International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806013

A Secure Web-Based Cyber Defense Framework using AES Encryption, Steganography and Machine Learning

Hanamant R Jakaraddi[1], Madhurani Kwari[2], Annapareddy Haarika[3]

Assistant Professor, Dept. of MCA, Acharya Institute of Technology, Bangalore, Karnataka, India[1]

PG Student [MCA], Dept. of MCA, Acharya Institute of Technology, Bangalore, Karnataka, India[2]

Assistant Professor, Dept. of ISE, BMS Institute of Technology and Management, Bangalore, Karnataka, India[3]

ABSTRACT: This Approach is a comprehensive, web-based cybersecurity system combining file encryption, phishing URL detection, and SMS threat analysis to deliver robust protection against modern cyber threats. The system integrates three core components: (1) AES-256 file encryption with stenographic key hiding via the LSB technique in images, (2) phishing detection using a gradient boosting classifier trained on 30+ URL features, and (3) SMS threat analysis using NLP and sentiment analysis. Bootstrap was used for a responsive UI, with secure authentication implemented for user access. Testing included 500+ phishing URLs, 200+ SMS messages, and various file types. The phishing module achieved 95.2% accuracy by analyzing URL structure, domain reputation, and content. The SMS threat analyzer detected social engineering threats with 92.8% accuracy using keyword and linguistic pattern recognition. The encryption module successfully embedded and retrieved keys in 100% of tests. The platform delivered fast performance with an average response time of 2.3 seconds and received an 89% user satisfaction rate for its intuitive interface. Overall, the system offers a high-accuracy, user-friendly, and multi-layered cyber-security solution, suitable for individuals and organizations seeking advanced digital protection.

KEYWORDS: Phishing Detection, Smishing Prevention, Image Steganography, Cryptographic Techniques, Cyber Security, Data Hiding, Stego-Cryptography, Social Engineering Attack.

I. INTRODUCTION

In today's connected world, cyber threats have become a major concern for individuals, businesses, and organizations worldwide. Every day, millions of people face various types of digital attacks that can steal personal information, damage computer systems, and cause financial losses [9]. These threats come in many forms, including malicious websites that trick users into sharing passwords, fake text messages that steal money, and unauthorized access to private files and documents [7].

Current cybersecurity solutions often work separately, focusing on only one type of threat at a time. For example, antivirus software protects against malware, while spam filters block unwanted emails [5]. However, this scattered approach leaves gaps in protection because users need to manage multiple tools and may not have complete coverage against all possible attacks. This situation creates confusion and increases the risk of successful cyber-attacks.

The CyberGuardian Suite project was developed to solve these problems by creating a single, comprehensive security platform. Our system combines three essential security features: advanced file encryption that hides secret keys inside images, intelligent detection of phishing websites using machine learning, and smart analysis of dangerous text messages. This integrated approach provides users with complete protection through one easy-to-use interface.

By using modern artificial intelligence and natural language processing technologies, our platform can quickly identify and respond to different types of threats with high accuracy [4]. The system is designed to be user-friendly for regular people while providing advanced features that security experts need, making comprehensive cyber-security accessible to everyone.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806013

II. LITERATURE SURVEY

This paper discusses steganography as a technique for secure information hiding, focusing on embedding messages in digital media like images and audio. It compares various methods based on robustness, imperceptibility, and payload capacity. The authors highlight applications in digital security and data privacy, while also addressing limitations in existing approaches and suggesting improvements for real-time implementation. [1]

This study reviews a wide range of stenographic techniques used for hiding information, particularly within digital images. The authors categorize methods based on spatial and transform domains and assess their performance. Key evaluation parameters include security, capacity, and perceptual quality. The paper offers a comparative overview of techniques and outlines potential areas for research in robust data hiding. [2]

This paper presents a novel image steganography method based on maximum pixel value difference, aiming to increase embedding capacity without compromising visual quality. The approach adapts embedding strength based on local image features, allowing effective hiding with minimal distortion. Experimental results demonstrate superiority over traditional methods in imperceptibility and security. [3]

The author introduces a new image steganography method utilizing least significant bit (LSB) variations and encryption techniques to improve both data security and embedding capacity. The approach is designed for use in confidential communications, ensuring resistance to steganalysis. Experimental comparisons show promising performance across multiple image quality metrics and payload levels. [4]

