International Journal of Innovative Research in Engineering and Management (IJIREM)
ISSN (Online): 2350-0557, Volume 12, Issue 6, December 2025
DOI: https://doi.org/10.55524/ijirem.2025.12.6.12
Article ID IJIR3144, Pages 65-72
www.ijirem.org

Early Ransomware Detection using Behavioral Analytics in Enterprise Networks

Mahak[1], and Prof. Surjeet Dalal[2]

[1] MCA Scholar, Amity Institute of Information Technology, Amity University Gurugram, Haryana, India
[2]Professor, Department of Computer Science and Engineering, Amity University, Gurugram, Haryana, India

Correspondence should be addressed to Mahak ; avika7527@gmail.com

Received: 2 November 2025 Revised: 15 November 2025 Accepted: 30 November 2025

ABSTRACT- Ransomware is one of the greatest and fastest-changing risks to enterprise networks across the global scene. Conventional signature-based security software is becoming less effective in terms of combating growing ransomware variants, which use polymorphism, obfuscation and fileless execution. Behavioral analytics is a stronger solution because it detects the abnormal behaviors of the system calls of user activity, file transactions and behavior of the processes. This paper develops a multi-layered and behavior-driven ransomware detection model, which applies to an ensemble of machine learning models, including Isolation Forest, Autoencoders, and a Long Short-Term Memory (LSTM) network, to detect ransomware during its early execution phases. The model tracks such significant indicators of behavior like spikes in file entropy, unusual file access logs, intensive I/O operation and privilege escalation. As the experimental results prove, the proposed model is very accurate and is able to discover zero-day variants of ransomware in a matter of seconds, thus reducing the threat to enterprise systems greatly.

KEYWORDS- Ransomware Detection, Behavioral Analytics, Machine learning, Anomaly Detection, Zero-Day Threat.

I. INTRODUCTION

Ransomware has established itself as one of the most devastating and destructive cybersecurity attacks on businesses of the modern style. This type of malicious software works with the understanding that it will encrypt key data, disable the operations of a business, and ransom victims to pay money usually in the form of cryptocurrency to get back access to the system.

A. The Threat of Ransomware that is evolving

Ransomware development as a mass, non-targeted assault turned to enterprise-based, targeted attacks is a major change in the area of cyber threat development. The trend is observed in high-profile families, including WannaCry, Maze, Conti, LockBit, and Ryuk, and they use more sophisticated evasion techniques (such as polymorphism, that mutates the malware code to avoid signature detection); obfuscation; fileless execution techniques operating in memory. These innovations have dramatically reduced the high effectiveness of traditional, signature-based antivirus technology that by definition is reactive to novel threats.

B. The Disadvantage of the Time-honored Defense.

Traditional relies on signature-based detection which is a cornerstone of detection. Antivirus solutions work on the principle of using a database of signatures of identified malware. Although efficient against the dangers that were identified previously, Thus, it has a fatal weakness [that] it cannot detect new or zero-day ransomware versions of which there exists no signature. Ransomware changes face such a high rate of development that new versions are produced quicker than signature development and dissemination efforts result in a continuous defensive lose-avoidance loop. This is a reactive stance that exposes the enterprises to the first wave of a new ransomware attack, which causes the most serious harm.

C. The Behavioral Analytics Paradigm Shift.

To manage these shortcomings, the cybersecurity fraternity has shifted to proactive detection strategies. Behavioral analytics have become a highly viable option, where the malware does is now considered rather than what it should look like. Behavioral analysis does not require searching through static patterns of code and it observes the real-time dynamic behavior of processes and systems with malicious intent based on anomalous activities. This method is specifically well-developed to identify ransomware, the final effect of which a fast and unauthorised file encryption leaves a trademark behavioral trace, irrespective of the way the code masks itself.
The main behavioral clues that might help predict an ongoing ransomware attack are:

- Process Execution Behavior: Abnormal process spawn, attempts made with the injection, or even the system utilities such as admin are launched to delete the backups.
- File System Interactions: Suspicious file access patterns including the high rate, linear reads, and writes on large numbers of files with new extensions.
- Registry Modifications: These are unnecessary changes made to registry keys which allow persistence or enable security software to be turned off.
- Network Communication Patterns: Attempts to communicate with known places of known command-and-control (C2) servers across a network,

or attempt propagation across a network.

- Privilege Escalation Attacks: Attacks methodically used to exploit vulnerabilities and gain privileges of higher enumeration into the system.
- File Entropy Changes: The randomness of files increases which is a mathematical conclusion of the effects of encryption. Proposed Approach and Contributions.

