International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802429

A Multi-Layer Image Cyber Security Model using Controlled Reconstruction for Secure Data Transmission

Mr. Mohan Raj. P[1], Mr. Kesavan. R[2], Ms. Subiksha. S[2], Ms. Subashini. S[2]

Assistant Professor, Department of Computer Science Engineering, Muthayammal Engineering College, Tamil Nadu, India[1]

UG Scholars, Department of Artificial Intelligence and Data Science Muthayammal College of Engineering, Tamil Nadu, India[2]

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: Cyber Secure transmission of sensitive information has become a critical requirement in modern cyber and defense communication systems. Conventional encryption techniques provide strong protection; however, they remain vulnerable when attackers gain access to encryption keys or intercept encrypted files. To address this limitation, this paper proposes a Multi-Security Image Cyber Model designed for highly confidential data transmission environments such as military communication networks.The proposed framework introduces a multi-image based security architecture where a set of five cover images is initially collected and processed. From this set, three images are dynamically selected using a controlled selection mechanism to reduce predictability. Sensitive data is then embedded within the selected images using a matrix-based embedding structure. The system generates a single reconstruction password at a predefined reference point, which acts as the unified key required to combine the three images and recover the hidden information.Unlike conventional methods that rely on a single encrypted carrier, the proposed model distributes security parameters across multiple images and integrates them through a tri-component reconstruction process. Even if an adversary intercepts the transmitted images or partially discovers the authentication key, reconstructing the original confidential data remains extremely difficult because the security structure depends on the correct image combination and reconstruction point.

The proposed approach offers enhanced resistance against brute-force attacks, interception threats, and unauthorized decoding, while maintaining efficient transmission performance. The architecture demonstrates a flexible and robust security model suitable for applications requiring high confidentiality, controlled reconstruction, and multi-layer cyber protection.

KEYWORDS: Image Security, Detections, cyber security, community computing, cybercrime

I. INTRODUCTION

In recent years The rapid growth of digital communication technologies has significantly increased the need for secure transmission of sensitive information. In critical sectors such as military communication, intelligence systems, and national security networks, protecting confidential data during storage and transmission is a major challenge. Traditional security techniques mainly rely on cryptographic algorithms to encrypt information before transmission. Although these approaches provide strong mathematical protection, they may still become vulnerable if encryption keys are intercepted or compromised during communication.In recent years, researchers have explored alternative approaches such as image-based data hiding and multi-layer security mechanisms to enhance protection levels beyond conventional encryption. Image steganography and multimedia security methods allow confidential information to be concealed within digital images, making the presence of hidden data less noticeable to unauthorized users. However, many existing techniques depend on a single cover image or a single encryption key, which creates a potential point of failure if the system is attacked or partially decoded.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802429

To overcome these limitations, advanced security models are required that distribute confidential information across multiple carriers and integrate multiple protection layers. Such approaches reduce the risk of unauthorized data reconstruction and improve resistance to cyber-attacks. Multi-image security systems provide an effective way to fragment information, hide data within several images, and require specific reconstruction procedures for retrieving the original content.

In this work, a Multi-Security Image Cyber Model is proposed for secure transmission of confidential data in sensitive environments. The proposed approach utilizes a group of five images, from which three images are dynamically selected for the data embedding process. The selected images are organized using a matrix-based structure and combined through a controlled reconstruction mechanism. A single password generated at a designated reference point is required to reconstruct the emedded data from the selected images.

The main objective of this system is to introduce an additional layer of security by distributing the authentication parameters across multiple images and controlling the reconstruction process through a unified access key. Even if an attacker intercepts the transmitted images or attempts to decode the password, the absence of the correct image combination and reconstruction point prevents the recovery of the original confidential data.The proposed framework aims to enhance the confidentiality, integrity, and robustness of secure data transmission systems while maintaining efficient processing and communication performance. Such a multi-layer security architecture can be applied in domains that require highly secure communication, including defense communication systems, intelligence data transfer, and cyber-secure information exchange platforms. people.