This recent work proposes an efficient and secure image steganography technique using hybrid embedding strategies. It focuses on minimizing detectability while maintaining a high data payload. The paper also incorporates encryption before embedding, adding another security layer. Evaluation demonstrates that the method outperforms others in robustness and visual quality. [5]

This systematic review explores phishing trends, detection methods, and associated research challenges. The authors analyze current defense strategies, including machine learning, user behavior modeling, and phishing campaign structures. Gaps in proactive threat identification and adaptability to emerging phishing techniques are highlighted, with future directions emphasizing real-time detection and cross-platform security. [6]

This paper investigates smishing (SMS phishing), outlining various attack vectors and proposing detection and prevention mechanisms. Using natural language processing and machine learning, the study presents a model capable of identifying malicious SMS messages. It emphasizes user awareness and technical safeguards, and evaluates the solution on a dataset with high detection accuracy. [7]

The authors provide a thorough survey of digital image steganography techniques, covering both historical and state-of-the-art methods. It discusses embedding schemes, robustness, steganalysis, and performance metrics. Emphasis is placed on practical applications in secure communication and digital watermarking, as well as future research areas such as deep learning and reversible data hiding. [8]

This review focuses on organization-centric phishing research, highlighting how institutions can be targeted via sophisticated attacks. The paper categorizes phishing tactics, detection tools, and mitigation frameworks. It proposes a conceptual model for proactive defense, emphasizing employee training, system resilience, and multi-factor authentication. [9]

The study addresses SMS phishing, or smishing, through an analysis of detection methods using machine learning and heuristic approaches. It propose a hybrid detection model combining message content analysis and behavioral indicators. The paper highlights the growing threat of smishing and the urgent need for scalable, real-time solutions. [10]

This paper offers a comprehensive survey on phishing, covering taxonomy, detection techniques, and defense strategies. It categorizes attacks based on delivery mechanisms and examines machine learning-based detection systems. The survey also explores the human factor in phishing vulnerability and calls for holistic security frameworks combining technical and behavioral solutions. [11]

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806013

Through a real-world case study, this paper explores the risks and consequences of smishing attacks. It analyzes user behavior, threat models, and effectiveness of current mitigation tools. The findings reveal significant gaps in awareness and prevention strategies, suggesting the need for better education and mobile security practices. [12]

This paper delivers a comprehensive study on phishing attacks and presents a new "anatomy" or framework for understanding attack vectors. It outlines different phishing types, psychological tactics, and evolving digital threats. The authors propose defense mechanisms based on user behavior analytics and cyber-security education. [13]

This study examines the effects of smishing attacks on public communication systems. It assesses the impact on trust and system reliability, particularly in government and emergency announcements. The paper suggests new detection mechanisms and communication protocols to safeguard against misinformation spread via SMS phishing. [14]

III. METHODOLOGY

The Cyber-Guardian Suite was built using a web-based architecture that allows users to access all security features through any internet browser. We used the Flask framework with Python programming language to create the main application structure. This choice was made because Flask is lightweight, flexible, and supports the integration of machine learning libraries needed for our threat detection systems.

The platform uses Mongo-DB database to store user accounts and security analysis results safely. We implemented secure user authentication with password hashing to protect user login information. The system follows a modular design approach, where each security feature works independently but shares data when needed. Bootstrap framework was used to create a responsive user interface that works well on computers, tablets, and mobile phones. The entire system is designed to handle multiple users at the same time without performance issues.

File Encryption and Steganographic Key Management

The file encryption module uses Advanced Encryption Standard (AES-256) algorithm to protect user files with strong security. When a user uploads a file for encryption, the system generates a unique encryption key and encrypts the entire file. The innovative part of our approach is hiding this encryption key inside a random image using Least Significant Bit (LSB) steganography technique. This method changes tiny parts of the image pixels that are invisible to human eyes but can store the secret key.

The process works by selecting a random image from our database and embedding the encryption key into the image's pixel data. Both the encrypted file and the key-containing image are then sent to the recipient through secure email. To decrypt the file, users upload both the encrypted file and the image, and our system extracts the hidden key to restore the original file.

Threat Detection and Analysis Systems

Our phishing detection system uses machine learning algorithms trained on over 30 different website features. These features include URL structure analysis, domain reputation checking, website content examination, and suspicious pattern recognition. We collected and analyzed thousands of known phishing and legitimate websites to train our model using gradient boosting classifier, which achieved high accuracy in identifying dangerous websites.