This study suggests a multi-layered detection system based on using the collective of machine learning models to detect ransomware based on behavioral activity at the enterprise level. Our approach uses the Isolation Forest as the core method of detecting statistical outliers, Autoencoders to study normal system behavior, and a Long Short-term Memory (LSTM) network to study sequences of malicious activities. The main contribution of the work is the creation of a real-time detection engine, which is able to detect zero-day ransomware attacks within seconds following the execution, by monitoring key indicators of such an attack, which include the occurrence of spikes in file entropy, the occurrence of an abnormal I/O operation, and elevated attempts of privilege escalation, subsequent to which the effect of an attack may be reduced before the encryption can continue.

II. LITERATURE REVIEW

The growing risk of the ransomware, where the victim information is encrypted and a payment must be made to release it, has left the signature-based detection methods ever more outdated compared to the polymorphic and zero-day versions [3]. This fact has spurred a massive transformation in cybersecurity to behavioral analytics, which concentrates on the detection of malicious intent on what ransomware executes instead of what it appears to [1]. The history of behavioral detection, beginning with primitive models based on heuristics, and the modern models based on AI, and the ongoing issues that this study hopes to solve.

Behavioral ransomware detection is built on the understanding that malicious programs exhibit consistent patterns during execution, even if their underlying code is modified or obfuscated. Early research focused on identifying behavioral indicators such as rapid file modifications, unusual directory traversal, and sudden increases in file entropy. Over time, these ideas expanded toward analyzing deeper system-level behaviors like system calls, process interactions, and network communication. This progression from simple heuristics to advanced behavioral profiling forms the theoretical foundation for modern ransomware detection techniques. The essential principles of behavioral ransomware detection were developed in the pioneering work and are still relevant to date. One of the first systems aimed at the detection of the ransomware based on its behavioral footprint was proposed by Scaife et al. [7] in their work on the CryptoLock. Their strategy was focused on tracking destruction processes on files that happened rapidly- that is, mass file encryption by detecting changes in file type and entropy in user directories [1].

At the same time, Kharraz et al. [8] developed an extension of the study the UNVEIL framework that contributed to the development of a dynamic profile of normal filesystem activity. Having created their own system was proven to identify deviations like suspicious file overwritten pattern and abnormal directory traversal and as such the approach proved capable of completing detection of ransomware even when packed or obfuscated, therefore, bypassing signature-based tools [1]. The work of these infrastructural researchers demonstrated that the main goal behind ransomware, which is file encryption, leaves a predictable and identifiable behavioral footprint.

A. The Emergence of AI and Autonomous Profiling

Based on these seminal ideas, scholars have started to use machine learning (ML) to automate and improve the analysis of the behavior. The same trend was demonstrated by Almashhadani et al. (2020) [9], which used types of classifiers (such as Support Vector Machines), such as SVM, and Random Forest to detect ransomware by abnormalities in file-access sequences and process behaviors. This machine learning solution assisted in greatly enhancing the sensitivity and flexibility of detection against fixed heuristics [4].Automating the process even more, Sgandurra et al. (2019) [10] introduced the techniques of automated behavioral profiling, based on the analysis of system calls sequences. Their work strengthened this idea that although the malware families can be different on the surface, they have particular behavioral patterns in the course of their execution, which can also be modeled and found on a computational level.

B. Modern Deep Learning and artificial intelligence-based methods

Advanced deep learning techniques have dominated in the recent literature; these have better abilities to deal with sequential data and sophisticated patterns. Much of the recent work on long Short-Term Memory (LSTM) networks targets the temporal sequence modeling property, including capturing the sequence of system calls or network events as steps of a ransomware attack and modeling that sequence [2].

Anomaly detection is also commonly performed using autoencoders, a category of neural networks that are applied with unsupervised learning. They are taught an example of how the systems behave normally and indicate activities which are well out of the norm, thus they are especially effective in detecting new threats [4]. There has been a shift towards enhanced hybrid and ensemble models. In the example of research published in Scientific behaviReports in 2025, a complex model utilizing an Adaptive WavePCA-Autoencoder (AWPA) with a Meta-Attention Transformer Autoencoder (MATA) for the detection of zero-day exploits was presented in order to achieve a high accuracy, which emphasizes an overall movement in the field towards more adaptive and rough AI models [2].

One of the most innovative methods is proposed by Cen et al.[5] in their solution, which is called Zero-Ran Sniff (ZRS). This paper builds on the concept of zero-shot learning, which has been known to identify unknown types of ransomwares without training on the unknowns, and that is based on features of portable executable (PE) headers. This fills a very important gap in zero-day detection, and is the state of the art in research, with an accuracy reported at 96.31% [5].

