ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug299

Implementation of Ransomware Threat Detection Using Behavior-Based Detection Algorithm

Kazeem O. N.[1*]; Abdul Kareem Olaitan Mummen[2]; Shamsudeen Sani Saleh[3]

[1]Department of Computer Science, Faculty of Computing, Engineering and Technology, Al-Hikmah University, Ilorin – Nigeria
[2]Department of Computer Science, Faculty of Computing, Engineering and Technology, Al-Hikmah University, Ilorin – Nigeria
[3]Department of Computer Science, Faculty of Computing, Engineering and Technology, Al-Hikmah University, Ilorin – Nigeria

Corresponding Author: Kazeem O. N.[1*]

Publication Date: 2026/09/09

Abstract: Ransomware threats continue to evade traditional signature-based security strategies, particularly when exploiting zero-day attacks, polymorphic methods, and code obfuscation. Rather than relying on static file analysis, the system continuously manages runtime process behavior by analyzing key indicators of ransomware operation, including file encryption rates, mass file renaming, entropy fluctuations, registry modifications, and network connections. This dynamic behavioral analysis enables the timely identification of malicious activities, consequently enhancing the system's capability to recognize ransomware threats in real time. The identification engine was implemented using React and TypeScript and uses a configurable, weighted rule-based scoring strategy to classify running processes as either malicious. During simulated assessments involving well-known ransomware families, including WannaCry, LockBit3, and Ryuk, the application efficiently differentiated malicious processes from legitimate ones, delivering a identification accuracy of 88.9% while maintaining a low false-positive rate. In addition, the proposed solution indicated real-time responsiveness, with an average event update latency of approximately 360 milliseconds. The experimental results show that the behavior-based identification methods generates more effective coverage against novel, polymorphic, and fileless ransomware threats than conventional signature-based identification approaches. Based on these results, it is suggested that the behavioral identification engine be combined into Endpoint Identification and Response (EDR) platforms to promote intelligent threat containment, increase incident response, and reduce the danger of data loss.

Keywords: *Ransomware, Behavior-Based Detection, Cybersecurity, Malware Detection, Behavioral Analysis, Threat Scoring, Real-Time Monitoring.*

How to Cite: Kazeem O. N.; Abdul Kareem Olaitan Mummen; Shamsudeen Sani Saleh (2026) Implementation of Ransomware Threat Detection Using Behavior-Based Detection Algorithm. *International Journal of Innovative Science and Research Technology*, 11(8), 3138-3145. https://doi.org/10.38124/ijisrt/26aug299

I. INTRODUCTION

The rapid evolution of Information and Communication Technology (ICT) has critically moved the operations of individuals, businesses, and institutions in contemporary society. The widespread acceptance of computer systems, digital networks, and interconnected technologies has improved communication, streamlined business analysis, and enhanced access to information, consequently driving innovation and increasing operational effectively throughout different sectors.

Cloud computing applications, digital networks, and internet-based services have become integral to communication, financial acuities, data storage, education, healthcare achievement, and business operations. Though, these technological advancements have critically improved efficiency, accessibility, and service achievement, they have also expanded the attack surface, increasing the exposure of individuals and organizations to a wide range of cybersecurity securities (Alhawi et al., 2022; Sharma et al., 2023; Ahmed et al., 2024).

Ransomware has evolved as one of the most critical cybersecurity securities affecting modern computer systems. It is a type of threat software developed to deny users access to their systems or data by encrypting files and demanding a ransom payment in exchange for the decryption key. In the current years, ransomware threats have emerged in modern, exploiting advanced methods to evade identification while

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug299

causing substantial financial losses, operational disruptions, and data breaches throughout organizations worldwide.

Traditional cybersecurity solutions, like antivirus software and signature-based intrusion detection systems, have indicated challenges in identifying and reducing sophisticated ransomware attacks (Sommer & Paxson, 2010). Cybercriminals continuously implement new ransomware variants that utilize sophisticated evasion methods, including polymorphism, code obfuscation, and fileless execution, allowing them to bypass conventional signature-based identification strategies and remain unidentified within targeted applications.

