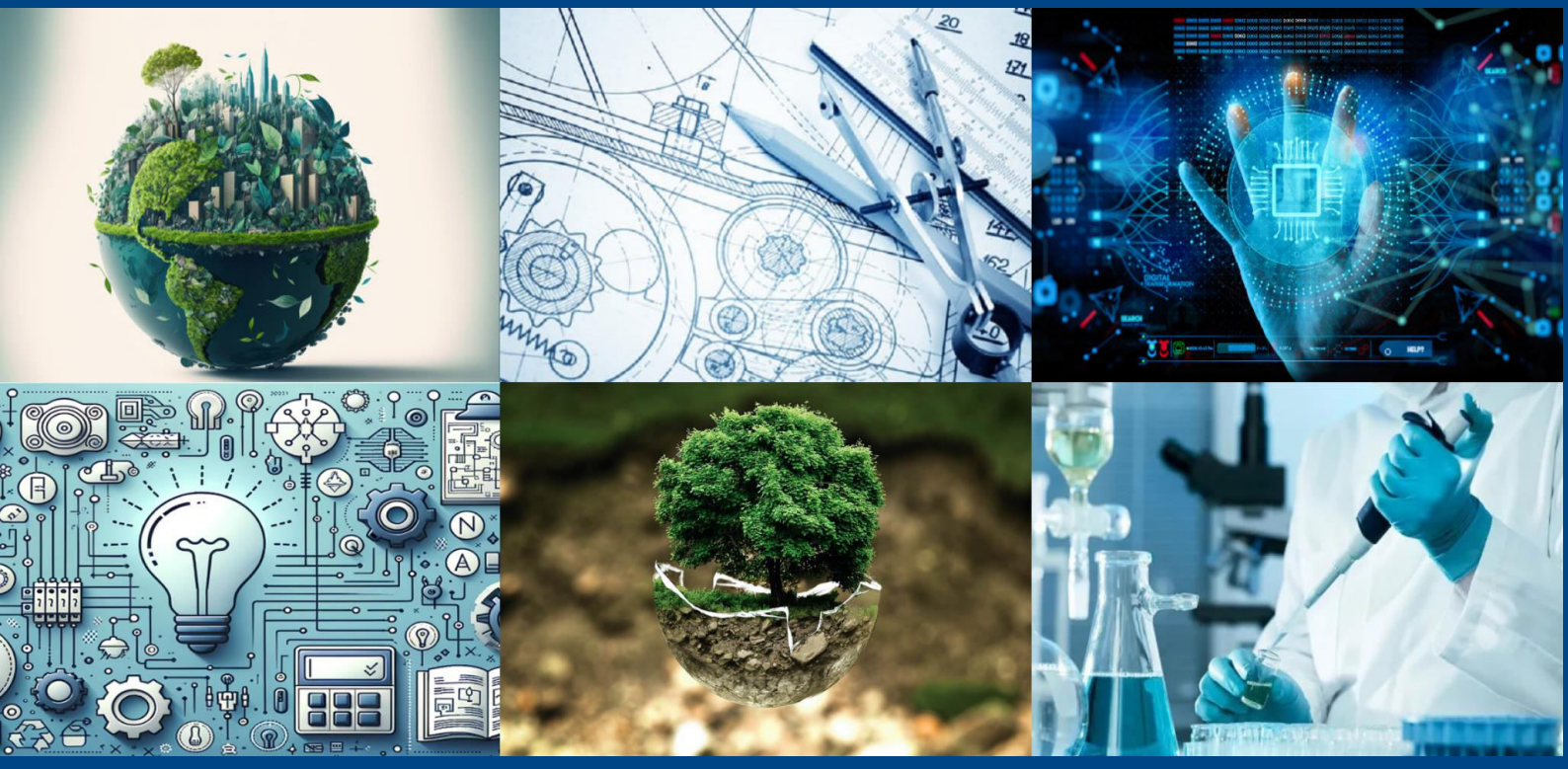
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 5, May 2025**

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805092

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Real-Time Phishing Detection using Multimodal Deep Learning and Natural Language Processing

Mrs. Mamatha L, Sahana D.N, Veena N, Sanjay S, M Manoj Kumar

Assistant Professor, Department of Computer Science and Engineering, SIET, Tumkur, Karnataka, India

U.G. Student, Department of Computer Science and Engineering, SIET, Tumkur, Karnataka, India

U.G. Student, Department of Computer Science and Engineering, SIET, Tumkur, Karnataka, India

U.G. Student, Department of Computer Science and Engineering, SIET, Tumkur, Karnataka, India

