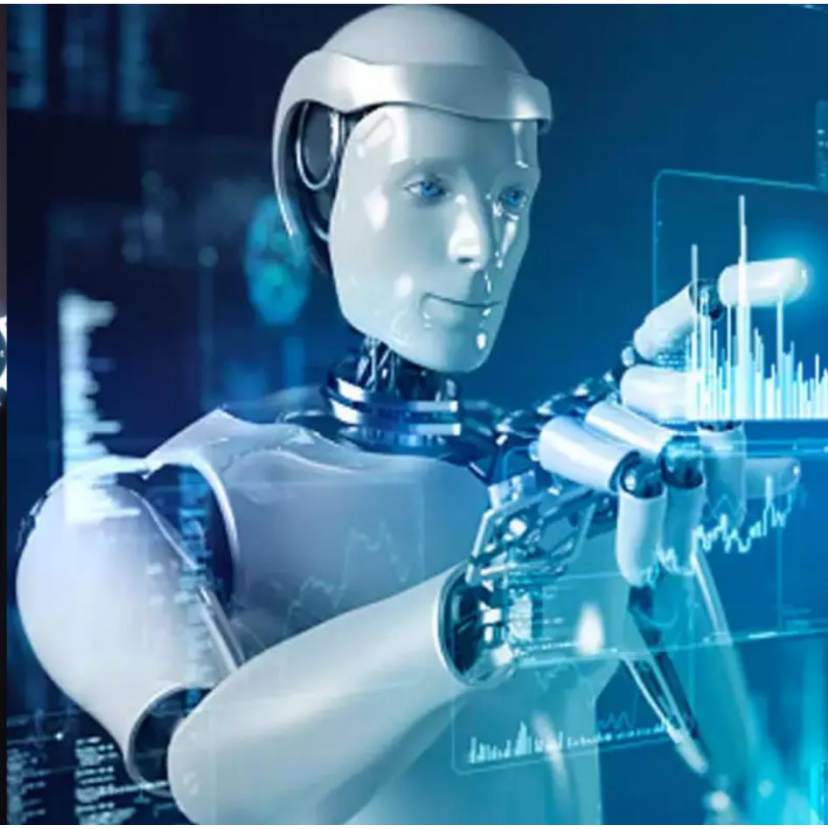
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

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



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503080|

Real Time Ransomware Detection using Behavioural Analysis

Tharshini S[1], Gowri Krishna S[2], Akshara A[3], Mrs. Jonisha S[4]

Student, Department of Information Technology, Arunachala College of Engineering for Women, Nagercoil, Tamil Nadu, India [1,2,3]

Assistant Professor, Department of Information Technology, Arunachala College of Engineering for Women, Nagercoil, Tamil Nadu, India [4]

ABSTRACT: Ransomware is still a major cybersecurity threat because it can encrypt crucial data in a matter of seconds and evade detection by traditional signature-based techniques. Zero-day variants that employ polymorphism and obfuscation are difficult for current antivirus software to detect. This paper proposes a lightweight, real-time behavioural ransomware detection framework based on entropy-driven feature extraction and unsupervised machine learning. The system continuously monitors file-level and file-system activities, including file entropy variation, CPU utilization, I/O throughput, and file modification frequency. An Isolation Forest model is trained on benign system behaviour to identify anomalous activity without the need for labelled ransomware samples. A three-tier automated mitigation engine is designed to prevent or stop malicious processes prior to extensive encryption. Experimental evaluation demonstrates rapid detection within 1–3 seconds with low system overhead, highlighting the feasibility of lightweight behavioural anomaly detection for proactive ransomware defence.

KEYWORDS: Ransomware detection, behavioural analysis, Isolation Forest, machine learning, real-time monitoring.

I. INTRODUCTION

Ransomware, which can encrypt private documents in a matter of seconds and demand payment from victims in order to restore their data, is currently one of the most disruptive forms of cybercrime. Ransomware poses a major threat to people, companies, and governments because the attack surface grows as modern systems become more interconnected. Pre-made malware signatures are primarily used by conventional antivirus software. However, signature-based detection is useless against new or unknown ransomware variants because attackers typically change their code, use polymorphic tactics, and use obfuscation. Behavioural analysis has emerged as a powerful alternative approach to get around these problems. By examining a process's behaviour rather than its code, it is possible to identify even extremely sophisticated strains of zero-day ransomware.

