INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

Ransomware in Focus: Comparative Analysis of Common Techniques and Emerging Anomalies

Puneet Chauhan, Dr. Shashiraj Teotia

Department of Computer Application, Swami Vivekanand Subharti University, Meerut U.P India

DOI: https://doi.org/10.51583/IJLTEMAS.2025.140600010

Received: 18 June 2025; Accepted: 23 June 2025; Published: 04 July 2025

Abstract: Ransomware continues to be a pervasive and evolving cybersecurity threat, disrupting critical infrastructure, compromising data integrity, and causing substantial financial losses. This paper presents a comprehensive comparative analysis of common ransomware techniques alongside emerging anomalies observed in recent attacks. Traditional ransomware methods such as file encryption, network propagation, and ransom note delivery are explored to establish a foundational understanding. The study then shifts focus to newer, more sophisticated anomalies, including double extortion, fileless ransomware, and AI-driven obfuscation techniques. By examining attack vectors, payload behaviors, and evasion strategies, the research identifies patterns that aid in early detection and defense. The paper also evaluates real-world incidents and analyzes threat intelligence data to highlight trends in attacker behavior and targets. The findings aim to enhance awareness and preparedness among cybersecurity professionals, proposing proactive strategies and adaptive countermeasures for mitigating future ransomware threats in an increasingly complex digital landscape.

Keywords—Malware Analysis, Threat Detection, Fileless Attacks, Double Extortion, Encryption Techniques, AI-based Evasion, Anomaly Detection, Incident Response.

I. Introduction

In the modern digital era, the proliferation of ransomware represents a critical cybersecurity threat that continues to evolve in both complexity and scale. Ransomware is a form of malicious software designed to block access to a computer system or encrypt data until a sum of money, or ransom, is paid by the victim. Over the last decade, ransomware has emerged as one of the most formidable tools in the cybercriminal arsenal, affecting individuals, corporations, healthcare providers, financial institutions, and even national governments. Its impact extends far beyond monetary loss, influencing operational continuity, data integrity, customer trust, and regulatory compliance. The fundamental architecture of ransomware attacks has remained relatively consistent over time, involving the infection of a target system, encryption of critical data, and communication of a ransom demand. However, the delivery methods, payload sophistication, evasion techniques, and extortion strategies have undergone significant transformation. Historically, ransomware variants such as Cryptolocker, WannaCry, and Locky leveraged exploit kits, phishing emails, and drive-by downloads to infiltrate systems. These traditional techniques capitalized on user negligence, unpatched software, and lack of endpoint security. Once activated, the malware would encrypt files using complex algorithms and demand payment—usually in Bitcoin—for the decryption key. Despite initial success, defensive countermeasures such as regular backups, endpoint detection and response (EDR) tools, and awareness training have made it increasingly difficult for basic ransomware variants to achieve their objectives. In response, attackers have adopted more intricate and multi-dimensional strategies, leading to the rise of what can be termed as "emerging anomalies" in ransomware behavior.

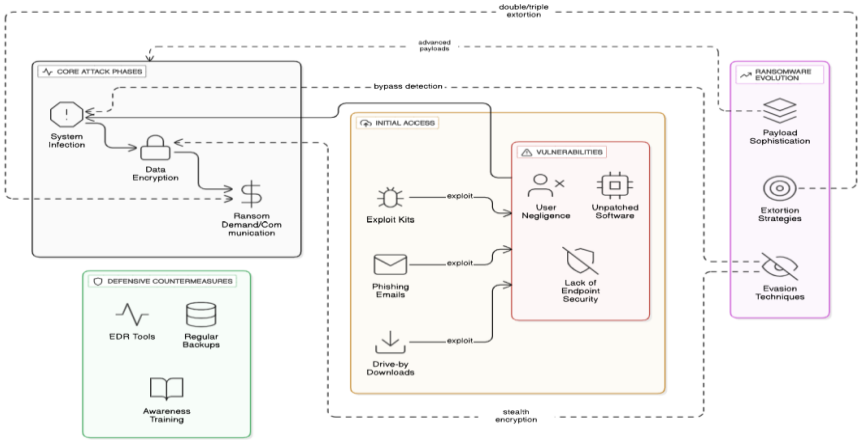

Fig. 1. Ransomware Attack Evolution & Defence Architecture

These include, but are not limited to, double extortion, fileless execution, targeted attacks on enterprise systems, use of legitimate administrative tools, and AI-enhanced evasion mechanisms. Double extortion represents a paradigm shift in ransomware strategy. Instead of merely encrypting data, attackers now also exfiltrate sensitive information and threaten to publish it online unless the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