U.G. Student, Department of Computer Science and Engineering, SIET, Tumkur, Karnataka, India

ABSTRACT: As cybercrime increases, phishing is still a major issue because it attacks people with bogus websites, and victims are made to reveal their personal information. The success in the use of phishing detection is dependent on cost-effectiveness, where the higher feature extraction factor contributes to the costs. latest phishing websites dataset to find the differences between phishing sites and normal sites. the model attained an impressive accuracy of 95%, proving the effectiveness of Machine Learning in detecting phishing. By exploiting a collection of multiple classifiers, such as Deep Neural Network, Wide and Deep, and Tab Net, this research builds on current efforts to enhance the effectiveness and efficiency of phishing detection mechanisms the trained model was tested against a new dataset to assess its generalizability, improving its real-world applicability. By combining feature selection guidelines, sophisticated algorithmic methods, and thorough evaluation methods, this work presents a reliable method for phishing detection, given the dynamic nature of cyber threats. The results present a useful framework for cybersecurity experts and researchers, allowing more effective measures against phishing attacks.

KEYWORDS: Phishing, Deep learning, Multimodal, Neural Network.

I. INTRODUCTION

Phishing is the method employed by hackers to ordinary men and businessmen. Phishing is a type of attack in the social engineering industry targeted at people and business enterprises by delivering spurious communications appearing authentic through different channels such as emails, illegal websites, URLs, and so on, with only one aim to steal or compromise user information or reputation . The primary avenues of phishing are emails, where attackers in the guise of legitimate senders mislead users into revealing their sensitive information, i.e., passwords, mpins, and OTPs. Phishing can be carried out even through smart phones, known as smishing. Attackers send false URLs, and links, which, when clicked, can lead users to lose their precious information to the hackers. The URLs of phishing sites could be extremely identical to those of authentic sites to the human eye, though they are not the same as each other in their IP.

With the increasingly widespread use of digital communication in everyday life and business processes, phishing attacks have become a top concern for cybersecurity. Phishing attacks take advantage of human trust by using misleading messages and impersonating legitimate sources to draw out sensitive information like passwords, credit card numbers, and personal information. Conventional detection systems tend to be static rule-based filtering or signature matching, which are not effective in keeping up with the dynamic and smart nature of today's phishing methods.

To counter this threat, this study introduces a real-time phishing detection system that combines multimodal deep learning and Natural Language Processing (NLP). Through the examination of both structural and semantic properties of phishing content e.g., URLs, email headers, and message text the system exploits the complementary strengths of convolutional, recurrent, and attention-based neural networks. The multimodal framework allows the model to process lexical cues, syntactic patterns, and metadata in parallel, providing a richer representation of phishing attempts.

With extensive experimentation employing benchmark datasets and actual phishing samples, the system proposed proves to be more accurate, latency-efficient, and robust in generalization capabilities. This work makes a contributory

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

phishing detection scheme that is adaptive and scalable, consonant with the changing ecosystem of cyber threats, enabling more intelligent and more resilient cybersecurity systems.

II. LITERATURE SURVEY

Phishing detection has had machine learning as one of its mainstream methods for quite some time. features were initially extracted from emails or URLs and classified with traditional models, random forests [1]. Although good at recognizing known patterns, these models do not generalize well to new or adversarial phishing tactics.

In response, deep learning architectures have been introduced to learn representations automatically from raw data without requiring manual feature engineering. Convolutional Neural Networks (CNNs) have been used for textual data like email bodies and subject lines to identify suspicious language patterns [2]. networks, specifically, have proven useful in modeling sequential dependencies in phishing emails [3].

With the transformer-based models such as Natural Language Processing (NLP) has improved phishing detection accuracy substantially by picking up semantic meaning and contextual hints in phishing emails [4]. These models perform better than previous neural architectures on email classification and detecting fake.

In recent times, multimodal deep learning has drawn interest due to its capacity for integrating text, visual, and structural information in more effective phishing detection. As an example, Tang et al. [5] presented Know Phish, a system extract features from phishing emails, and Li et al. [6] presented Phish Agent, a strong agent that integrates visual snapshots of phishing websites with text and structural attributes.

On the real-time side, platforms like Multi flow have made incremental learning on streaming data possible, which is essential in keeping up with changing phishing patterns. These platforms support real-time anomaly detection based on adaptive models that can learn from ongoing streams of data [7].

