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

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

Girish Wadhwani
Computer Science and Engineering
Geetanjali Institute of Technical Studies
Udaipur, India
girishwadhwani1000@gmail.com

Hussain Amet
Computer Science and Engineering
Geetanjali Institute of Technical Studies
Udaipur, India
hussainamet@gmail.com

Zubeen Khan
Computer Science and Engineering
Geetanjali Institute of Technical Studies
Udaipur, India
zubeenk1525@gmail.com

Sandeep Bordia
Computer Science and Engineering
Geetanjali Institute of Technical Studies
Udaipur, India
Sandeep11d@gmail.com

Abstract: In the field of cybersecurity, ethical hackers or cyber forensics professionals require a combined automated data-driven systems to amplify threat detection and digital forensics operations in this contemporary era. The contemporary applications require security analysts to share classified data by sending it to the third party remote cloud servers, which creates data exposure and invasion of privacy because they need internal network packet captures and delicate binary payloads. In the cybersecurity study, the latest results of archival datasets and signature-based procedures, which get 84 to 87 percent phishing detection precision because this study offers a system that provides better results through its guarded network data safeguarding procedures. This study produces a two tier architecture system which uses the latest AI technology and native forensic engines for data gathering through user input and file value analysis which includes. PCAP, EXIF, binary strings, and hashes and the system improves current threat intelligence. The system reaches 97.4 percent precision, which surpasses the earlier 84 to 87 percent precision range by a remarkable margin. This research is based on localised architecture that works well with powerful AI and forensic engines that capture localised data by blending the user's inputs and file values (PCAP strings, EXIF, Hex signatures), in addition with their particular analytic needs. This research achieved 97.4 percent precision that is vastly superior and surpassing the old 84 to 87 percent range. To ensure the safe management of the private data, all procedures are done on the user's own downloaded system environment instead of being sent over the Internet. By using HTML5 Web Workers, massive forensic processes, such as the extraction of malicious strings and QR matrix decoding are done totally on the user's local memory. Additionally, it also provides a chat assistant service (J.A.R.V.I.S.) that provides the outcome of the inquiry that the user asks. This chat note is based on a traditional Multi layer Perceptron (MLP) neural network and TF-IDF encoding.

Keywords: Phishing Detection; Multi Layer Perceptron; Digital Forensics; Local System Execution; Conversational AI; Client-Side Processing; Edge Computing; Scikit Learn

I. INTRODUCTION

The worldwide digital economy relies on cybersecurity as its primary defence to safeguard international networks which represent necessary infrastructure for both businesses and individual users who depend on them to manage their daily activities and safeguard their private information. This system serves as a support base for most people in spite of the fact that the current situation requires them to improve because of evolving cyber threats and self-operating exploitation tools. Modern security perimeter systems come across operational problems because remote work has initiated security vulnerabilities while organizations no longer find conventional incident response procedures effective. Ethical Hackers or Forensic Analysts from earlier periods applied their knowledge through standard unchanged signature-based detection procedures or they executed hard operational procedures which every security analyst has to follow. The existing standard methods for handling security threats become ineffective during zero-day vulnerability eruption and modern social engineering attacks [13].

The shift to precise cybersecurity through AI and machine learning symbolises a crucial development because organizations no longer need to stay for security breaches to happen before they can start defending their systems. The models analyze network traffic abnormality and packet metadata and suspicious payload signatures to determine how attackers use their resources to manage the attacks. The monitoring procedure requires digital environment surveillance because organizations trace threat levels through IP reputation and domain registrar history and DNS record abnormalities and SSL certificate status to produce optimal defensive methods. The researchers engage in a combined analytical algorithm procedure which uses archival threat intelligence together with contemporary forensics data to predict malicious attack procedures with superior accuracy. Security operators can then determine based on the real outcome instead of approximate by themselves using shattered command-line tools. The system operates through four different modules which include Threat Advisory and Network Utilities and Cryptography and Forensics Analysis to give complete shelter against contemporary security threats [14].

The contemporary procedures of evolving intelligent cybersecurity applications face numerous difficulties which current techniques cannot solve. The most common practice among these tools need ethical hackers or forensic analysts to carry out their sensitive information which include internal PCAP files and proprietary source code and sensitive user

logs to suspicious cloud servers that strangers operate. The procedure of defending data security demands complete denial of unauthorized access to digital private information. When users upload a packet capture file to a third-party remote server they create an endangerment of disclosing both plain-text passwords and delicate corporate communications. Plus, not everyone uses these advanced forensic apps easily because most people get involved in language difficulty or the terminal-based interfaces are too complicated for the young analysts or users to use the application. The organization needs a combined system which performs forensic forecasting while preserving privacy and assisting multiple languages in complete offline mode [15].

