Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 12, Issue 2, pp: (7-18), Month: May - August 2025, Available at: www.noveltyjournals.com

A Comprehensive Survey of Intelligent Techniques for Ransomware Mitigation in Corporate Networks

[1]Gloria N. Ezeh, [2]Udoka F. Eze, [3]Baldwin C. Asiegbu, [4]Charles O. Ikerionwu, [5]Mathew E. Nwanga, [6]Vivian C. Mbamala.

[1, 2,5,6]Department of Information Technology, Federal University of Technology, Owerri, Nigeria.

[3]Department of Entrepreneurship and Innovation, Federal University of Technology, Owerri, Nigeria.

[4]Department of Software Engineering, Federal University of Technology, Owerri, Nigeria.

DOI: https://doi.org/10.5281/zenodo.15584433

Published Date: 03-June-2025

Abstract: One of the most devastating cybersecurity threats today is ransomware, which mostly targets corporate infrastructures where the availability of critical data and services is paramount. Identifying new and polymorphic ransomware strains frequently presents a challenge for existing signature-based protection. For proactive mitigation, innovative techniques like machine learning (ML), deep learning (DL), and hybrid models are increasingly being used. A detailed and technical review of modern intelligent techniques for ransomware detection, prevention, and response in corporate settings is provided in this paper. We discuss a taxonomy of techniques, assess their design methods thoroughly, talk about the datasets and performance indicators that are currently accessible, and point out flaws that still need to be tackled. In addition, we present a strategic roadmap for future research by shedding light on new trends, including adversarial resilience and federated learning.

Keywords: **Corporate Network Security, Cybersecurity, Hybrid Models, Machine Learning, Ransomware.**

1. INTRODUCTION

With the use of sophisticated evasion strategies, such as code obfuscation, polymorphism, and lateral movement across corporate networks, ransomware has grown increasingly complicated. Ransomware could result in a significant operational and financial impact on organizations, as demonstrated by attacks like WannaCry, NotPetya, and Maze. While traditional security measures like perimeter firewalls, rule-based intrusion detection systems (IDS), and signature-based antivirus frequently detect known threats, they have trouble countering zero-day or hidden ransomware variations. By employing the capacity to learn, adapt, and react independently to changing threat landscapes, intelligent methods provide a paradigm revolutionary in ransomware mitigation. In corporate environments where scalability, precision, and low latency are essential, this study focuses on intelligent systems of this type, especially those that integrate AI/ML/DL.

2. RANSOMWARE THREAT LANDSCAPE AND MOTIVATION FOR INTELLIGENT DEFENSE

2.1 Evolution of Ransomware Attacks

From opportunistic, small-scale attacks on individual users to strategic, large-scale operations targeting corporate and institutional infrastructure, ransomware attacks have evolved into corporate networks. At first, ransomware targeted residential users with basic social engineering techniques like phony software upgrades or email attachments. These early versions, such as locker ransomware, interfered with user access but did not permanently destroy data, and recovery was frequently achievable using simple tools. However, ransomware started to develop with more sophisticated technical features and focused strategies as threat actors realized the increased potential for profit and disruption within enterprises.

An important turning point was the shift to crypto-ransomware, which encrypts files using powerful encryption techniques. Attackers now force companies to pay ransoms to restore vital activities after causing significant data loss. Prominent instances like TeslaCrypt, Locky, and CryptoLocker illustrated the harm ransomware could do in business settings.

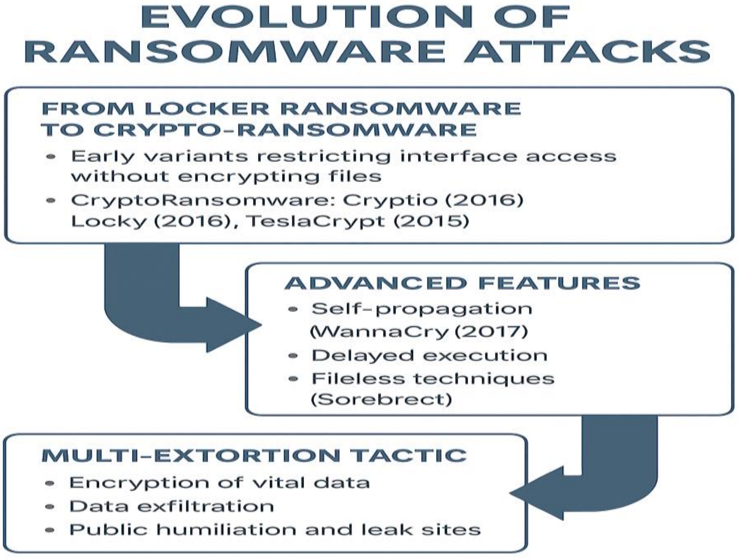
EVOLUTION OF RANSOMWARE ATTACKS
FROM LOCKER RANSOMWARE TO CRYPTO-RANSOMWARE
• Early variants restricting interface access without encrypting files
• CryptoRansomware: Cryptio (2016) Locky (2016), TeslaCrypt (2015)
ADVANCED FEATURES
• Self-propagation (WannaCry (2017)
• Delayed execution
• Fileless techniques (Sorebrect)
MULTI-EXTORTION TACTIC
• Encryption of vital data
• Data exfiltration
• Public humiliation and leak sites

Figure 1: Evolution of Ransomware Attacks from simple file-locking mechanisms to highly complex, multi-phase initiatives targeting enterprise infrastructures.

