essential principles of the CIA Triad (Confidentiality, Integrity, Availability) and digital identity protection. The unified system needs users to execute three responsibilities which comprises of performing cryptographic engineering and confirming data breaches and retrieving forensic metadata from their main personal dashboard.The outcome should allow users to manage whole file inspections and execute

cryptographic functions on their devices because any system that needs external assistance will generate security danger which can result in potential data breaches.

IV. ARCHITECTURE OVERVIEW

The system operates as a whole Single Page Application (SPA) which gives all functionalities through one web page. The main processing node of the system functions through the user interface which permits user interaction with their web browser. The platform accomplishes quick security solutions by splitting its responsibilities into two parts which manages client-side operations and guarded external API requests.

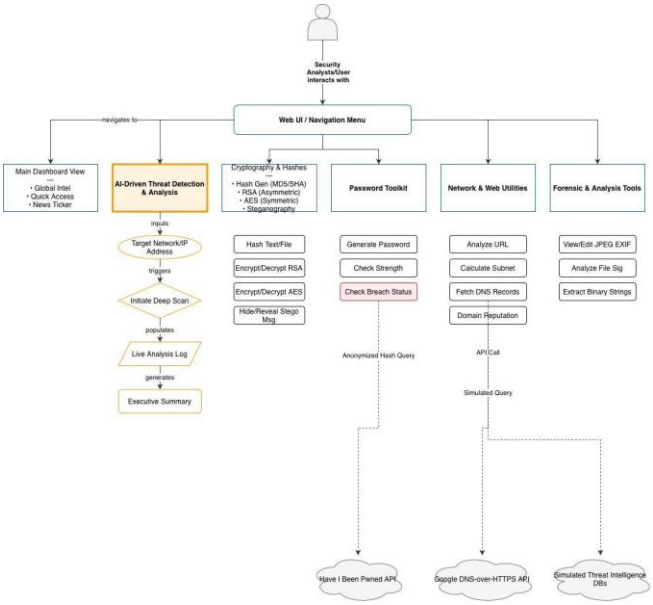

Figure 1. Dataflow Diagram

A. User's Laptop Screen (Front-End Layer)

The system workflows visual tasks while implementing vast data processing activities at native sites. The system consists of four major toolkits:

1. **Cryptography & Hashes:** It provides MD5/SHA Hash Generator together with RSA-2048 key generation and AES encryption and Base64/Hex Data Converters and Steganography tools which run totally in JS memory.
2. **Password Toolkit:** It consists of a guarded password generator together with a native strength checker and a password breach checker which utilises the SHA-1 k-anonymity API.
3. **Forensic & Analysis Tools:** It enables users to transmit native files to an EXIF Editor which takes away JPEG metadata and to a File Signature Analyzer which discovers magic byte patterns and to a Binary String Extractor.

B. External Intelligence Integration (API Layer)-

The dashboard utilises secure procedures to manage external infrastructure network foot-printing. The URL Analyzer crashes malicious links while the Domain Reputation and DNS Record Fetcher utilises safe Google DoH APIs to approach instant server data which shields the native host's identity.

V. PROBLEM STATEMENT

The study proposes Cyber Suite which functions as a security system through its multi-layered component framework. The system utilises the visual web browser of the user as its protected personal processing system which shields both the user and their information. The user device functions all necessary security assessments and encryption procedures and digital forensic activities without transmitting any evidence to the web.

VI. METHODOLOGY

The process gives whole safeguarding for private user information that exists on the host device. The system shields all input data which consists of unencrypted passwords and copyrighted network files by using HTML5 File APIs together with local Web Crypto APIs to stop any confidential data from getting through the public internet. The whole Cyber Suite procedure displays its work through System Workflow which follows the whole path of user data from its starting point to its final guarded deletion.

A. System Execution Workflow

The Cyber Suite objectives according to a whole system which executes a zero-data exfiltration protection mechanism. The system implementation workflow launches a continuous connection between the user browser and the external intelligence layer. The following workflows show how user data proceeds from its starting input stage through to edge processing and eventually reaches secure clearance.