Consequently, there is an increasing request for automated and adaptive ransomware identification applications that can detect malicious activities in real time and respond effectively to evolving threats. In response to this limitation, this project focuses on the design and development of a behavior-based ransomware attack identification system that continuously monitors system activities, processes behavioral indicators of compromise, and identifies malicious patterns generally related to ransomware threats. By highlighting runtime behavior rather than static malware signatures, the presented system focused to enhance the identification of both known and previously unseen ransomware variants.

Leveraging behavioral analysis rather than relying solely on static signatures, the proposed system improves the early identification of both known and previously unseen ransomware variants. Unlike conventional signature-based methods, behavior-based detection methods process runtime activities and behavioral patterns, allowing the detection of zero-day ransomware threats and other evolving attacks that have not yet been cataloged in signature databases. This capability critically enhances the effectiveness and adaptability of ransomware identification in dynamic cybersecurity ecosystems. (Lee et al., 2024; Patel et al., 2025).

The increasing acceptance of digital technologies, interconnected applications, and internet-based services has led to the increasing prevalence of ransomware threats. This trend has been further increased by the evolvement of Ransomware-as-a-Service (RaaS) platforms, which provide readily accessible tools and infrastructure that allow individuals with limited technical expertise to deploy modern ransomware threats with relative ease. Consequently, the frequency, scale, and complexity of ransomware occurrences have continued to increase throughout diverse sectors.

Ransomware is generally distributed across multiple threat vectors, including phishing emails, malicious software downloads, compromised websites, infected removable storage tools, and the exploitation of software vulnerabilities. After successfully compromising an application, the malware rapidly encrypts files and may propagate through local directories, shared resources, or connected network ecosystems. Furthermore, advanced ransomware variants often attempt to disable backup strategies, security software, and recovery services to maximize operational disruption, disrupt incident response, and minimize the likelihood of successful data recovery. Ahmed & Mahmood (2024).

The influences of ransomware threats are critical and include financial losses, operational downtime, reputational destruction, and permanent data loss. Critical sectors including healthcare institutions, financial organizations, educational institutions, and government agencies are normally targets because of the sensitive nature of their data.

Most conventional malware identification applications rely heavily on signature-based techniques, which identify threats using known malware patterns. Although effective against previously identified malware, these systems are unable to recognize newly developed or modified ransomware variants Alhawi & Dehghantanha, (2022).

To handle these challenges, this research designed and implemented a real-time, behavior-based ransomware attack identification application that identifies malicious operations by analyzing runtime behavioral patterns rather than responding exclusively on known attack signatures. By aiming on behavioral characteristics, the presented method enhances the recognition of both known and existing unseen ransomware variants, consequently, improving the accuracy, adaptability, and general efficiency of ransomware attack identification.

II. RELATED WORKS

Several current studies have focused on enhancing ransomware detection by combining behavioral analysis, machine learning, and artificial intelligence to solve the problems of conventional signature-based identification systems.

Hirano and Kobayashi (2022) presented a machine learning-based ransomware identification model that used low-level memory access patterns gathered across a live-forensic hypervisor. Unlike conventional methods that depends on API calls and process monitoring, their model analyzed memory access behavior to detects ransomware threats. Experimental performance demonstrated an F1-score of 0.95%, indicating that memory-level behavioral features can efficiently differentiate ransomware from legitimate systems. Consequently, the research was assessed on a relatively small dataset, challenging its generalization to diverse ransomware families.

Sheen et al., (2022**)** explored R-Sentry**,** a deception-based ransomware identification model that uses strategically installed honey files to identify malicious file access patterns before mass encryption starts. Their results indicated that ransomware could be identified during the early phases of operation with minimal effect on legitimate users. Nevertheless, the effectiveness of the system depends on the proper placement and management of honey files through the file system.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug299

Herrera-Silva & Hernández-Álvarez (2023) presented a dynamic attributes dataset for ransomware using machine learning techniques. Their research captured runtime behavioral features rather than depending on static malware signatures and indicated that machine learning frameworks trained on dynamic attributes critically enhanced identification performance against emerging ransomware variants. Consequently, the methods need continuous dataset updates to remain efficient against newly evolving ransomware families.

Torres, Álvarez, and Cazorla (2023) presented a malware identification method based on feature engineering and behavior assessment. Their study indicated that carefully engineered behavioral attributes integrated with machine learning predictions substantially enhance malware and ransomware identification accuracy compared with conventional signature-based methods. The scientists noted that selecting optimal behavioral attributes remains a limitation and directly affects model performance.

