Journal of
Cyber Security

Tech Science Press

https://doi.org/10.32604/jcs.2026.082741

REVIEW

A Comprehensive and Critical Analysis of Ransomware Detection, Prevention, Mitigation, and Recovery Approaches

Dakshnamoorthy Manivannan*

Department of Computer Science, University of Kentucky, Lexington, KY, USA

*Corresponding Author: Dakshnamoorthy Manivannan. Email: manivann@cs.uky.edu

Received: 21 March 2026; Accepted: 21 May 2026; Published: 06 July 2026

ABSTRACT: Ransomware has emerged as one of the most disruptive and financially damaging forms of cybercrime, affecting individuals, enterprises, and critical infrastructures worldwide. Over the past decade, ransomware attacks have evolved from simple file-encryption malware to sophisticated, multi-stage campaigns involving data exfiltration, double extortion, and ransomware-as-a-service (RaaS) ecosystems. In response, a large body of research has proposed diverse techniques for detecting, preventing, mitigating, and recovering from ransomware attacks. This paper presents a comprehensive survey of ransomware research spanning behavioral and runtime detection, machine learning and deep learning-based approaches, network and SDN-based detection, platform-specific defenses for mobile and IoT environments, storage- and hardware-assisted protection mechanisms, deception-based defenses, and backup and recovery strategies. In addition, the survey examines adversarial evasion techniques, blockchain-based analysis of ransomware payments, economic and policy perspectives, and the real-world operational impacts of ransomware attacks, particularly in critical sectors such as healthcare. Based on a synthesis of the literature, we identify key open challenges related to adversarial robustness, dataset availability, evolving threat models, and the need for integrated cross-layer defense architectures. Finally, we outline promising research directions for developing scalable, resilient, and trustworthy ransomware defense mechanisms capable of addressing the rapidly evolving ransomware threat landscape.

KEYWORDS: Ransomware detection; ransomware prevention; ransomware mitigation; computer security; network security; machine learning; deep learning; explainable AI; cybersecurity

1 Introduction

Ransomware has evolved into one of the most pervasive and damaging cyber threats facing modern digital infrastructure. First observed in the late 1980s, ransomware attacks have transitioned from rudimentary denial-of-access mechanisms to highly organized, financially motivated operations capable of crippling enterprises, public institutions, and critical services. At its core, ransomware is a form of cyber extortion in which adversaries encrypt, lock, ex-filtrate, or destroy victims' data and demand payment, typically in cryptocurrency, in exchange for restoration or non-disclosure. While early ransomware primarily relied on simple file encryption, contemporary attacks increasingly combine cryptographic denial, data theft, operational disruption, and psychological coercion, significantly amplifying their impact.

Cryptographic ransomware remains the dominant variant, exploiting strong encryption primitives to render data inaccessible. Ironically, encryption, long regarded as a cornerstone of data confidentiality and privacy, has been repurposed by attackers as a weapon to deny access rather than protect it. Despite decades of technical progress in cybersecurity, the fundamental characteristics of ransomware attacks have remained

remarkably consistent: unauthorized encryption, coercive communication, and monetization through anonymous or pseudonymous payment channels. These defining traits distinguish ransomware from other malware classes and make them a critical focal point for detection, prevention, and mitigation research.

In recent years, ransomware operations have matured into sophisticated ecosystems. The emergence of double and triple extortion schemes, where attackers ex-filtrate sensitive data prior to encryption and threaten public disclosure or secondary attacks, has fundamentally altered the risk landscape. Victims are often forced to make decisions under severe information asymmetry, uncertain recovery guarantees, and ambiguous attacker signaling. The widespread adoption of Ransomware-as-a-Service (RaaS) has further lowered the barrier to entry, enabling loosely affiliated actors to share infrastructure, tooling, and revenue. As a result, ransomware is no longer a stand-alone executable artifact but a coordinated socio-technical phenomenon shaped by economics, geopolitics, human negotiation, and cyber-criminal governance.

The increasing frequency, scale, and severity of ransomware incidents have led to substantial financial losses and societal harm. High-profile attacks on healthcare systems, energy infrastructure, supply chains, and public services have demonstrated that ransomware can directly threaten human safety, national security, and economic stability. The accelerated shift toward remote work, cloud services, and interconnected cyber-physical systems has expanded the attack surface across information technology (IT), operational technology (OT), industrial control systems (ICS), and software supply chains. Healthcare and Internet of Things (IoT)-enabled environments are particularly vulnerable due to their reliance on resource-constrained devices, real-time data availability, and strict availability requirements.

From a defensive perspective, ransomware detection and prevention have proven challenging. Traditional signature-based antivirus systems are effective against known samples but fail to generalize to rapidly evolving variants. In response, research has increasingly shifted toward behavior-based and dynamic analysis techniques that monitor file system activity, system calls, memory usage, API invocations, and runtime execution patterns. While such approaches improve resilience to polymorphism and obfuscation, they introduce new limitations, including execution overhead, dependence on controlled environments, susceptibility to evasion, and difficulties in reproducible evaluation. Advanced ransomware can fingerprint virtualized or sandboxed environments, delay payload execution, selectively encrypt files, or deactivate itself when command-and-control (C&C) infrastructure is disrupted, thereby undermining dynamic detection pipelines. Machine learning and deep learning methods now play a central role in ransomware detection and classification. These techniques leverage static, dynamic, and hybrid features to identify malicious behavior and, increasingly, classify ransomware into families for threat intelligence and response prioritization. However, many proposed models rely on narrow datasets, binary classification assumptions, or opaque decision processes that limit interpretability and operational trust. The lack of explainability, standardized benchmarks, and realistic deployment-level evaluations hinders both comparative analysis and real-world adoption. Moreover, adversarial adaptation, where attackers actively probe and evade learned detection features, remains insufficiently addressed in much of the existing literature. At the same time, emerging computational paradigms such as quantum computing are expected to further reshape the cybersecurity landscape. Although current ransomware primarily relies on classical cryptographic primitives for file encryption and key exchange, future advances in quantum algorithms, particularly Shor's algorithm, may threaten widely used public-key cryptosystems. Consequently, there is growing interest in post-quantum cryptography (PQC) and quantum-resistant security mechanisms that can preserve long-term confidentiality and resilience. In the ransomware context, this creates a dual implication: quantum-capable adversaries could eventually exploit weaknesses in existing cryptographic infrastructures, while defenders may adopt PQC-based secure storage, backup protection, and key-management frameworks to strengthen resilience against future threats. Although quantum-enabled ransomware remains largely theoretical, incorporating