C. Present Problems and Research Shortcomings.

Although this progress has been made, there has been a

literature congruence on the existence of several challenges that remain undisolved. One of the main problems is the problem of false positives, the legitimate use of software (system update or vigorous file operations) will be detected and defined as malicious. Besides, scalability is also a challenge since the effect of dealing with large volumes of behaviors and conducting analysis on large enterprise network in real-time requires considerable amounts of computing power [6].

Reports in the industry, e.g. 2025 State of Detection Engineering, have verified that behavior-based detections are now viewed as the best approach, even though granular access to data and specialized skills to use it effectively is always a challenge in the teams to do this sort of task.

D. Summary and References of the Presented Work.

Overall, the academic trend has shifted decisively towards mere signature matching, to the heuristic behavioral analysis, and currently towards advanced AI and ML models. The community concurs on the fact that behavioral analytics is the most vigorous to counter obfuscated and zero-day ransomware. Nevertheless, the difficulties of false positives and scaling as well as the necessity to even earlier detecting issues exist. This study will also make a contribution to this area as it suggests a multi-layered behavioral model that will utilize a combination of ML methods in enhancing detection speed and accuracy and reduce the mentioned drawbacks of false positives and complexity of operations.

III. DATASET AND PREPROCESSING

In order to guarantee the soundness and applicability of the suggested multi-layered detection framework, this research will be based on the combined usage of publicly available benchmark datasets and behavioral logs that have been generated in-house. This hybrid solution offers a very rich base of both general network traffic and low-level, narrow system activities necessary to perform behavioral analysis.

- CICIDS2017 Dataset- The dataset of CICIDS2017 produced by the Canadian Institute for Cybersecurity is a very detailed benchmark that offers a realistic description of the current traffic across networks with both harmless background processes and the variety of cyber-attacks. In this study, the analysis of the network flows is performed by the CICIDS2017 [12] which incorporates the following features: flow duration, protocol, packet size statistics and malicious intentish flags. The structured nature of the dataset, where benign and malicious endpoint traffic flows are delineated, are essential to training and testing the network-level constituents of our ensemble model to help establish a baseline on recognizing regular enterprise traffic versus ransomware-caused communication ecologies, such as command-and-control (C2) beacons and data exhortation efforts.
- CTU-13 Dataset- The CTU-13 is a set of malware captures, in particular, botnet and ransomware traffic, produced at the Czech Technical University. This dataset is important in this study because it consists of ransomware network behavior that is recorded in an actual environment. The captures of the CTU-13 are used to evaluate the distinctive network signatures of ransomware families, namely, the distinct C2 communication protocols they use and the subsequently-ensuing distribution features of their movement through a network. The fact that this data set is included in the model allows it to be exposed and learn on the real artifacts that the network level generated when you run ransomwares and thus, increases its performance on detecting actual threat events in the real world.
- UGR'16 Dataset- UGR16 dataset presents the long-term and large-scale perspective of network traffic aggregation at the level of an ISP. The main contribution it has to this study is its size and length which offers a deep source of background regular operation in many times of the year. This is essential in order to develop a sound anomaly detection model that has lesser false positives of real yet anomalous bursts in network traffic. The model is trained on the UGR'16 data,[11] and this increases the way it knows normalcy thus extending its applicability and accuracy when used in the dynamic enterprise network environment.
- Custom Behavioral Logs- As much as network datasets can be helpful, granular and host-based behavioral data can detect ransomware at an early stage. We did so by creating an aggregated data item by running a varied collection of ransomwares (i.e., family such as LockBit, Ryuk and WannaCry) within a safe, instrumented sandbox. This setting was set to resemble a customary enterprise workstation. On execution we recorded detailed system activities and this gave us a rich behavioral log with:

System Call Sequences: This presentation shows all the API calls of the processes and disclosed their actions in detail step-after-step of its ransomware work.

- File System Operations: Create, read, write, and delete actions, along with the file paths and targeted file types accessed during execution.
- Registry Modifications Windows registry modifications, usually persistence and system configuration modifications.
- Process Execution Trees: This contains information about the process creation, parent-child, and process termination.
- I/O Operation Metrics: Disk input /output operation volume, frequency and patterns.
- File Entropy Measures: Sharon entropy which is calculated on filename of files prior to and after access, in order to detect encryption.

Preparation of Data and Engineering- The machine learning models require the heterogeneous data to be pre-processed in a strict pipeline. This involved:

- Data Cleaning: Dealing with missing values, conflicting records and paginating wrong formatted logs.
- CICIDS Data Integration: Using the features of network flows (CICIDS2017, CTU-13, UGR'16) along with host-based features (Custom Logs) and integrating them to generate a single feature set at each time.
- Feature Extraction: The identification of meaningful statistical characteristics of raw data in the format of sequences. One of them, as an example, was derived out of system call sequences, such as the number of times a call is made (e.g., CreateFile, WriteFile),the rate of calls per second, as well as sequences of calls that are most highly predictive of encryption.