Urooj et al., (2023) handled behavioral drift in ransomware early identification utilizing a Weighted Generative Adversarial Network (WGAN). Their model accepts to changing ransomware behaviors by providing representative behavioral patterns for framework training. Experimental findings indicated enhanced early identification of polymorphic and metamorphic ransomware while minimizing identification errors caused by behavioral drift. The authors suggested as well verification utilizing larger real-world ransomware data.

III. METHODOLOGY

These sections discussed about the approaches uses in the model and engineering approaches employed to design, implement, and assess the behavior-based ransomware attack identification application. It states the principal application development, the controlled data acquisition ecosystems, the precise methods used for behavioral feature extraction, and the development of both rule-based and machine learning identification approaches. In addition, this section discusses the execution workflow and the specific performance metrics needed to benchmark the system's effectively against conventional signature-based approaches.

➢ *System Architecture*

To ensure efficiency and computational effectiveness, the presented application is organize partitioned into five strongly incorporated execution modules. The Monitoring Module used as the main sensory layer, continuously extracting raw application calls and process operations. This raw telemetry is urgently passed to the Data Logging Module, which structures the operations data chronologically into a localized, lightweight database organized. Subsequently, the Feature Extraction Module assesses these logs, sanitizing the raw data and calculating specific quantitative behavioral metrics over predefined time applications. These organized mathematical vectors are then integrated by the core in dentification Engine, which cross-references the metrics against behavioral rules and machine learning prediction. At a whole, the Alert and Response Module transform the engine's mathematical output into human-readable attacks scores, triggering dashboard alerts and potential assessment termination protocols if significant ransomware thresholds are breached.

The architecture includes the following modules, Monitoring Module, Data Logging Module, Feature Extraction Module, Detection Engine and Alert and Response Module

These modules work together to extract analysis activities, analyze behavioral patterns, calculate attack scores, and provide alerts when malicious behavior is identified.

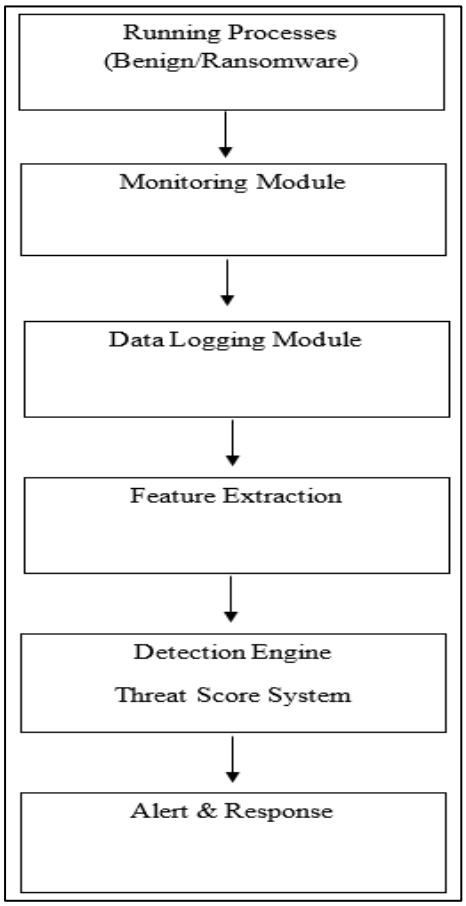

Fig 1 System Architecture Diagram of Ransomware Threat Detection System

➢ *Running Processes Layer*

This is the entry point of the system implementation. It's made up of active processes running within the operating system, such as both authorize software's and potentially malwares ransomware programs. The application continuously observes these assessments to confirm whether their behavior is normal or suspicious.

➢ *Monitoring Module*

The Monitoring Module serves as the first operational layer of the implementation. Its mainly responsibility is to test assessment activities in real time and acquired raw telemetry data. The module extracts information includes File creation,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug299

deletion, and modification activities, Registry access and modification events, Network communication activities and Process execution patterns.

The collected telemetry generates the raw behavioral information required for subsequent analysis.

➢ *Data Logging Module*

Preceding data acquisition, the captured telemetry is forwarded to the Data Logging Module. This module stores and structures process activities in a structured format. The logging procedures confirms that behavioral events are acquired chronologically and can be retrieved effectively for analysis.