1.1 Problem Statement

Much research has been done on phishing detection strategies. The heuristic-based approach and the blacklist-based detection method are common phishing detection strategies. A consistent list of websites that are flagged as phishing sites is kept up to date using the blacklist-based method; if a user requests a page and it appears in the list, the connection is refused. This method is widely employed and has a low false-positive rate; yet, the quality of the list that is kept determines how accurate it is. As such, one of its drawbacks is that it can't identify transient phishing websites. The heuristic-based detection method uses information gleaned from the analysis and extraction of phishing site attributes to identify phishing sites. To suggest a fresh approach to phishing detection based on heuristics that addresses the drawbacks of the blacklist-based method. We put the suggested method into practice and evaluated its performance through experimentation. The suggested method determines whether a requested site is a phishing site by extracting features from the URLs of pages that users request and applying those features. This method can help lessen the harm caused by phishing assaults since it can identify phishing websites that blacklist-based methods are unable to identify.

II. SURVEY OF DETECTIONS

2.1. Survey of review Phishing detection using machine learning techniques- Online reviews are a great source of information that can be used to ascertain the general public's opinion on items or services, and they are frequently the main deciding factor for customers when making a purchase. Manufacturers and retailers are very worried about customer feedback and reviews because of their impact. A dependence on internet evaluations raises the possibility that dishonest people would fabricate reviews in order to fraudulently promote or minimize goods and services. Opinion (review) phishing is the activity of manipulating and poisoning reviews (i.e., creating fictitious, dishonest, or misleading evaluations) for financial advantage. It's critical to have methods for spotting review phishing as not all internet reviews are reliable and truthful. By obtaining significant characteristics from the text using Natural Language Processing (NLP), a review of Phishing detection can be carried out with different machine learning methods. Aside from the content itself, reviewer information can also be utilized to help in this process. In this work, we examine the popular machine learning methods that have been put out to address the issue of review phishing detection as well as the effectiveness of various strategies for review phishing classification and detection. Most recent work has concentrated on supervised learning techniques, which necessitate labeled data, which is hard to get by in online review phishing. Given the millions of online evaluations that exist and the millions more that are created every day, research on Big Data techniques is interesting. We have not yet located any papers that investigate how big data analytics might be used to review phishing detection. This paper's main objective is to present a thorough and robust comparison of recent studies on the detection of review phishing using different machine learning approaches and to develop a methodology for carrying out additional research.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802429

2.2 Fast and effective clustering of Phishing URL's based on structural similarity- Phishing URLs cost businesses and individual users a great deal of money, time, and storage space every year. Locating and prosecuting Phishing URL's perpetrators as well as its eventual stakeholders should enable direct attack of the issue's core cause. In this research, we offer a methodology to quickly and effectively partition vast amounts of Phishing URLs into homogeneous campaigns using classification. This will help facilitate a challenging analysis that needs to be performed on big quantities of unclassified raw URLs structural resemblance. The framework makes use of the category Clustering Tree (CCTree), a revolutionary category clustering algorithm, and a set of 21 attributes that are typical of the email structure. The approach is assessed and verified using common tests carried out on three datasets containing more than 200k authentic, current phishing URLs.

2.3. Cosdes: A collaborative Phishing detection system with a novel e-mail abstraction scheme.- hese days, email communication is essential, yet the issue of email phishing keeps getting worse. The major goal of the similarity matching method for phishing detection is to prevent phishing attempts by keeping track of known phishing sites created through user feedback. Previous works mostly portray each email by a brief abstraction taken from the body of an email. Nevertheless, these email abstractions are insufficiently effective in near-duplicate detection because they fail to capture the dynamic nature of phishing attempts. In this work, we suggest a unique email abstraction method that uses the structure of emails as a representation of emails. We provide a process to create the email abstraction from HTML content in emails, and this newly created abstraction is better able to represent the Phishing's near-duplicate phenomenon. Additionally, we create a comprehensive Phishing detection system called COsdes (Collaborative Phishing Detection System), which has a progressive update strategy and an effective near-duplicate matching technique. The system Cosdes are able to maintain the most recent data for near-duplicate detection thanks to the progressive updating scheme. We assess Cosdes using real-time data data gathered from an actual email server and demonstrate how our system performs better in real-world applications and detection results than previous methods.