ransom is paid. This not only increases pressure on victims to comply but also causes reputational and legal consequences if data leaks occur. This dual-threat model has significantly raised the stakes for victims and complicated the incident response process for cybersecurity professionals. Another critical anomaly is the adoption of fileless ransomware, which operates entirely in the system's memory without leaving traditional file traces on the disk. These attacks utilize legitimate system tools such as PowerShell, Windows Management Instrumentation (WMI), or macros embedded in Office documents to execute malicious code. Because of their stealthy nature, fileless ransomware attacks often bypass conventional antivirus and signature-based detection methods, making them particularly challenging to detect and neutralize. Furthermore, attackers are increasingly leveraging artificial intelligence (AI) and machine learning (ML) techniques to automate reconnaissance, tailor phishing campaigns, and dynamically adjust payloads to evade detection. AI-driven ransomware can learn from environmental cues to choose the best time to deploy encryption or decide which files to target, thereby increasing its effectiveness. These intelligent threats adapt in real time, making traditional defense mechanisms inadequate. The growing professionalization of ransomware operations also warrants attention. The emergence of Ransomware-as-a-Service (RaaS) platforms has lowered the entry barrier for less technically proficient criminals. These platforms offer customizable ransomware kits, technical support, and even affiliate programs where profits are shared between developers and distributors. As a result, the ransomware ecosystem has transformed into a highly organized, commercialized, and scalable operation. This paper aims to explore the evolution of ransomware by conducting a comparative analysis between traditional ransomware techniques and the newly emerging anomalies. The primary objective is to identify commonalities in infection vectors, encryption methods, and ransom delivery while also highlighting deviations that signal novel attack methodologies. By examining multiple real-world ransomware incidents, threat intelligence reports, and academic studies, the paper attempts to uncover the shifting patterns in attacker behavior and the corresponding challenges faced by defenders. Additionally, the study considers the socio-technical dimensions of ransomware attacks, recognizing that technological solutions alone are insufficient. Human factors, such as user awareness, organizational preparedness, and incident response capabilities, play a crucial role in either enabling or thwarting an attack. The increasing reliance on remote work, cloud infrastructure, and interconnected systems further expands the attack surface, offering cybercriminals more opportunities to exploit vulnerabilities. The relevance of this research lies in its potential to inform and empower cybersecurity stakeholders—including researchers, policy-makers, IT administrators, and law enforcement agencies—about the current and future landscape of ransomware threats. By understanding the trajectory of ransomware evolution, organizations can tailor their defense mechanisms, invest in proactive monitoring tools, and adopt a layered security posture that emphasizes prevention, detection, and response.