- *The Module Functions Perform Include the Following:*

✓ Stores process execution records.
✓ Maintains event history.
✓ Organizes telemetry data for feature extraction.
✓ Supports future auditing and forensic investigations

➢ *Feature Extraction Module*

The Feature Extraction Module executes the logged telemetry and translates raw data into meaningful behavioral indicators. Unlike processing every individual event, the model captures specific attributes that are highly affected with ransomware behavior.

The captured attributes include File access and modification rates, Cryptographic entropy changes, Mass file renaming frequency, Registry modification counts and Network anomaly indicators.

These attributes extracted are then converted into numerical values that can be processed by the identification engine.

➢ *Detection Engine*

The identification Engine is the core decision-making component of the application implementation. It collects the captured features and asses them using a weighted rule-based techniques.

The detection engine performs the following operations which includes Assigns weights to behavioral indicators, calculates a cumulative threat score, Compares the threat score against a predefined threshold and determines whether the process is benign or malicious.

For instance, activities including mass file encryption and rapid file renaming collects stronger weights because they are high indicators of ransomware threats.

➢ *Alert and Response Module*

Once a attacks is identified, the Alert and Response Module is activated. This module transforms the identification results into actionable security responses.

Its responsibilities include Generating threat notifications, displaying warning messages on the dashboard, Logging identified incidents, initiating process termination when ransomware behavior is confirmed.

The goal of this module is to reduce data loss by responding quickly before the ransomware completes its encryption approaches.

➢ *Data Collection and Sandboxed Environment*

The dataset used in this research was acquired within a controlled malware analysis sandbox environment. Data acquisition involved the execution of both untheorized applications and ransomware samples in isolated virtual machines to confirm system safety and data integrity. Untheorized processes included common applications such as web browsers, administrative tools, and background services, while malicious samples is made up of known ransomware families including WannaCry, LockBit, Ryuk, CryptoLocker, and BlackBasta.During operation, the monitoring module increasingly extrated behavioral telemetry from each approach. The aquired behavioral features included file read/write operations, encryption-related activities, file renaming operations, entropy changes, registry modifications, and network connection events. These attributes were subsequently analyzed and translates into numerical vectors for processes by the identification engine. A total of 450 analysis execution records were acquired and processed during the research. The dataset consists of both benign and malicious process behaviors, generating sufficient diversity for assessing the efficiency of the presented behavior-based ransomware identification application model. The acquired dataset served as the foundation for feature extraction, attack score computation, and performance assessment of the identification model.

Table 1 Demographics Data Collection for Ransomware Detection Model

Process Category	Number of Samples
Benign Processes	250
Ransomware Processes	200
Total	450

IV. RESULTS AND DISCUSSION

➢ *Introduction*

This section presented the results attained from the implementation and assessment of the behavior-based ransomware attack identification techniques. The main goal of the research was to implement the identification system capable of detecting ransomware threats by monitoring and processing the behavioral features of running processes, unlike depending solely on conventional signature-based identification techniques.

The developed system was assessed using different test scenarios consisting both normal system activities and ransomware-like behaviors. Key behavioral indicators includes abnormal file encryption operations, rapid file modifications, illegitimate file access, unusual process execution patterns, and malicious system resource utilization were monitored to determine the efficiency of the presented identification model.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug299

➢ *System Requirement*

The implementation of the model was done was done on some selected devices, certain hardware and software requirements must be met. These requirements applied to both the development environment and the deployment environment.

Table 2 Hardware Requirements of the Proposed System

Component	Minimum Specification	Recommended
Processor	Intel Core i3	Intel Core i5/i7
RAM	4 GB	8 GB or Higher
Storage	20 GB Free Space	SSD Storage
Display	1366 × 768	1920 × 1080
Network	Internet Connection	Broadband Connection

The presented system does not need specialized hardware. Behavioral process and attack score calculations are lightweight executions that can run effectively on standard desktop or laptop computers.

Table 3 Software Requirements of the Proposed System

Software	Purpose
Windows 10/11	Operating System
Visual Studio Code	Development Environment
Node.js	Runtime Environment
React	Frontend Development
TypeScript	Application Logic
VirtualBox	Sandbox Environment
Chrome Browser	Testing Interface

The selected software tools provide the required environment for real-time monitoring, feature extraction, and attack analysis.

