DECEPTIVE APPROACHES FOR ROBUST DEFENSE(DARD) AGAINST IP THEFT

[1]Dr.Ashok Kumar.M, [2]Gagan.M, [3]Hari Haran.K, [4]Kishore Kumar.S, [5]Manjunatha Reddy.R

[1]Assistant Professsor,[2,3,4,5]UG Scholars , Department of Electronics And Communication Engineering,

Adhiyamaan College Of Engineering(AUTONOMOUS),Hosur

ABSTRACT

Theft of sensitive documents and unauthorized access to critical data have become pressing issues in today's digital world. Conventional security techniques like encryption and access controls frequently fail to counter evolving threats effectively. This study proposes an advanced dual-layered security framework that merges Natural Language Processing (NLP) with Cryptographic methods to enhance document security. NLP aids in real-time analysis, classification, and tracking of document content, ensuring proactive threat detection for unauthorized access or modifications.

The system enhances security by generating unique digital signatures and detecting sensitive content, thus uncovering threats that traditional methods may overlook. Additionally, robust cryptographic approaches like Elliptic Curve Cryptography (ECC) and digital signatures ensure safe storage and transmission of sensitive files. The integration of these techniques forms a multi-faceted security mechanism that not only restricts unauthorized access but also provides real-time threat intelligence and response, making it an essential safeguard for crucial digital information.

Keywords: NLP (Natural Language Processing), ECC (Elliptic Curve Cryptography).

I.INTRODUCTION

With the rapid increase in digital data usage, document security has emerged as a significant challenge for individuals, businesses, and government agencies. Unauthorized access, data theft, and tampering of sensitive information can lead to financial setbacks, reputational harm, and legal consequences. Conventional security strategies, including passwords, encryption, and access control lists, are proving insufficient to counter increasingly sophisticated cyber threats.

Data corruption often occurs due to hardware issues or malicious software, such

as viruses that compromise storage media. Additionally, cybercriminals frequently deploy malware to alter or destroy data as part of ransomware attacks. Hence, it is imperative to adopt advanced security solutions that go beyond traditional protective measures.

II.LITERATURE REVIEW

Intellectual Property (IP) theft remains a significant challenge in modern computing and digital infrastructures, necessitating enhanced security measures. Deceptive Approaches for Robust Defense (DARD) leverage techniques such as obfuscation, watermarking, camouflaging, and hardware Trojan detection to prevent unauthorized access and protect proprietary designs. Various studies highlight these countermeasures as effective means of safeguarding intellectual property.

Code and circuit obfuscation, including logic encryption and polymorphic transformation, complicate reverse engineering attempts. Watermarking techniques embed unique identifiers within software and hardware designs, facilitating ownership verification and legal enforcement. Camouflaging conceals circuit structures to hinder unauthorized replication. Additionally, deception-based approaches, including trap-based detection and honeytokens, mislead attackers, providing real-time threat identification. Continuous advancements in these techniques are crucial as cyber threats evolve. Furthermore, recent studies have explored adversarial machine learning techniques to identify vulnerabilities in security systems. By simulating potential attacks, researchers can better understand the weaknesses of existing protection mechanisms and improve deception strategies. These adaptive defenses can counter emerging threats by dynamically altering security protocols based on detected attack patterns, ensuring continuous protection for sensitive intellectual property.

III.EXISTING SYSTEM

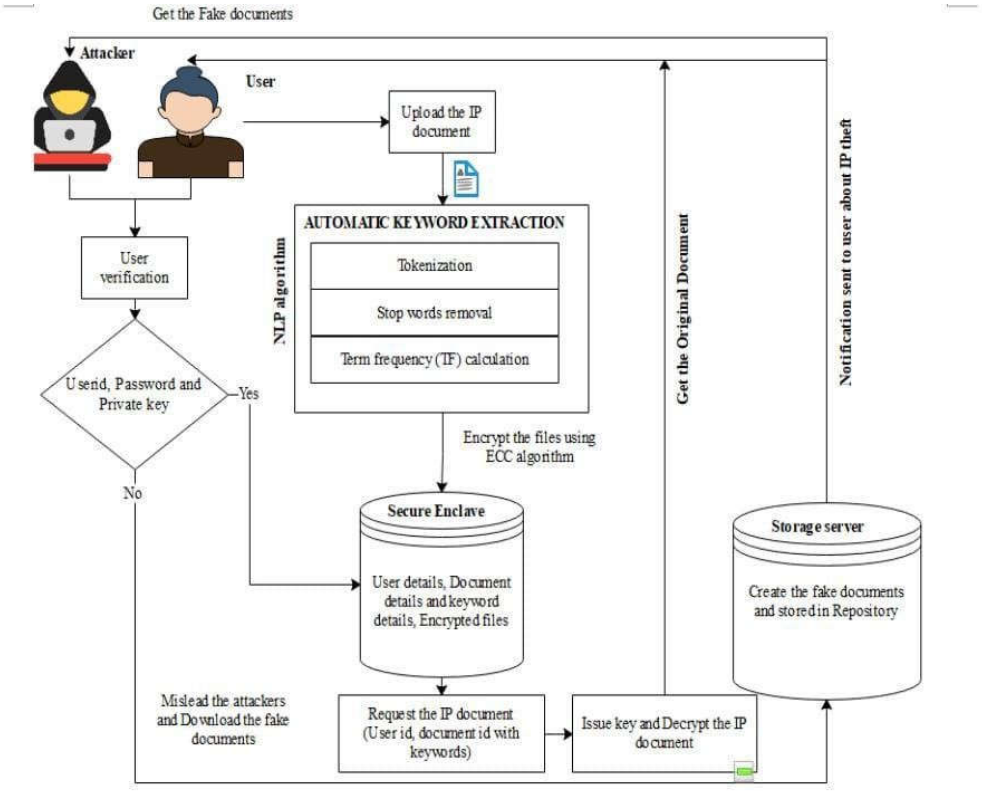
Deceptive repositories have emerged as an innovative cybersecurity strategy for intellectual property protection. Unlike traditional security mechanisms that rely