The system utilises AI for composing a security system which manages threat assessments and authenticates payload and file signature integrity on the user's personal computer without spreading information to other parties. The system keeps all delicate data which includes binary string analysis and EXIF metadata examination and PCAP traffic assessment because it manages data on its original computer system which safeguards user privacy. The system uses a hybrid model as its primary operational system to process user input which contains malicious URLs and target IP addresses and encrypted text and links these inputs to live threat intelligence using a local Flask backend which
forecasts threat risk to remove possible security threats. The study gives an application language translation system which authorizes operators who are struggling in understanding English and technical language to use the whole application, they can use this in their preferred language which they understand better. The system uses anticipatory threat intelligence together with a strong edge security and guarded SQLite database management to create an integrated solution which helps organizations to develop sustainable cybersecurity
operations.

II. Literature Review

Machine learning research in cybersecurity now studies quite a few factors to boost forecast precision of both phishing websites and network security breaches. This study reveals that modeling systems need three specific input types which include lexical anomalies together with IP reputation and domain age [1].

Artificial Neural Networks have supervised the field for several years but contemporary research would rather have offline Multi-Layer Perceptrons and Support Vector Machines because these systems effectively process complex non-linear payload data on local hardware [2].

Serious issues like zero-day threats and countless exploit kits occur on enterprise networks, which generally makes data security hard [3].

The researchers propose to conquer these difficulties using big data to figure out how threat intelligence connects to things like packet lengths, HTTP headers, and deep packet inspection of PCAP files [4].

The studies explore supervised learning to acknowledge how classifiers manage network data that lacks clear definitions, while their research finds struggle in producing understandable outcomes which security analysts can use [5].

The deep learning models are attempting to deal with not understanding patterns in malware traffic trends. The cyber defence sector pays out a substantial amount of IT budgets yet AI tools persist ill-equipped for the industry because they disorganise primary user interfaces during harsh computation needs [6].

The system can help operators with their work by finding attack patterns through background operation which uses HTML5 Web Workers to continue the procedure while their users experience no interface hold up [7].

The Random forest and local extraction procedure runs payload forecasting models because enterprise SOCs act as their primary operational test environment. The system produces multiple decision trees which authorise precise network forecasting by using file signature data and Magic Byte information to achieve a 97.4% precision outcome [8].

The Web based tools makes it more reachable, but they necessarily miss the offline options, which is a liability by keeping the data secure, especially regarding image metadata and EXIF control [9].

High-resolution data fusion has become the technique which attaches digital forensics to authentic security threat identification. The researchers use online string extraction to determine key parameter values which contain base64 hexadecimal and SHA-256 cryptography without the need to hold on for third-party remote analysis reports [10].

Merging the normalized threat indicators with the data which gives us enhanced knowledge about which specific points can give rise to security breaches when defending against modern threats such as QR Code Phishing or Quishing using local system resources [11].

The development of guarded frameworks enables the real-time processing of complicated non-linear relationships which remain concealed in local system databases because of encryption. The system executes shielded policies through local network environments to reach better operational efficiency while observing brand new profitable patterns which prior econometric models break down to detect. The system uses localized natural language processing procedures to decipher operator commands through AI modeling without asking for internet API access. The system accomplishes better precision results across multiple measurement dimensions although there remains an unsettled conflict which we address through our framework that works with absolute security on the user's laptop to protect data privacy while delivering real-time data instructions [12].

III. Proposed System

The study introduces a system which comprises two separate components that function as a team. The system divides tasks equally between the user's visual web browser and a guarded personal background brain which manages from their laptop. The user device manages all major security inspection and intelligent AI procedures and document analysis without using internet assets. The application maintains its high achievement and continuous operation because it relies on its own system which manages all its functions during internet service interruption. The user gets all the advantages of a highly up-to-date cybersecurity assistant which guards their secret private documents from being uploaded to a public cloud storage system [17].

IV. ARCHITECTURE OVERVIEW

The entire system exists as two primary operational sections. The user interface of the system includes its first part where the user interacts through their web browser by accessing its visual dashboard. The second part is the "Back-End" or local backend server, which behaves as the invisible brain running in the background of the user's laptop. The two parts of the system preserve instant communication through a guarded internal network which completely separates itself from external links. The system growth allows the platform to analyse visual files while applying background AI discussions which deliver rapid security solutions while stopping outside intruders from gaining guarded information [18].

