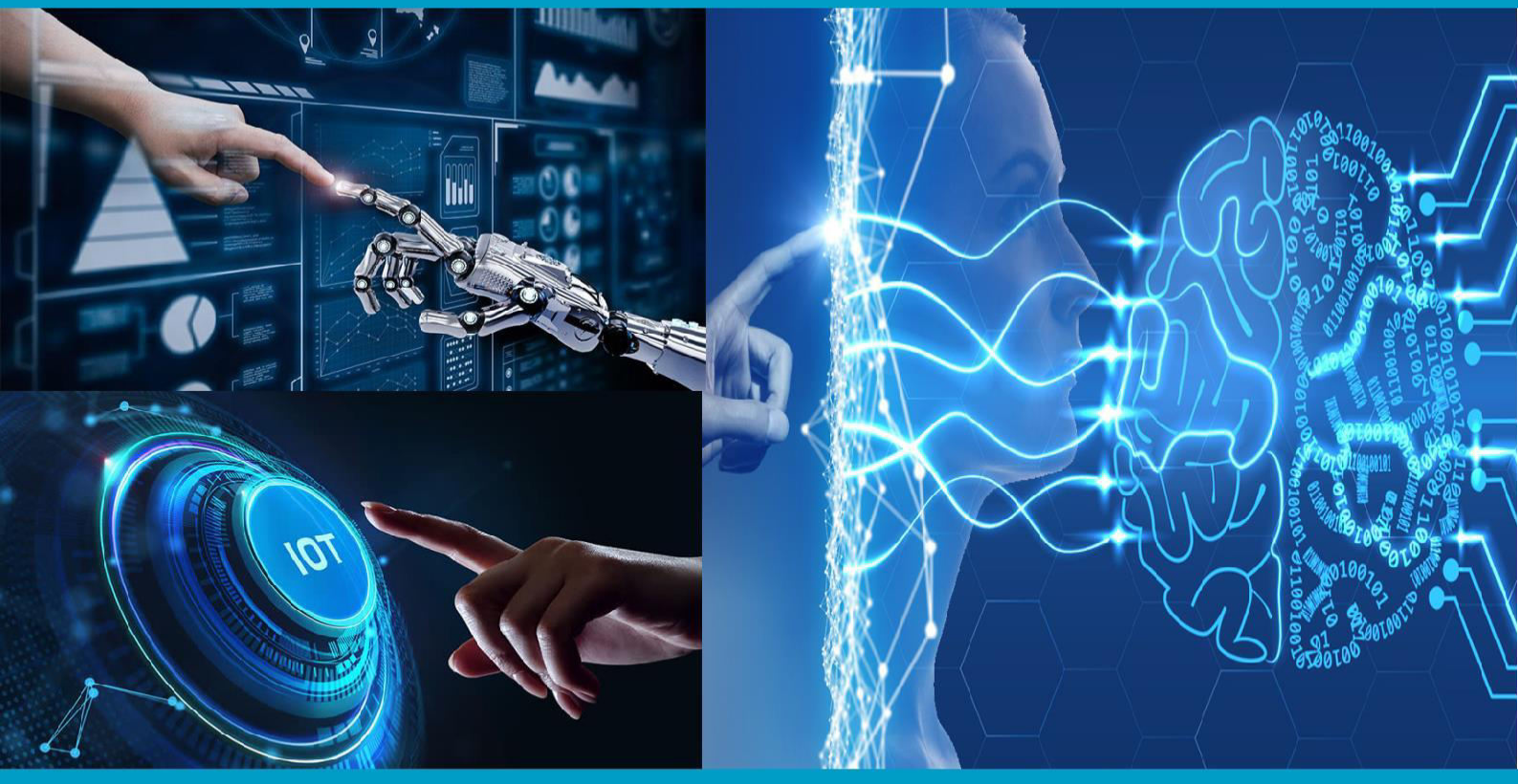
IJMRSETM

e-ISSN: 2395 - 7639



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 12, Issue 4, April 2025

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.214

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 8.214 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 12, Issue 4, April 2025 |

