WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Integrating Finger Vein Biometrics and Visualization for AI-Resilient Cyber Defence

Mr. C. Ganesh[1], Ms. R. Hemadharshini[2]

[1]Assistant Professor, Department of MCA, (Vivekanandha Institute of Information and Management Studies).
[2]Student, Department of MCA, (Vivekanandha Institute of Information and Management Studies).

ABSTRACT

AI-powered cyber-attacks are becoming more advanced and effective, impacting nearly every phase of modern cyber defense efforts. Traditional cyber security defences struggle to detect AI-Enhanced cyber-attacks, which autonomously exploit system vulnerabilities without human intervention. Existing security models face challenges in distinguishing benign and malicious activities due to complex decision boundaries and limited sample datasets. For example, in the process of gathering information before an attack, AI-Enhanced tool such as MalGAN can be deployed. This types of tools automatically find weak spots in security systems on their own without needing a human hacker to guide them in cyber-defence systems. However, existing countermeasures cannot detect the attacks launched by most AI-Enhanced tools. This paper introduces an initial step toward defending against AI-driven cyber threats through the use of data fingerprinting and visualization techniques. The proposed methodology, called AI-Enhanced Cyber-Defense Systems (AIECDS), focuses on integrating these techniques to strengthen cybersecurity frameworks. By using fingerprinted data and visual analysis applied here through the Finger Vein Dataset the system aims to enhance threat detection capabilities. One of the key benefits of this approach is its ability to simplify the decision-making process for machine learning models by reducing the complexity of decision boundaries, making it easier to distinguish between normal and malicious activity. The processed data is then analyzed by comparing acquisition Images with Model Images to generate structured image templates. These fingerprinted data and visualization techniques helps in simplifying the machine learning models, improving detection efficiency even for malicious threats with limited sample sizes. The work was validated by demonstrating how the fingerprints extracted from the Finger Vein Dataset enable the visual discrimination. The validation process involved comparing Acquired Images and Model Images, generating structured image templates that highlight anomalies. This approach was applied as a use case for cyber threat discovery through fingerprint-based network session analysis, enhancing detection accuracy and system security.

Keywords: AI-Enhanced cyber-attacks; Data fingerprinting; Visualization techniques; Finger Vein

I.INTRODUCTION

Cyber security threats have escalated in complexity due to AI-Enhanced cyber-attacks that autonomously exploit vulnerabilities in defence systems. Global events such as COVID-19 and the armed conflict between Russia and Ukraine have further intensified these threats, creating challenges in protecting critical cyber assets. Traditional cybersecurity defences often rely on machine learning models, particularly anomaly detection techniques, which are susceptible to data poisoning and adversarial manipulations. A major limitation of existing AI-driven cyber-defence systems is the reliance on lab-generated data, which does not accurately represent real-world attack scenarios. Effective AI-Enhanced cybersecurity solutions must be trained on real-world and real-time attack datasets to improve detection efficiency. However, challenges such as data availability, sensitivity, and privacy concerns hinder access to such datasets. Researchers have found that visualized datasets simplify learning for AI models by transforming complex, multimodal data into structured representations. This study introduces a framework for AI-driven cyber defense, referred to as AIECDS, which utilizes data fingerprinting and visualization techniques to improve threat identification and classification accuracy. The approach aims to mitigate weaknesses in existing cybersecurity frameworks by integrating biometric-driven data processing for improved authentication and anomaly detection. The remainder of this paper discusses related work in cybersecurity threats, followed by a detailed explanation of the proposed methodology, data fingerprinting techniques, and their application in network security.

Objectives

Training machine learning models on visualized data has proven to be more successful than training on raw data. This is because researchers have identified that visualizations can represent complex, large, multimodal datasets as simple datasets, which simplifies the learning task for AI models. This opens up an opportunity for developers of cyber-defense systems to develop AI enhanced tools that can be trained on visualized data. Furthermore, visualized representations of data create an opportunity to extract more meaningful real-world data from threat-related environments such as computer networks.