forward-looking cryptographic defenses and post-quantum security models into ransomware mitigation strategies is becoming increasingly important.

Beyond endpoint detection, ransomware mitigation and recovery introduce additional challenges. OS-level defenses can be compromised by privileged adversaries, while storage-level solutions lack semantic visibility into file system structures and application behavior. Blockchain-based ransom payment analysis has improved visibility into cryptocurrency flows, yet most studies focus on individual addresses and overlook macro-level transaction patterns and victim response behaviors. The scarcity of labeled ransomware data, especially in payment networks and large-scale enterprise environments, further complicates impact assessment and defense validation.

Despite extensive academic and industrial attention, current ransomware research exhibits notable gaps. Many studies rely on outdated assumptions, limited samples, or isolated technical perspectives, often neglecting governance frameworks, incident response practices, cyber insurance dynamics, and coordinated law-enforcement actions. At the same time, ransomware continues to evolve under the influence of geopolitical tensions, state-aligned threat actors, and international counter-ransomware initiatives. These dynamics underscore the need to study ransomware holistically—as an ecosystem encompassing technical mechanisms, organizational structures, economic incentives, and human decision-making.

The goal of this survey is to provide a comprehensive and critical synthesis of ransomware detection, prevention, mitigation, and recovery techniques proposed over the past decade, with particular emphasis on developments from the last three years, during which research activity has accelerated significantly. We systematically classify existing approaches across multiple dimensions, analyze their assumptions and limitations, and identify persistent open challenges that hinder practical deployment. By integrating insights from peer-reviewed literature, government advisories, and industry reports, this survey aims to bridge the gap between academic innovation and operational resilience. In doing so, it provides a structured foundation for future research and a reference framework for practitioners seeking robust, explainable, adaptive, and future-ready defenses against ransomware.

Cross-cutting Research Challenges: Based on the surveyed literature, we identify the following key challenges:

- **C1: Dataset Realism and Benchmarking**—Lack of realistic, diverse, and continuously updated datasets.
- **C2: Adversarial Robustness**—Vulnerability to evasion, poisoning, and adaptive attacks.
- **C3: Generalization and Concept Drift**—Poor cross-dataset generalization and lack of long-term robustness.
- **C4: Explainability and Trustworthiness**—Limited interpretability and lack of trustworthy explanations for ML/DL-based systems.
- **C5: Computational Efficiency and Scalability**—High overhead and limited scalability in real-world systems.
- **C6: Deployment and Integration Constraints**—Challenges in integrating solutions into operational environments.
- **C7: Cross-Layer Coordination**—Lack of unified frameworks across host, network, storage, and cloud layers.
- **C8: Recovery and Resilience**—Weak integration of recovery, backup, and response mechanisms.
- **C9: Economic and Policy Factors**—Misaligned incentives and limited integration of economic and regulatory perspectives.
- **C10: Emerging and Evolving Threat Models**—Rapid evolution of ransomware tactics and attack surfaces.

Table 1 summarizes the above key cross-cutting challenges identified in this survey and outlines corresponding research directions. Unlike subsection-specific limitations given in each subsection, these challenges capture fundamental gaps that span multiple ransomware defense paradigms and system layers. The mapping highlights that future research must move beyond isolated solutions toward adaptive, cross-layer, and deployment-aware frameworks that address adversarial robustness, dataset realism, and evolving threat models in a unified manner.

Table 1: Cross-cutting challenges and research directions in ransomware defense.

ID	Challenge Theme	Key Limitations	Research Directions	Applicable Domains
C1	Dataset Realism and Benchmarking	Existing datasets are outdated, small-scale, and fail to capture modern ransomware behaviors (e.g., exfiltration, multi-stage attacks); lack of standardized evaluation protocols.	Develop large-scale, continuously updated, and multi-platform datasets; establish standardized benchmarking frameworks; incorporate real-world workloads and longitudinal data.	ML/DL-based detection, IoT, CPS
C2	Adversarial Robustness	Detection systems are vulnerable to evasion, poisoning, and mimicry attacks; lack of adversarial evaluation benchmarks.	Design adversarially robust models; develop invariant behavioral features; introduce standardized adversarial testing frameworks; integrate adversarial training.	ML/DL-based detection, behavioral detection
C3	Generalization and Concept Drift	Models trained on static datasets fail under evolving ransomware behaviors and cross-environment deployment.	Develop adaptive and online learning methods; incorporate domain adaptation and continual learning; perform cross-dataset validation.	ML/DL-based detection, semi-supervised systems
C4	Explainability and Trustworthiness	Limited interpretability of ML/DL-based models; lack of explanation fidelity and user trust in decisions.	Develop robust and domain-specific XAI techniques; evaluate explanation fidelity and stability; integrate human-in-the-loop validation.	XAI-enabled ML-based systems, SOC environments