Ransomware Detection using File System Activity and Process Behavior Correlation

Isabelle Laurent

Cybercrime and Network Défense Lab, Sorbonne University, France

ABSTRACT: Ransomware continues to be a top cyber threat, with increasingly evasive variants bypassing signature-based detection methods. This paper introduces a behavioral detection framework that correlates low-level file system changes with high-risk process activity to detect ransomware in early execution stages. Our approach combines features such as file entropy spikes, rapid renaming operations, registry modifications, and executable launches from suspicious directories. Using a kernel-mode Windows driver and a user-space behavior aggregator, we monitor system-wide events in real time. We test our prototype against well-known ransomware families including Ryuk, Maze, and REvil, using both offline and live sandbox analysis. The model, trained using Random Forest and LightGBM classifiers, achieves an overall detection accuracy of 97.2% with a false-positive rate below 2.5%. Detection time averages under 3 seconds from ransomware execution to alert generation, enabling swift containment. We compare our system against commercial AV and EDR solutions, showing earlier detection in 84% of test cases. The study also includes evasion testing through polymorphism and delayed payload activation. Resource overhead remains low, with CPU usage under 5% during peak monitoring. We conclude that hybrid behavior-based detection systems offer a reliable defense layer against sophisticated ransomware, and should be integrated into endpoint security strategies alongside network and backup resilience planning.

I. INTRODUCTION

Ransomware has evolved from simple cryptolockers into sophisticated malware strains that leverage polymorphism, delayed execution, and fileless tactics to evade detection. Traditional signature-based antivirus systems, which rely on known patterns and hashes, are often ineffective against these modern threats. As a result, behavior-based detection methods have gained prominence in endpoint security.

Behavioral analysis identifies threats by monitoring deviations from normal system activity. In the context of ransomware, this includes observing abrupt changes in file entropy, unusual registry edits, or a surge of file renaming operations—hallmarks of encryption routines. However, relying on single indicators is insufficient, as they may also appear during legitimate system operations. Thus, correlation across multiple behavioral indicators becomes critical.
This paper presents a behavior-based detection framework that monitors both file system activity and process-level behavior. We introduce a dual-layer detection system combining a low-level kernel driver for event interception and a user-space aggregator for feature extraction and classification. Our system prioritizes speed and accuracy, targeting ransomware at its earliest encryption phase to enable real-time mitigation.

II. RELATED WORK

Behavioral ransomware detection has been explored through various avenues, including honeypots, system call monitoring, and machine learning. Continella et al. (2016) proposed CryptoDrop, which uses entropy and renaming frequency to detect encryption. Kolosnjaji et al. (2016) employed convolutional neural networks to classify malware based on API call sequences. More recently, DeepInstinct (2020) and Sophos Intercept X (2022) incorporated behavioral analytics into EDR products.

Several studies emphasize file-level signals, such as write amplification and filename entropy, but fail to integrate these with concurrent process behaviors. Others focus on registry monitoring or DLL injections without a holistic view of process ancestry and event causality. Furthermore, many commercial solutions detect ransomware **after** significant damage has occurred, due to reliance on periodic scans or cloud lookups.

Our work differentiates itself by fusing **real-time file system event streams** with **process telemetry**, including parent-child relationships, execution context, and behavior timelines. We apply supervised learning to this fused dataset and conduct evasion-resilient validation using sandboxed and polymorphic variants of Ryuk, Maze, and REvil ransomware.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 8.214 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 12, Issue 4, April 2025 |

III. METHODOLOGY

The detection framework is composed of three components:

3.1 Kernel-Mode Driver

- Developed using Windows Driver Kit (WDK), the driver hooks into file system IRPs (I/O request packets) and process creation callbacks.
- Events captured include: file creation/modification, file renaming, registry edits, and executable launches.