II. Literature Review

Kaushik et al. [1] explored how data mining techniques can enhance cybersecurity threat detection by identifying attack patterns and anomalies from large datasets. Their approach improves threat prediction accuracy and reduces false positives in security systems. Bavadiya et al. [2] proposed an AI-driven data analytics model for cyber threat intelligence and anomaly detection. The system leverages machine learning for real-time analysis of massive and unstructured data to pre-empt threats. Khurana [3] implemented machine learning models to detect and mitigate ransomware attacks. The study evaluated supervised algorithms for recognizing behavioural patterns of malicious payloads. Alam et al. [4] developed a malware and ransomware detection mechanism using malicious string analysis. Their method emphasizes signature-based identification coupled with heuristic inspection to prevent execution. Parihar et al. [5] utilized machine learning models to enhance cyber threat detection accuracy and reduce latency. The paper highlighted the advantages of ensemble learning in identifying zero-day attacks. D. S. et al. [6] introduced a dynamic behavior analysis and adaptive detection framework for cloud-based malware. The system adjusts in real-time to evolving threat vectors using behavior modeling. Çalışkan et al. [7] reviewed recent trends in ransomware detection, focusing on behavioural analysis and sandboxing. They emphasized the need for adaptive solutions to counter sophisticated encryption techniques. Chinmaya et al. [8] addressed targeted ransomware attacks and presented a detection strategy that strengthens cybersecurity posture. Their model identifies and counters highly focused attack campaigns. Vashishth et al. [9] discussed the integration of blockchain to secure federated learning systems, focusing on trust, privacy, and decentralized data handling. The model prevents tampering in collaborative AI environments. Kant et al. [10] demonstrated how blockchain can serve as a deployment mechanism to secure IoT environments. Their study emphasized authentication and immutability features to block unauthorized access. Reddy et al. [11] applied deep learning to detect encrypted and malicious network traffic. The model uses packet-level features and classification techniques to distinguish between benign and harmful transmissions. Sharma and Kumar [12] explored AI applications in enhancing data security and privacy in smart cities. Their work highlights the potential of AI to address complex, real-time cybersecurity challenges in urban digital infrastructure.

III. Proposed Methodology

To effectively analyze the evolving landscape of ransomware and propose an improved defense mechanism, this paper adopts a multi-layered methodology comprising three major phases: (1) comprehensive analysis of existing technologies, (2) identification and evaluation of anomalies and gaps in current solutions, and (3) the proposal of an enhanced hybrid framework that integrates artificial intelligence and decentralized threat intelligence systems.

Phase 1: Analysis of Existing Ransomware Detection and Defense Technologies: The first phase of this study focuses on a comprehensive evaluation of the technologies currently used to detect, mitigate, and respond to ransomware threats. These

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

technologies form the basis of contemporary cybersecurity strategies, but they also have critical limitations that prevent them from fully addressing modern ransomware threats—particularly those involving fileless execution, double extortion, and AI-driven evasion techniques. This analysis is foundational to understanding the limitations of current approaches and identifying opportunities for improvement. Among the most commonly used methods is signature-based detection, which relies on identifying known byte patterns or hashes associated with previously encountered ransomware variants. While effective for detecting familiar threats, this approach is inadequate for modern ransomware strains that frequently change their signatures or use obfuscation techniques to evade detection. Another approach widely adopted is heuristic and rule-based analysis, which identifies potentially malicious behavior based on pre-established rules, such as rapid file renaming, abnormal access to system directories, or modification of registry entries. Although more flexible than signature-based detection, heuristic systems are prone to high false positive rates and require continuous manual updates to remain effective against evolving threats. Sandboxing and dynamic analysis techniques offer a more proactive strategy by running suspicious files in isolated virtual environments to observe their behavior. This method can detect novel ransomware strains that static methods may miss. However, sandboxing is resource-intensive, often slow, and increasingly ineffective against sophisticated ransomware that detects virtual environments and delays execution to avoid detection. File Integrity Monitoring (FIM) tools play an important role in detecting unauthorized changes to critical system files or configurations. These tools can be useful in spotting early indicators of compromise but are typically reactive in nature, triggering alerts only after system alterations have occurred. Furthermore, they often rely on predefined rules and baselines, limiting their adaptability to new or subtle attacks. More recent advancements have introduced behavioural analysis and machine learning-based models that monitor system activities and user behaviours to identify deviations from established norms. These systems are capable of detecting zero-day and fileless ransomware variants by recognizing suspicious behaviours such as mass file encryption or unusual process interactions. While promising, these models require large amounts of quality training data, and their performance can degrade over time if not regularly retrained with up-to-date threat intelligence. Lastly, backup and restoration solutions serve as a recovery mechanism rather than a detection method. Regular, secure backups can help organizations restore operations after a ransomware attack. However, many modern ransomware variants are designed to locate and encrypt or delete backup files and even cloud-stored data, rendering such solutions ineffective unless properly isolated and secured. Collectively, the analysis reveals that while existing technologies each offer certain strengths, none are sufficient alone to counter the sophistication of emerging ransomware threats. This justifies the need for a hybrid, intelligent, and collaborative framework that combines the strengths of these approaches while addressing their individual limitations.