(Continued)

Table 1 (continued)

ID	Challenge Theme	Key Limitations	Research Directions	Applicable Domains
C5	Computational Efficiency and Scalability	High computational and memory overhead limits deployment in real-time, cloud, and resource-constrained environments.	Design lightweight detection models; optimize inference pipelines; leverage edge/fog computing; develop energy-efficient architectures.	IoT, IIoT, CPS, cloud systems
C6	Deployment and Integration Constraints	Many solutions require OS, firmware, or infrastructure modifications; limited integration with real-world systems.	Develop deployable and modular architectures; ensure compatibility with existing systems; integrate with SIEM/SOC pipelines; minimize operational overhead.	Enterprise, cloud, mobile systems
C7	Cross-Layer Coordination	Lack of integration across host, network, storage, and cloud layers; fragmented visibility.	Design unified cross-layer detection frameworks; enable data fusion across telemetry sources; standardize interfaces and protocols.	Enterprise, cloud, CPS
C8	Recovery and Resilience	Recovery mechanisms assume intact backups; limited integration with detection; weak handling of exfiltration-based ransomware.	Develop tamper-resistant backup systems; design adaptive and partial recovery techniques; integrate detection with recovery workflows.	Storage systems, enterprise IT
C9	Economic and Policy Factors	Misaligned incentives (e.g., ransom payments, cyber insurance); limited integration of policy and economic perspectives.	Develop game-theoretic models; align technical defenses with policy interventions; improve regulation and cross-border enforcement.	Governance, cybersecurity policy

(Continued)

Table 1 (continued)

ID	Challenge Theme	Key Limitations	Research Directions	Applicable Domains
C10	Emerging and Evolving Threat Models	Rapid evolution of ransomware (fileless, exfiltration-based, cross-layer attacks); defenses lag behind attacker innovation.	Design adaptive and predictive defense systems; incorporate threat intelligence; develop frameworks for emerging attack surfaces (cloud, browser, hardware).	All domains

Organization of the Paper

The remainder of this paper is organized as follows. Section 2 reviews recent survey articles on ransomware detection, prevention, and mitigation, and critically analyzes their scope and limitations to motivate the need for the present survey. In addition, this section also summarizes the major contributions of this survey. Section 3 describes the selection methodology for selecting papers to review, including inclusion and exclusion criteria, and illustrates the review process using a PRISMA-style flow diagram (Fig. 1). It also discusses some background for the paper. Section 4 presents a comprehensive classification, characterization, and synthesis of ransomware-related research published since 2016. The surveyed studies are organized into well-defined categories based on detection techniques, prevention techniques, system models, and threat assumptions, with the overall taxonomy summarized. For each category, we provide a critical comparative analysis, discuss representative approaches, and identify open research challenges. Section 5 provides references to additional relevant studies, including peer-reviewed conference papers, technical reports, and unrefereed preprints, that fall outside the primary scope of this survey and are therefore not discussed in detail.

Section 6 consolidates and discusses cross-cutting open issues and grand challenges that span multiple categories, including robustness to adversarial adaptation, key limitations, deployment feasibility, as well as mapping of attack capabilities to vulnerable defenses and countermeasures and suitability of evaluation metrics for various approaches. Finally, Section 7 concludes the paper by summarizing the key findings of the survey, highlighting overarching insights derived from the comparative analysis, and outlining promising directions for future research in ransomware detection, prevention, mitigation, and recovery.

2 Existing Recent Survey Papers

This section analyzes existing ransomware-related surveys, published after 2020, motivates the need for this survey, summarizes the major contributions of this survey.

Fernando et al. [1] review ML/DL-based ransomware detection and analyze the impact of malware evolution, with emphasis on emerging IoT threats. However, their focus remains largely detection-centric and does not extend to broader system-level or socio-technical considerations. Wang et al. [2] analyze ransomware-related Bitcoin transactions to uncover payment flows and attacker strategies. While providing valuable economic insights, their work is limited to the financial dimension and does not integrate detection, prevention, or operational defenses.

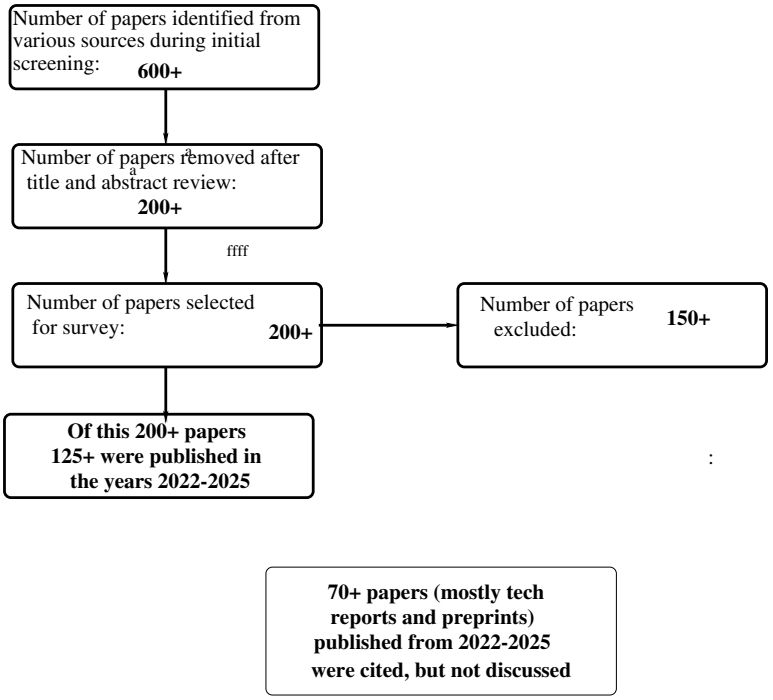

Figure 1: PRISMA-style diagram representing the inclusion/exclusion criteria for selecting the papers.