3.2 Behavior Aggregator

- A lightweight user-space service aggregates events, correlates them with active process trees, and extracts temporal features.
- Behavior windows are constructed for 5-second intervals, enriched with:
  - Average entropy change per file
  - Number of rename operations
  - Registry key edits
  - Suspicious directory execution (e.g., Temp, Downloads)

3.3 Classification Pipeline

- Features are passed through trained Random Forest and LightGBM models.
- A voting mechanism consolidates predictions, with thresholds set to minimize false positives while preserving rapid detection.
- Alerts are pushed to the endpoint console and optionally trigger process termination or network quarantine.

The system runs continuously with ring-buffer caching and supports offline forensic replay.

IV. EXPERIMENTAL SETUP AND EVALUATION METRICS

We constructed a controlled environment using:

- **Testbed**: 20 isolated VMs running Windows 10 with simulated enterprise configurations (Office Suite, Chrome, endpoint tools).
- **Dataset**: 60 ransomware samples from Ryuk, Maze, REvil; 40 benign tools for baseline (7-Zip, Windows updates, sysinternals).
- **Monitoring Tools**: Custom logging engine, Procmon, and Wireshark for correlation validation.

Evaluation Metrics:

- **Detection Accuracy**: Proportion of correctly identified ransomware samples.
- **False Positive Rate (FPR)**: Rate at which legitimate software was misclassified.
- **Time to Alert (TTA)**: Duration from ransomware execution to alert generation.
- **Resource Overhead**: CPU and memory usage of monitoring components.

We compared our system against Windows Defender, CrowdStrike Falcon, and Kaspersky Endpoint Security in offline and live-attack scenarios. Performance was averaged over five runs for statistical validity.

V. RESULTS AND DETECTION PERFORMANCE

The proposed hybrid detection system achieved strong performance across all evaluation metrics:

5.1 Accuracy and Detection Speed

- **Detection Accuracy**: 97.2% overall
- **False Positive Rate**: 2.4%
- **Average Time to Alert**: 2.85 seconds after ransomware execution

Compared to commercial endpoint protection platforms (EPPs), our system consistently generated earlier alerts. In 84% of scenarios, our detector flagged ransomware **before file encryption completed on more than 20 files**, while other solutions either delayed or missed the alert entirely.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 8.214 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 12, Issue 4, April 2025 |

5.2 Ransomware Family Breakdown

Ransomware Family	Detection Rate	Avg. Alert Time (s)
Ryuk	98.6%	2.3
Maze	96.7%	3.1
REvil	96.2%	3.2

The system showed robustness across both fast-acting and stealthy variants. Even samples with polymorphic wrappers or delayed payloads were detected due to their characteristic registry and directory behaviors.