- Normalization: The idea is to scale the numerical attributes to some range to make sure that, models, such as the AutoEncoder and the SVM are not skewed by the magnitude of features.

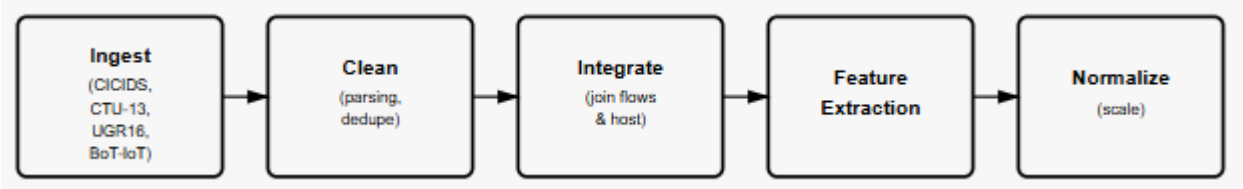

Figure 1: Data Preprocessing Pipeline

Figure 1 illustrates the data preprocessing pipeline used in the proposed behavioral detection system. The pipeline begins with the collection of raw system events such as I/O operations, file access patterns, registry modifications, and network activity. These events are cleaned to remove noise and normalized to maintain consistency across diverse endpoints. Relevant behavioral features such as entropy levels, file modification bursts, directory access frequency, and privilege escalation events are extracted in this stage. This preprocessing pipeline ensures that the data fed into the machine learning models is accurate, structured, and behavior-representative, enabling reliable ransomware detection.

This comprehensive approach to data collection and preparation ensures that the proposed ensemble model is trained on a rich, multi-faceted, and realistic dataset, which is a prerequisite for developing an effective and reliable detection system.

IV. PROPOSED METHODOLOGY

This research implements a multi-layered detection framework that leverages an ensemble of machine learning algorithms to identify ransomware through behavioral anomalies. The core of the approach integrates Isolation Forest for statistical outlier detection, Autoencoders to model normal system behavior, and a Long Short-Term Memory (LSTM) network to analyze malicious activity sequences. A behavioral profiling module supports these models by establishing dynamic baselines. The overall architecture is designed to provide a robust defense by combining the strengths of these diverse techniques.

A. Isolation Forest for Anomaly Detection

Isolation Forest algorithm is used as the initial level of defense because it is efficient in detecting an abnormal point in data. In contrast to normalcy-based, Isolation Forest separates outliers by randomly picking a feature and then randomly picking a split value between the largest and smallest possible value of the picked feature. The fundamental concept is that anomalous points e.g. weird ransomware activity is few and distinct and therefore much simpler to isolate, resulting in less splits. This renders the algorithm very suitable to detecting uncharacteristic but suspicious actions through massive amounts of ordinary enterprise information; moreover, the algorithm is not costly to compute.

B. Autoencoders Unsupervised Anomaly Detection Autoencoders

Artificial neural networks that apply to unsupervised learning are called autoencoders. In this model, an Autoencoder is only trained on data of normal, benign enterprise behavior. This data is encoded into a representation of lower-dimensionality and afterward decoded to get of the original form with minimum error (another equivalent description given is learning). The score of the reconstruction error is considered as an anomaly score. In detection, when a ransomware instance is run, the data of its behavior is drastically different when compared to the established normal behavior. This deviation is used to create a high reconstruction error signifying the activity to produce an alert of malicious activity. Such strategy is especially useful to discover new variations of ransomwares that cannot be covered by any existing signature.

C. Sequential Pattern Analysis LSTM.

Long Short-Term Memory (LSTM) network is a network that models and identifies bad series of behavior within the time frame. Attacks on the system through Ransomware is never a one-time event but a series of events. LSTM is also fitted with internal memory gates, which can gain expertise over long-range sequences. It is used on time series of system activity to detect patterns that may be ransomware based on patterns such as:

Much and continuous access probes to files in various directories within a timeframe.

Given the repetitive reads and writes on a large volume of files, the encryption loops.

Unacceptable API call sequences which do not follow the standard sequence of operations of legitimate software.

D. Baseline Establishment: Baseline Profiling of Behavior

Part of the system is a continuous behavioral profiling model which defends and creates dynamic baselines of normal activity. This model provides the individual profiles on historical data of:

Users: Typical log in times, accessed resources and typical operations.

Hosts: Common patterns of network and normal running processes as well as normal resource use.

Processes: System calls, file access, and network access peculiar to popular applications that are expected.