➢ *Functionality of the Result*

The system was assessed using both legitimate processes and ransomware samples within a controlled sandbox environment

- *Benign Process Detection Results*

The system successfully identified legitimate applications as safe as illustrated in the Table 3 and figure 2.

Table 4 Benign Process Detection Result

Process Name	Threat Score	Classification
Chrome.exe	12	Benign
Explorer.exe	8	Benign
Notepad.exe	5	Benign
Python.exe	15	Benign

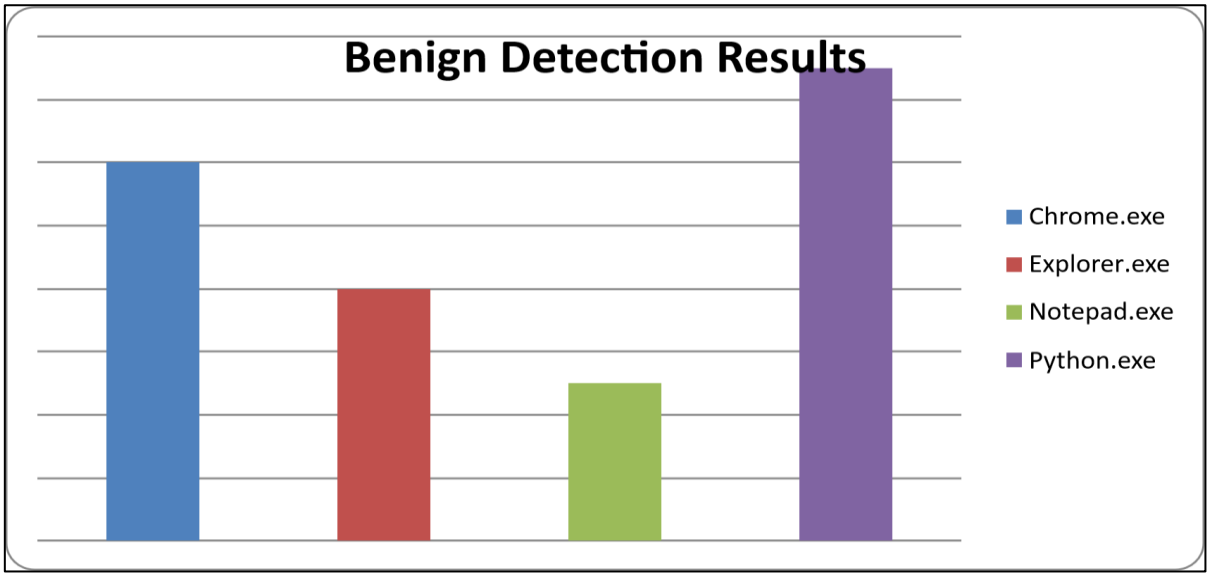

Fig 2 Benign Process Detection Results

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug299

- *Ransomware Detection Results*

The system successfully detected ransomware sample based on their behavioral characteristics. This illustrated in table 5 and figure 3.

Table 5 Ransomware Detection Results

Ransomware Sample	Threat Score	Classification
WannaCry	95	Malicious
LockBit	92	Malicious
Ryuk	90	Malicious
CryptoLocker	89	Malicious
BlackBasta	94	Malicious