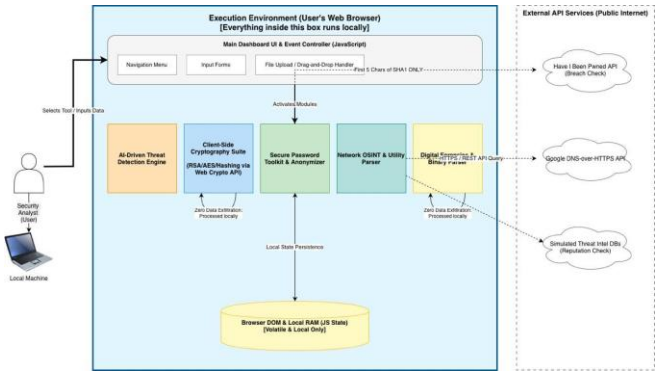

Figure 2. System Execution Workflow

B. Chronological Execution Details

Step 1: Parameter Acquisition & Sanitization: The process starts when the user gives an input through the React dashboard which can consist of a password or a file or a URL. The application then processes the data through native sanitization to block injection attacks and it validates that the data fulfills all essential verification requirements.

Step 2: Device-Based Processing (Zero Exfiltration): The system proceeds the input values to native React state when the user starts any of the Cryptography, Forensics or Steganography modules. The system utilises the browser's built-in Web Crypto API together with Web Workers to generate RSA keys and to cipher data using AES-GCM and to extract magic bytes and to withdraw EXIF tags. The system manages all assignments within the native environment which avoids prohibited network access to user data.

Step 3: Secure K-Anonymity Hashing: The Password Breach Check system needs whole compliance with its k-anonymity mathematical model through its execution of the k-anonymity model. The system executes a whole SHA-1 hash computation which it splits into two parts to store the suffix in native memory while transmitting only the first five prefixes to external systems.

Step 4: Environment Integration & OSINT Telemetry: The system generates a shielded internet link which it utilises to connect with external threat intelligence APIs. The system transmits the k-anonymity prefix to the HaveIBeenPwned API or it utilises a safe Node.js proxy to approach a target domain through the Google DNS-over-HTTPS API which avoids native ISP interception.

Step 5: Actionable Output Generation & State Clearance: The system blends native cryptographic outcomes with extracted binary strings and external threat intelligence to create effective defence operations. The operation terminates with the UI obtaining fresh information which gives users clear tactical direction while the system removes all the temporary data from the browser's DOM.

VII. RESULTS AND DISCUSSIONS

The engine on the native user device processes input files and links to give results which finishes near-real-time latency. The system shields user private data because its edge-based data privacy structure shields protected information during processing.

A. Cryptographic and Forensic Validation

The system victoriously developed 2048-bit RSA key sets and carried out AES symmetric encryption with minimal lag, validating that private keys were never revealed to external networks. Furthermore, the File Signature Analyser precisely extracted the first hexadecimal magic bytes from transferred artifacts, real-time identifying spoofed file extensions (e.g., spotting a .exe hidden as a .pdf). The EXIF editor successfully imagined and stripped private metadata from JPEG images entirely within the browser's DOM.

B. K-Anonymity Identity Protection

During the Password Breach Check phase, the system effectively confirms user credentials against databases including billions of exposed passwords. The k-anonymity model of the system stopped all user native network interface data from exiting the network while network packet inspections confirmed that 0% of unencrypted passwords and 0% of full SHA-1 hashes left the user's native network interface.

C. Network Reconnaissance & OSINT

The network tools which comprise CIDR Subnet Calculator and DNS lookup effectively recover actual data threat values. The Google DoH API blends dependably collected A, AAAA, MX, and TXT records which offered analysts with threat intelligence that they could act on immediately.