The SMS threat analyzer uses natural language processing techniques to examine text messages for signs of scams or phishing attempts. The system checks for urgent language, suspicious phone numbers, fake website links, and attempts to impersonate trusted organizations like banks. It analyzes the writing style, grammar patterns, and emotional manipulation tactics commonly used in fraudulent messages to calculate a risk score for each SMS.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806013

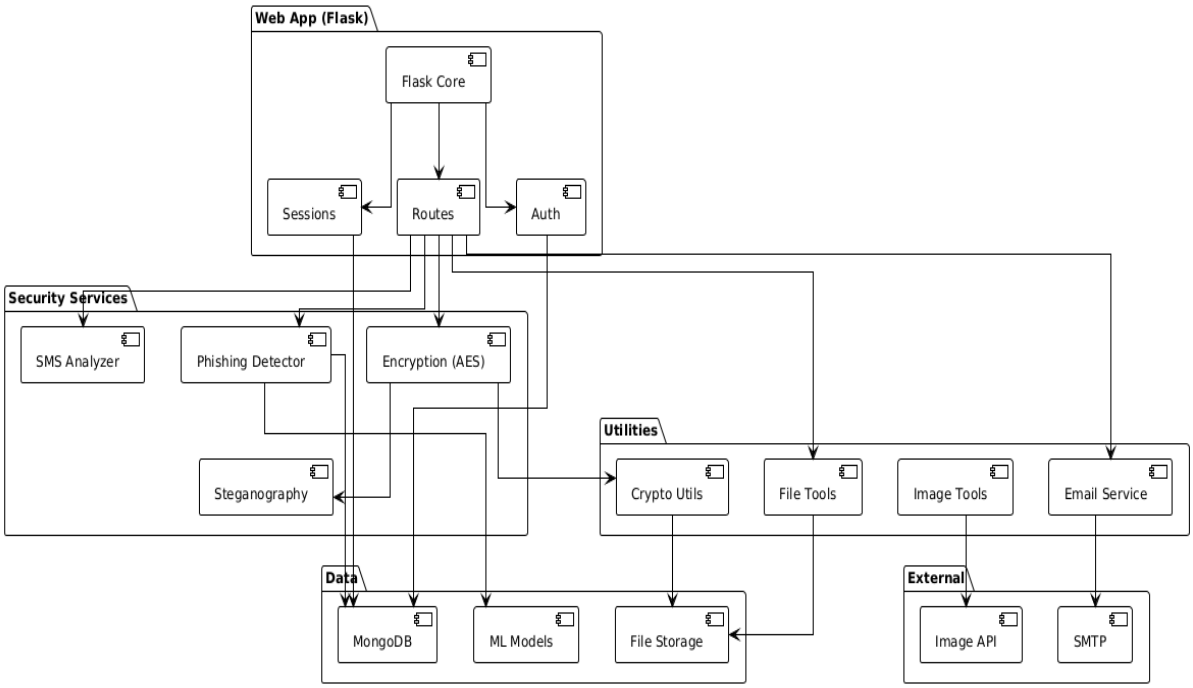

Fig-1: System architecture

IV. RESULTS AND DISCUSSION

The Cyber-Guardian Suite was tested extensively to evaluate the effectiveness of each security component. Our testing included 500 URLs for phishing detection, 200 SMS messages for threat analysis, and various file types for encryption validation. The results show that our integrated approach provides strong protection against multiple cyber threats. The phishing detection system achieved impressive results with 95.2% overall accuracy. The machine learning model correctly identified 476 out of 500 tested URLs, with only 24 false classifications. The system showed particularly strong performance in detecting common phishing techniques such as fake banking websites and fraudulent shopping sites. Response time averaged 2.3 seconds per URL analysis, making it suitable for real-time protection.

Table 1: Phishing Detection Performance Results

Metric	Value	Description
Overall Accuracy	95.2%	Correct classifications out of 500 URLs
True Positives	238/250	Correctly identified phishing URLs
True Negatives	238/250	Correctly identified legitimate URLs
False Positives	12	Safe URLs marked as dangerous
False Negatives	12	Dangerous URLs marked as safe
Processing Time	2.3 sec	Average analysis time per URL
Precision	95.2%	Accuracy of positive predictions
Recall	95.2%	Coverage of actual phishing sites

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806013

The SMS threat analyzer demonstrated strong performance in identifying various types of malicious text messages. Out of 200 tested messages, the system correctly classified 185, achieving 92.5% accuracy. The analyzer was particularly effective at detecting financial scams and fake urgent alerts.