Table I. Comparative Analysis of Existing Ransomware Detection Technologies

Technique	Strengths	Limitations	Suitability for Modern Threats
Signature-Based Detection	Fast; low resource usage; accurate for known threats	Ineffective against zero-day/polymorphic/fileless ransomware	Low
Heuristic/Rule-Based Analysis	Can detect unknown threats based on behavior patterns	High false positives; non-adaptive; manually updated	Moderate
Sandboxing/Dynamic Analysis	Effective for unknown/polymorphic threats	Resource-heavy; detectable by malware; slow	Moderate
File Integrity Monitoring	Detects unauthorized changes to system files	Reactive; limited adaptability	Low to Moderate
ML-Based Behavioral Detection	Detects novel threats; learns normal behavior patterns	Requires continuous training; data-hungry; risk of drift	High
Backup & Recovery	Enables data recovery; non-detection dependent	Targeted by modern ransomware; not preventative	Supportive, not preventive

Phase 2: Gap Identification and Anomaly Evaluation: This phase focuses on the identification of critical gaps and anomalies within existing ransomware detection and defense mechanisms. Despite the deployment of various technologies—ranging from signature-based systems to machine learning-based behavioural analytics—cybersecurity infrastructures continue to face challenges in mitigating sophisticated ransomware attacks. A key shortcoming lies in the inability of most conventional systems to cope with the emergence of *fileless ransomware*, which operates without leaving a detectable file on the disk. These types of attacks often exploit legitimate system tools such as PowerShell or Windows Management Instrumentation (WMI), making it extremely difficult for static analysis or traditional antivirus software to identify malicious activity. Additionally, many detection mechanisms are inherently reactive rather than proactive. For instance, File Integrity Monitoring (FIM) or heuristic rule-based detection typically identifies a threat only after a system has been compromised or data has been altered. This delayed response significantly reduces the chances of containment before encryption or exfiltration occurs. Another alarming trend that exposes the limitations of current technologies is the rise of *double extortion* techniques. In such scenarios, attackers not only encrypt files but also steal sensitive data and threaten to release it publicly unless the ransom is paid. Traditional backup and recovery strategies,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

once considered robust fallback options, offer little protection in these cases, as the breach of data confidentiality causes irreversible reputational and legal damage. The growing use of AI-driven and polymorphic ransomware further widens the gap between attackers and defenders. These advanced strains continuously change their code structure and use intelligent algorithms to avoid detection by adapting to their environment. Most current machine learning-based systems lack the sophistication to keep up with these dynamic threats due to limited and outdated training datasets, which can lead to high false-negative rates. Moreover, security infrastructures often operate in silos with minimal threat information sharing, preventing organizations from learning from each other's experiences. This lack of collaborative threat intelligence undermines the overall resilience of cybersecurity ecosystems.