Ransomware has improved substantially over time, from simple file-locking mechanisms to highly complex, multi-phase initiatives targeting enterprise infrastructures. This evolution can be categorized into several stages as shown in Figure 1, with the below detailed explanation:

1. From locker ransomware to crypto-ransomware: Early ransomware variants, like the 2007 WinLock, were primarily locker ransomware, which restricted access to the system's interface without encrypting files; these attacks frequently displayed a fullscreen window demanding ransom, but data was not permanently damaged and could occasionally be restored through safe mode or system recovery tools. In contrast, newer variants have advanced into crypto-ransomware, which uses sophisticated encryption algorithms (like AES, RSA) to render data inaccessible. Examples include:

i. CryptoLocker (2013): came into existence as one of the first crypto-ransomware malware to go viral, it utilizes public key cryptography to encrypt data permanently until the private key is obtained.

ii. Locky (2016) and TeslaCrypt (2015) employed enhanced encryption and propagation techniques.

This change marked an abrupt increase in ransomware's impact, making it much more difficult to recover data without paying the ransom.

2. Advanced features: The advanced features include anti-sandboxing, delayed execution, and self-propagation (e.g., WannaCry exploiting SMBv1). To increase its impact and avoid detection, modern ransomware uses a variety of advanced techniques:

i. Self-propagation: In just a few hours, WannaCry (2017) impacted over 200,000 systems in more than 150 countries through the use of the SMBv1 vulnerability (EternalBlue) to propagate automatically across networks.

ii. Delayed execution: Certain strains cause time delays before encryption or execution starts, enabling them to evade behavioral detection systems that concentrate on fast execution.

iii. Fileless techniques: Ransomware, like Sorebrect, doesn't use file system traces or regular disk-based detection because it operates exclusively in memory. These strategies indicate a move toward more persistent, hidden threats that can get past conventional defenses.

3. Multi-extortion tactics: Advanced ransomware operations have expanded into multi-extortion attacks, in which the criminals employ various coercive techniques at the same time. The multi execution tactics include:

i. Encryption of vital data: When victims are unable to access operational files, business operations are frequently interrupted.

ii. Data exfiltration: Confidential data is frequently obtained prior to encryption. If the ransom is not paid, the attackers then threaten to sell or reveal the data, escalating the consequences to one's reputation and legal standing.

iii. Public Humiliation and Leak Sites: Threat actors run "shame sites" on the dark web where they expose or sell stolen data in an attempt to impose pressure on victims to pay.

The success rate and funds yield of ransomware attacks are rising as a result of this multilayered strategy. These strategies have become standard in ransomware-as-a-service (RaaS) environments due to their formalization by well-known companies such as Maze, REvil, and Conti.

2.2 Methods of Attack

Ransomware accesses corporate networks via some processes, each of which leverages particular weaknesses in system setups, human behavior, or old software. It is important to understand these points of attack in order to create proactive and sophisticated countermeasures. The attack vectors include:

1. Phishing Emails and Malicious Attachments: The most common first access vector for ransomware deployment continues to be phishing. To fool users into opening malicious documents or clicking embedded links, attackers create socially engineered emails that look like official communication, such as bills, HR notices, or shipping confirmations. These attachments supply payloads that begin the ransomware infection process; they are mainly Word documents, PDFs, or bundled executables with macro capabilities [1]. Advanced Phishing tactics could include:

i. Spear-phishing: Customized targeting relying on previously acquired organizational or personal data [2].

ii. Payload Obfuscation: According to [3], payload obfuscation is the method of preventing detection through the use of scripting languages such as PowerShell, JavaScript, or VBA macros.

iii. Multi-stage droppers: Is the process where initial attachments downloads secondary ransomware payloads after sandbox evasion [4]. These payloads can trigger lateral movement throughout the network, escalate privileges, and create persistence after they have been executed [5].

2. Remote Desktop Protocol (RDP) Brute Force Attacks: RDP is a valid remote access service, which is constantly exploited because of weak credentials, unsecured ports, or lack of network segmentation. Threat actors employ automated tools like Shodan to search for publicly unsecured RDP services, then execute brute-force or credential-stuffing assaults to gain illegal access [6]. After establishing access, attackers have the following options:

i. Manually install ransomware with complete administrative rights [7].

ii. Turn down backup and endpoint security services [2].

iii. Drop various malicious tools, such as spying tools and keyloggers [5].

Because RDP allows customized attacks and thorough pre-encryption monitoring, RDP exploitation has been the most common vector for ransomware gangs like Dharma, SamSam, and Conti [1].

3. Drive-by Downloads and Exploit Kits: Users become infected in drive-by download instances just by going to deceptive or compromised websites, usually without any user involvement. These websites can utilize exploit kits such as Angler, Neutrino, or Rig to identify and take advantage of weaknesses in the visitor’s browser, plugins (e.g., Flash, Java), or underlying operating system [2]. Exploit kits often follow an organized workflow:

i. Redirect: Malvertising or script injections are utilized to silently divert the victim to a landing page [3].

ii. Vulnerability detection: Unpatched software versions are scrutinized by the kit [4].

iii. Delivery of the payload: The ransomware payload gets sent and launched after a suitable exploit medium has been found [5].

These attacks become particularly dangerous in corporate settings with weak patch maintenance, behavioral endpoint controls, and web filtering [1].