Moussaileb et al. [3] propose a lifecycle-based taxonomy mapping defenses to attack stages, whereas McIntosh et al. [4] focus on evaluation frameworks and methodological rigor. Both contribute structured analysis, but remain limited in scope and lack cross-layer integration and recent coverage. Alqahtani and Sheldon [5] and Smith et al. [6] primarily survey crypto-ransomware detection techniques, emphasizing modeling approaches and accuracy challenges. Their focus is narrowly detection-oriented, with limited discussion of deployment, recovery, or adversarial robustness.

Aldauiji et al. [7] examine ransomware from a cyber-threat-intelligence perspective, while Oz et al. [8] provide a cross-platform overview across PCs, mobile, and IoT systems. Although broader in scope, these works lack a unified analytical framework and do not fully capture recent developments in ransomware tactics and defenses. More recent surveys such as Ispahany et al. [9] and Alzahrani et al. [10] continue to emphasize ML-based detection and dataset analysis, with improved coverage of recent works. However, they remain largely detection-focused and do not provide deep comparative analysis or cross-layer synthesis.

Overall, existing surveys are fragmented across detection, economics, or platform-specific perspectives, with limited integration across technical, operational, and policy dimensions. Most also emphasize pre-2022 work and do not fully reflect the rapid evolution of modern ransomware, including exfiltration-driven attacks and RaaS ecosystems.

In contrast, this survey provides a comprehensive and critical cross-layer synthesis, integrating detection, prevention, mitigation, recovery, and economic perspectives. It emphasizes comparative analysis, adversarial robustness, and real-world deployment challenges, offering a unified and up-to-date framework for understanding modern ransomware defense. Table 2 highlights these distinctions.

Table 2: Comparison of existing ransomware surveys with the present survey.

Survey	Year	Focus	Key Contributions	Limitations	Difference from This Survey
Fernando et al. [1]	2020	ML/DL detection	Reviews ML/DL-based ransomware detection; analyzes malware evolution; discusses IoT trends.	Detection-centric; limited coverage of mitigation, recovery, and recent advances.	Our survey provides a holistic, up-to-date synthesis beyond detection, including defense, recovery, and ecosystem-level analysis.
Wang et al. [2]	2021	Bitcoin analysis	Analyzes ransomware payments and fund flows (2012–2021) using clustering and classification.	Focus limited to economic/payment analysis; lacks technical defense coverage.	We integrate economic insights within a broader technical and operational ransomware framework.
Moussaileb et al. [3]	2021	Lifecycle defenses	Maps countermeasures to ransomware lifecycle stages; identifies research gaps.	Limited focus on ML/DL, adversarial aspects, and emerging threat models.	Our survey extends lifecycle analysis with unified taxonomies, adversarial insights, and broader coverage.
McIntosh et al. [4]	2021	Mitigation evaluation	Proposes evaluation framework; compares mitigation techniques across studies.	Focused on evaluation; narrower technical scope.	We complement evaluation insights with a comprehensive cross-layer taxonomy and analysis.
Alqahtani and Sheldon [5]	2022	Crypto-ransomware detection	Surveys detection methods; highlights accuracy and robustness issues.	Detection-focused; limited coverage of other defense aspects.	Our survey includes detection but also prevention, mitigation, recovery, and emerging threats.
Smith et al. [6]	2022	Detection techniques	Reviews detection approaches and open issues in modeling.	Primarily detection-centric; lacks system-level and economic perspectives.	We provide a full-spectrum analysis across technical and organizational dimensions.
Aldauiji et al. [7]	2022	CTI-based detection	Explores CTI models and datasets for ransomware detection.	Specialized focus; limited system-level and recovery analysis.	Our survey incorporates CTI within a broader, integrated ransomware defense framework.
Oz et al. [8]	2022	Cross-platform survey	Analyzes ransomware across PCs, mobile, and IoT/CPS; discusses evolution and defenses.	Covers work mostly up to 2020; limited focus on recent advances and adversarial issues.	Our survey is more recent and expands analysis to adversarial, economic, and recovery aspects.
Ispahany et al. [9]	2024	ML detection architectures	Summarizes ML-based detection designs and limitations.	Restricted to ML-based detection.	We extend beyond ML to include cross-layer defenses and broader ecosystem analysis.