2.4. Apache Mahout: Scalable machine learning and data mining.-Building scalable machine learning libraries is Mahout's mission. Scalable to reasonably large data sets is what we mean when we say scalable. We use the map/reduce paradigm to construct our key algorithms for batch-based collaborative filtering, clustering, and classification on top of Apache Hadoop. We do not, however, limit contributions to Hadoop-based implementations; contributions running on a single node or on a cluster that is not based on Hadoop are also welcome. The core libraries have undergone extensive optimization to enable strong performance even with non-distributed algorithms. scalable to back up your commercial argument. * Scalable: Mahout is offered under an Apache Software license that is beneficial to businesses community. Building a dynamic, responsive, and diverse community is Mahout's aim in order to promote conversations about possible use cases as well as the project itself. Visit the mailing lists for additional information.

III. EXISTING SYSTEM

In current secure communication systems, protecting sensitive information is commonly achieved through traditional cryptographic techniques and standard data encryption algorithms. Methods such as symmetric encryption and public-key cryptography are widely used to secure confidential data before transmission across communication networks. These approaches convert readable data into encrypted form using a secret key so that only authorized users with the correct key can decrypt and access the original information.

Another commonly used approach is image steganography, where secret data is hidden within digital images. In these systems, a single image is typically used as the cover medium, and the confidential information is embedded into the image pixels using techniques such as Least Significant Bit (LSB) substitution or transform-domain embedding. The modified image is then transmitted to the receiver, who extracts the hidden data using a predefined key or algorithm.

Although these methods provide a certain level of security, they still have several limitations. Many existing systems rely on a single carrier medium, such as one encrypted file or one cover image. If an attacker intercepts the transmitted file and manages to break the encryption key or identify the hidden data pattern, the entire confidential information can be exposed. In addition, single-key security models create a potential vulnerability because the compromise of one key can lead to complete system failure. Furthermore, most existing image-based security systems do not incorporate multi-layer authentication or distributed security mechanisms. The absence of multiple validation points makes the system more susceptible to brute-force attacks, interception attacks, and unauthorized reconstruction of hidden data. As cyber threats continue to evolve, these limitations highlight the need for more advanced data protection frameworks that integrate multiple security layers and reduce the risk of information leakage.Therefore, a more robust and secure approach is required to overcome these weaknesses. This motivates the development of a multi-image based security

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802429

model that distributes confidential data across multiple images and requires controlled reconstruction through a unified authentication mechanism.

3.1 Drawbacks:

A Phishingmer may transmit more than 100,000 bulk URLs in an hour with very little money.
Transmission and storage bandwidth are wasted by junk mail.
The reason phishing is problematic is that we, the receiver, are made to bear the expense.
Phishing URLs will hog disk space.
Waste time, generate malicious virus, and have a major negative impact on users' phishing links.

IV. PROPOSED SYSTEM

It is more difficult to handle electronic phishing when dealing with a large number of URLs in the recipient's inbox and shielding them from phishing URL attacks. It depends on how each recipient interprets the communication and how they plan to use email exchanges. An official or authoritative figure who used to take action against it can view a phishing attempt as a ham to the average person. Certain emails could also be considered phishing because they frequently utilize phrases associated with phishing, even if they are issued by the authorities in charge of control or with the noble intention of warning people against phishing.