2.3 Inadequacy of Traditional Methods

Traditional ransomware mitigation approaches, though essential, suffer serious challenges in recognizing and responding to new ransomware attacks due to the constantly changing nature of malware creation and attack techniques. Below are some of the flaws of the underlined techniques:

i. Static Signatures Fail to Detect Polymorphic Samples: Detecting known trends in malware code is the basis of signature-based antivirus software. However, as a way to dynamically change the ransomware's binary structure and make static signatures useless, ransomware authors are increasingly using polymorphism and code obfuscation techniques [2]. This limits the capacity of ordinary signature scanners to offer immediate protection due to high false-negative rates, mainly against zero-day and quickly evolving ransomware variants [8].

ii. Rule-Based Systems Have Maintenance and Rigidity Challenges: To identify suspicious activities or anomalies, rule-based detection systems use established heuristics and logic. These methods are rigid, even though they can be helpful in some situations. This is because new ransomware strains might take advantage of unmonitored behaviors or defy static rules [3]. Moreover, developing and sustaining rules takes a lot of manual labor and domain knowledge, which delays the adaptation of defenses against new threats. The high risk of false positives further strains security teams with resource-intensive investigations [4].

iii. Time-Delay or User-Interaction Conditions Can Help Deter Sandboxing: By running dubious files in independent settings and monitoring behavior, sandbox environments offer dynamic analysis. Nevertheless, in order to avoid detection, newer ransomware variations adopt anti-sandbox and anti-VM tactics like halting execution, identifying user presence, or analyzing system artifacts [2,3]. These evasive techniques weaken the efficacy of sandbox-based detection technologies by enabling ransomware to stay dormant during analysis and only activate in situations that are real [5].

3. TAXONOMY OF INTELLIGENT RANSOMWARE MITIGATION TECHNIQUES

The "Taxonomy of Intelligent Techniques for Ransomware Mitigation" image provides a hierarchical and organized depiction of the fundamental computational tactics used to counteract ransomware threats. Machine Learning (ML), Deep Learning (DL), Hybrid Intelligent Systems, and Fuzzy and Heuristic Systems are the four main categories into which this taxonomy is painstakingly divided. These categories represent different degrees of algorithmic complexity and learning paradigms.

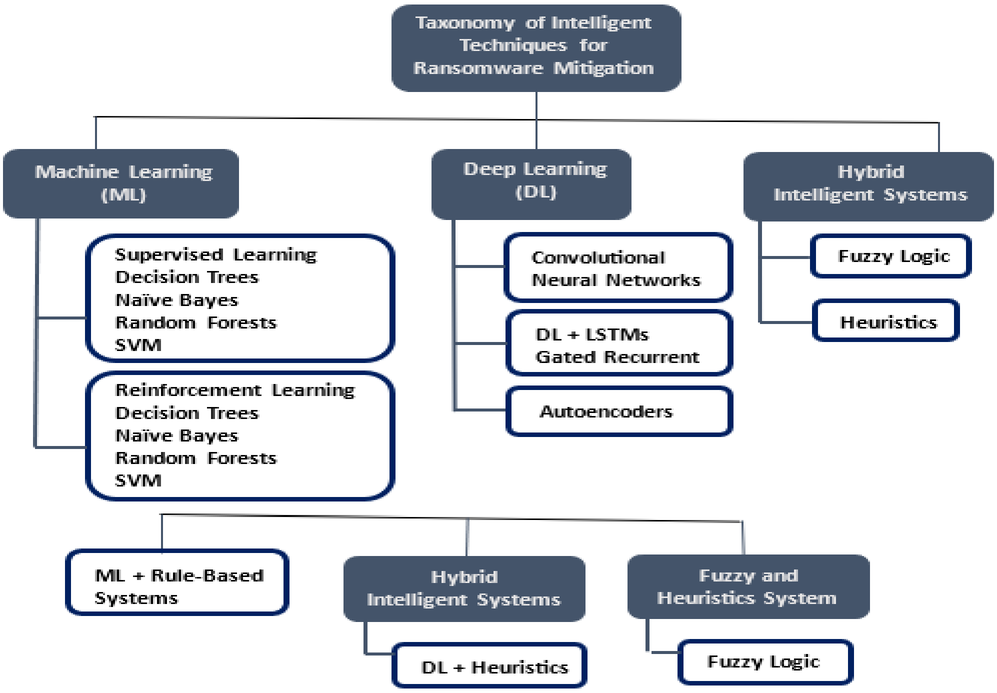

Figure 2: Taxonomy of Intelligent Techniques for Ransomware Mitigation

Supervised learning, unsupervised learning, and reinforcement learning are the three main learning paradigms that make up the first tier of machine learning (ML). Among the frequently used algorithms in supervised learning are Random Forests, Naïve Bayes, Decision Trees, and Support Vector Machines (SVM). These algorithms, which are usually employed for binary or multi-class classification and rely on labeled datasets, are able to differentiate ransomware from benign entities by using past patterns [9,2]. Unsupervised learning, on the other hand, includes techniques that are very good at detecting anomalies, like K-Means Clustering, DBSCAN, and Isolation Forests. These algorithms are essential for detecting zero-day ransomware attempts since they work with unlabeled data [8]**.** A more dynamic method called reinforcement learning is built on agents that interact with their surroundings to learn the best mitigation techniques. Through iterative feedback mechanisms, policies are progressively improved in response to ransomware activities [3].