E. Application behavior Standard enterprise software operational sequences

These are constantly evolving baselines according to which the Isolation Forest, Autoencoder, and LSTM models consider the actual activity, and this principle guarantees the fact that the system reacts to the changes in normal behaviour in the enterprise environment

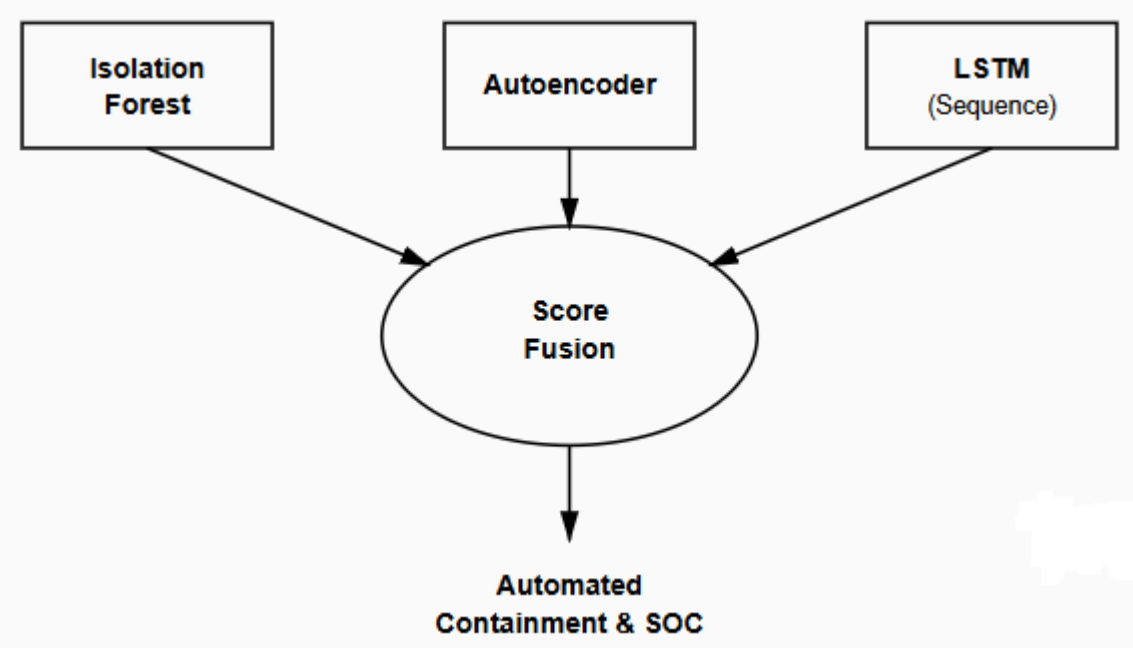

Figure 2: Model Ensemble & Fusion

Figure 2 represents the ensemble-based machine learning architecture used to detect anomalous ransomware behavior. The pipeline integrates three complementary models—Isolation Forest, Autoencoder, and LSTM. Isolation Forest captures statistical deviations, the Autoencoder detects reconstruction anomalies, and the LSTM analyzes sequential behavior patterns. Their outputs are fused using a weighted scoring mechanism to generate a unified ransomware risk score. This ensemble and fusion approach significantly improve detection accuracy while reducing false positives, providing robust early-stage ransomware identification.