Static analysis, hash matching, and signatures are the main focuses of current ransomware detection techniques. These tactics are ineffective when ransomware employs techniques like packing, encryption, or self-modification to evade detection. As a result, many ransomware attacks are only detected after files have been encrypted. It is obviously necessary to have a behavior-driven, real-time system that can identify abnormal activity before significant damage is done, such as sudden file modifications, entropy spikes, strange I/O patterns, or unexpected process behaviour. This project aims to bridge that gap by developing a small, self-sufficient, real-time ransomware detection system.

The primary objective is to develop a real-time ransomware detection system that continuously monitors file system and process-level activity using lightweight operating system monitoring techniques. The system looks for and extracts important behavioral characteristics such as CPU utilization, memory consumption, I/O throughput, entropy variations, file operation frequency, and process creation patterns. An unsupervised machine learning model based on isolation forests is used to detect anomalous process behavior without the use of pre-made malware samples. Additionally, an automated mitigation engine is developed to prevent ransomware-like activities from propagating and encrypting files. The project also involves developing an interactive real-time dashboard to visualize system activity, anomaly scores, and mitigation logs. Lastly, a number of simulated ransomware attack scenarios are used to test the efficacy of the suggested framework in order to evaluate detection accuracy and system dependability.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503080|

II. LITERATURE SURVEY

Numerous studies have looked into ransomware detection using a range of methods, such as machine learning, heuristic analysis, and signature-based detection. Signature-based techniques, which compare files with known malware signatures kept in databases, were the mainstay of traditional detection systems. These methods work well for spotting known threats, but they can't find newly created or altered ransomware variants.

Researchers have looked into dynamic analysis methods that track system behaviour while programs are operating in order to get around this restriction. These methods examine behavioural indicators that are frequently linked to ransomware attacks, such as odd file modification patterns, abnormal CPU usage, and quick file encryption.

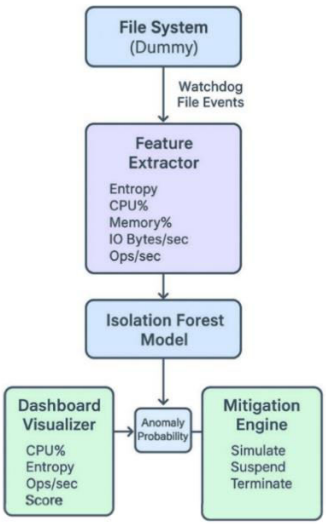
In recent years, machine learning methods have become increasingly popular for ransomware detection. Supervised learning algorithms such as Support Vector Machines (SVM) and Random Forest classifiers have been widely used to classify malicious and benign behaviours. However, these techniques typically require large amounts of labelled training data, which is often difficult to obtain in real-world scenarios.

As an alternative, unsupervised learning approaches such as anomaly detection have been introduced. These methods learn patterns of normal system behaviour and identify deviations that may indicate malicious activity. The Isolation Forest algorithm is one such technique that is particularly effective in detecting anomalies in large datasets.

Despite these developments, many existing solutions still depend on extensive training data or struggle to detect ransomware at an early stage. Therefore, this research proposes a lightweight behavioural monitoring system based on anomaly detection to identify ransomware attacks in real time.

III. PROPOSED METHODOLOGY AND DISCUSSION

The proposed system is designed to detect ransomware attacks by continuously monitoring the behavioural patterns of running processes in real time. Instead of relying on traditional signature-based detection methods, the system focuses on identifying abnormal behaviour that may indicate malicious activity. The overall architecture of the system is composed of four major components: behavioural monitoring, feature extraction, anomaly detection, and mitigation.



In the first stage, the behavioural monitoring module continuously observes system activities generated by running processes. These activities include file operations such as file creation, modification, and deletion, along with system resource usage such as CPU utilization, memory consumption, and disk input/output operations. The module also

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

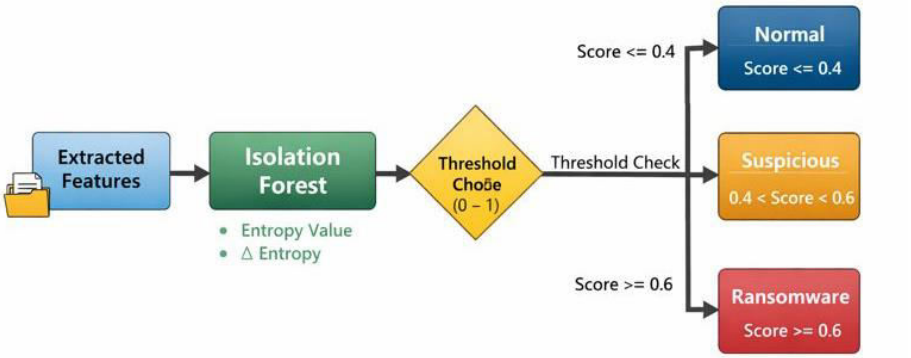
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503080|

monitors process creation events to identify suspicious processes that may attempt to perform unauthorized operations. All these activities are collected directly from the operating system and stored as raw behavioural data for further analysis.