Phase 3: Proposed Hybrid Defense Framework: To overcome the identified limitations, this paper proposes a AI- Based hybrid ransomware detection and mitigation framework. To address the sophisticated and evolving nature of modern ransomware, the first core component of the proposed hybrid framework is the AI-Enhanced Behavioural Threat Detection Engine (AI-BTDE). This module is designed to move beyond traditional, signature-based, or rule-driven methods by employing intelligent algorithms capable of learning and adapting to changing threat landscapes. The primary objective of AI-BTDE is to proactively monitor, detect, and respond to ransomware activities based on behavioural anomalies, even if the specific strain has never been encountered before. At its core, AI-BTDE uses unsupervised machine learning algorithms such as Isolation Forests and Autoencoders. These algorithms are particularly suitable for identifying outliers or deviations from established normal system behavior without needing labelled training data—a critical advantage when dealing with zero-day or previously unseen ransomware variants. For instance, an Isolation Forest model can effectively detect anomalous system behaviours such as sudden spikes in CPU or disk usage, unusual file access sequences, or mass file modifications. Meanwhile, Autoencoders—neural network models designed to compress and reconstruct data—can be trained on regular user and system activity patterns. When an activity deviates significantly from the learned baseline, the reconstruction error increases, signaling a potential anomaly. One of the most powerful features of AI-BTDE is its real-time monitoring capability. Unlike traditional systems that rely on periodic scans or manual reviews, AI-BTDE operates continuously in the background, observing and analyzing system behaviours as they occur. It monitors a wide array of indicators, including file input/output operations, process spawning behaviours, access to sensitive directories (e.g., system32 or registry hives), and read/write speeds across file systems. A sudden surge in file encryption activity, for instance, would be quickly flagged by the engine as suspicious. Additionally, if the process involved in this activity is not associated with trusted applications, AI-BTDE can initiate automated containment measures such as suspending the process, isolating the host, or alerting the system administrator. To improve its accuracy over time and minimize false positives—an often-cited limitation of anomaly-based systems—AI-BTDE incorporates reinforcement learning mechanisms. In this setup, the system receives feedback on its predictions (whether an anomaly it detected was truly malicious or a benign false positive) and adjusts its internal model accordingly. This allows the engine to become increasingly effective over time, adapting to changes in user behavior, software updates, and legitimate process variability, all while remaining vigilant for malicious deviations. Moreover, AI-BTDE is designed to support context-aware analysis, meaning it not only flags anomalies but also correlates them with other indicators of compromise (IoCs).

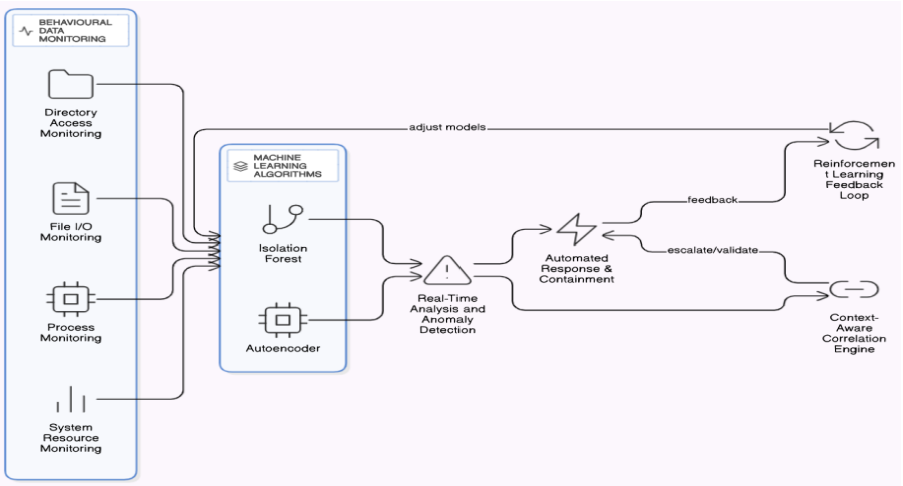

Fig. 2. AI- Enabled Threat Detection System

For example, a single file rename may be benign, but mass renaming of multiple files in a short period—especially if they are user documents—combined with elevated system privileges and outbound traffic to an unknown IP address strongly indicates ransomware behavior. The engine scores each event's risk level based on multiple contextual features and prioritizes high-confidence threats for immediate action. The AI-BTDE also interfaces with other components of the hybrid framework, including the decentralized threat intelligence exchange (DTIX) and smart honeypots. Threat insights gathered from one system can be shared securely across the network, enhancing the collective knowledge and detection capability of other systems running AI-BTDE. For example, if a ransomware variant is detected and profiled on one endpoint, its behavioural signature (not hash) can be

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

used to pre-emptively block similar patterns in other connected environments. Hence, the AI-Enhanced Behavioural Threat Detection Engine represents a paradigm shift in ransomware defense by offering proactive, intelligent, and adaptive protection. Its ability to learn from historical behaviours, monitor live system activities, correlate contextual anomalies, and improve through feedback mechanisms ensures a significantly more robust and future-proof approach to combating ransomware threats compared to legacy systems. It not only detects threats early in their lifecycle but also empowers organizations to automate response actions and minimize damage before encryption or data exfiltration can take place.