To prevent these types of misclassifications and to rigorously guard against Phishing attacks with minimal training requirements The suggested approach is arrived at. This methodology will use the likelihood that multiple distinct terms will occur in an email and their likelihood of being phished to draw inferences about the email's legitimacy. The suggested methodology classifies emails using SVM classifiers in order to determine if they are phishing or legitimate. SVM primarily works to achieve two goals: first, it accurately classifies emails into ham and phishing URLs; second, it classifies emails based on the relative frequency of words that indicate ham or phishing, using an approach that ensures none of the recipient's healthy emails should be identified as phishing.

Generally speaking, SVM classifiers use training data to classify a group of objects to determine the type of data that falls into a particular category. It will classify it into the appropriate category if it discovers something similar throughout the testing process. To comprehend the underlying classification mechanism, the following is a description of the basic work function of such an NB classifier.

4.1 Advantages:

Conserve storage and network bandwidth Screen sent and received messages.Look for malware.

4.2 SYSTEM ARCHITECTURE

Phishing's are To overcome the limitations of conventional encryption and single-image steganography methods, this work proposes a Multi-Security Image Cyber Model for highly secure transmission of confidential data. The proposed system introduces a multi-layer protection mechanism where sensitive information is distributed across multiple images instead of relying on a single carrier. This approach significantly reduces the possibility of unauthorized reconstruction even if some parts of the transmitted data are intercepted.In the proposed framework, the system initially collects five different images that act as potential carriers for secure data embedding. From these images, three images are dynamically selected using a controlled selection mechanism. The random selection process increases unpredictability and prevents attackers from identifying which images actually contain the embedded information.

Once the images are selected, confidential data is embedded within these images using a matrix-based embedding structure. The three selected images are logically arranged in a matrix format, which allows the system to distribute the encoded data across multiple image layers. This distributed structure ensures that the complete information cannot be recovered from a single image alone.

To further strengthen the security architecture, the system generates a single reconstruction password at a predefined reference point. This password acts as a unified authentication key that is required to combine the selected images and retrieve the original hidden information. The reconstruction process only occurs when the correct images and the corresponding password are provided together at the authorized reconstruction point.

An important feature of the proposed model is that even if an attacker intercepts the transmitted images or partially discovers the authentication key, reconstructing the original data remains extremely difficult. Without the correct combination of images and the proper reconstruction point, the hidden information cannot be accurately recovered.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802429

This multi-layer structure provides strong protection against brute-force attacks, interception attempts, and unauthorized decoding.

The proposed system therefore introduces a robust and flexible cyber security framework that integrates multi-image embedding, controlled image selection, and centralized reconstruction authentication. This architecture enhances the confidentiality and integrity of sensitive data while maintaining efficient transmission performance, making it suitable for applications such as military communication, defense data exchange, and high-security information systems.

V. MODULES

- Data set Acquisition
- Image collection module
- Dynamic Image Selection
- Password Generation

The proposed Multi-Security Image Cyber Model is designed to provide a multi-layer protection mechanism for confidential data transmission. The system architecture consists of several functional stages including image acquisition, dynamic image selection, secure data embedding, password generation, transmission, and controlled reconstruction. Each stage contributes to the overall security and ensures that the original information can only be recovered under authorized conditions.

Image Collection Module
In the first stage, the system collects a set of five digital images that serve as potential carrier images for hiding confidential information. These images may be obtained from a secure image repository or predefined dataset. The use of multiple images increases the complexity of the security structure and reduces the probability of successful data interception.

Dynamic Image Selection Model
From the available image set, three images are dynamically selected through a controlled selection mechanism. The selection process may involve randomization or algorithmic filtering to prevent predictability. This step ensures that the attacker cannot easily determine which images contain the embedded information.

Data Embedding Model
After the images are selected, the confidential data is embedded into the selected images using a matrix-based embedding technique. The images are arranged in a logical matrix structure, and portions of the sensitive data are distributed across the image pixels. This distributed embedding approach ensures that no single image contains the complete information.

Password Generation Model
To strengthen the security layer, a single reconstruction password is generated at a predefined reference point within the system. The password is derived using parameters related to the selected images and embedding structure. This password acts as the main authentication key required for reconstructing the original information.