With the shift to Deep Learning (DL), the taxonomy classifies increasingly intricate models with superior automatic feature extraction and hierarchical pattern recognition capabilities. Convolutional Neural Networks (CNNs) use spatial analysis of binary structures or images of system behavior to identify ransomware [10]. Recurrent architectures—more especially, Gated Recurrent Units (GRUs) and Long Short-Term Memory (LSTM) networks—are good in recording the temporal sequences of ransomware activities. They are especially helpful for examining system logs and time-series network traffic [11]. A more sophisticated anomaly detection method without explicit labeling is provided by Autoencoders, an unsupervised deep learning model that is used to reconstruct input data and identify deviations suggestive of ransomware through increased reconstruction errors [12].

The term "Hybrid Intelligent Systems" refers to the combination of several methods to take advantage of the complementary qualities of various models. To improve detection accuracy and lower false positives, this includes combinations such as ML + Rule-Based Systems, which combine statistical learning with domain-specific expert rules [4]. Similarly, DL + Heuristics leverages deep learning’s capacity for abstraction with heuristic-driven interpretability and responsiveness [2]. Moreover, Ensemble Learning and Voting Classifiers aggregate predictions from multiple base models to enhance decision robustness, mitigating the risks associated with adversarial evasion and model bias [9]. Lastly, methods that put interpretability and operational speed first include fuzzy and heuristic systems. By allowing for approximation thinking and taking into account the uncertainty present in ransomware activities, fuzzy logic systems offer resilience in ambiguous situations [13]. Heuristic techniques, on the other hand, quickly detect harmful patterns by using pre-established rules or signature-based methods. These are particularly helpful in situations when quick detection is crucial, such as real-time or resource-constrained settings [8]. Altogether, this taxonomy includes a broad range of intelligent strategies, spanning from core ML models to complex hybridized systems, each contributing uniquely to the multifaceted challenge of ransomware detection and prevention. It offers a framework for comprehending how cybersecurity defenses are changing and helps practitioners and academics choose and create suitable models according to threat profiles and contextual needs.

3.1 Taxonomy of Ransomware Detection Techniques

Static analysis, dynamic analysis, and hybrid analysis are the three main methodologies that are often used to classify ransomware detection strategies. Each of these approaches has its own advantages and disadvantages when it comes to identifying and evaluating ransomware threats.

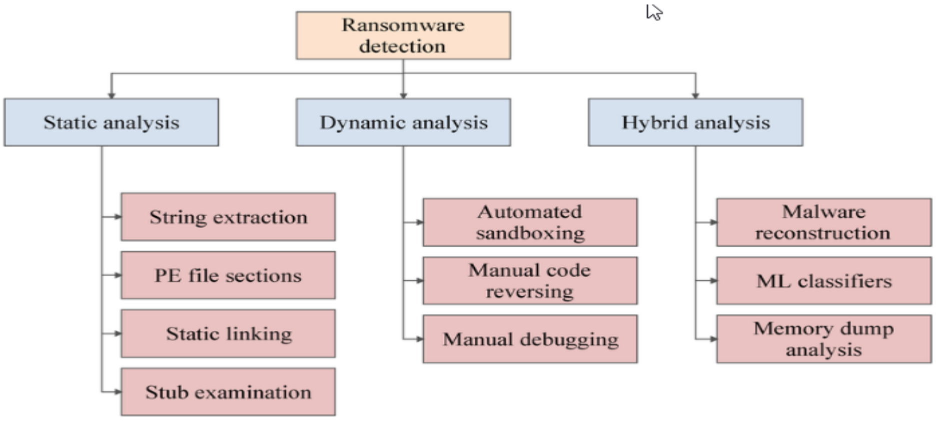

Figure 3: Taxonomy of Ransomware Detection Techniques

Figure 2 depicts the Taxonomy of Ransomware Detection Techniques. In the figure, Static analysis, dynamic analysis, and hybrid analysis are the three main methodologies that are often used to classify ransomware detection strategies. Each of these approaches has its advantages and disadvantages when it comes to identifying and evaluating ransomware threats. Examining malware binaries without running them is known as static analysis. Because it eliminates the danger of executing potentially harmful code, it is beneficial in terms of efficiency and security. To find ransomware signs like ransom notes, dubious URLs, or embedded commands, common static analysis approaches include string extraction, which recovers readable ASCII or Unicode strings within a binary [14]. Another method involves looking at PE (Portable Executable) file segments. Since ransomware frequently alters these sections to hide its payload, analysts evaluate the content and structure of particular headers and segments for irregularities. The way that binaries link to libraries and API calls is also examined using static linking analysis; unusual or excessive couplings could be a sign of harmful routines or obfuscation tactics [14]. Stub inspection also focuses on decrypting and examining encrypted stubs or loaders, which are commonly employed by ransomware to avoid detection in the first place. On the other hand, dynamic analysis entails running the suspected malware in a sandbox or other controlled and isolated environment to watch how it behaves in real time. Among the most popular methods is automated sandboxing, which records and monitors the malware's runtime activities, such as file encryption, registry modifications, and network interactions [15]. Another technique is manual code reversing, in which malware experts manually dissect and examine the code logic to understand complex or encrypted routines. In the same vein, manual debugging enables the analyst to step through the execution process and more closely examine memory use and unusual behavior. These methods work very well for identifying ransomware behaviors that are polymorphic and metamorphic, particularly those that are intended to only activate in certain situations [16].