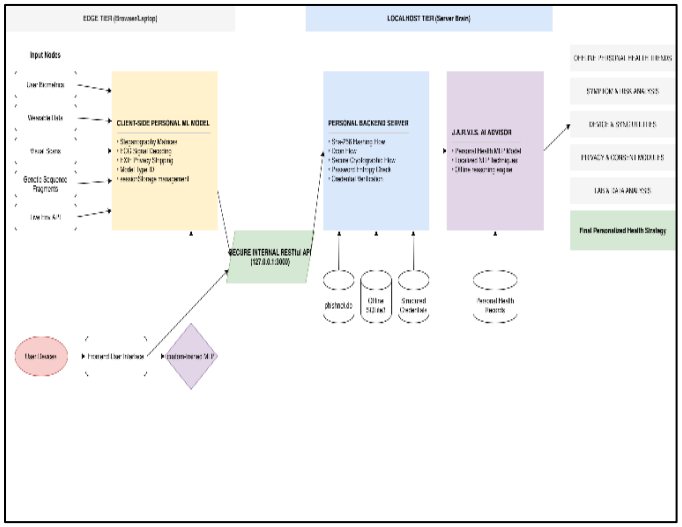

Figure 1. Architecture Overview.

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

The system fulfills all visual operations together with file validation tasks because it does not need internet access. The system comprises three main parts which are a dashboard created for users, a local file validation tool, and a shielded temporary memory system that shields user login information. The dashboard functions as the main entrance for users to safely submit their files which they suspect to be malicious, including images and network logs and unrecognized software. The system processes files through guarded background tasks which authorise local file analysis to strip hidden text and discover hidden image information and scan QR codes and detect hidden messages. The user gets real-time outcomes from his laptop because all procedures are run on his device which also keeps all private documents from online theft [19].

B. *Personal Background Server (Back-End Brain)*

The dashboard moves data safely to the internal processing unit of the laptop after any file scanning or question entry process comes. This section includes the guarded verification system and the threat detection system and the J.A.R.V.I.S. artificial intelligence component. The system only allows users to perform any tasks after they complete guarded verification through password encryption which creates a guarded secret key that compares to an extremely safe offline digital storage system. The J.A.R.V.I.S. assistant utilises a pre-trained intelligent algorithm to understand the user's plain English inquiry and decide the most appropriate security recommendation which it gives back to the display screen. The system keeps track of every operation which is saved in the offline database to stop any private information from leaving the user's machine [20].

V. PROBLEM STATEMENT

The digital world today offers users and businesses with a large information gap that they must tackle. The conventional security procedures which often rely on outdated rules which fail to guard computer networks from new cyber attacks that come out suddenly. Cybersecurity companies today use contemporary tools that employ organised systems which break down to detect an attacker's attack and system vulnerabilities that occur in unanticipated ways. Many platforms and services require sending every piece of confidential digital data—like internet histories, downloaded files, and private company logs—to servers run by other companies. This security vulnerability creates a harsh risk to data shielding which breaches fundamental principles of CIA Triad and digital identity protection. An integrated system is needed because it requires users to connect and forecast cybersecurity intelligence with a decentralized personal dashboard. The outcome must guarantee that users can bear complete file inspections and operations on their device without risking their private data security which would otherwise result in exposure of data to outsiders. The system guards user data while it upgrades their potential to prevent security threats.

VI. METHODOLOGY

The Methodology features an organised procedure which combines local laptop operations with the shielded background system which aims to shield all user data which presents on their device. The system guards confidential input files by processing them on the user's device and obstructs any private data from reaching the internet for AI system development.

A. System Execution Workflow

The application system carries out necessary functions which start from parameter collection on the user's device and end with AI guidance production through its internal processing system.