After collecting the behavioural data, the feature extraction module processes the raw information to generate meaningful indicators that can be used for detecting abnormal behaviour. Several important features are extracted from the collected data, including changes in file entropy, the frequency of file operations performed by processes, delta entropy values between file states, CPU utilization levels, memory usage patterns, and disk input/output activity. These features help in identifying unusual behaviour that commonly occurs during ransomware attacks, such as rapid encryption of files and abnormal resource usage.



The extracted features are then analyzed using the Isolation Forest algorithm, which is an unsupervised machine learning technique widely used for anomaly detection. This algorithm works by learning patterns of normal system behaviour and isolating observations that significantly deviate from these patterns. Since ransomware typically exhibits behaviour that differs from normal applications, the model can effectively identify such anomalies even if the ransomware variant has not been previously encountered.

When the calculated anomaly score exceeds a predefined threshold value, the mitigation module is activated. This module is responsible for taking immediate defensive actions to reduce the potential damage caused by ransomware. The mitigation process may include suspending suspicious processes, terminating potentially malicious tasks, and preventing further file encryption operations. These actions help protect important system files and reduce the risk of large-scale data loss.

In addition to the detection and mitigation mechanisms, a real-time monitoring dashboard was developed using Flask and Plotly to provide a visual representation of system behaviour. The dashboard displays important system metrics such as CPU utilization, file operation rates, entropy variations, and anomaly scores. It also shows alerts and mitigation actions performed by the system. This visualization enables users to monitor system activity in real time and gain better insight into potential security threats.

Overall, the proposed methodology combines behavioural monitoring with machine learning-based anomaly detection to provide an efficient and proactive approach for identifying ransomware attacks at an early stage.

IV. RESULTS

The proposed system was evaluated using multiple simulated ransomware attack scenarios in order to measure its detection capability and overall system performance. The experimental setup consisted of a Windows-based environment running on a system equipped with an Intel i5 processor and 8 GB of RAM. Various ransomware-like behaviours were simulated to test the robustness of the detection mechanism. These behaviours included rapid bulk file encryption, selective encryption of specific file types, and slow encryption attacks designed to evade detection systems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

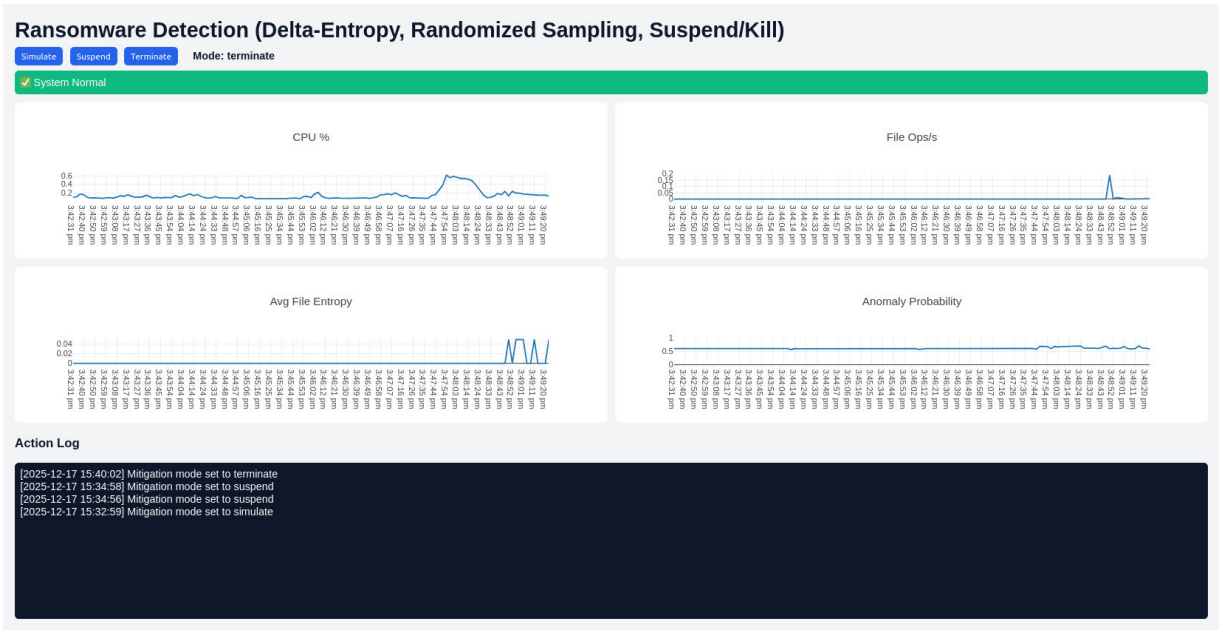
Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503080|