(Continued)

Table 2 (continued)

Survey	Year	Focus	Key Contributions	Limitations	Difference from This Survey
Alzahrani et al. [10]	2025	Platform-specific detection	Reviews Windows/Android detection methods and datasets.	Platform-specific and detection-focused.	Our survey provides cross-platform, cross-layer coverage including mitigation and recovery.
This survey	**2026**	**Comprehensive ransomware research landscape**	**Provides a holistic and critical synthesis of ransomware detection, prevention, mitigation, recovery, and response; proposes unified taxonomies for detection and defense mechanisms; analyzes adversarial evasion, emerging threat models, blockchain/payment tracing, economic and policy perspectives, and operational impacts on critical sectors; emphasizes advances from the last decade, especially the post-2022 surge in research.**	—	**Distinguished by its breadth, recency, cross-layer perspective, and integration of technical, economic, organizational, and policy dimensions into a single survey framework.**

Contributions of This Survey

The principal contributions of this survey are as follows:

- **Comprehensive and up-to-date literature coverage.** Provides a broad survey of ransomware research published during the past decade, with particular emphasis on recent advances in detection, prevention, mitigation, recovery, and response across enterprise, cloud, IoT, IIoT, CPS, and healthcare environments.
- **Multi-dimensional taxonomy contribution.** Introduces a unified taxonomy that categorizes ransomware research across multiple dimensions simultaneously, including detection paradigm, deployment environment, defense layer, analytical technique, operational objective, and adversarial resilience. Unlike many prior surveys that rely on a single classification perspective, the proposed taxonomy enables more structured cross-domain comparison and synthesis.
- **Cross-layer ransomware defense framework.** Presents a systematic classification framework for ransomware defenses spanning host-level, network-level, storage-level, hardware-assisted, deception-based, blockchain-assisted, and recovery-oriented mechanisms, thereby providing a holistic view of how different defense layers interact and complement each other.
- **Comparative analytical synthesis of detection approaches.** Provides a critical comparison of behavioral, ML/DL-based, network-based, storage-level, and hybrid ransomware detection techniques with respect to detection capability, explainability, deployment feasibility, adversarial robustness, scalability, false positives, and time-to-detection trade-offs.

- **Analysis of emerging ransomware threat models.** Examines the evolution of modern ransomware ecosystems, including double/triple extortion, Ransomware-as-a-Service (RaaS), fileless ransomware, selective and intermittent encryption, exfiltration-based attacks, and cross-platform ransomware targeting cloud, IoT, and virtualized environments.
- **Integrated economic, operational, and policy perspective.** Synthesizes technical and non-technical aspects of ransomware, including attacker incentives, cryptocurrency-enabled monetization, ransom negotiation dynamics, cyber insurance implications, and regulatory and law-enforcement responses.
- **Critical assessment of blockchain-based payment analysis.** Reviews blockchain analytics approaches used for ransomware payment tracking, attribution, and cryptocurrency flow analysis, while also highlighting limitations related to scalability, privacy-preserving transactions, and incomplete attribution.
- **Identification of recurring limitations and research gaps.** Synthesizes common weaknesses observed across the literature, including dataset bias, lack of standardized benchmarks, insufficient adversarial evaluation, limited explainability, scalability issues, and gaps between research prototypes and real-world deployment.
- **Future research directions and next-generation defense insights.** Highlights promising future directions, including adaptive and cross-layer ransomware defenses, explainable and adversarially robust detection, standardized evaluation methodologies, post-quantum security considerations, and resilient recovery-oriented architectures.

This survey distinguishes itself through a *critical, comparative, and cross-layer synthesis* of ransomware research, highlighting limitations, assumptions, and deployment challenges, and providing a unified, forward-looking framework for ransomware defense.

3 Methodology Used for Selecting Papers and Background

3.1 Methodology Used for Selecting Papers

To ensure rigor, transparency, and reproducibility, we adopted a systematic survey methodology inspired by PRISMA guidelines. Major digital libraries, including IEEE Xplore, ACM Digital Library, Springer, Elsevier, and arXiv, were searched using combinations of keywords such as *"ransomware detection", "ransomware defense", "ransomware recovery", "machine learning", "cyber extortion", and "ransomware mitigation"*. The search focused on publications from 2016 to 2025, with particular emphasis on studies published after 2022 to capture the rapid evolution of ransomware research in recent years.

Inclusion criteria: (i) peer-reviewed articles or widely cited preprints, (ii) clear relevance to ransomware detection, prevention, mitigation, or recovery, (iii) substantive technical, empirical, or analytical contribution.

Exclusion criteria: (i) non-technical reports or opinion articles, (ii) duplicate or highly incremental studies, (iii) papers lacking sufficient methodological or experimental detail, (iv) works outside the scope of ransomware defense.

The initial search yielded approximately 600 papers. During the first screening stage, titles and abstracts were reviewed, resulting in the removal of more than 200 papers that were either outside the scope of the survey, lacked technical depth, or originated from lower-impact venues. The remaining 350+ studies underwent a more detailed abstract- and content-level assessment, leading to the exclusion of approximately 150 additional papers that did not directly address ransomware detection, prevention, mitigation, or recovery. Ultimately, nearly 200 high-quality and representative studies were selected for comprehensive analysis and comparison.

More than 125 of the selected papers were published between 2022 and 2025, reflecting the significant recent growth of ransomware research. The remaining references include foundational works, influential earlier studies, and prior surveys that provide historical context and background. The final corpus was then systematically categorized based on dimensions such as detection paradigm, deployment environment, defense layer, analytical technique, and operational objective.

Overall, the resulting papers provides a comprehensive and representative foundation for analyzing the evolution, strengths, limitations, and practical applicability of ransomware defense mechanisms across diverse systems and deployment environments. The PRISMA-style flow diagram Fig. 1 presents clearly defined screening stages, paper counts, and explicit exclusion at each stage of the selection process.

3.2 Some Background Related to Machine Learning

Machine Learning (ML) has become a key component of modern cybersecurity, enabling automated analysis of large-scale and evolving threat data. In ransomware detection and prevention, ML techniques are widely used to identify malicious behavior, detect anomalies, and classify attacks.