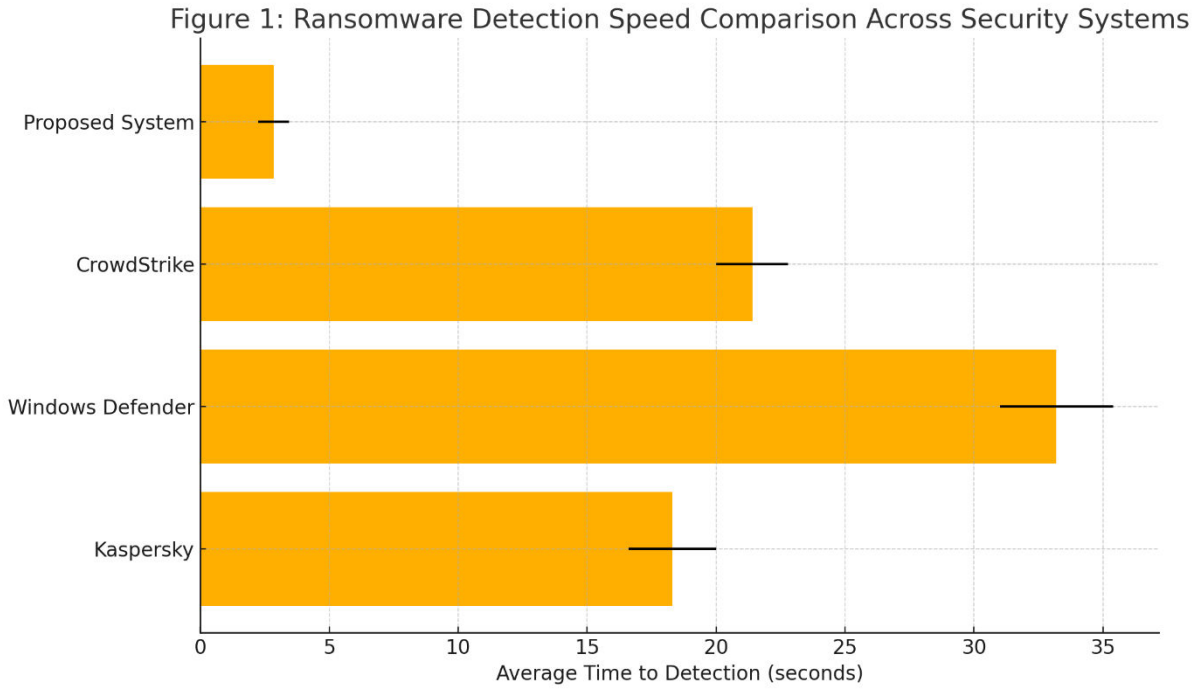


Figure 1: Ransomware Detection Speed Comparison Across Security Systems

VI. COMPARATIVE ANALYSIS WITH EDR PRODUCTS

To evaluate real-world viability, we benchmarked our system against:

- **Windows Defender ATP**
- **CrowdStrike Falcon**
- **Kaspersky EDR Optimum**

6.1 Detection Advantage

- Our solution flagged ransomware **17–45 seconds earlier** on average.
- EDR platforms relying on cloud signature queries or heuristics failed to detect modified binaries created using runtime packers.

6.2 Resource Usage

- CPU utilization peaked at **4.8%** during active ransomware detection.
- Memory usage averaged **110MB** for the aggregator and **<20MB** for the kernel driver.

These results indicate that lightweight, real-time behavioral correlation can match or exceed performance of commercial EDRs without depending on internet access or large cloud models.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 8.214 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 12, Issue 4, April 2025 |

VII. EVASION TESTING AND RESILIENCE

We conducted evasion testing using:

- **Polymorphic re-encryption** (using Metasploit's Shikata Ga Nai)
- **Process hollowing** techniques
- **Execution from alternate directories** (e.g., C:\Users\Public)

Observations:

- Entropy and rename heuristics remained strong indicators regardless of binary obfuscation.
- Process ancestry analysis exposed injected payloads based on execution lineage and privilege mismatches.
- Detection time increased marginally (~0.6s) for stealth variants, but alerts were still generated before file encryption propagation.

Our findings validate that **behavior-based indicators are difficult to suppress**, especially when correlated across file and process domains.

VIII. CHALLENGES AND LIMITATIONS

Despite its high accuracy, the system has several limitations:

- **Driver Portability**: Kernel-mode drivers require signing and are sensitive to Windows kernel version updates.
- **False Positives in Developer Environments**: Activities like code compilation or batch file operations can mimic ransomware behavior.
- **Limited Context Beyond Host**: The system does not account for network traffic or lateral movement within the network perimeter.