Given the shortcomings of both static and dynamic approaches, hybrid analysis has surfaced as a more complete answer that combines the advantages of both paradigms. Malware reconstruction is a hybrid technique in which the components of the malware are broken down using static analysis, and a whole threat model is reassembled using dynamic analysis that monitors execution routes and environmental interactions [17]. The inclusion of machine learning classifiers further strengthens this method, allowing the integration of characteristics extracted from both static and dynamic analysis. Even in the case of novel strains, these classifiers can detect and categorize ransomware with high accuracy because they have been trained on vast datasets [16]. Memory dump analysis is another hybrid technique that examines secret operations, including encryption keys, command-and-control exchanges, and decrypted payloads by recording the memory state of an active process [17]. [18] Added that new methods, such as spectral entanglement fingerprinting, examine system behavior in the frequency domain and detect unusual cross-frequency fingerprints that are characteristic of ransomware execution.

The increasing complexity of ransomware detection methods is reflected in this taxonomy. The shift from traditional static and dynamic techniques to intelligent hybrid approaches shows how dedicated the cybersecurity community is to using layered, adaptive, and AI-driven solutions to counter the growing danger of ransomware.

4. REVIEW OF KEY INTELLIGENT APPROACHES

This section looks at trendy intelligent techniques used for ransomware detection and mitigation, emphasizing their methods, effectiveness, and real-world applications in corporate network environments.

4.1 Supervised Machine Learning: Supervised machine learning algorithms can learn from labeled datasets and generalize to unseen samples. As a result, they are widely used for ransomware classification. Examples include:
i. Random Forest (RF): [19] Used Random Forest (RF), an ensemble method that uses multiple decision trees to improve classification robustness, to classify ransomware based on behavioral features like file operations and process activity, and attained an accuracy of over 95% on controlled datasets. RF's ensemble nature allows it to handle noisy data and decreases overfitting, making it ideal for ransomware detection tasks.

ii. Support Vector Machine (SVM): SVM is a strong binary classifier that determines the best hyperplane to divide samples into malicious and benign categories. Although SVMs are good at detecting ransomware, their real-time application in vast corporate networks is limited by their potential scaling problems with very large datasets and high-dimensional feature spaces [20].

ii. XGBoost: This gradient boosting system is scalable and has proven to be highly effective in real-time ransomware detection situations. According to [20], XGBoost is a potential option for dynamic threat landscapes where quick adaptability is essential because it has higher accuracy and quicker training periods than standard classifiers.

4.2 Unsupervised Methods: By spotting unusual patterns without the need for labeled data, unsupervised learning techniques are essential for recognizing new or zero-day ransomware attacks. Some of the techniques include:

i. Isolation Forests: This algorithm isolates anomalies by randomly partitioning data and measuring path lengths to identify outliers in system activity logs. It has been effectively applied for detecting unusual file system and network behaviors indicative of ransomware activity [8].

ii. Autoencoders: These neural network models learn compressed representations of normal behavior. Deviations in reconstruction errors indicate potential ransomware activity. Autoencoders provide robust anomaly detection, particularly in environments lacking comprehensive labeled ransomware datasets [12].

4.3 Deep Learning: Deep Learning models uses Hierarchical feature extraction to examine complex malware traits, both static and dynamic. Examples are:

i. Convolutional Neural Networks (CNNs): In order to differentiate ransomware from safe software, CNNs have been used for static byte-level analysis of ransomware binaries. They do this by identifying spatial patterns in executable code [10].

ii. Long Short-Term Memory (LSTM) Networks: LSTM models are excellent at simulating sequential data, including command execution traces and system logs, and they may identify temporal irregularities linked to ransomware encryption and spread [11].

iii. Hybrid CNN-LSTM Architectures: These architectures combine the temporal sequence modeling of LSTMs with the spatial feature extraction of CNNs to improve detection performance, capturing both dynamic behavioral sequences and static signatures [12].

4.4 Hybrid Systems: In order to capitalize on the advantages of several paradigms, hybrid detection frameworks integrate machine learning with conventional signature or rule-based intrusion detection systems (IDS). These layered systems leverage ML's flexibility and IDS's domain-specific rule enforcement to provide robust defenses in a variety of corporate environments [4]. For instance, combining Random Forest classifiers with Suricata IDS allows for the efficient detection of both known ransomware signatures and novel anomalies, improving overall detection rates while maintaining manageable false positive rates [19].

4.5 Case Studies: In order to assist with practical trade-offs and to guide the deployment of appropriate techniques in corporate networks, Table 1 below compares different intelligent ransomware detection approaches across key metrics such as accuracy, false positive rate (FPR), detection latency, and scalability.

Table I: Comparison of intelligent approaches by accuracy, FPR, latency, and scalability

Approach	Accuracy (%)	FPR (%)	Latency (ms)	Scalability
Random Forest [19]	95+	3	100	Moderate
SVM [20]	90-95	5	150	Limited
XGBoost [20]	97	2	90	High
Isolation Forest [8]	88	7	80	High
Autoencoders [12]	92	4	120	Moderate
CNN-LSTM Hybrid [12]	96	3	110	Moderate
RF + Suricata IDS [19]	95+	2.5	130	Moderate-High

5. DATASETS AND EVALUATION METRICS

High-quality datasets and suitable evaluation metrics to gauge model performance are essential for efficient ransomware detection and mitigation. A description of the benchmark datasets frequently used in ransomware research is given in this section, along with the main metrics used to assess intelligent detection systems.