Data Imbalance: Data imbalance in datasets occurs when the number of samples belonging to one class is significantly larger than the number of samples belonging to another class. In cybersecurity and ransomware detection datasets, benign samples often vastly outnumber malicious samples. For example, a dataset may contain 95% normal activity and only 5% ransomware activity. Class imbalance can severely affect the performance of detection systems. Machine Learning models trained on highly imbalanced datasets tend to become biased toward the majority class, causing them to predict benign behavior more frequently while failing to detect minority-class attacks. As a result, a model may achieve very high overall accuracy while still producing a high False Negative Rate (FNR), meaning many ransomware instances go undetected. This is particularly dangerous in ransomware detection because missing even a small number of attacks can lead to significant damage. Imbalanced datasets may also distort evaluation metrics, making accuracy alone unreliable. Therefore, researchers often use techniques such as oversampling, under-sampling, data augmentation, cost-sensitive learning, and metrics like Recall, F1-score, ROC-AUC, and Precision-Recall to properly evaluate and improve ransomware detection systems when imbalanced datasets are used.

Ransomware-Specific Interpretation of Evaluation Metrics: In ransomware detection, evaluation metrics must be interpreted in terms of security risk and operational impact.

True positive rate (TPR): Measures correctly detected ransomware; high TPR is critical to avoid missed attacks.

False negative rate (FNR): Captures missed ransomware; even small values pose severe risk.

False positive rate (FPR): Indicates false alarms; high FPR disrupts normal operations and reduces trust.

Time-to-detection (TTD): Amount of time elapsed between the moment ransomware begins its malicious activity and the moment the security system successfully detects it.

Precision: Measures reliability of alerts; low precision increases investigation overhead.

F1-score: Balances precision and recall, useful for imbalanced datasets.

Accuracy: Can be misleading under class imbalance.

ROC-AUC: Evaluates model discrimination across thresholds.

Overall, ransomware detection prioritizes minimizing false negatives while maintaining acceptable false positives, with the balance depending on deployment context (e.g., endpoints, cloud, or critical infrastructure).

3.3 Evaluation Challenges and Standardization

While metrics such as accuracy, precision, recall, F1-score, and ROC-AUC are widely reported, their interpretation in ransomware detection requires careful consideration. In real-world deployments, ransomware events are rare, making *false positive rate (FPR)* and *time-to-detection* more critical than aggregate accuracy. Moreover, many studies evaluate models on static and balanced datasets, which can inflate performance due to distributional bias and lack of temporal drift. Cross-dataset generalization, robustness to adversarial manipulation, and evaluation under realistic workloads remain underexplored.

Beyond predictive performance, practical deployment requires consideration of: (i) computational overhead and latency, (ii) scalability in cloud and IoT environments, (iii) explainability and analyst interpretability, (iv) resilience against evasion and poisoning attacks.

These gaps highlight the need for standardized benchmarks and evaluation protocols aligned with real-world ransomware scenarios.

Table 3 summarizes representative datasets commonly used in ransomware research. These datasets span multiple modalities, including binary analysis, network traffic, memory forensics, and IoT telemetry, reflecting the diverse nature of ransomware detection approaches. However, many datasets suffer from limitations such as lack of realism, outdated attack scenarios, and limited coverage of modern ransomware behaviors such as data exfiltration and multi-stage attacks. This highlights the need for more comprehensive and continuously updated benchmarking datasets.

Table 3: Representative datasets used in ransomware detection research.

Dataset	Year	Type	Data Modality	Key Features
VirusShare [11]	Ongoing	Malware Repository	Binary samples	Large collection of ransomware and malware binaries; widely used for static and dynamic analysis.
Malicia Dataset [12]	2015	Malware Dataset	Binary + API calls	Contains ransomware and benign samples; used for ML-based malware classification.
EMBER Dataset [13]	2018	Malware Dataset	Static features (PE files)	Large-scale labeled dataset for malware classification; includes feature vectors extracted from binaries.
CIC-MalMem-2022 [14]	2022	Memory-based	Memory dumps	Focuses on ransomware detection using memory analysis; includes benign and ransomware processes.
CIC-IDS2017 [15]	2017	Network Intrusion	Network traffic flows	Includes ransomware-related traffic; widely used for network-based detection benchmarking.

(Continued)

Table 3 (continued)

Dataset	Year	Type	Data Modality	Key Features
CSE-CIC-IDS2018 [16]	2018	Network Intrusion	Network flows	Improved version of CIC-IDS2017; includes modern attack scenarios including ransomware traffic.
UNSW-NB15 [17]	2015	Network Intrusion	Network traffic	Contains synthetic attack traffic including malware behaviors; used for anomaly detection.
IoT-23 Dataset [18]	2020	IoT Network	Network traffic	Captures IoT malware traffic including ransomware-like behavior; useful for IoT security research.
ToN_IoT Dataset [19]	2020	IoT/IIoT	Network + telemetry	Includes telemetry, system logs, and network traffic; supports cross-layer ransomware detection.
UCI Android Malware Dataset [20]	2017	Mobile Malware	APK features	Includes ransomware samples for Android; supports static and dynamic analysis.

Table 4 contains a list of frequently used acronyms (Abbreviations) in the literature that are used in this paper. Acronyms of specific algorithms/schemes discussed in this paper are not included in this list.

Table 4: Abbreviations used in this paper.

Abbreviation	Elaboration	Detailed Description
AE	Auto Encoder	It is a type of ANN used to learn efficient codings of unlabeled data.
ANN	Artificial Neural Network	First developed in the 1950s, inspired by the structure and functioning of brain.
CNN	Convolutional Neural Network	A type of ANN.
CPS	Cyber Physical Systems	Systems that help in integrating sensing, computation, control and networking and connecting them to the Internet and to each other.
DL	Deep learning	Machine learning based on Deep Neural Network (DNN).
DNN	Deep Neural Network	A type of ANN.
DT	Decision Tree	A flowchart-like structure used for classification of data.