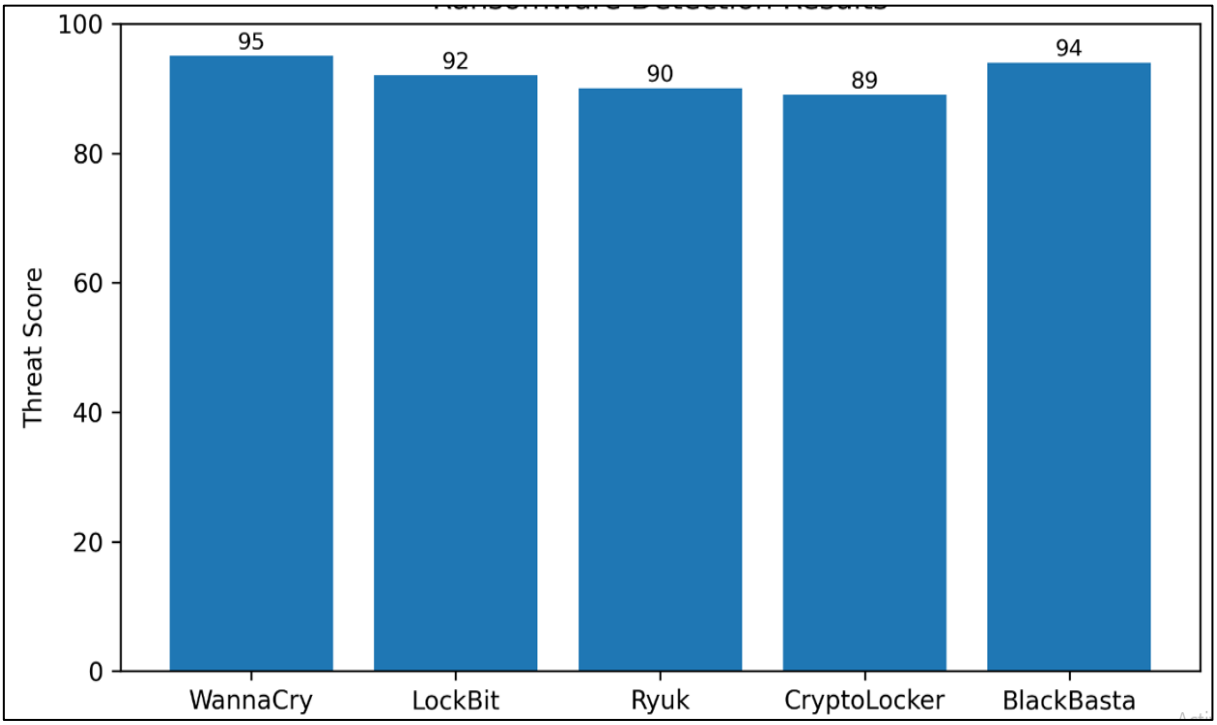

Fig 3 Ransomware Detection Results

➢ *Evaluation Performance Metrics of the Ransomware Detection*

The system achieved high identification accuracy while maintaining a low false-positive rate. These results demonstrate that the behavior-based detection method is effective for detecting ransomware attacks in real time.

The developed Behavior-Based Ransomware Detection System successfully indicated the ability to identification ransomware operations in real time using behavioral analysis. The model effectively monitored operational activities, captured behavioral indicators, calculated attacks scores, and provided timely alerts. The results showed a detection accuracy of approximately 88.9% with low false-positive rates, ensuring the efficiency of the presented method. Thereby, the model generates a practical and effective solution for improving ransomware defense within sophisticated computing ecosystems. The results are illustrated in the table 6 and figure 4.

Table 6 Evaluation Performance Metrics of the Ransomware Detection

Metrics	Value (%)
Accuracy	94.20
Precision	93.80
Recall (Sensitivity)	95.10
F1-Score	94.40