5.1 Benchmark Datasets: Below are the benchmark datasets:

i. CICIDS 2017–2018: CICIDS datasets, which were created by the Canadian Institute for Cybersecurity, provide extensive network traffic scenarios that incorporate a variety of attack types, including ransomware activity. These datasets include labeled network flow data, which is important for supervised learning approaches in network-level ransomware detection [21]. For instance, the CICIDS2017 dataset is one of the biggest publicly accessible datasets for ransomware and intrusion detection, with over 3 million flows.

ii. VirusShare / VirusTotal: Ransomware binaries are among the extensive collections of malware samples available in VirusShare and VirusTotal, which are essential for both static and dynamic malware analysis. Although it is only partially accessible and requires special access, VirusShare is an extensive database of malware hashes and binaries. In contrast, VirusTotal provides online scanning services that aggregate antivirus findings from several engines, making behavioral analysis and static signature easier [22].

5.2 Datasets specific to ransomware: Below are some datasets specific to ransomware characteristics:

i. EldeRan: A dataset specifically curated for ransomware behavioral logs, featuring about 582 ransomware samples with detailed dynamic analysis reports. For training and testing behavior-based detection models that emphasize runtime features over static signatures, this publicly accessible dataset is useful [23].

ii. RanSAP: An open dataset that offers low-level storage access patterns of 7 prominent ransomware samples, 5 benign programs, and 21 ransomware variants. It captures data on read/write operations and entropy metrics using the BitVisor hypervisor. For creating machine learning-based ransomware detection systems that concentrate on storage behavior, RanSAP is useful [24].

Table II: Ransomware Detection Datasets

Dataset	Type	Labels	Public Access	Size
CICIDS2017	Network Traffic	Labeled	Yes	3 million flows
VirusShare	Static Files	Partially	Restricted	1 million samples
EldeRan	Behavior Logs	Yes	Yes	582 ransomware samples
RanSAP	Storage Access Logs	Yes	Yes	1,495 CSV files

Ransomware detection and mitigation rely heavily on high-quality datasets to train and evaluate intelligent models. The table presents four commonly used datasets—CICIDS2017, VirusShare, EldeRan, and RanSAP—which differ in type, label availability, accessibility, and size.

5.3 Evaluation Metrics: Choosing the right assessment metrics is essential for gauging the efficacy and usefulness of ransomware detection models. Below are explanations of some evaluation metrics:

i. Accuracy: Indicates the percentage of cases (both benign and ransomware) that are accurately classified. Despite being commonly utilized, accuracy by itself could be deceptive in datasets that are unbalanced.

ii. F1-score, Precision, and Recall: Precision indicates detection quality with few false alarms by calculating the ratio of true positives to all positive predictions. The number of real ransomware samples that were accurately recognized is known as recall (or sensitivity). According to [25], the F1-score is a balanced metric that is calculated as the harmonic mean of precision and recall.

iii. Detection Latency: The time between ransomware initiation and detection is critical, especially in real-time environments where delays can result in data encryption and loss [26].

iv. False Positive Rate (FPR) and False Negative Rate (FNR): FPR is the percentage of benign samples that are wrongly classified as ransomware, which is crucial in averting disruption to legitimate processes; FNR indicates missed ransomware detections, which affect system security [27].

v. Resource Overhead: Practical deployment requires consideration of computational resource consumption, including CPU, memory usage, and power efficiency, which is especially important for corporate networks with restricted resources [12].

6. CHALLENGES AND RESEARCH GAPS

Even with the promising advances in intelligent ransomware mitigation, there are still several significant obstacles and unfulfilled research gaps that restrict the application and efficacy of these strategies in actual business settings. Below are techniques that describe some challenges and research gaps.

6.1 Label Scarcity and Data Imbalance: The disparity between benign samples and labeled ransomware in the available datasets is one of the main issues. Due to the large diversity of benign data compared to the relatively scarce number of ransomware instances, machine learning models tend to favor the majority class, which lowers ransomware detection rates [28]. This has been addressed by investigating data augmentation methods like Generative Adversarial Networks (GANs) to create ransomware samples synthetically, increasing model robustness and decreasing overfitting [29].

6.2 Model Generalization: Intelligent models often suffer from poor generalization when utilized across different corporate network environments. This is mainly due to overfitting on certain datasets with little variety, resulting in reduced detection accuracy when faced with new ransomware variants or network configurations [30]. In order to improve model portability and robustness, this limitation necessitates the creation of transfer learning frameworks and domain adaptation strategies.

6.3 Real Time Constraints: Because ransomware attacks change so quickly, detection systems that can make inferences in real time with low latency are required. Nevertheless, despite their strength, deep learning models frequently have high computational costs that prevent their use in settings with limited resources, like edge devices or extensive corporate networks [12]. One of the main areas of research is still balancing accuracy with lightweight, efficient structures.

6.4 Adversarial Robustness: Recent research has shown that many ransomware detection methods are vulnerable to adversarial attacks, where attackers carefully change input features to evade detection without generating alarms [31]. This vulnerability reduces the trustworthiness of intelligent systems, driving the need for adversarial training and robust defense mechanisms to harden models against such evasion strategies.

6.5 Explainability: Many deep learning models' black-box nature makes it difficult for them to be adopted in high-assurance corporate networks where interpretability and transparency are essential. Building trust among cybersecurity professionals and adhering to regulatory requirements requires Explainable AI (XAI) techniques that offer insights into model decisions [32]. The ongoing issue is to create interpretable models without compromising detection performance.

7. FUTURE RESEARCH DIRECTIONS

Several potential research directions have been developed to solve the present constraints and difficulties in ransomware mitigation using intelligent strategies. Enhancing detection accuracy, scalability, interpretability, and real-time responsiveness in corporate settings is the goal of these future developments.