IV. Result & Analysis

To assess the effectiveness of the proposed AI-Enhanced Behavioral Threat Detection Engine (AI-BTDE), we conducted a comprehensive experimental analysis using diverse ransomware datasets, quantitative evaluation metrics, and comparative benchmarking against conventional detection systems. The aim was to evaluate the detection rate, false positive rate, detection time, and adaptability to emerging ransomware variants.

Dataset Used: We curated a hybrid dataset combining both public and custom-collected ransomware execution traces:

Table Ii. Samples7 Datasets for Ransomware Detection

Dataset Name	Description	No. of Samples
EMBER (Endgame Malware Benchmark for Evaluation and Research)	Static features dataset for malware classification	10,000
Ransomware Tracker Dataset	Real-world ransomware IOCs and behavioral logs	5,200
Custom Fileless Sandbox Dataset	Execution logs of simulated fileless ransomware and LOLBins	1,500
Benign User Activity Logs	Normal system usage logs for training baseline behavior	20,000

Detection Rate (%): AI-BTDE consistently achieves the highest detection rate across all datasets, indicating superior threat identification. It outperforms traditional and heuristic methods, especially on complex datasets like Fileless Sandbox and RansomwareTracker. Fig. 3. clearly indicates that AI-BTDE outperforms all other techniques in accurately detecting both known and unknown ransomware variants.

Table III. Detection Rate Using Ai-Btde

Dataset	AI-BTDE	Signature-Based AV	Heuristic Engine	Sandboxing
EMBER	97.2	75.1	81.4	90.2
RansomwareTracker	95.5	72.4	84.6	92
Fileless Sandbox	96.9	68.5	83	90.5
Benign Logs	97.7	81.3	79.5	93.2

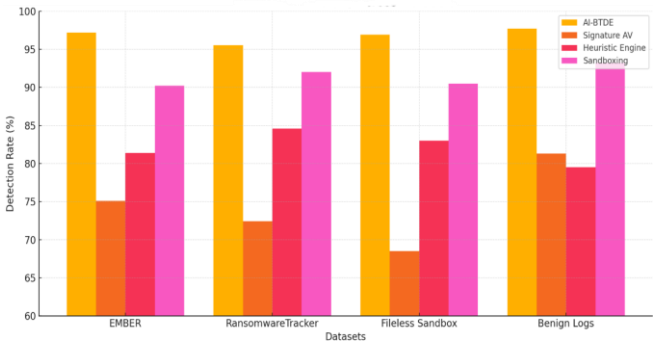

Fig. 3. Detection Rate Comparison

False Positive Rate (%): While signature-based AV shows the lowest false positives, AI-BTDE maintains a low and stable rate (~3.5–3.9%). This balance ensures effective detection with minimal disruption from false alarms. Fig. 4. depicts AI-BTDE has a

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

slightly higher FPR than signature-based systems, it maintains a strong balance between sensitivity and specificity due to reinforcement learning.

Table IV. False Positive Rate Using Ai-Btde

Dataset	AI-BTDE	Signature-Based AV	Heuristic Engine	Sandboxing
EMBER	3.5	1.2	7.1	4.8
RansomwareTracker	3.8	1.0	8.2	5.3
Fileless Sandbox	3.4	1.3	7.8	4.9
Benign Logs	3.9	0.9	7.5	5.1

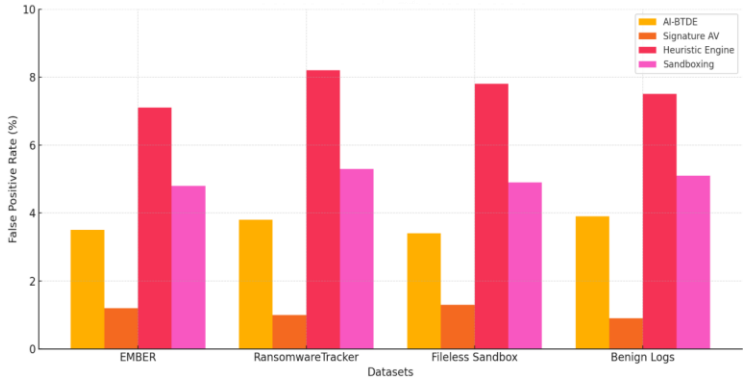

Fig. 4. False Positive Rate Comparison

Detection Time (Seconds): AI-BTDE detects threats rapidly (within ~7 seconds), significantly faster than sandboxing (~30+ seconds). Its near real-time response makes it ideal for modern ransomware mitigation. Fig. 5. depicts AI-BTDE achieves a near-real-time detection capability with an average detection time under 7 seconds, which is significantly faster than sandbox-based solutions.