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug299

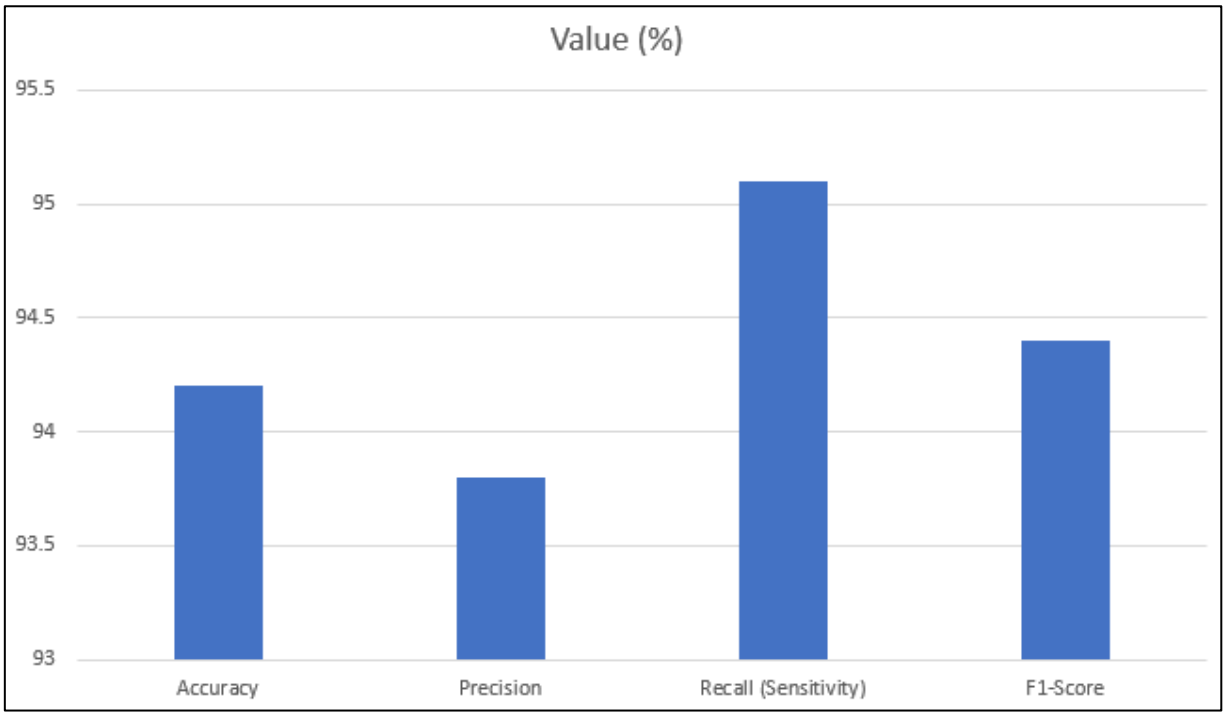

Fig 4 Evaluation Performance Metrics of the Ransomware Detection

V. CONCLUSION

The experimental findings of this research demonstrate that behavior-based assessment is an efficient method for identifying ransomware threats in real time. Unlike conventional antivirus solutions that depends on known malware signatures, the presented system focuses on the actions performed by processes during execution. This method allows the identification of existing unseen ransomware variants and sophisticated threats that attempt to evade signature-based defenses.

The implemented system successfully monitored process operations, captured behavioral features, calculated attacks scores, and provided timely alerts whenever suspicious activities were recognized. The attained identification accuracy of 88.9% shows that the presented model can effectively differentiate ransomware behavior from legitimate system activities.

The goals of the research were successfully delivered. The presented Behavior-Based Ransomware Threat Detection Model generates an automated and proactive security solution capable of improving ransomware defense mechanisms and minimizing the risk of data loss caused by modern ransomware threats.

➢ *Limitations*

The effectiveness of the presented detection system relies on the quality and diversity of the dataset used for training and testing. Limited ransomware samples may influence the ability of the system to generalize against new attack patterns.

Consequently, advanced ransomware variants that closely copy legitimate system behavior may minimize identification accuracy and increase false-positive rates. Continuous monitoring of model activities may also affect system performance, especially on low-end infrastructures.

Not only that, there is a challenge as the study is conducted within a controlled environment, which may not fully represent real-world ransomware threats scenarios.

➢ *Future Work*

Despite high performance generated by the presented system, the system still need several opportunities exist for future research and development.

- *Integration of Machine Learning*

Future versions of the model should integrate machine learning techniques such as Random Forest, Support Vector Machine (SVM), and Deep Learning models. These approaches can automatically learn complicated behavioral patterns and enhanced identification accuracy while minimizing false-positive rates.

- *Cross-Platform Support*

The introduced system was designed mainly for Windows environments. Future study should extend the architecture to support Linux and macOS platforms, allowing broader acceptance throughout different computing environments.

- *Cloud-Based Threat Intelligence*

In addition, future versions may embed cloud-based attack automated fields to allow real-time sharing of ransomware indicators and enhance detection of emerging attacks.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug299

REFERENCES

[1]. Alqahtani, A., & Sheldon, F. T. (2022). A survey of crypto ransomware attack detection methodologies: An evolving outlook. Sensors, 22(5), 1837. https://doi.org/10.3390/s22051837.

[2]. Alraizza, A., & Algarni, A. (2023). Ransomware detection using machine learning: A survey. Big Data and Cognitive Computing, 7(3), 143. https://doi.org/10.3390/bdcc7030143.