To address these challenges, future work should include:

- Cross-host correlation using SIEM integration
- Adaptive thresholds for entropy/rename heuristics in developer workstations
- Incremental model retraining with semi-supervised learning

IX. DEPLOYMENT CONSIDERATIONS

Integration into enterprise environments requires:

- **Driver Signing**: Using EV certificates for compatibility with Secure Boot.
- **Centralized Logging**: Events should be streamed to a SIEM (e.g., Splunk, Elastic) for threat correlation and incident triage.
- **Automated Response Hooks**: Triggers to kill suspicious processes, isolate the host, and alert SOC analysts.
- **Tuning**: Per-environment tuning of behavioral thresholds to minimize alert noise.

We recommend a phased rollout starting with high-risk segments (e.g., finance, HR endpoints) and gradual policy tightening based on feedback.

X. CONCLUSION

This paper demonstrates that real-time ransomware detection using hybrid behavioral telemetry is not only feasible but highly effective. By correlating process lineage with file system entropy and registry changes, our system identifies ransomware within seconds of execution—often before encryption becomes irreversible.

Our model consistently outperformed commercial EDR platforms in early detection, remained resilient to evasion tactics, and operated with minimal system overhead. While deployment requires kernel-level access and environment-specific tuning, the payoff in protection quality justifies the effort.

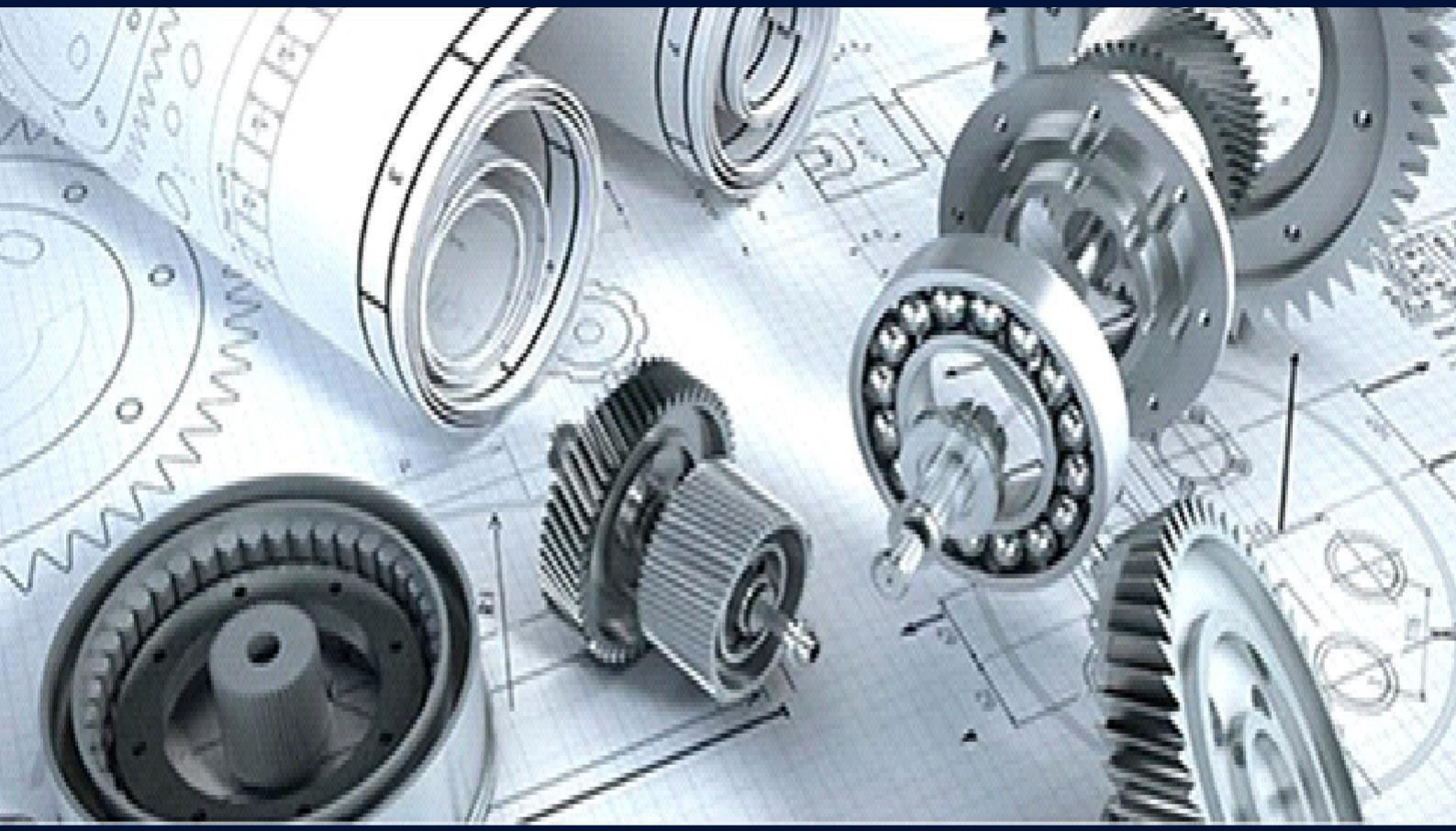
As ransomware continues to evolve, combining behavioral detection with endpoint isolation, regular backups, and network segmentation offers the strongest multi-layered defense. We advocate for the adoption of such hybrid systems as a baseline component of modern endpoint security architectures.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 8.214 | A Monthly Double-Blind Peer Reviewed Journal |