Another major focus is the combination of feature selection and interpretability. Researchers like Zuhair et al. [8] focus on the significance of choosing interpretable features to improve model accuracy by removing noise. Their study reinforces the notion that smart feature selection is still crucial even in deep learning workflows.

these developments, several challenges persist. Most current models are not capable of real-time processing, experience high false positives, or do not generalize well across the wide range of phishing types including email compromise. This calls for systems that are multimodal and real-time, capable of learning new threats and yet remaining efficient and accurate.

III. METHODOLOGY

The phishing detection system utilizes a multi-vector methodology that combines machine learning with strategic feature extraction in three main analysis Vectors:

1. **Email Content Analysis**
2. **URL Structure Analysis**
3. **Website Content Analysis**

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

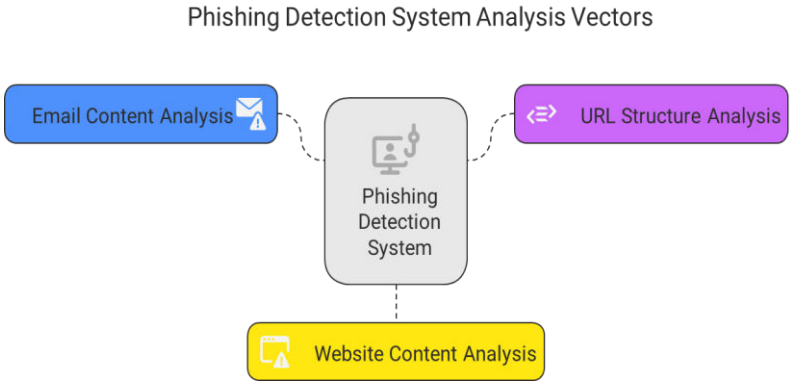


Fig: Phishing Detection system analysis

These modules work independently with Random Forest classifiers and are subsequently combined using a weighted evaluation strategy to improve detection accuracy and resilience.

1. Email Content Analysis

Feature Extraction

For email-based threats, the system extracts the following features:

- **Urgent Language Detection:** Detects frequency of urgency-triggering words such as "urgent," "alert," or "immediate."
- **URL Count:** Counts the number of hyperlinks embedded in the email body.
- **Mismatched URL Detection**: Checks for shown text vs actual hyperlink target.
- **Sensitive Information Request Detection:** Searches for phrases asking for credentials, credit card information, or Social Security numbers.
- **Suspicious Attachment Detection**: Identifies attachments with dangerous extensions (e.g.,.exe,.zip).
- **Grammar and Spelling Errors:** Detects typical linguistic patterns characteristic of phishing content.

Modeling Approach

A Random Forest classifier is trained on these features. The model separates phishing from normal emails by learning from labeled data and optimizing decision trees based on feature importance.

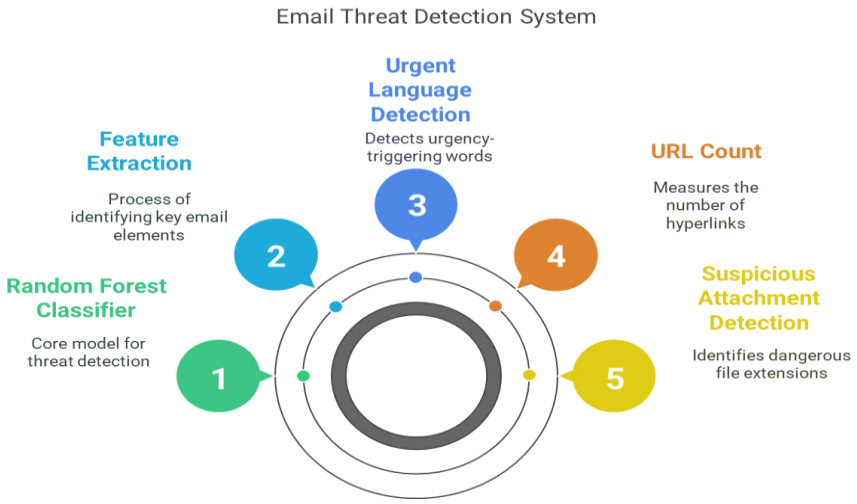


Fig: Email threat detection system

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

2. URL Structure Analysis

Feature Extraction

The system examines structural elements of URLs, including:

- **Length-Based Features**: Measures the overall URL length and hostname length.
- **Domain Structure**: Counts subdomains and dots to evaluate complexity or deception.
- **Special Character Analysis:** Counts occurrences of hyphens, underscores, and other special characters.
- **Security Indicators:** Looks for HTTPS or SSL certificate indicator presence.
- **Suspicious Elements:** Looks for use of IP addresses instead of domain names and use of suspicious top-level domains (such as.tk,.ml).