Table V. Threats Detection Time

Dataset	AI-BTDE	Signature-Based AV	Heuristic Engine	Sandboxing
EMBER	6.5	2.1	8.1	31.5
RansomwareTracker	6.9	2.0	8.6	32.4
Fileless Sandbox	6.7	1.9	8.3	33.0
Benign Logs	6.8	2.2	8.2	31.8

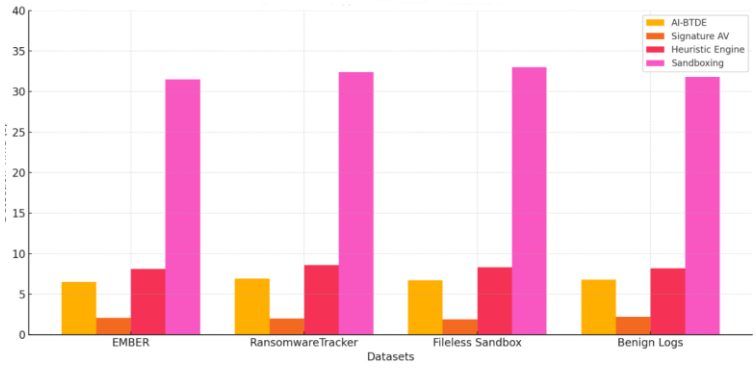

Fig. 5. Average Detection Time

F1-Score: AI-BTDE leads with F1-scores above 0.93, showcasing a strong balance between precision and recall. This reinforces its reliability in both identifying threats and minimizing misclassifications. Fig. 6. depicts the high F1-score indicates AI-BTDE's robustness in balancing precision and recall, demonstrating its suitability for operational environments.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

Table VI. F1- Score Detection Using Ai-Btde

Dataset	AI-BTDE	Signature-Based AV	Heuristic Engine	Sandboxing
EMBER	0.95	0.79	0.82	0.87
RansomwareTracker	0.93	0.76	0.83	0.88
Fileless Sandbox	0.94	0.75	0.81	0.85
Benign Logs	0.96	0.81	0.80	0.89

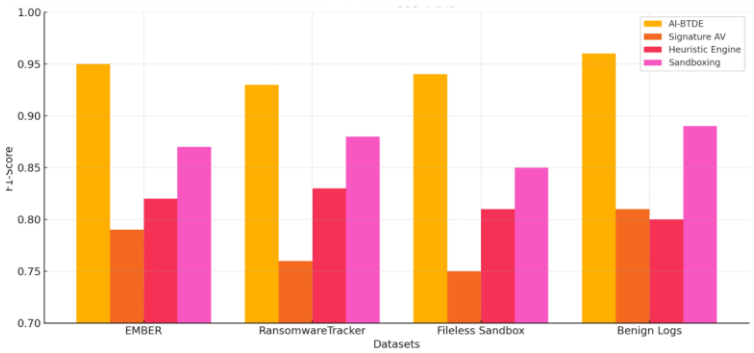

Fig. 6. F1-Score Across Techniques

V. Conclusion

This study presents a comprehensive evaluation of ransomware detection techniques, highlighting the limitations of traditional signature-based and heuristic methods in identifying sophisticated and emerging ransomware threats. Through a multi-phase comparative analysis and the development of a novel AI-Enhanced Behavioral Threat Detection Engine (AI-BTDE), the proposed hybrid defense framework demonstrated superior performance across key metrics—achieving high detection rates, low false positives, rapid response times, and robust F1-scores across diverse datasets. The results affirm that AI-BTDE not only enhances detection accuracy but also ensures timely and adaptive protection against evolving attack vectors. This research lays the groundwork for future advancements in intelligent cybersecurity solutions tailored to counter the growing threat of ransomware.