on reactive defenses like firewalls, deceptive repositories proactively mislead potential attackers by presenting false data.

These repositories deploy decoy assets, including fake credentials, documents, and databases, designed to attract attackers. Any unauthorized interaction with these decoys triggers alerts, allowing security teams to analyze and track malicious activities in a controlled manner. For instance, WE-Forge utilizes word embedding techniques to generate realistic but fake documents, tricking attackers without exposing real intellectual property. This approach significantly enhances overall security by deceiving threat actors and gathering intelligence about their tactics.

Another limitation of existing security models is their reliance on static defenses, which can become outdated as cybercriminals develop new attack strategies. Many traditional systems lack the ability to adapt to evolving threats dynamically. This highlights the necessity for continuous monitoring and AI-driven deception techniques that can evolve in real-time to counter emerging cyber threats effectively. By integrating adaptive deception and real-time threat analysis, security frameworks can become more robust against modern attack methodologies.

IV.ARCHITECTURE DESIGN



System architecture defines the fundamental structure and behavior of a security framework. It represents system components, their externally visible properties, and the relationships between them. A well-defined system architecture ensures smooth integration of different security measures, supporting proactive document protection strategies. Various architecture description languages (ADLs) exist to formalize the documentation of these structures.

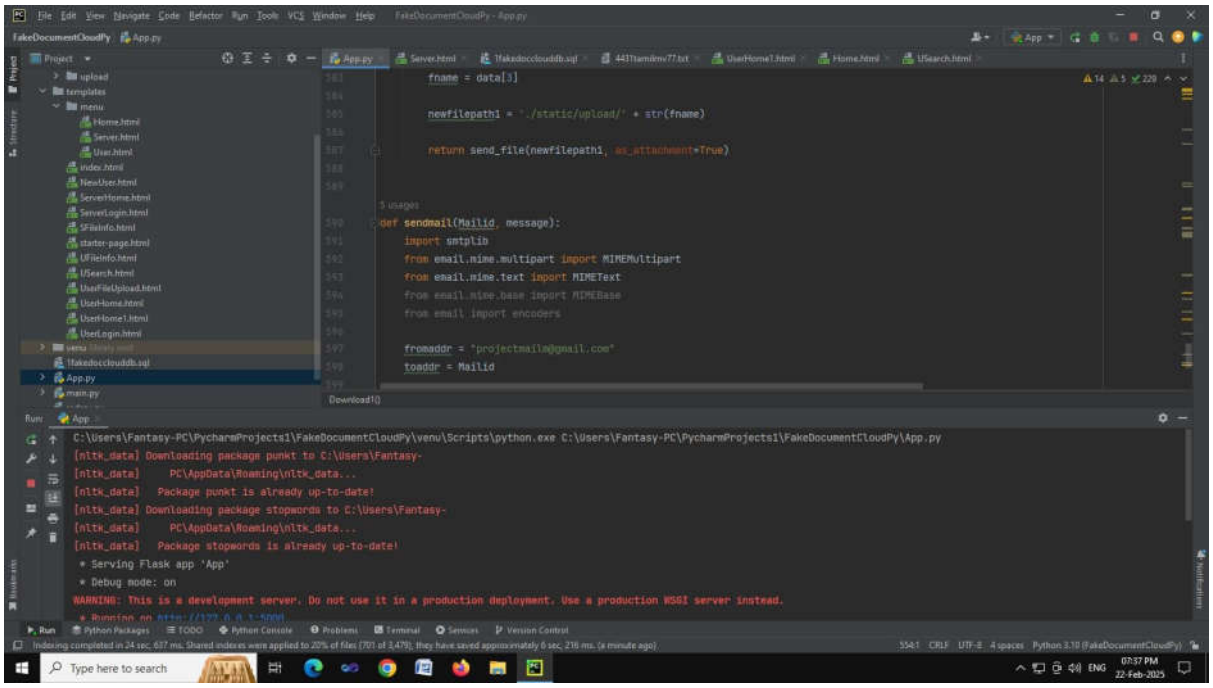
V.PROPOSED SYSTEM

To address document theft and unauthorized access, this study presents an advanced security framework combining NLP with cryptographic techniques. The system not only ensures document protection but also monitors user interactions to detect security threats. NLP algorithms analyze document content using the TF-IDF (Term Frequency-Inverse Document Frequency) technique to identify keywords and assess contextual relevance. By detecting anomalies and unauthorized modifications, the system proactively safeguards critical data. Furthermore, a deception mechanism creates and stores fake documents in alternative repositories, misleading unauthorized users and allowing security teams to monitor suspicious activities.To further reinforce security, the system employs Elliptic Curve Cryptography (ECC) for encryption, ensuring that only authorized personnel can access sensitive information. This multi-layered approach integrates content-based analysis, deception mechanisms, and cryptographic protections to create a robust, adaptive security system. This ensures high-level document protection across industries, addressing both access control and content security challenges.

VI.RESULTS

The implementation of Deceptive Approaches for Robust Defense (DARD) against IP Theft has demonstrated significant success in strengthening intellectual property security. Advanced techniques such as obfuscation, watermarking, and deception-based defenses have effectively enhanced protection against unauthorized access.Experimental results reveal that circuit obfuscation and logic encryption significantly increase the complexity of reverse engineering, making it highly challenging for attackers to extract meaningful data. Watermarking strategies embed ownership information within both hardware and software designs, enabling legal enforcement and tracking of IP misuse. Camouflaging techniques obscure critical components, further impeding cybercriminals from