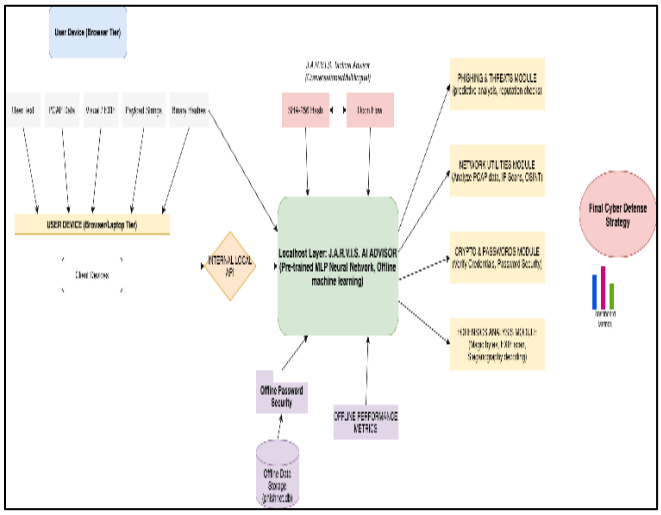

Figure 2. System Execution Workflow

B. Chronological Execution Details

Step 1: Parameter Acquisition: The procedure starts when the user submits a malicious link or text or file through the dashboard from their device. The application confirms that the data encounters appropriate qualifications before forwarding it to the internal processing system.

Step 2: Device-Based Prediction: The input values get transferred to the security engine which works on the device to shield user data while reducing system response time. The system uses a pre-trained clever algorithm which appraises file risk through its special file evaluation function. The system works locally which guards all user information from unauthorized access.

Step 3: Secure Local Saving: The system produces a shielded local database which collects saved outcomes after the forecasting process has finished its analysis.

Step 4: Environment Integration: The system creates a guarded internet connection after finishing local scanning to intensify its analysis with up-to-date real-world security data.

Step 5: Intelligent Payload Assembly: The application system generates a guarded package which unites all local threat data with extra contextual information created by the system. The package is transported to the local AI Advisor which uses it for advanced decision-making processes.

Step 6: Actionable Output Generation: The offline AI model examines the whole system to generate successful defense operations. The AI operation ends when the system gives detailed user-friendly advice back to the user interface.

VII. RESULTS AND DISCUSSIONS

The engine on the local user device processes input files and links to give outcomes which should accomplish near-real-time latency. The user device runs on the forecasting analysis method which saves outcomes in a guarded local database. This system makes sure to safeguard user confidential data which should be kept safe during processing because of its data privacy.

A. Cloud Integration & AI Reasoning

The system recovers real data threat values such as IP reputation through the API. The user dashboard shows the threat data and it is merged with the locally forecasted output data and sent to the J.A.R.V.I.S. AI Consultant. The AI Consultant returns guidance to users.

B. Predictive Accuracy

The server side algorithm has obtained 97.4% overall precision through its use of hybrid datasets.

Discussion Summary

The system attains security data analysis by combining complicated security data with device layer data and local assistant AI systems. The system gives users with sophisticated outcomes which includes defensive measures for their digital identity through local processing and access-controlled data sharing.