(Continued)

Table 4 (continued)

Abbreviation	Elaboration	Detailed Description
FL	Federated Learning	A Machine Learning Model designed to use on data spread across multiple nodes.
HFL	Heterogeneous Federated Learning	A Machine Learning Model designed to use on data spread across multiple heterogeneous nodes.
IDS	Intrusion detection system	A system designed for detecting intrusions in computer networks.
IIoT	Industrial Internet of Things	Interconnected sensors and other devices networked together with other industrial applications.
IoT	Internet of Things	Network of objects/devices connecting and exchanging data with other devices and systems over the Internet.
K-NN	K-Nearest Neighbors	A classification method.
LIME	Local Interpretable Model-agnostic Explanations	XAI model proposed by Ribeiro et al. [21].
LR	Linear Regression	A linear approach for modeling the relationship between a scalar response and one or more dependent variables.
JRIP	A rule-based classification algorithm	This classification algorithm is derived from RIPPER (Repeated Incremental Pruning to Produce Error Reduction). JRIP is the Java implementation of RIPPER.
J48	A decision tree algorithm	Java implementation of C4.5, a decision tree-based supervised classification algorithm developed by Ross Quinlan [22].
MLP	Multilayer Perceptron	A class of feed-forward ANNs.
NIDS	Network Intrusion detection System	An intrusion detection system designed for detecting intrusions at the network level.
NLP	Natural Language Processing	A field of AI that enables computers to understand, interpret, generate, and interact using human language.
RF	Random Forest	An ensemble learning method for classification.
RNN	Recurrent Neural network	A class of ANNs.

(Continued)

Table 4 (continued)

Abbreviation	Elaboration	Detailed Description
SDN	Software Defined Networking	An approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.
SHAP	SHapley Additive exPlanations	Proposed by Lundberg and Lee [23] to generate explanations for the predictions of black-box models.
SMOTE	Synthetic Minority Oversampling	A method for balancing data by over-sampling the minority (abnormal) class and under-sampling the majority (normal) class [24].
SVM	Support Vector Machine	SVM can learn from sample examples and assign labels to unknown objects. It can help in solving classification and regression problems. It supports standard kernel functions and lets the user choose their own function.
XAI	Explainable AI	A set of processes and methods that allows human users to comprehend and trust the results and output created by Machine Learning (ML) algorithms [25].

4 Research Works Surveyed in This Paper

In this section, we systematically classify, characterize, and critically synthesize ransomware-related research published in leading peer-reviewed journals and top-tier international conferences, primarily from venues such as IEEE, ACM, Elsevier, and Springer. The surveyed literature is organized into two principal classes: (i) detection-focused studies that aim to identify ransomware activity using behavioral, statistical, or learning-based techniques, and (ii) prevention, mitigation, and recovery oriented works that seek to limit damage, enable system restoration, and reduce attacker leverage. Within each class, we further categorize the research and provide a critical comparative analysis of the studies, emphasizing their core contributions, strengths, limitations, and the open challenges associated with each line of work. *We note that this classification and categorization are not intended to be rigid or exhaustive, as certain studies naturally span multiple classes or categories*. Fig. 2 provides our taxonomy of the ransomware research presented in the literature.

4.1 Ransomware Detection-Focused Research Works

In this subsection, we systematically categorize detection-oriented research and review representative studies within each category. For each category, we provide a critical synthesis of the literature, highlighting

key design principles, strengths, and limitations, and outline the open research challenges that remain to be addressed.