II. LITERATURE SURVEY

[1]. UNSW-NB15: A COMPREHENSIVE DATA SET FOR NETWORK INTRUSION DETECTION SYSTEMS (UNSW-NB15 NETWORK DATA SET)

Authors: Nour Moustafa And Jill Slay

One of the key challenges in this research domain is the lack of a comprehensive, up-to-date network-based dataset that accurately represents current network traffic patterns, includes a wide range of stealthy intrusion types, and offers in-depth information about network behavior. Traditional benchmark datasets such as KDD98, KDDCUP99, and NSL-KDD were developed over a decade ago to support the evaluation of network intrusion detection systems. However, numerous recent studies have highlighted that these datasets no longer adequately represent today's evolving threat landscape or the nature of modern, low-footprint cyber-attacks. To address this limitation, the UNSW-NB15 dataset was developed. It combines realistic modern benign traffic with synthetic but representative attack behaviors. The dataset's features were derived using a combination of both established and innovative techniques. It is publicly available and intended to support ongoing cybersecurity research.

[2]. A SURVEY ON MACHINE LEARNING TECHNIQUES FOR CYBER SECURITY IN THE LAST DECADE

Authors: Kamran Shaukat, Suhuai Luo And Vijay Varadharajan

The rapid expansion of the Internet and widespread adoption of mobile applications have significantly broadened the scope of cyberspace. This growth has also made cyberspace increasingly susceptible to persistent and automated cyberattacks. To address these evolving threats, cybersecurity techniques have advanced to improve the detection and response mechanisms against such attacks. However, traditional security systems have become inadequate, as cybercriminals have developed sophisticated methods to bypass them. These conventional approaches often fail to effectively identify novel and polymorphic threats. In recent years, machine learning (ML) has emerged as a crucial component in enhancing cybersecurity capabilities across various applications. Despite its growing success, ML-based systems face notable challenges in maintaining reliability and trust, particularly due to the presence of adversaries who deliberately seek to exploit ML vulnerabilities. This paper presents an in-depth review of the challenges ML faces in defending cyberspace, with a focus on its applications in intrusion detection, spam filtering, and malware detection in both computer and mobile networks over the past decade. It also summarizes commonly used ML algorithms, widely adopted security datasets, key ML tools, and evaluation metrics for classification tasks. In conclusion, the paper explores the prevailing challenges and limitations of applying machine learning in cybersecurity and presents a thorough bibliography along with an overview of the most recent advancements and emerging trends in the field.

[3]. DEEP REINFORCEMENT LEARNING FOR CYBER SECURITY

Authors: Thanh Thi Nguyen And Vijay Janapa Reddi

The rapid expansion of Internet-connected systems has significantly increased their exposure to cyber threats. Due to the growing complexity and evolving nature of cyberattacks, security mechanisms must be capable of adapting quickly, scaling effectively, and responding efficiently. To tackle these challenges, machine learning—particularly deep reinforcement learning (DRL)—has been widely explored. By integrating deep learning with reinforcement learning, DRL demonstrates strong potential in addressing complex, dynamic, and high-dimensional problems within cyber defense. This paper presents an extensive review of deep reinforcement learning (DRL) applications within the field of cybersecurity. It covers significant topics including the use of DRL for protecting cyber–physical systems, autonomous intrusion detection methods, and multi-agent DRL frameworks applied in game-theoretic models to develop effective cyber defense strategies.The paper also includes in-depth discussions on current methodologies and outlines potential avenues for future research. The intent is to offer a solid foundation for continued exploration into how DRL can be leveraged to manage increasingly sophisticated cybersecurity challenges.

III.EXISTING SYSTEM

One of the key challenges in cyber defense lies in the growing complexity of cyber-attacks, insufficient data protection, inadequate security practices, and overreliance on vulnerability-based defense strategies. These issues collectively weaken the overall security perimeter. A significant barrier to improvement is the lack of access to real-world datasets, as well as the difficulty in extracting actionable insights from live network environments. Existing studies have shown that many prototype systems for network-based cyber defense rely on basic telemetry and averaged statistics for feature extraction. This simplification can lead to higher sensitivity during inference and delays in accurately classifying cyber threats.