7.1 Federated Learning: Federated learning protects privacy and compliance with data protection laws by allowing several organizations to work together to build ransomware detection models without exchanging raw data [33]. For corporate networks where it is difficult to concentrate critical data, this decentralized method is especially suitable. Future research should concentrate on creating effective, safe federated learning frameworks that can manage dynamic ransomware threats and diverse network environments.

7.2 Adversarial Robust Models: To strengthen ransomware detectors, it is necessary to create strong training techniques that use adversarial instances because existing models are susceptible to adversarial attacks [34]. Model resilience against evasion approaches can be increased by integrating techniques like certified robustness, defensive distillation, and adversarial training into ransomware detection scenarios.

7.3 Lightweight Edge AI: Lightweight AI models that can operate on devices with limited resources are becoming more and more necessary as IoT and endpoint devices proliferate across corporate networks [35]. To enable on-device ransomware detection with low latency and little overhead, subsequent studies should investigate model compression, pruning, and effective architectures like TinyML.

7.4 Synthetic Dataset Generation: Training efficient models is still hampered by the lack of labeled ransomware data. To improve generalization and decrease overfitting, training datasets can be supplemented with a variety of ransomware samples using Generative Adversarial Networks (GANs) and other synthetic data creation approaches [29]. The creation of high-fidelity synthetic data that accurately replicates ransomware activities should be the main goal of future research.

7.5 Explainable AI (XAI): Explainable models that offer transparent decision-making are essential for boosting confidence and adoption of AI-based ransomware countermeasures [32]. To enable cybersecurity analysts to comprehend model alarms and make well-informed mitigation decisions, future research should look into interpretable architectures and post-hoc explanation techniques.

7.6 Integration with SDN/NFV: Software Defined Networking (SDN) and Network Function Virtualization (NFV) promote flexible and programmable network infrastructures that can dynamically react to ransomware attacks [36]. Integrating intelligent ransomware detection with SDN/NFV offers real-time traffic rerouting, network segmentation, and deployment of virtualized security functions for scalable, adaptive defense mechanisms.

8. CONCLUSION

Constant innovation is required to keep up with the arms race between ransomware creators and defenders. A promising way forward is provided by intelligent approaches, which allow for automatic and adaptive threat mitigation. The present landscape has been broken down and categorized in this research, along with important contributions and future directions that could result in more reliable and scalable solutions. For researchers and practitioners dedicated to improving the state of ransomware defense, we hope this work offers a strong foundation.

REFERENCES

[1] Symantec, “Internet security threat report,” Symantec Corporation, 2017. Available: https://www.symantec.com/security-center/threat-report

[2] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, “Cutting the gordian knot: A look under the hood of ransomware attacks,” in *Int. Conf. Detection Intrusions Malware Vulnerability Assessment*, 2015, pp. 3–24. Available: https://doi.org/10.1007/978-3-319-23035-5_1

[3] N. Andronio, S. Zanero, and F. Maggi, “HelDroid: Dissecting and detecting mobile ransomware,” in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, 2015, pp. 49–58. Available: https://doi.org/10.1145/2818000.2818005

[4] S. Mohurle and M. Patil, “A brief study of Wannacry ransomware attack,” *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 5, pp. 1938–1940, 2017. Available: https://doi.org/10.26483/ijarcs.v8i5.4036

[5] Europol, “Internet Organized Crime Threat Assessment (IOCTA) 2021,” European Union Agency for Law Enforcement Cooperation, 2021. Available: https://www.europol.europa.eu/iocta-report

[6] Trend Micro, “RDP attacks and ransomware: What you need to know,” *Trend Micro Research*, 2021. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/rdp-attacks-and-ransomware

[7] L. Abrams, “Maze Ransomware publicly shaming victims who don’t pay,” *BleepingComputer*, 2019. Available: https://www.bleepingcomputer.com/news/security/maze-ransomware-publicly-shaming-victims-who-dont-pay/

[8] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, “Cryptolock (and drop it): Stopping ransomware attacks on user data,” in *Proc. 36th IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2016, pp. 303–312. Available: https://doi.org/10.1109/ICDCS.2016.46

[9] D. Aslan, O. Kaya, and T. Acarman, “Detection of ransomware attacks using machine learning algorithms,” *J. Inf. Secur. Appl.*, vol. 52, p. 102486, 2020. Available: https://doi.org/10.1016/j.jisa.2020.102486

[10] S. Chakraborty, A. Jaiswal, and D. Mukherjee, “A deep learning approach to ransomware detection and analysis,” *Int. J. Comput. Appl.*, vol. 179, no. 43, pp. 22–28, 2018. Available: https://doi.org/10.5120/ijca2018917391

[11] Y. Hou, W. He, and Y. Luo, “An LSTM-based anomaly detection method for ransomware in enterprise networks,” *IEEE Access*, vol. 8, pp. 217599–217609, 2020. Available: https://doi.org/10.1109/ACCESS.2020.3040978

[12] T. Tang, Y. Tang, and Z. Liu, “Autoencoder-based ransomware detection with dynamic analysis,” *Secur. Commun. Netw.*, vol. 2019, Article ID 2017924, 2019. Available: https://doi.org/10.1155/2019/2017924

[13] L. A. Zadeh, “Fuzzy sets,” *Inf. Control*, vol. 8, no. 3, pp. 338–353, 1965. Available: https://doi.org/10.1016/S0019-9958(65)90241-X