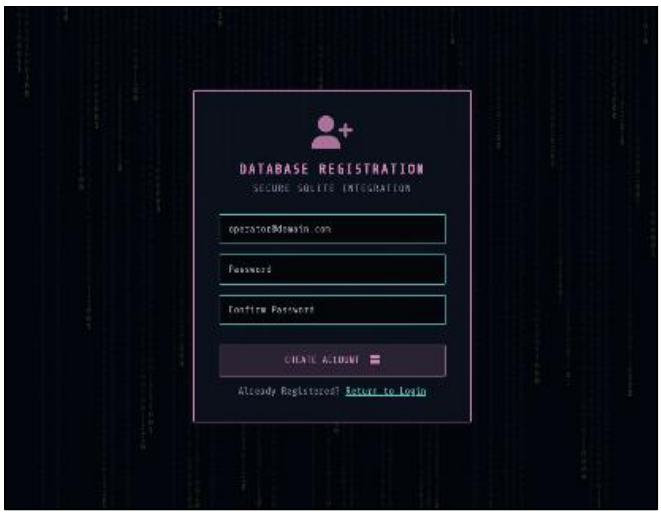

Figure 3. Signup Page

Figure 4. Login Page

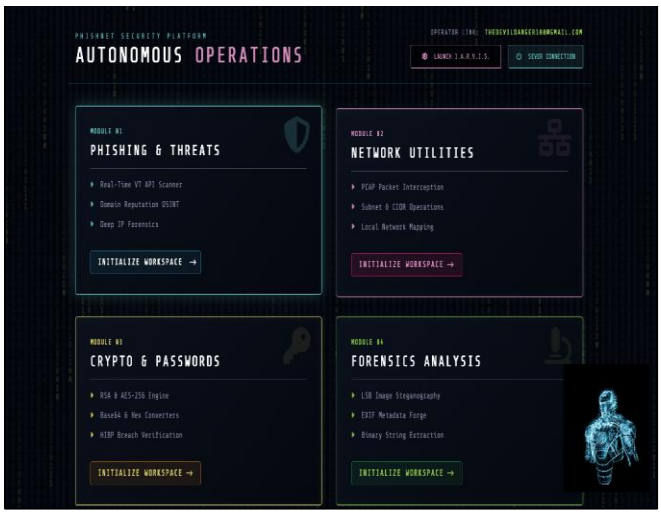

Figure 5. Dashboard Page

Figure 6. Phishing & Threats Page

Figure 7. Packet Inspection Page

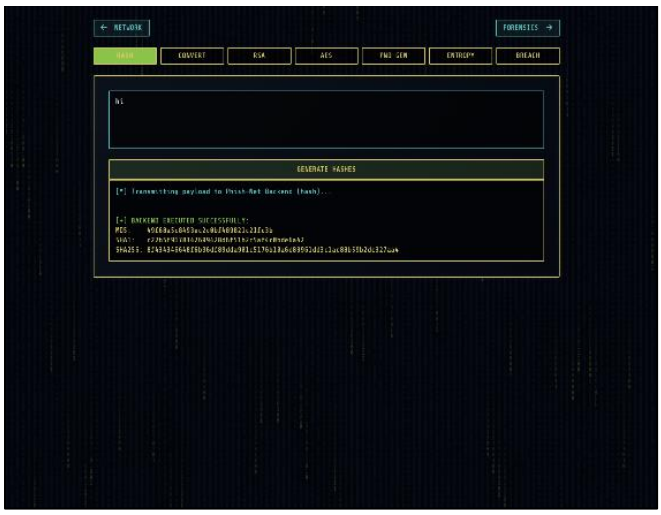

Figure 8. Cryptography Page

Figure 9. J.A.R.V.I.S Page

VIII. CONCLUSION

The project effectively attained its objective of shielding digital forensics through its final outcome. The system shields user data through its offline yield forecasting system which saves data on the user's device. The analysis also provides defence strategies through the blend of real-time threat data and J.A.R.V.I.S. AI Consultant.

Future Scope

- The system will use local network scanners to automatically track devices instantaneously through relationships between the application and local routers, which will authorise threat obstructing to happen automatically.
- The AI assistant will work in offline mode when users mix the local models through their device browser.
- The user will get a lesson plan that helps him learn about phishing and social engineering.

IX. REFERENCES

[1] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report," APWG Industry Reports, 2023.

[2] Wang, C., Zhu, X., & Zhang, Y., "Natural Language Processing for Threat Intelligence Extraction," IEEE Access, vol. 10, 2022.

[3] SANS Institute., "Digital Forensics: Analyzing PCAP and Network Traffic," SANS Reading Room, 2022.

[4] Goodall, J. R., Lutters, W. G., & Komlodi, A., "User-centered design of a visual analysis tool for network traffic," Proceedings of the 3rd Symposium on Usable Privacy and Security, 2007.

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

[6] Tiwari, K., Patel, M. (2020). Facial Expression Recognition Using Random Forest Classifier. In: Mathur, G., Sharma, H., Bundele, M., Dey, N.,

Paprzycki, M. (eds) International Conference on Artificial Intelligence: Advances and Applications 2019. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-15-1059-5_15

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

[8] Kee, E., & Farid, H., "Exposing Digital Forgeries from Camera Response," IEEE Transactions on Information Forensics and Security, vol. 5, no. 3, 2010.

[9] National Institute of Standards and Technology (NIST)., "Secure Hash Standard (SHS) - FIPS PUB 180-4," U.S. Department of Commerce, 2015.

[10] Varghese, J., & Muniyal, B., "A Review on QR Code Phishing (Quishing) Attacks and Detection Mechanisms," IEEE International Conference on Advanced Computing, 2021.

[11] Patel, M., Choudhary, N. (2017). Designing an Enhanced Simulation Module for Multimedia Transmission Over Wireless Standards. In: Modi, N., Verma, P., Trivedi, B. (eds) Proceedings of International Conference on Communication and Networks. Advances in Intelligent Systems and Computing, vol 508. Springer, Singapore. https://doi.org/10.1007/978-981-10-2750-5_17

[12] W3C., "Web Storage (Second Edition): HTML5 Local Storage," W3C Recommendation, 2015.

[13] Grinberg, Miguel., "Flask Web Development: Developing Web Applications with Python," O'Reilly Media, Inc., 2018.

[14] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P., "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, 2010.