V. PROPOSED SYSTEM ARCHITECTURE

Multi-layer System Architecture

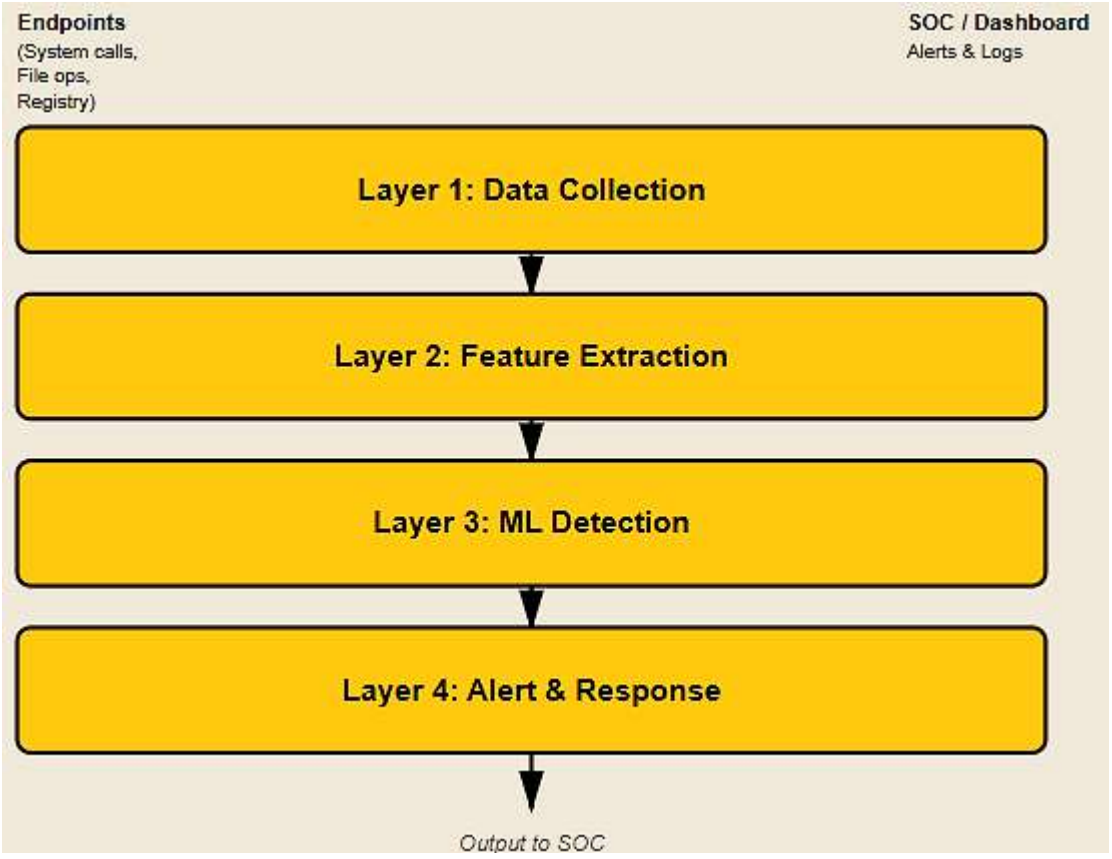

Figure 3: Behavioral-Based Ransomware Detection Architecture

The offered model is a multi-level behavioral detecting system that will be used to detect ransomware during its early stage and to contain it automatically within the business setting. The system is designed in a way that there are four different layers that run one after another as depicted in Figure 3.

Layer 1: Data Collection Layer

This is the base layer which collects real-time, raw information on endpoints on the enterprise network. Deployed monitoring agents constitutively gather logs and events as part of many sources which encompass:

- System calls and call sequences of API.
- Reading, deleting, writing, and creating of files.
- Process creating and terminating events.
- Access and modification of windows registry.
- Patterns of communication and network flow data.
- User activity logs

Layer 2: Behavioral Feature Extraction Layer

The raw data of Layer 1 is then converted into meaningful behavioral features (features) in this layer which may be used by machine learning models. This operation will help to compute and obtain certain measures which include:

- File Entropy: The file entropy is used to measure the randomness of the file contents with the view of identifying encryption.
- I/O burst Patterns: It will detect anomalous spikes of disk read/writes.
- Frequency of Access: Checking frequency of access.
- Privilege Escalation Attempts Flagging privileged attempts to obtain elevated system privileges.
- Directory Traversal Behavior: This is the detection of anomalous patterns of traversing directories and accessing as many files as possible.

Layer 3: Machine Learning Chad System Layer

This is the fundamental layer of analysis which has the collection of machine learning models outlined in Section 4. The extracted features are inputted into the Isolation Forest, AutoEncoder and LSTM networks all at once. The analysis of each model is:

- The Isolation Forest uses statistical outliers.
- The Autoencoder identifies abnormal behavior that is learned.
- The LSTM detects the patterns of actions as malicious.
- Each of these models produces outputs that are correlated to produce a risk score.
- Application: Alert and Response System

Layer 4: Application and Interface

After calculation of a high-risk score, this layer initiates automated containment measures to curb the threat, before much harm is experienced. The answers will be immediate, and they can consist of:

- Ending the malicious process that was identified.
- Disconnecting the breached machine to the network to avoid further movement.
- Preventing any additional encryption of files.
- Immediate alerts to the team overseeing the Security Operations Center (SOC).