[14] P. Idliman, W. Balfour, B. Featheringham, and H. Chesterfield, "Entropy-synchronized neural hashing for unsupervised ransomware detection," *arXiv preprint*, arXiv:2501.18131, 2025. Available: https://arxiv.org/abs/2501.18131

[15] C. J. W. Chew, V. Kumar, P. Patros, and R. Malik, "Real-time system call-based ransomware detection," *Int. J. Inf. Secur.*, vol. 23, pp. 1839–1858, 2024. Available: https://doi.org/10.1007/s10207-024-00819-x

[16] M. Hirano and R. Kobayashi, "Machine learning-based ransomware detection using low-level memory access patterns obtained from live-forensic hypervisor," *arXiv preprint*, arXiv:2205.13765, 2022. Available: https://arxiv.org/abs/2205.13765

[17] S. Zhang, C. Hu, L. Wang, M. J. Mihaljevic, S. Xu, and T. Lan, "A malware detection approach based on deep learning and memory forensics," *Symmetry*, vol. 15, no. 3, p. 758, 2023. Available: https://doi.org/10.3390/sym15030758

[18] D. Ayanara, A. Hillingworth, J. Casselbury, and D. Montague, "Spectral Entanglement Fingerprinting: A novel framework for ransomware detection using cross-frequency anomalous waveform signatures," *arXiv preprint*, arXiv:2502.01275, 2025. Available: https://arxiv.org/abs/2502.01275

[19] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, "Automated dynamic analysis of ransomware: Benefits, limitations and use for detection," in *2016 IEEE Secur. Privacy Workshops (SPW)*, 2016, pp. 320–326. Available: https://doi.org/10.1109/SPW.2016.43

[20] R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Evaluating XGBoost for ransomware detection," *J. Cyber Secur. Technol.*, vol. 4, no. 2, pp. 110–125, 2020. Available: https://doi.org/10.1080/23742917.2020.1758593

[21] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy (ICISSP)*, 2018, pp. 108–116. Available: https://doi.org/10.5220/0006638701080116

[22] Google VirusTotal, "VirusTotal: Free online virus, malware and URL scanner," 2021. Available: https://www.virustotal.com/

[23] A. Mohaisen, M. Mohaisen, and O. Alrawi, "EldeRan: A dynamic analysis approach for detecting ransomware,"*Comput. Secur.*, vol. 68, pp. 23–37, 2017. Available: https://doi.org/10.1016/j.cose.2017.04.003

[24] M. Hirano, T. Tsutsui, and Y. Yoshida, "RanSAP: A ransomware storage access pattern dataset for machine learning-based ransomware detection," *Data Brief*, vol. 39, p. 107558, 2022. Available: https://doi.org/10.1016/j.dib.2021.107558

[25] M. Sokolova and G. Lapalme, "A systematic analysis of performance measures for classification tasks," *Inf. Process. Manag.*, vol. 45, no. 4, pp. 427–437, 2009. Available: https://doi.org/10.1016/j.ipm.2009.03.002

[26] W. U. Hassan, M. H. Rehman, K. Kim, and D. Kim, "Ransomware detection and mitigation techniques: A review," *J. Netw. Comput. Appl.*, vol. 149, p. 102122, 2019. Available: https://doi.org/10.1016/j.jnca.2019.102122

[27] R. Zuech, T. M. Khoshgoftaar, and R. Wald, "Intrusion detection and Big Heterogeneous Data: a survey," *J. Big Data*, vol. 2, no. 1, pp. 1–41, 2015. Available: https://doi.org/10.1186/s40537-014-0004-1

[28] M. Buda, A. Maki, and M. A. Mazurowski, "A systematic study of the class imbalance problem in convolutional neural networks," *Neural Netw.*, vol. 106, pp. 249–259, 2018. Available: https://doi.org/10.1016/j.neunet.2018.07.011

[29] Z. Wang, Q. Zhang, Y. Zhang, J. Liu, and Y. Wang, "Data augmentation for ransomware detection using generative adversarial networks," *J. Inf. Secur. Appl.*, vol. 55, p. 102620, 2020. Available: https://doi.org/10.1016/j.jisa.2020.102620

[30] H. Kim, S. Kang, S. Park, and H. Lee, "Cross-environment ransomware detection using domain adaptation," *IEEE Access*, vol. 8, pp. 194498–194510, 2020. Available: https://doi.org/10.1109/ACCESS.2020.3036982

[31] A. Demontis et al., "On adversarial attacks and defences for machine learning in malware detection," *arXiv preprint*, arXiv:1712.03141, 2019. Available: https://arxiv.org/abs/1712.03141

[32] R. Guidotti et al., “A survey of methods for explaining black box models,” *ACM Comput. Surv.*, vol. 51, no. 5, pp. 1–42, 2018. Available: https://doi.org/10.1145/3236009

[33] Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated machine learning: Concept and applications,” *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019. Available: https://doi.org/10.1145/3298981

[34] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, “Towards deep learning models resistant to adversarial attacks,” *Int. Conf. Learn. Represent.*, 2018. Available: https://arxiv.org/abs/1706.06083

[35] N. D. Lane et al., “DeepX: A software accelerator for low-power deep learning inference on mobile devices,” in *Proc. 15th Annu. Int. Conf. Mobile Syst. Appl. Serv.*, 2018, pp. 199–212. Available: https://doi.org/10.1145/3210240.3210323

[36] D. Kreutz et al., “Software-defined networking: A comprehensive survey,” *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, 2015. Available: https://doi.org/10.1109/JPROC.2014.2371999.