DISADVANTAGES:

- Machine learning-based Intrusion Detection Systems (IDS) have transitioned from manually engineered features to deep learning approaches, which require less feature engineering.
- This shift has led to more complex models but only modest gains in performance.
- Detecting threats with very small or rare malicious samples remains a significant challenge.

IV.PROPOSED SYSTEM

Since the captured images often contain noise, fingerprint patterns are extracted only after applying noise reduction and normalization techniques. To improve authentication accuracy, multiple fingerprint patterns are preserved and analyzed. This step is essential in the overall authentication process. Vein patterns are generally categorized into four broad methodological approaches: tracking-based, transform-based, filter-based, and threshold-based methods. Additionally, research has shown that training machine learning models on visualized data often yields better results compared to raw data. This is because visualizations can simplify large, complex, and multimodal datasets, making it easier for AI systems to learn and make accurate predictions.

ADVANTAGES:

- Enhanced threat detection rates with reduced response time
- Support for adaptive learning through reinforcement learning techniques
- Improved ability to identify adversarial and previously unknown attacks
- Effective detection of threats using limited or small-scale datasets
- Real-time training and evaluation of AI-powered defense systems in real-world scenarios

V. METHODOLOGY

OVERVIEW OF THE PROJECT

Previous research has highlighted a significant gap in machine learning applications for cybersecurity many models have yet to be evaluated in real-time or operational environments. This presents a major limitation, as the effectiveness of detection models in controlled settings doesn't always translate to practical deployment. Several studies have stressed the importance of using high-quality, real-world, and real-time data to build reliable cyber defense solutions.This paper takes an initial step toward addressing this data challenge by introducing a methodology for developing AI-enhanced cyber defense tools. The proposed approach emphasizes two core tasks: data fingerprinting and visualization, both aimed at improving threat detection and system robustness.The structure of the paper is as follows: it begins with a review of recent work on AI-based threats and the limitations of current machine learning defenses. Next, it presents a detailed explanation of the proposed methodology, followed by its application in a use case involving fingerprinting network sessions for cyber threat identification.Researchers have observed a growing use of AI-powered tools across multiple phases of the cyber-attack lifecycle. For instance, during the reconnaissance stage, tools like MalGAN can generate adversarial malware designed to bypass conventional malware detectors by disguising malicious intent. In later stages, such as Command and Control (C2), advanced tools like DeepLocker have been developed to hide malware payloads that activate only under specific conditions. These tools leverage adversarial learning to modify and obscure code, making detection far more difficult.This study builds on such insights to propose a defensive framework capable of countering the evolving nature of AI-driven threats through intelligent data analysis and visualization.

MODULES

a. Data Collection and Preprocessing
b. Feature Extraction Using LBP
c. Authentication and Matching
d. Visualization with Hilbert Curve

MODULE DESCRIPTION

a. Data Collection and Preprocessing

We employ the Finger Vein Dataset from Kaggle, which consists of 3,000 grayscale images captured under controlled lighting conditions. Preprocessing steps include:

- Grayscale conversion,
- Histogram equalization,
- Noise removal using Niblack thresholding,
- Region of Interest (ROI) extraction.

These steps ensure uniform image quality and enhance feature clarity.

b. **Feature Extraction Using LBP**

Local Binary Patterns (LBP) are applied to extract texture features from finger vein images. The technique encodes each pixel based on its neighborhood, producing a binary representation of local textures. These LBP histograms form the biometric fingerprint for each user.