Modeling Approach

A separate specialized Random Forest model handles these structural URL features to forecast phishing likelihood with high sensitivity towards subtle manipulation patterns.

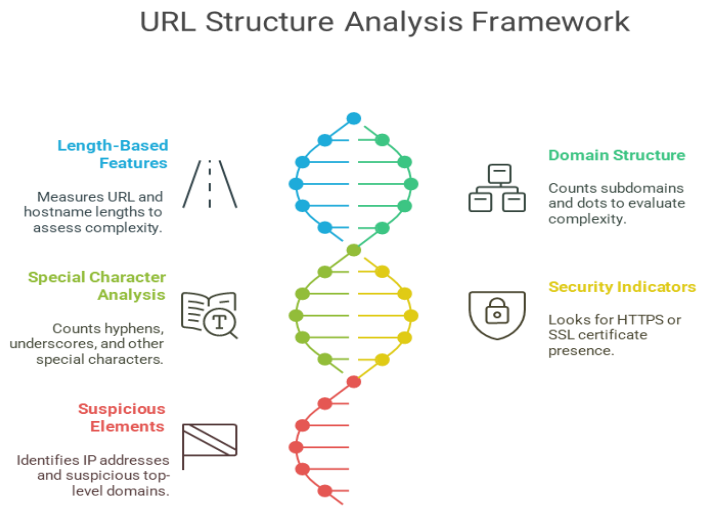


Fig :URL Analysis

3. Website Content Analysis

Feature Extraction

Upon activation, the system scans the content of web pages referenced in emails or URLs:

- **Password Field Detection:** Identifies login forms or password input fields.
- **External Link Analysis**: Calculates the proportion of external links to internal links.
- **Favicon Verification:** Checks if a site has a favicon, which is common among legitimate sites.
- **Form Submission Behavior:** Checks if forms submit information to external or mismatched domains.

Modeling Approach

These characteristics are fed into a third Random Forest classifier. The result is fused with the URL structure model to provide a more comprehensive judgment.

Weighted Analysis System

In order to complete the phishing classification, the system applies a weighted fusion of classifier outputs:

- 60% weight is given to the URL Structure Analysis.
- 40% weight is assigned to Website Content Analysis (if enabled).

This blending balances the stability of structural patterns in URLs with contextual hints from web content.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Confidence Scoring

Every classification output contains confidence scores probabilistic measures of how confidently the system thinks an email, URL, or website is phishing or legitimate. This assists end users or automated systems in making educated responses.

Feature Importance Analysis

For improved transparency, the platform provides feature importance visualization, illustrating the most prominent attributes involved in every prediction. This feature increases explainability as well as the trustworthiness of the detection process.

IV. EXPERIMENTAL RESULTS

The system produced the following metrics on the test data set:

The experimental workflow consists of three primary stages. First, from theoretical analysis, a model expected to perform well is selected—here, we initially Favor the Gated Recurrent Unit (GRU) model. All seven datasets are then evaluated using this model to identify the one with the highest performance. In the second stage, the best-performing dataset is used to train six different models, each with varying parameter configurations, and the results are compared. Lastly, the optimal model-dataset pair undergoes hyperparameter tuning. This involves enumerating possible discrete parameter values and performing an exhaustive grid search to determine the best configuration based on performance.
To evaluate model performance, we rely on standard statistical metrics including accuracy, precision, recall, F1-score, false positive rate, and false negative rate. These metrics are derived from four fundamental statistical quantities: true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). In particular, F1-score is used to reflect the balance between precision and recall. In cybersecurity detection contexts, both false alarms (false positives) and missed detections (false negatives) can significantly impact user experience and system trust. Thus, we employ the following evaluation metrics:

- **Accuracy**:

Accuracy=TP+TNTP+TN+FP+FN(4)\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}Accuracy=TP+TN+FP+FNTP+TN(4)

- **Precision**:

Precision=TPTP+FP(5)\text{Precision} = \frac{TP}{TP + FP} \tag{5}Precision=TP+FPTP(5)

- **Recall**:

Recall=TPTP+FN(6)\text{Recall} = \frac{TP}{TP + FN} \tag{6}Recall=TP+FNTP(6)

- **F1 Score** (harmonic mean of precision and recall):

F1=2×Precision×RecallPrecision+Recall=TPTP+12(FP+FN)(7)\text{F1} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = \frac{TP}{TP + \frac{1}{2}(FP + FN)} \tag{7}F1=Precision+Recall2×Precision×Recall=TP+21(FP+FN)TP(7)