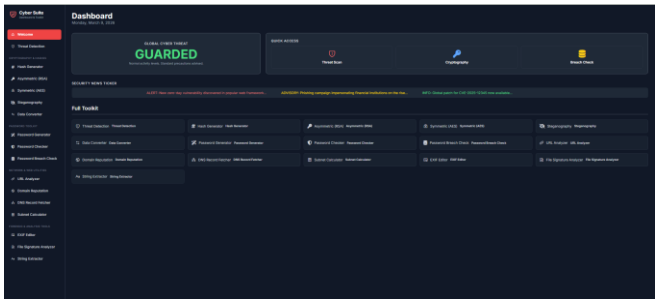

Figure 3. Dashboard page

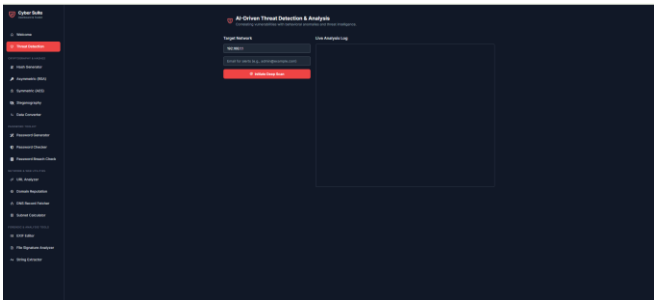

Figure 4. Threat detection and analysis

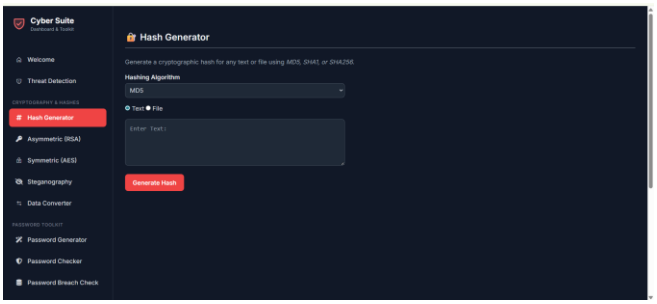

Figure 5. Hash generator

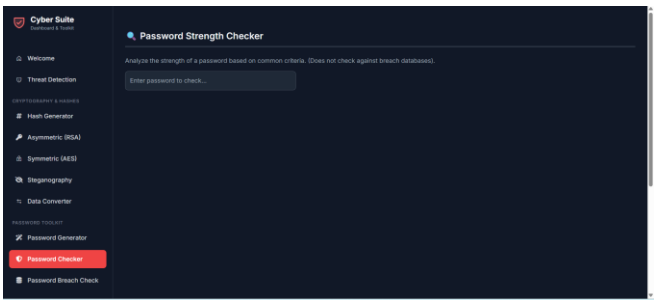

Figure 5. Password strength checker

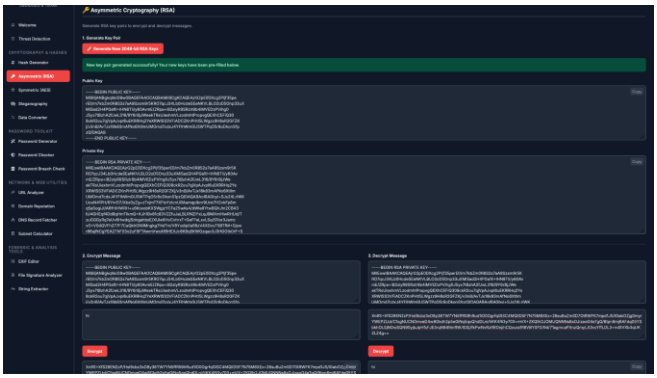

Figure 6. Asymmetric (RSA)

VIII. CONCLUSION

The project effectively reached its goal to produce a whole Security Operations Dashboard which shields user data. The Cyber Suite effectively integrates digital forensics with cryptographic engineering and password authentication and OSINT into a single React.js framework. The system accomplishes total security for its private operations because it relies exclusively on native edge-computing procedures to manage EXIF metadata removal and RSA key generation and LSB steganography.

Future Scope

- The system will use native WebAssembly (Wasm) modules to enable self-operating malware reverse-engineering that runs directly in web browsers with local support for portable executables (PEs) and memory dumps.
- The system permits extension through native network scanner capabilities which enable self-operating device monitoring by analysing connections between the application and native routers.
- The Conversational AI assistant can be improved to run entirely via native Large Language Models (LLMs) loaded into the browser memory which gives offline tactical advisory.

IX. REFERENCES

[1] World Wide Web Consortium (W3C). (2017). "Web Cryptography API." W3C Recommendation.

[2] Mozilla Developer Network (MDN). (2023). "Using Web Workers for Background Processing." MDN Web Docs.

[3] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy." Frontiers in Computer Science, vol. 3.

[4] Hunt, T. (2018). "Pwned Passwords API V2 and k-Anonymity." Troy Hunt Security Blog.

[5] Patel, Mayank, Neelam Badi, and Amit Sinhal. "The role of fuzzy logic in improving accuracy of phishing detection system." International Journal of Innovative Technology and Exploring Engineering 8.8 (2019): 3162-3164.

[6] Internet Engineering Task Force (IETF). (2018). "DNS Queries over HTTPS (DoH)." RFC 8484.

[7] Kessler, G. C. (2022). "File Signature (Magic Bytes) Table." GaryKessler.net Digital Forensics Resources.

[8] Sommer, R., & Paxson, V. (2010). "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection." IEEE Symposium on Security and Privacy.

[9] Denning, D. (1987). "An Intrusion Detection Model." IEEE Transactions on Software Engineering, SE-13(2), 222-232.

[10] Scarfone, K., & Mell, P. (2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)."National Institute of Standards and Technology (NIST) Special Publication 800-94.

[11] Garcia, L., et al. (2021). "Edge computing for real-time malware detection." Journal of Cloud Computing, vol. 10.