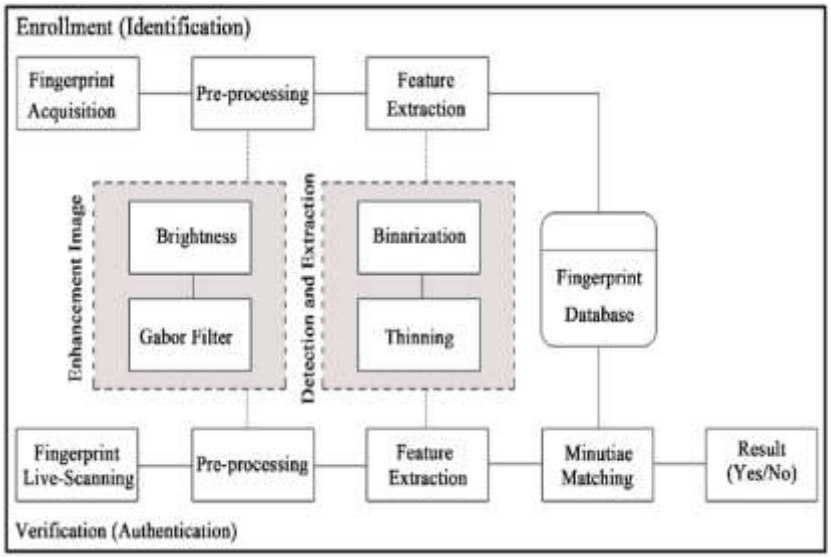
c. **Authentication and Matching**

The system compares acquired LBP patterns with stored templates using XOR-based similarity. A threshold (T = 22,000) determines whether access is granted or denied. This mechanism ensures reliable identity verification and prevents unauthorized access.

d. Visualization with Hilbert Curves

By mapping sequential data onto a two-dimensional space using the Hilbert curve, spatial relationships are preserved. This approach helps the system visually identify normal versus anomalous behaviors in network session data, enhancing clarity and facilitating timely anomaly detection.