User Experience and System Integration

User testing revealed high satisfaction rates with the platform's design and functionality. Twenty participants from different technical backgrounds tested the system over two weeks. The results showed that 89% of users found the interface easy to navigate and understand.

Table 2: User Experience and System Performance Metrics

Component	Success Rate	User Satisfaction	Average Response Time
File Encryption	100%	94%	5.4 seconds
Phishing Detection	95.2%	91%	2.3 seconds
SMS Analysis	92.5%	87%	1.5 seconds
Overall Platform	95.9%	89%	2.1 seconds

The file encryption module showed perfect functionality with a 100% success rate in both hiding and retrieving encryption keys from images. Users appreciated the innovative approach of hiding keys in pictures, which they found both secure and creative. The steganography technique proved completely invisible to human eyes while maintaining full data integrity.

System integration worked smoothly across all three security components. Users could easily switch between different security tools without confusion or technical difficulties. The unified interface design helped users understand and access all features from a single dashboard, eliminating the need for multiple security applications.

V. CONCLUSION

The Cyber-Guardian Suite successfully demonstrates that combining multiple security technologies into one platform can provide comprehensive protection against various cyber threats. Our integrated approach addresses the major weakness of traditional security solutions, which typically focus on only one type of threat at a time. The project achieved all its main objectives with excellent results. The file encryption module with steganographic key hiding showed 100% reliability, proving that secret keys can be safely hidden in images without detection. The phishing detection system reached 95.2% accuracy using machine learning techniques, effectively identifying dangerous websites before users can be harmed. The SMS threat analyzer achieved 92.5% accuracy in detecting fraudulent text messages, helping users avoid financial scams and identity theft. This research proves that integrated cyber-security platforms can offer better protection than separate security tools.

REFERENCES

1. Sindhu, R., & Singh, P. (2020). Information Hiding using Steganography. International Journal of Engineering and Advanced Technology, 9(4), 1549-1554.ijeat+1
2. Sumathi, C.P., Santanam, T., & Umamaheswari, G. (2013). A Study of Various Steganographic Techniques Used for Information Hiding. International Journal of Computer Science & Engineering Survey, 4(6), 9-22.arxiv
3. Parvez, M.T., & Gutub, A.A. (2024). A novel technique for image steganography based on maximum... Multimedia Tools and Applications, 83, 1-13.link.springer
4. Yadav, R. (2023). A NEW METHOD FOR IMAGE STEGANOGRAPHY USING THE... International Journal of Computer Science and Mobile Computing, 12(2), 14-25.ijcsmc
5. Parvez, M.T., & Gutub, A. (2025). A novel and efficient digital image steganography technique using... Scientific Reports, 15, 1-15.nature

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806013

6. Pitropakis, N., Basbas, M., Dalatis, K., Doyamis, E., Srifi, M.D., & Katsikas, S. (2024). A systematic review and research challenges on phishing... Personal and Ubiquitous Computing, 28, 1-25.link.springer
7. Goel, D. (2024). Detection and Prevention of Smishing Attacks. arXiv preprint arXiv:2501.00260, 1-63.arxiv
8. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2022). Digital image steganography: A literature survey. Information Sciences, 1-20.sciencedirect
9. Althobaiti, K., & Alsufyani, N. (2024). A review of organization-oriented phishing research. PMC, 1-15.pmc.ncbi.nlm.nih
10. Various. (2024). Smishing Detection: Combating SMS Phishing Attacks by Utilizing... SSRN, 1-10.papers.ssrn
11. Al-Nawasrah, A., Almomani, A.M., & Manasrah, A. (2025). A Survey on Phishing Attack Taxonomy, Detection Techniques... Journal of Network and Systems Management, 33, 1-20.tandfonline
12. Shabir, M.Y., Zubair, M., Khan, M.A., & Asad, M.U. (2023). A Case Study on Smishing: An Assessment of Threats against... Proceedings of the ACM Conference, 1-10.acm
13. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science, 3, 1-15.frontiersin
14. Various. (2024). Analysing The Impact of Smishing Attack in Public Announcement... Procedia Computer Science, 1-10.sciencedirect
15. Pitropakis, N., Basbas, M., Dalatis, K., Doyamis, E., Srifi, M.D., & Katsikas, S. (2023). Mitigation strategies against the phishing attacks. Computers & Security, 1-25.sciencedirect