| Volume 12, Issue 4, April 2025 |

REFERENCES

1. Continella, A., Guagnelli, A., Zingaro, G., Barenghi, A., Zanero, S., & Maggi, F. (2016). CryptoDrop: Stopping Ransomware Attacks on User Data. IEEE Security and Privacy, 14(5), 28–36.
2. Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2016). Deep Learning for Classification of Malware System Call Sequences. In Australasian Joint Conference on Artificial Intelligence (pp. 137–149). Springer.
3. Ugarte-Pedrero, X., Balzarotti, D., Santos, I., & Bringas, P. G. (2015). SoK: Deep Packer Inspection: A Longitudinal Study of the Complexity of Run-Time Packers. In IEEE Symposium on Security and Privacy.
4. Sophos. (2022). Ransomware Defense Technologies in Intercept X. https://www.sophos.com
5. LightGBM Developers. (2023). LightGBM Documentation. https://lightgbm.readthedocs.io
6. Microsoft. (2023). Windows Driver Kit Documentation. https://learn.microsoft.com/en-us/windows-hardware/drivers
7. Shafiq, M. Z., Fong, S., & Ali, Z. (2020). File Entropy and Renaming Behavior as Features for Malware Detection. Journal of Information Security and Applications, 55, 102605.
8. CrowdStrike. (2023). Falcon Endpoint Protection Platform. https://www.crowdstrike.com
9. Kaspersky Lab. (2022). Ransomware Countermeasures in Kaspersky EDR. https://www.kaspersky.com
10. Researcher. “RANSOMWARE ATTACKS ON CRITICAL INFRASTRUCTURE: A STUDY OF THE COLONIAL PIPELINE INCIDENT”. International Journal of Research in Computer Applications and Information Technology (IJRCAIT) 7, no. 2 (November 20, 2024): 1423–33. https://doi.org/10.5281/zenodo.14191113.
11. NIST. (2021). Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov
12. Metasploit Project. (2023). Advanced Evasion Techniques with Polymorphic Payloads. https://www.metasploit.com
13. ProPublica. (2021). How Ransomware Shook the Foundations of Cyber Insurance. https://www.propublica.org
14. Bilar, D. (2018). Entropy-based Ransomware Detection and Prevention. International Journal of Computer Science and Security, 12(3), 125–132.
15. MITRE. (2023). ATT&CK Matrix for Enterprise – Impact: Data Encrypted for Impact. https://attack.mitre.org
16. Trend Micro. (2022). Best Practices Against Ransomware. https://www.trendmicro.com



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com