VI.SYSTEM ARCHITECTURE



VII.EXPERIMENTAL RESULTS

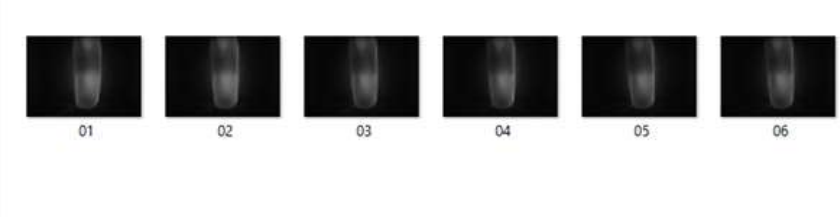


Figure 1: Acquired Fingervein Image

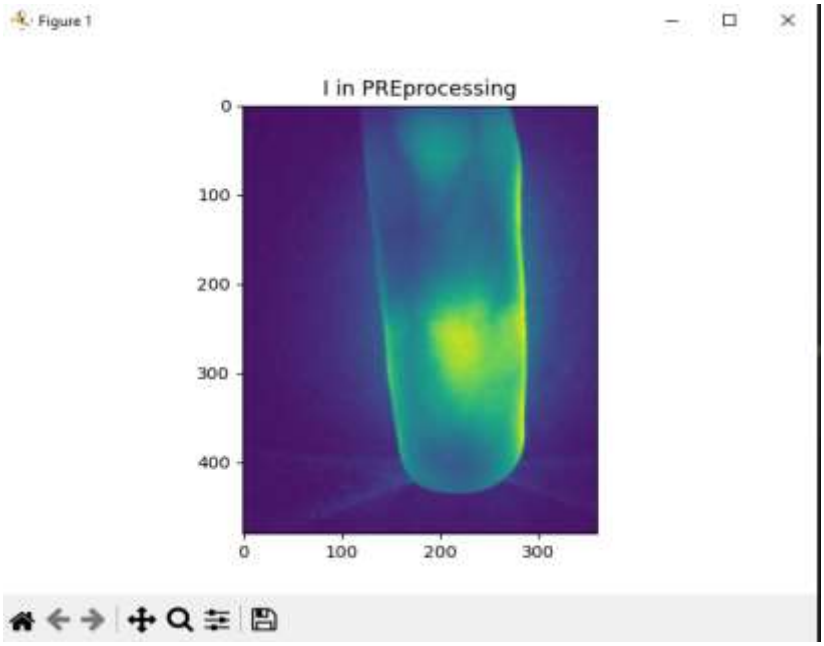


Figure 2:Image after Preprocessing

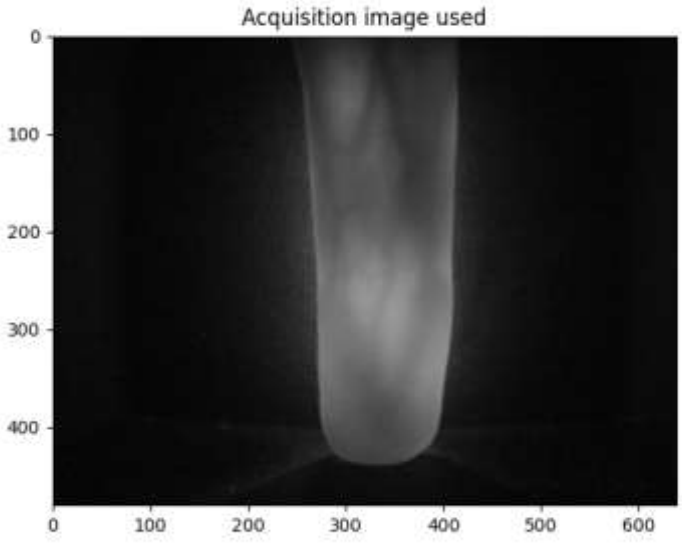


Figure 3:Acquisition Image used

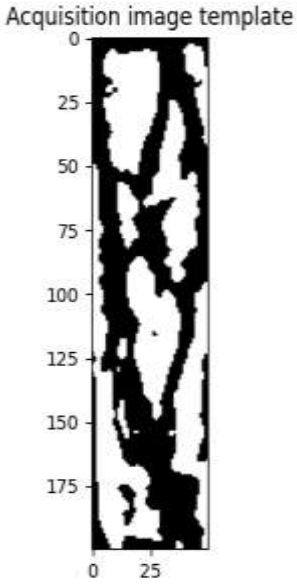


Figure 4:Acquisition Image Template

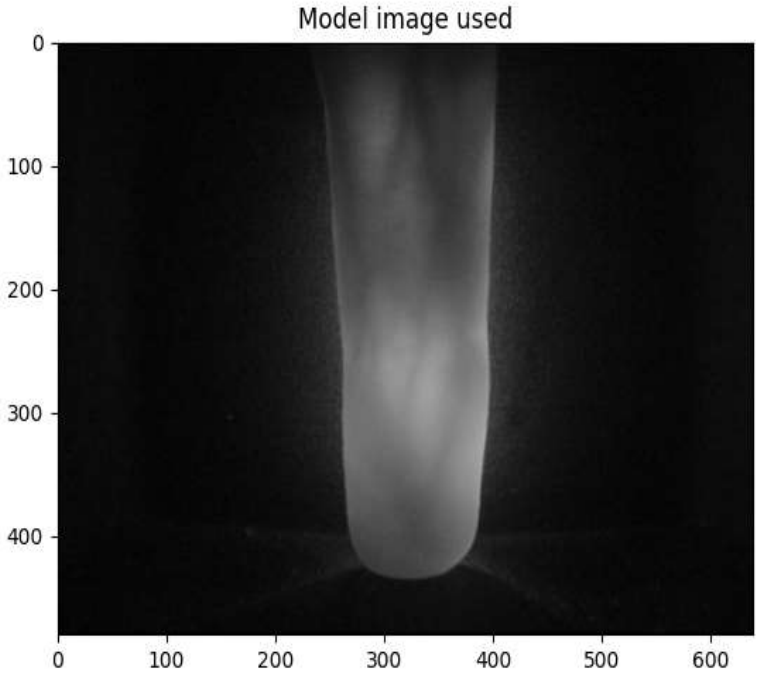


Figure 5:Model Image Used

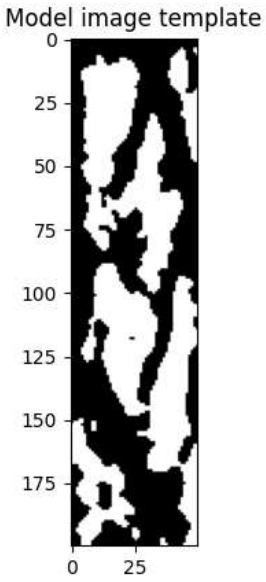


Figure 6:Model Image Template

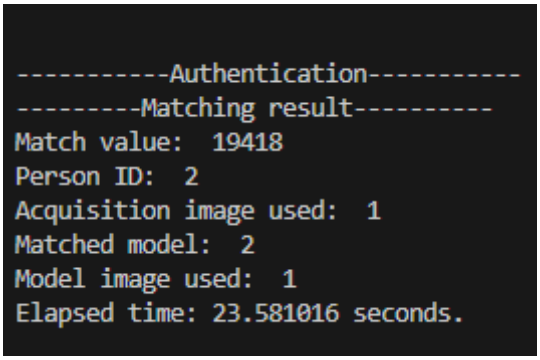


Figure 7:Matching Result with Score

VIII.CONCLUSION

The research proves the efficacy of fingerprinting and visualization of data in enhancing AI-powered cybersecurity mechanisms. Using the Finger Vein Dataset, the approach mitigates complexity in decision boundaries to enable accurate threat identification even from small sample sizes. Classification accuracy is enhanced through the fingerprinted data, and visualization methods identify unusual patterns in cyber network sessions. The verification process indicates that biometric-based cybersecurity frameworks can strengthen authentication and anomaly detection against AI attacks. The combination of Local Binary Patterns (LBP) and sophisticated preprocessing provides stronger security measures in real-time systems. The results validate that fingerprint-based cyber defence can weaken adversarial AI attacks and simplify machine learning models to make them more secure. This approach helps develop changing cybersecurity methods, opening doors to stronger security against automatic cyberattacks. Subsequent work can further narrow down these methods by increasing datasets and incorporating actual attack scenarios into biometric authentication systems.

X. FUTURE WORK

Future enhancements to the proposed system could include integration with real-time cybersecurity monitoring tools, enabling threat detection as attacks unfold. Additional features such as:

- **Live analysis of network traffic from enterprise environments**