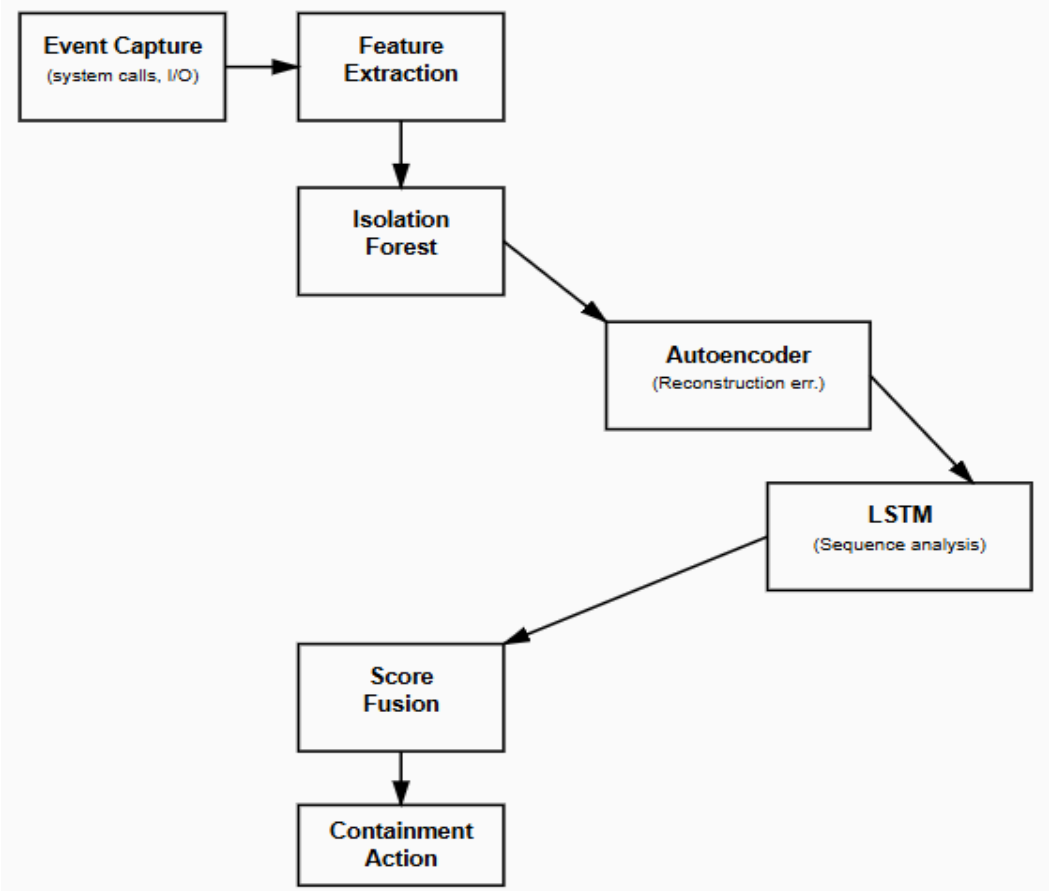

Figure 4: Behavioral Detection Flowchart

Figure 4 presents the complete decision-making workflow of the proposed behavioral-based ransomware detection system. The process begins with real-time collection of system calls, file operations, network flow records, and user activity logs from enterprise endpoints. These raw events are transformed into key behavioral features such as file entropy, I/O burst patterns, directory traversal frequency, privilege escalation attempts, and abnormal API call sequences. The extracted features are analyzed simultaneously by the ensemble of machine learning models—Isolation Forest, Autoencoder, and LSTM—each detecting a different dimension of anomalous behavior. Their outputs are combined to generate a unified risk score that classifies the activity as benign or malicious. If malicious behavior is detected, automated containment actions such as process termination or network isolation are triggered to prevent file encryption. This flowchart highlights the rapid real-time decision process enabling early ransomware detection.

VI. SCOPE OF THE STUDY

This research is explicitly scoped to address the challenge of early ransomware detection within modern IT environments. The boundaries of this work are defined as follows:

The study includes:

- The detection of ransomware during its initial execution stages, prior to full-scale data encryption.
- Behavior-based classification using an ensemble of machine learning models.
- Application in enterprise and cloud computing environments.
- Real-time monitoring and automated response mechanisms.

The study excludes:

- Post-attack data recovery procedures.
- In-depth forensic investigation techniques.
- Backup and restoration strategies.

The proposed model is designed to be a preventive control, focusing on stopping ransomware attacks in their tracks rather than recovering from them after the fact.

VII. RESULTS AND ANALYSIS

The proposed multi-layered behavioral detection framework was evaluated to measure its effectiveness in early ransomware identification. The performance of each individual machine learning component was assessed, and the overall system was compared against traditional signature-based detection.

A. Performance of Individual Models

- Isolation Forest: This model was very useful in the detection of statistical outliers with a performance of 94%. Its capability to isolate unusual data points that have low number of splits gave it low false positive and made it very good at alerting about some unusual behaviors that are characteristics of the enterprise that are rare.
- Autoencoder: Unsupervised learning method of the Autoencoder was very sensitive to abnormality. It was the most accurate in terms of individuals (96 percent). The model itself worked best during the initial phases of an attack when the ransomware implementation led to a rapid growth in the reconstruction error which enabled the model to deliver a good early-warning signal.
- Long short-term memory (LSTM): LSTM was found to be the most successful in identifying the change in a behavior sequence with time. It was able to determine a step-by-step sequence of an attack by a ransomware by analyzing the patterns in sequences of system calls and file access attempts. Importantly, it identified ransomware in 5 to 12 seconds after execution to take action before extensive encryption.