Secure Transmission Model
The encrypted images are then transmitted through the communication network. Since the data is distributed across multiple images, intercepting one image does not provide meaningful information to an attacker. This design increases resistance to interception attacks and unauthorized access.

Reconstruction and Data Recovery Model
At the receiver side, the system verifies the correct combination of the three selected images along with the generated password. Only when these conditions are satisfied does the system reconstruct the matrix structure and extract the embedded confidential data. If the incorrect images or an invalid password are used, the reconstruction process fails and the original information remains protected.

Overall, the proposed system model integrates multi-image embedding, controlled selection, and centralized reconstruction authentication to provide a secure and reliable data transmission framework suitable for high-security applications such as military communication and confidential data exchange.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802429

VI. CONCLUSION

The protection of sensitive information during digital communication is becoming increasingly important, particularly in environments where data confidentiality is critical. This study introduced a multi-layer image-based security framework designed to strengthen data protection during transmission. The proposed approach distributes confidential information across several images and controls the reconstruction process through a unified authentication mechanism.

In the developed model, a group of five images is initially considered, from which three images are selected for secure data embedding. The embedded information is organized using a matrix-oriented structure and protected by a reconstruction password generated at a designated reference point. This mechanism ensures that the hidden information can only be recovered when the correct image combination and authentication key are available simultaneously.

The distributed nature of the proposed framework increases the difficulty for unauthorized users attempting to recover the original data. Even if transmitted images are intercepted, the absence of the correct reconstruction parameters prevents successful extraction of the confidential content. As a result, the proposed design enhances the overall security level compared with conventional single-image or single-key protection techniques.

The proposed approach demonstrates potential for secure communication systems where maintaining confidentiality is essential. The framework may be further extended to support advanced image processing techniques and stronger cryptographic mechanisms for improved protection in future cyber-secure communication environments.

VII. FUTURE ENHANCEMENT

Obtaining precise categorization, with 0% of phishing emails being misclassified as ham emails and ham emails being misclassified as phishing emails. The attempts would be made to stop phishing emails, which are a greater cause for concern these days and carry phishing attacks. Additionally, the approach can be expanded to prevent Denial of Service (DoS) attacks, which are now known as Distributed Denial of Service Attacks (DDoS) because they occur in a distributed manner.

REFERENCES

1. R. Zhang, S. Cui, and C. Zhao, “A Three-Factor-Based Authentication Scheme of 5G Wireless Sensor Networks for IoT System,” in Proc. Int. Conf. Commun. Signal Process. Syst., 2018, pp. 875–880.
2. Y. Shi, Y. Zhao, R. Xie, and G. Han, “Designing a structural health monitoring system for the large-scale crane with narrow band IoT,” in Proc. IEEE 23rd Int. Conf. Comput. Supported Cooper. Work Design (CSCWD), 2019, pp. 239–242.
3. Y. Zhu, G. Jia, G. Han, Z. Zhou, and M. Guizani, “An NB-IoT-based smart trash can system for improved health in smart cities,” in Proc. IEEE 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), 2019, pp. 763–768.
4. D. He, S. Zeadally, B. Xu, and X. Huang, “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular adhoc networks,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 12,
5. pp. 2681–2691, Dec. 2015.
6. J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, “PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks,” IEEE Trans. Depend. Secure Comput., vol. 18, no. 2, pp. 722–735, Mar./Apr. 2021.
7. C.Nagarajan and M.Madheswaran - ‘Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques’- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
8. C.Nagarajan and M.Madheswaran - ‘Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter’ - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
9. C.Nagarajan and M.Madheswaran - ‘Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis’- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
10. S.Tamilselvi, R.Prakash, C.Nagarajan,“Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller” Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802429

11. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
12. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
13. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- *Acta Electrotechnica et Informatica Journal* , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
14. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- *Springer, Frontiers of Electrical and Electronic Engineering*, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
15. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- *Iranian Journal of Electrical & Electronic Engineering*, Vol.8 (3), pp.259-267, September 2012.
16. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
17. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
18. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
19. Anand, L., Maurya, M., Seetha, J., Nagaraju, D., Ravuri, A., & Vidhya, R. G. (2023, July). An intelligent approach to segment the liver cancer using Machine Learning Method. In 2023 4th international conference on electronics and sustainable communication systems (ICESC) (pp. 1488-1493). IEEE.
20. Rajendran, S., Sundarapandi, A. M. S., Krishnamurthy, A., & Thanarajan, T. (2022). An intelligent face recognition technology for iot-based smart city application using condition-cnn with foraging learning pso model. International Journal of Pattern Recognition and Artificial Intelligence, 36(14), 2256018.
21. Murugeshwari, B., & Sujatha, R. (2014). Preservation of Privacy for Multiparty Computation System with Homomorphic Encryption. International Journal of Emerging Technology and Advanced Engineering, 4(3), 530-535.
22. Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
23. Samrat, B., Thomas, P. K., Kumar, S., Benila, A., Bhardwaj, R., & Vigenesh, M. (2024, December). Industrial informatics in optimizing software-defined vehicles for logistics. In 2024 IEEE 2nd International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP) (pp. 1-9). IEEE.
24. Soundappan, S. J. (2024). AI-driven customer intelligence in enterprise lakehouse systems Sentiment Mining Governance-Aware Analytics and Real-Time Data Synchronization. International Journal of Advanced Engineering Science and Information Technology.
25. Rajasekar, M. (2024). AI-Powered Cyber-Secure Federated Learning on AWS for Next-Generation Digital Banking Analytics. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(3).
26. Deivendran, P., Babu, P. S., Malathi, G., Anbazhagan, K., & Kumar, R. S. (2023). Emotion Recognition for Challenged People Facial Appearance in Social using Neural Network. arXiv preprint arXiv:2305.06842.
27. Sugumar, R., & Murugeshwari, B. (2016). An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks.
28. Pandey, V. K., Mishra, S., Rengarajan, A., Savita, & Roomi, M. M. (2024, March). Enhancing Weather Forecasting with Machine Learning Techniques. In International Conference on Renewable Power (pp. 147-156). Singapore: Springer Nature Singapore.
29. Mathew, A., & Alex, H. (2025). Federated Learning for Secure Genomic Research: Privacy-Preserving AI Solutions for Precision Medicine. Science and Technology: Developments and Applications Vol. 9, 36-43.
30. Selvi, G. V., Anbarasan, A. B., Murthy, B. A., & Prabavathy, S. (2023). An Application Oriented Integrated Unequal Clustering Algorithm for Wireless Sensor Network. In Underwater Vehicle Control and Communication Systems Based on Machine Learning Techniques (pp. 140-154). CRC Press.
31. Soundappan, S. J. (2025). Next Generation AI Enabled Holistic Cognitive Platform for Secure Cloud Network Intelligence Enterprise Systems and Digital Trust Optimization. International Journal of Computer Technology and Electronics Communication, 8(5), 11534-11542.
32. Rajasekar, M. (2024). Real-Time Predictive DevOps Intelligence for Risk-Aware Digital Business Processes in Cloud and SAP Ecosystems. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10713-10718.
33. Jagadeesh, S., & Sugumar, R. (2017). A comparative study on artificial bee colony with modified ABC algorithm. European Journal of Applied Sciences, 9(5), 243–248.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802429