- **Support for multiple biometric traits (e.g., iris, facial recognition)**
- **Automated threat response and alert systems**

Moreover, adding a feedback loop where security analysts can validate or flag system decisions would help the model adapt and improve over time. Expanding the framework to handle a broader range of attack types and datasets will increase its usefulness across different industries.

REFERENCE:

1. O. Çaylı, "AI-Enhanced Cybersecurity Vulnerability-Based Prevention, Defence, and Mitigation using Generative AI," *Orclever Proc. Res. Dev.*, 2024.
2. J. Oloyede, "AI-Driven Cybersecurity Solutions: Enhancing Defence Mechanisms in the Digital Era," *SSRN*, 2024.
3. B. Y. Kasula and P. Whig, "Enhancing Cybersecurity Defences: A Comprehensive Exploration of Applied Artificial Intelligence Strategies," *SpringerLink*, 2025.
4. N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," *Elsevier*, 2022.
5. K. Shaukat, S. Luo, and V. Varadharajan, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," *Springer*, 2024.
6. T. T. Nguyen and V. J. Reddi, "Deep Reinforcement Learning for Cyber Security," *IEEE Trans. Cybern.*, 2023.
7. Y. Zhang et al., "A Score-Level Fusion of Fingerprint Matching With Fingerprint Liveness Detection," *IEEE Access*, vol. 8, pp. 8208–8216, 2020.
8. J. Shen et al., "Finger Vein Recognition Algorithm Based on Lightweight Deep Convolutional Neural Network," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–10, 2022.
9. Y. Yin et al., "Finger Vein Recognition Based on Multi-Scale Feature Extraction," *Pattern Recognit. Lett.*, vol. 128, pp. 42–49, 2019.
10. S. Prabhakar, A. K. Jain, and J. Wang, "Fingerprint Recognition Using Minutiae-Based Matching," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 8, pp. 888–892, 2003.
11. H. Xu et al., "Deep Learning-Based Finger Vein Recognition: A Survey," *Neural Comput. Appl.*, vol. 33, pp. 18943–18961, 2021.
12. T. Matsuda et al., "Finger Vein Authentication Using a Novel Feature Extraction Method," *J. Biometr. Secur.*, vol. 2, no. 4, pp. 45–53, 2020.