During the testing phase, the system continuously monitored system activities such as file operations, CPU utilization, memory usage, and disk input/output behaviour. The behavioural monitoring module collected these metrics in real time and passed them to the anomaly detection model for analysis. The system was able to successfully identify abnormal behavioural patterns associated with the simulated ransomware activities.

Experimental observations indicate that the proposed system detected ransomware behaviour within approximately 1–3 seconds after the attack began. This early detection capability is crucial in preventing large-scale file encryption and minimizing potential data loss.

The anomaly detection model demonstrated strong performance in identifying suspicious activities while maintaining minimal system overhead. The system consumed only a small amount of additional CPU and memory resources, ensuring that normal system performance was not significantly affected.



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503080|

In addition, the monitoring dashboard provided real-time visualization of key system metrics, including CPU usage, file operation rate, entropy variation, and anomaly probability scores. These visualizations helped in understanding system behaviour during both normal and attack conditions and allowed users to observe mitigation actions taken by the system. Overall, the experimental results confirm that behavioural monitoring combined with machine learning techniques can effectively detect ransomware attacks at an early stage. The proposed system provides a lightweight and proactive defence mechanism capable of identifying both known and previously unseen ransomware threats, thereby helping to prevent extensive file encryption and system damage.

V. CONCLUSION

This research presented a real-time ransomware detection system based on behavioural analysis and anomaly detection. Unlike traditional signature-based approaches, the proposed system focuses on monitoring system behaviour to identify suspicious activities. By using an Isolation Forest machine learning model, the system can detect unknown ransomware variants without requiring large labelled datasets. The system also includes automated mitigation mechanisms to prevent large-scale file encryption once malicious behaviour is detected. Experimental evaluation demonstrated that the proposed approach can detect ransomware attacks quickly with high accuracy and minimal system impact. Therefore, behavioural monitoring combined with anomaly detection provides a promising solution for protecting systems against modern ransomware threats. Future work may focus on improving detection accuracy using hybrid machine learning models and integrating the system with enterprise-level security platforms.

REFERENCES

1) K. Cabaj, M. Gregorczyk, and W. Mazurczyk, “Software-Defined Networking-Based Ransomware Detection Using HTTP Traffic Characteristics,” IEEE Access, vol. 8, pp. 123929–123944, 2020.
2) F. Sgandurra, L. Muñoz-González, R. Mohsen, and E. Lupu, “Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection,” in Proceedings of IEEE European Symposium on Security and Privacy Workshops, 2016.
3) L. Breiman, “Isolation Forest,” in Proceedings of IEEE International Conference on Data Mining (ICDM), 2008.
4) M. Vinayakumar, K. Soman, and P. Poornachandran, “Applying Deep Learning Approaches for Network Traffic Prediction,” Journal of Artificial Intelligence Research, 2019.
5) Continella, A. Guagnelli, G. Zingaro, and G. Giacinto, “ShieldFS: A Self-Healing, Ransomware-Aware Filesystem,” in Proceedings of ACM Conference on Computer and Communications Security, 2016.
6) S. Scaife, H. Carter, P. Traynor, and K. Butler, “CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data,” in IEEE International Conference on Distributed Computing Systems, 2016.
7) Y. Chen and Y. Luo, “Ransomware Detection Using Machine Learning Techniques,” Computers & Security, vol. 105, 2021.
8) R. Perdisci, I. Corona, and G. Giacinto, “Early Detection of Malicious File Encryption Activity,” in IEEE Security & Privacy Workshops, 2018.
9) Patcha and J. Park, “An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends,” Computer Networks, vol. 51, no. 12, 2007.
10)D. Sgandurra and L. Muñoz-González, “Detecting Ransomware via Entropy-Based Behavioral Analysis,” International Journal of Information Security, 2019.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details