34. Murugeshwari, B., Sarukesi, K., & Jayakumar, C. (2010, March). An efficient method for knowledge hiding through database extension. In 2010 International Conference on Recent Trends in Information, Telecommunication and Computing (pp. 342-344). IEEE.
35. Reddy, K. V. V. K., & Vimal, V. R. (2024, July). A novel approach on improved segmentation and classification of remote sensing images using AlexNet compared over linear discriminant analysis with improved accuracy. In 2024 Second International Conference on Advances in Information Technology (ICAIT) (Vol. 1, pp. 1-6). IEEE.
36. Gowthami, D., & Vigenesh, M. (2024). Distributed and Lightweight Intrusion Detection for IoT: A Lightweight Pyramidal U-Net With Tri-Level Dual Inception-Based Framework. In The Convergence of Self-Sustaining Systems With AI and IoT (pp. 154-173). IGI Global Scientific Publishing.
37. Anand, P. V., & Anand, L. (2023, December). An Enhanced Breast Cancer Diagnosis using RESNET50. In 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1-5). IEEE.
38. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
39. Dhinakaran, D. (2022). Joe Prathap P. M, Selvaraj D, Arul Kumar D and Murugeshwari B," Mining Privacy-Preserving Association Rules based on Parallel Processing in Cloud Computing,". International Journal of Engineering Trends and Technology, 70(3), 284-294.
40. Poornima, G., & Anand, L. (2024, April). Effective Machine Learning Methods for the Detection of Pulmonary Carcinoma. In 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) (pp. 1-7). IEEE.
41. Rengarajan, A., Jayakumar, C., & Sugumar, R. (2012). Optimization Of Recent Attacks Using Internet Protocol. National Journal of System and Information Technology, 5(1), 8.
42. Mathew, A., & Romasco, L. (2024). Forensic Investigation of Artificial Intelligence Systems. Research Updates in Mathematics and Computer Science Vol. 4, 154-164.
43. Vekariya, V., Kumar, S., & Rengarajan, A. (2024). A distinctive and smart agricultural knowledge-based framework using ontology. In Sustainability in Digital Transformation Era: Driving Innovative & Growth (pp. 207-213). CRC Press.
44. Soundappan, S. J. (2020). Big data analytics in healthcare: Applications for pandemic forecasting. International Journal of Advanced Research in Computer Science & Technology, 3.
45. Sugumar, R. (2024). AI-Augmented Quality Engineering for Performance Optimization and Test Orchestration in Distributed Systems. International Journal of Science, Research and Technology, 7(5), 12835-12846.
46. Soundappan, S. J., & Sugumar, R. (2016). Optimal knowledge extraction technique based on hybridisation of improved artificial bee colony algorithm and cuckoo search algorithm. International Journal of Business Intelligence and Data Mining, 11(4), 338–356.
47. Mathew, A. (2025). Ahead of the breach: Predictive threat intelligence in aviation inspired by Scattered Spider attacks. Multidisciplinary International Journal of Research and Development (MIJRD), 4(6), 54–58.
48. Soundappan, S. J. (2021). DataOps: Orchestrating Reliable ML Data Pipelines. International Journal of Research and Applied Innovations, 4(4), 5533-5537.
49. Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. South Asian Research Journal of Engineering and Technology, 2(6), 62–64.
50. Anand, L., Tyagi, R., & Mehta, V. (2024, January). Food recognition using deep learning for recipe and restaurant recommendation. In Proceedings of Eighth International Conference on Information System Design and Intelligent Applications (pp. 269-279). Singapore: Springer Nature Singapore.
51. Kumar, A., & Anand, L. (2025). A Novel EEG-Based Deep Learning Framework for Enhancing Communication in Locked-In Syndrome Using P300 Speller and Attention Mechanisms. KSII Transactions on Internet and Information Systems (TIIS), 19(11), 3841-3855.
52. Soundappan, S. J. (2022). AI-Based Fault Detection and Isolation for Reliability in Modern Power Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(4), 7106-7110.
53. Chandra, S., Rengarajan, A., Sahoo, G. S., & Sharma⁴, S. (2024, October). Identifying Neuronal Damage and Plasticity by Analyzing Changes in Diffusion Tensor. In Proceedings of the 5th International Conference on Data Science, Machine Learning and Applications; Volume 2: ICDSMLA 2023, 15–16 December, Hyderabad, India (Vol. 2, p. 433). Springer Nature.