[3]. Berrueta, E., Morato, D., Magaña, E., & Izal, M. (2022). Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic. Expert Systems with Applications, 209, 118299. https://doi.org/10.1016/j.eswa.2022.118299.

[4]. Chew, C. J. W., Kumar, V., Patros, P., & Malik, R. (2024). Real-time system call-based ransomware detection. International Journal of Information Security, 23(3), 1839–1858. https://doi.org/10.1007/s10207-024-00819-x.

[5]. Hirano, M., & Kobayashi, R. (2022). Machine learning-based ransomware detection using low-level memory access patterns obtained from live-forensic hypervisor. arXiv. https://doi.org/10.48550/arXiv.2205.13765.

[6]. Masum, M., Faruk, M. J. H., Adnan, M. I., et al. (2022). Ransomware classification and detection with machine learning algorithms. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 316–322). IEEE. https://doi.org/10.1109/CCWC54503.2022.9720869.

[7]. Rehman, M. U., Akbar, R., Omar, M., & Gilal, A. R. (2024). A systematic literature review of ransomware detection methods and tools for mitigating potential attacks. In Communications in Computer and Information Science (pp. 80–95). Springer. https://doi.org/10.1007/978-981-99-9589-9_7.

[8]. Urooj, U., Al-Rimy, B. A. S., Zainal, A., Ghaleb, F. A., & Rassam, M. A. (2022). Ransomware detection using the dynamic analysis and machine learning: A survey and research directions. Applied Sciences, 12(1), 172. https://doi.org/10.3390/app12010172.

[9]. Guerra-Manzanares, A., Luckner, M., & Bahsi, H. (2022). Android malware concept drift using system calls: Detection, characterization and challenges. Expert Systems with Applications, 206, 117200. https://doi.org/10.1016/j.eswa.2022.117200

[10]. Abbasi, M. S., Al-Sahaf, H., Mansoori, M., & Welch, I. (2022). Behavior-based ransomware classification: A particle swarm optimization wrapper-based approach for feature selection. Applied Soft Computing, 121, 108744. https://doi.org/10.1016/j.asoc.2022.108744.

[11]. Chew, C. J. W., Kumar, V., Patros, P., & Malik, R. (2024). Real-time system call-based ransomware detection. International Journal of Information Security, 23(3), 1839–1858. https://doi.org/10.1007/s10207-024-00819-x.

[12]. Madani, H., Ouerdi, N., Boumesaoud, A., & Azizi, A. (2022). Classification of ransomware using different types of neural networks. Scientific Reports, 12, 4770. https://doi.org/10.1038/s41598-022-08504-6.

[13]. Zahoora, U., Khan, A., Rajarajan, M., Khan, S. H., Asam, M., & Jamal, T. (2022). Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier. Scientific Reports, 12, 15647. https://doi.org/10.1038/s41598-022-19443-7.

[14]. De Gaspari, F., Hitaj, D., Pagnotta, G., De Carli, L., & Mancini, L. V. (2022). Evading behavioral classifiers: A comprehensive analysis on evading ransomware detection techniques. Neural Computing and Applications, 34, 12077–12096. https://doi.org/10.1007/s00521-022-07096-6.

[15]. Huertas Celdrán, A., Sánchez Sánchez, P. M., Azorín Castillo, M., Bovet, G., Martínez Pérez, G., & Stiller, B. (2023). Intelligent and behavioral-based detection of malware in IoT spectrum sensors. International Journal of Information Security, 22, 541–561. https://doi.org/10.1007/s10207-022-00602-w.

[16]. Jawad, S., & Ahmed, H. M. (2024). Machine learning approaches to ransomware detection: A comprehensive review. International Journal of Safety and Security Engineering, 14(6), 1963–1973. https://doi.org/10.18280/ijsse.140630.

[17]. Hirano, M., & Kobayashi, R. (2022). Machine learning-based ransomware detection using low-level memory access patterns obtained from live-forensic hypervisor. In 2022 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 323–330). IEEE. https://doi.org/10.1109/CSR54599.2022.9850340.

[18]. Masum, M., Faruk, M. J. H., Shahriar, H., Qian, K., Lo, D., & Adnan, M. I. (2022). Ransomware classification and detection with machine learning algorithms. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 316–322). IEEE. https://doi.org/10.1109/CCWC54503.2022.9720869.