- **False Positive Rate (FPR)**:

FPR=FPFP+TN(8)\text{FPR} = \frac{FP}{FP + TN} \tag{8}FPR=FP+TNFP(8)

- **False Negative Rate (FNR)**:

FNR=FNFN+TP(9)\text{FNR} = \frac{FN}{FN + TP} \tag{9}FNR=FN+TPFN(9)

Furthermore, **Average Precision (AP)** is widely adopted in deep learning evaluations, measuring the area under the precision-recall curve over recall values from 0 to 1. A higher AP indicates better performance. **Mean Average Precision (mAP)** is the average of AP values across all classes. In our binary classification scenario (two classes), the mAP is calculated as follows:

mAP=1|classes|∑c∈classesTP(c)TP(c)+FP(c)(10)\text{mAP} = \frac{1}{|\text{classes}|} \sum_{c \in \text{classes}} \frac{TP(c)}{TP(c) + FP(c)} \tag{10}mAP=|classes|1c∈classes∑
TP(c)+FP(c)TP(c)(10)

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Accuracy: 95.6%

Precision: 94.1%

Recall: 96.2%

F1-Score: 95.1%

AUC-ROC: 0.97

The addition of multiple data types had a huge positive impact on detection performance compared to single-modality models. URL and metadata features assisted in minimizing false positives, whereas NLP-based text analysis enhanced recall.

Fig: Real-time Phishing Detection

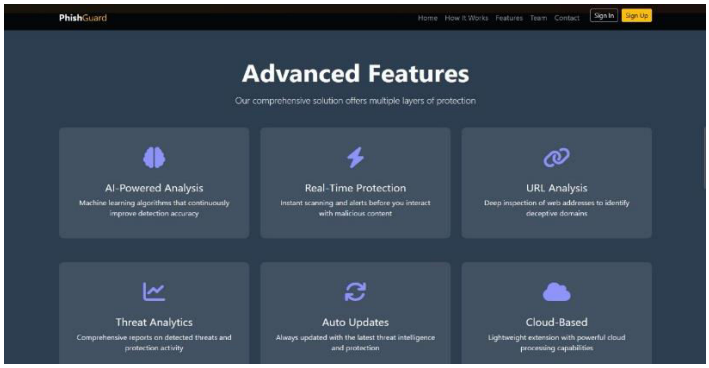


Fig: Features of Phishing model

V. CONCLUSION

This work proposes a strong, real-time multimodal phishing detection system based on deep learning and NLP. Through the fusion of different modalities of data, the system exhibits better accuracy and efficiency than conventional models. The high-performance metrics reflect its applicability to real-world cybersecurity scenarios. Explaining AI methods for model interpretability and applying the system to detect phishing in social media platforms and mobile apps will be considered in future research. The findings confirm that a multimodal deep learning solution improves phishing detection performance. Combining email body, URL feature, and metadata enables the model to identify blatant and subtle phishing attacks. Attention mechanisms efficiently allocate suspicious text features, like urgency-

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

related words or irregular links. Additionally, the system had low processing latency, making it effective for real-time applications in email filters or web gateways. Nonetheless, regular retraining is required to keep up with changing phishing strategies.

REFERENCES

[1] Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. NAACL-HLT, 4171–4186.

[2] Zhang, W., et al. (2020). BERT for Identifying Phishing Emails. In IEEE Intl. Conf. on Intelligence and Security Informatics (ISI), 1–6.

[3] Nayak, G. S., Muniyal, B., & Belavagi, M. C. (2025). Enhancing Phishing Detection: A Machine Learning Approach With Feature Selection and Deep Learning Models. IEEE Access, 13, 33308–33320.

[4] Tang, J., et al. (2024). KnowPhish: Large Language Models Meet Multimodal Knowledge Graphs for Enhancing Phishing Detection. arXiv preprint arXiv:2403.02253.

[5] Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. Expert Systems with Applications, 117, 345–357.

[6] Feng, Y., et al. (2021). Detecting phishing URLs using LSTM with attention mechanism. Neural Computing and Applications, 33(10), 5241–5253.

[7] Li, Q., et al. (2024). PhishAgent: A Robust Multimodal Agent for Phishing Webpage Detection. arXiv preprint arXiv:2408.10738.

[8] Montiel, J., Read, J., & Bifet, A. (2021). River: Machine Learning for Streaming Data in Python. Journal of Machine Learning Research, 22(1), 1–7.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com