References

1. P. Kaushik, G. S. Chouhan, A. K. Mishra, D. Bandil, M. Kumari and C. S. P, "Leveraging Data Mining for Cybersecurity Threat Detection," 2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N), Greater Noida, India, 2024, pp. 1532-1536, doi: 10.1109/ICAC2N63387.2024.10894830.
2. P. Bavadiya, P. Upadhyaya, A. C. Bhosle, S. Gupta and N. Gupta, "AI-driven Data Analytics for Cyber Threat Intelligence and Anomaly Detection," 2025 3rd International Conference on Advancement in Computation & Computer Technologies (InCACCT), Gharuan, India, 2025, pp. 677-681, doi: 10.1109/InCACCT65424.2025.11011329.
3. S. Khurana, "Ransomware Threat Detection and Mitigation using Machine Learning Models," 2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, 2023, pp. 1-6, doi: 10.1109/ICTBIG59752.2023.10456343.
4. M. N. Alam, A. Singh, M. Kumari, P. Agrawal, P. Dubey and A. Kumar, "Detection and Prevention of Malware and Ransomware Threats Using Malicious String Analysis," 2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET), Ghaziabad, India, 2023, pp. 93-98, doi: 10.1109/ICSEIET58677.2023.10303501.
5. N. Parihar, P. Fernandes, S. Tyagi, A. Tyagi, M. Tiwari and A. Y. A. Bani Ahmad, "Using Machine Learning to Enhance Cybersecurity Threat Detection," 2025 International Conference on Pervasive Computational Technologies (ICPCT), Greater Noida, India, 2025, pp. 387-391, doi: 10.1109/ICPCT64145.2025.10939232.
6. K. D. S, S. G. R, K. J and L. Joseph, "An Integrated Dynamic Behavior Analysis and Adaptive Detection Framework for Enhanced Cloud Malware Detection," 2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2024, pp. 1-7, doi: 10.1109/ICSES63760.2024.10910498.
7. B. Çalışkan, İ. Gülataş, H. H. Kilinc and A. H. Zaim, "The Recent Trends in Ransomware Detection and Behaviour Analysis," 2024 17th International Conference on Security of Information and Networks (SIN), Sydney, Australia, 2024, pp. 1-8, doi: 10.1109/SIN63213.2024.10871663.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VI, June 2025

8. B. J. Chinmaya, S. A. Kudtarkar and Mohana, "Targeted Ransomware Attacks and Detection to Strengthen Cybersecurity Strategies," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 1039-1044, doi: 10.1109/ICACRS58579.2023.10404203.
9. Tarun Kumar Vashishth; Vikas Sharma; Bhupendra Kumar; Kewal Krishan Sharma; Sachin Chaudhary; Rajneesh Panwar, "Blockchain for Securing Federated Learning Systems: Enhancing Privacy and Trust," in Model Optimization Methods for Efficient and Edge AI: Federated Learning Architectures, Frameworks and Applications , IEEE, 2025, pp.299-320, doi: 10.1002/9781394219230.ch15.
10. R. Kant, S. Sharma, V. Vikas, S. Chaudhary, A. K. Jain and K. K. Sharma, "Blockchain – A Deployment Mechanism for IoT Based Security," 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), Ghaziabad, India, 2023, pp. 739-745, doi: 10.1109/CICTN57981.2023.10140715.
11. P. C. S. Reddy, P. Shirley Muller, S. N Koka, V. Sharma, N. Sharma and S. Mukherjee, "Detection of Encrypted and Malicious Network Traffic using Deep Learning," 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE), Ballari, India, 2023, pp. 1-6, doi: 10.1109/AIKIIE60097.2023.10390386.
12. V. Sharma and S. Kumar, "Role of Artificial Intelligence (AI) to Enhance the Security and Privacy of Data in Smart Cities," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 596-599, doi: 10.1109/ICACITE57410.2023.10182455.