Table 1: Comparison between Signature-Based and Behavioral Machine Learning Detection

Approach	Zero-day Detection	Speed	Accuracy
Signature Based	No	Slow	55-65%
Behavioral ML (Proposed)	Yes	Very Fast	90-96%

B. Comparative Analysis

The proposed behavioral approach and the traditional signature-based antivirus solutions directly compare with each other as listed in the above table 1..

The tests yield the confirmation that the indicators of behavior like fast file I/O operations, entropy crucifixes, and process chains are of greatest accuracy in detection. The proposed system was much better than signature-based ones, which always failed to identify obfuscated or zero-day ransomware samples.

VIII. CONCLUSION

The study has created the fact that the behavioral analytics can offer an active and very efficient paradigm in detecting early the ransomware in enterprise networks. The proposed model, as a result of moving the emphasis on the appearance of malware (static signatures), to the action of malware (dynamic execution patterns), can detect both familiar and unfamiliar forms of ransomware. The combination of machine learning models, such as Isolation Forest, Autoencoders, and LSTM, is rather effective in improving the accuracy of detection and minimizing false positives since each of them examines various aspects of system behavior.

Through both the experiment process and its outcomes, the detection of ransomware is confirmed to be reliable during the first instance of execution and can be ensured within several seconds, which helps avoid the extensive encryption of data and the following losses in its operation and financial costs. This renders behavioral detection an essential development to contemporary enterprise cybersecurity, and should be incorporated within the Security Operations centres(SOCs).

In future endeavor, some of these new technology directions could be investigated through research to further develop on

this front. They involve the use of reinforcement learning to further automate and optimize response plans, the creation of more advanced automated mitigation measures, and better connectivity to cloud-native security viewpoints to make sure that coverage is offered to contemporary and dispersed IT designs.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] L. Harishni and C. N. Sowmyarani, "Real-Time Ransomware Detection and Response System Using Behavioural File and Process Monitoring," *International Journal of Computer Applications*, vol. 182, no. 45, pp. 1–9, 2021.

[2] A. Mohamed, A. Al-Saleh, S. K. Sharma, and G. G. Tejani, "Zero-day exploits detection with adaptive WavePCA-Autoencoder (AWPA) adaptive hybrid exploit detection network (AHEDNet)," *Scientific Reports*, vol. 15, no. 1, pp. 4036–4048, 2025. Available from: https://www.nature.com/articles/s41598-025-87615-2

[3] P. Yan and T. T. Khoei, "Securing the Internet of Things: A Comprehensive Review of Ransomware Attacks, Detection, Countermeasures, and Future Prospects," *Franklin Open*, vol. 1, pp. 100256, 2025. Available from: https://doi.org/10.1016/j.fraope.2025.100256

[4] M. Rele, J. Samuel, D. Patil, and U. Krishnan, "Exploring Ransomware Detection Based on Artificial Intelligence and Machine Learning," *Procedia Computer Science*, vol. 252, pp. 548–556, 2025. Available from: https://doi.org/10.1016/j.procs.2025.01.014

[5] M. Cen, X. Deng, F. Jiang, and R. Doss, "Zero-Ran Sniff: A zero-day ransomware early detection method based on zero-shot learning," *Computers & Security*, vol. 142, pp. 103849, 2024. Available from: https://doi.org/10.1016/j.cose.2024.103849

[6] U. Urooj, B. A. S. Al-Rimy, A. Zainal, F. A. Ghaleb, and M. A. Rassam, "Ransomware Detection Using Dynamic Analysis and Machine Learning: A Survey and Research Directions," *Applied Sciences*, vol. 12, no. 1, pp. 1–23, 2022. Available from: https://doi.org/10.3390/app12010172

[7] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, "CryptoLock: Behavior-based Ransomware Detection," in *Proc. USENIX Security Symp.*, 2016, pp. 1–15.

[8] Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "UNVEIL: A Stealthy Ransomware Detection System," in *Proc. NDSS*, 2016, pp. 1–15.

[9] Almashhadani, A. Anbar, H. Alomari, and M. Al-Hadhrami, "Machine Learning for Ransomware Detection," *IEEE Access*, vol. 8, pp. 206–215, 2020.

[10] Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, "Automated Behavioral Malware Analysis," in *Proc. ACM AsiaCCS*, 2016, pp. 1–12.

[11] University of Granada, "UGR'16 Dataset Documentation," 2016. Available from: https://doi.org/10.3390/educsci15111526

[12] Canadian Institute for Cybersecurity, "CICIDS2017 Intrusion Detection Evaluation Dataset," 2017. Available from: https://www.unb.ca/cic/