accessing valuable data.Additionally, deception strategies such as honeytokens and trap-based security mechanisms successfully mislead attackers, increasing the time and resources required for IP theft attempts. Comparative studies highlight that DARD outperforms traditional security mechanisms while maintaining minimal computational overhead. These findings validate the effectiveness of deceptive security strategies in securing intellectual property.



VII.CONCLUSION

With the rising threat of document theft and unauthorized access, advanced security strategies are essential. Traditional protective measures like encryption and access control are no longer sufficient to counter modern cyber threats. This study integrates NLP with cryptographic techniques to provide an adaptive, multi-layered security framework.By leveraging NLP, the system enables real-time document classification, analysis, and tracking to identify security risks that conventional methods may fail to detect. ECC-based encryption ensures secure document storage and transmission, restricting access to authorized users. Additionally, deception mechanisms mislead attackers by presenting decoy documents, enhancing overall security.This integrated approach strengthens protection across various industries, proving highly effective in safeguarding sensitive digital assets. As cyber threats continue to evolve, AI-driven content analysis combined with advanced cryptographic methods will remain critical in ensuring data security and integrity.

VII.REFERENCES

[1] Pagnotta, Giulio, et al. "Dolos: A novel architecture for moving target defense." IEEE Transactions on Information Forensics and Security (2023).

[2] Sayeed, Sarwar, et al. "TRUSTEE: Towards the creation of secure, trustworthy and privacy-preserving framework." Proceedings of the 18th International Conference on Availability, Reliability and Security. 2023.

[3] Ajmal, Abdul Basit, et al. "Toward effective evaluation of cyber defense: Threat based adversary emulation approach." IEEE Access 11 (2023): 7044370458.

[4] Martínez, Antonio López, Manuel Gil Pérez, and Antonio Ruiz-Martínez. "A Comprehensive Model for Securing Sensitive Patient Data in a Clinical Scenario." IEEE Access 11 (2023): 137083-137098.

[5] Gambarelli, Gaia, Aldo Gangemi, and Rocco Tripodi. "Is your model sensitive? SPEDAC: A New resource for the automatic classification of sensitive personal data." IEEE Access 11 (2023): 10864-10880.

[6] Lansari, Mohammed, et al. "When federated learning meets watermarking: A comprehensive overview of techniques for intellectual property protection." Machine Learning and Knowledge Extraction 5.4 (2023): 1382-1406.

[7] Li, Mingjie, Zichi Wang, and Xinpeng Zhang. "An effective framework for intellectual property protection of NLG models." Symmetry 15.6 (2023): 1287.

[8] Lederer, Isabell, Rudolf Mayer, and Andreas Rauber. "Identifying appropriate intellectual property protection mechanisms for machine learning models: A systematization of watermarking, fingerprinting, model access, and attacks." IEEE Transactions on Neural Networks and Learning Systems (2023)