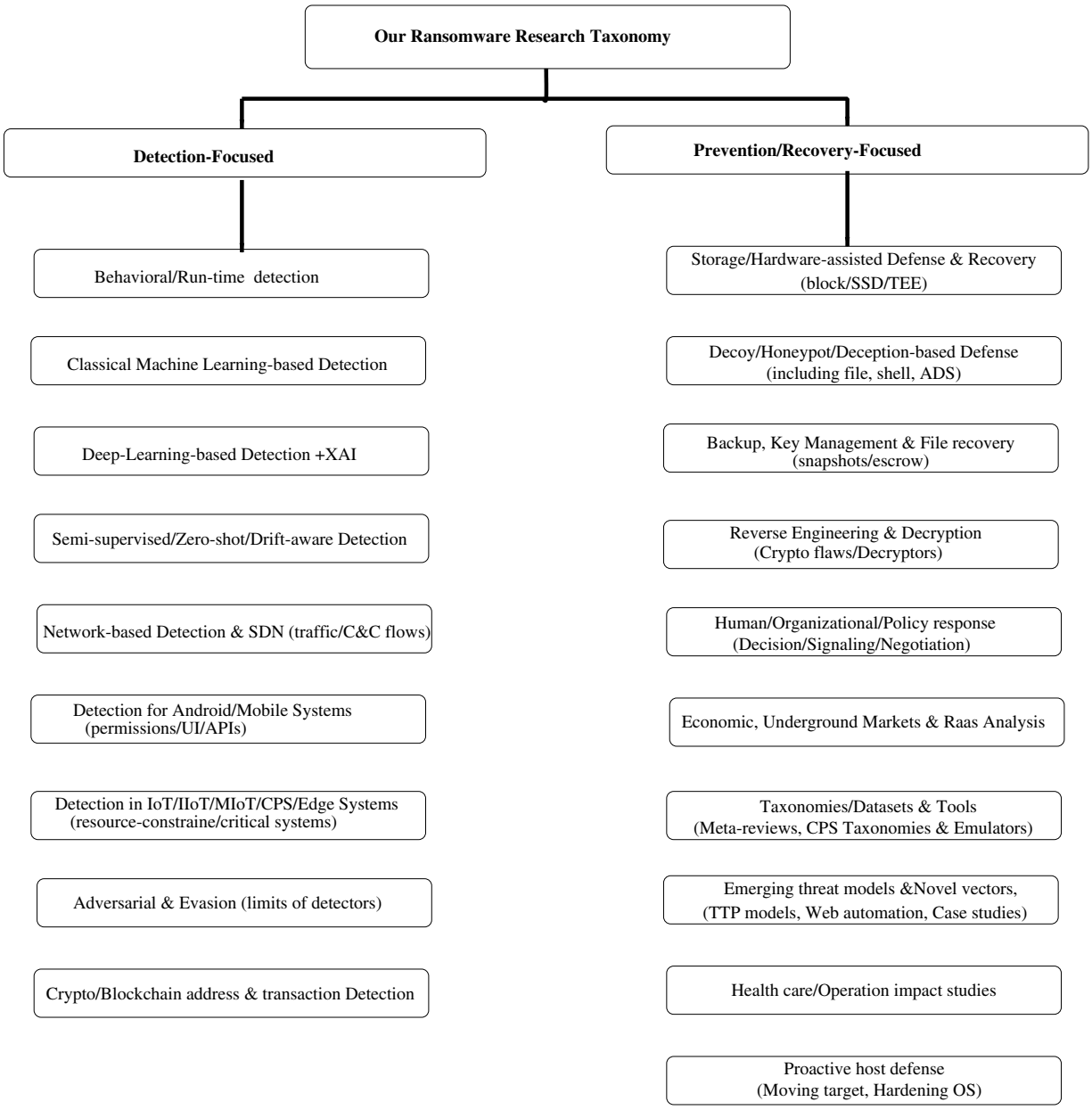

Figure 2: Our taxonomy of ransomware research surveyed in this paper.

4.1.1 Research Works That Use Behavioral/Runtime Approaches for Detection

In this subsection, we comparatively analyze ransomware detection approaches that infer attacks from abnormal runtime behavior. Across the literature, the central intuition is consistent: ransomware must eventually interact with system resources–especially files, processes, APIs, registry entries, memory, or the desktop–in ways that differ from benign software. The main differences among existing works lie in *where* they monitor behavior (user level, API level, kernel/hypervisor level), *how early* they aim to detect the attack

(pre-encryption vs. during encryption), and *what trade-offs* they make among detection speed, robustness, overhead, and deployability.

Early systems such as CryptoDrop [26] and UNVEIL [27] established the practical feasibility of behavior-based ransomware detection. Both exploit the observation that ransomware must manipulate user files or desktop artifacts to achieve its objective, but they do so differently. CryptoDrop emphasizes *online early warning* through correlated file-access indicators and rapid process termination, making it particularly valuable for limiting damage. UNVEIL, in contrast, relies on a synthetic execution environment to observe suspicious file and desktop manipulations, offering richer behavioral visibility but under more controlled conditions. Works such as Chen and Bridges [28] and Homayoun et al. [29] extend this line of research by showing that execution traces are not only useful for detection, but also for extracting discriminative behavioral patterns and even attributing activity to ransomware families. The key insight from these early studies is that runtime behavior provides stronger semantic signals than purely static artifacts, although many results still depend on controlled experimental settings.

A major subsequent research direction centers on Windows API-call analysis, which offers a more fine-grained and machine-learning-ready behavioral representation. Hampton et al. [30] show that API-call frequencies already provide meaningful separation between ransomware and benign processes, while later studies improve on this idea through richer modeling choices. For example, PEDA and its extensions [31,32] emphasize *pre-encryption detection* by combining fast hashing with API-based learning, reflecting a design choice that prioritizes early intervention over deeper but slower analysis. Hwang et al. [33] capture sequential dependencies through Markov modeling, Ullah et al. [34] and Molina et al. [35] show that compact feature representations can capture reconnaissance and evasion behavior, and Herrera-Silva and Hernández-Álvarez [36] strengthen the empirical side of the literature through more recent cross-dataset evaluations. Compared with earlier log-driven methods, API-centric approaches generally offer better granularity and are easier to integrate with learning pipelines, but they are also more exposed to adversarial API obfuscation, delayed execution, and runtime overhead. Thus, their main strength is sensitivity to fine behavioral patterns, whereas their main weakness is brittleness under adaptive attackers.

Another important branch of the literature moves the observation point deeper into the system stack to improve tamper resistance and capture lower-level signals. Javaheri et al. [37] and Zhang et al. [38] use kernel-level instrumentation, while Tang et al. [39] employ virtual machine introspection below the guest OS, and McIntosh et al. [40] explore dynamic user-driven access control as a means of intercepting suspicious file accesses. Compared with user-level or API-level monitoring, these approaches are generally more resistant to evasion and privilege manipulation, and they can sometimes detect attacks earlier in the execution chain. However, that improved robustness comes at the cost of substantially greater deployment complexity, privileged integration requirements, and potential portability challenges. The broader lesson is that deeper visibility often improves resilience, but also makes real-world adoption harder.

Several works focus specifically on detecting ransomware before substantial encryption begins, highlighting a recurring tension between *earliness* and *evidence quality*. Kok et al. [32] and Al Sabeh et al. [41] target environment-inspection and reconnaissance APIs to stop attacks before encryption starts, while Ramesh and Menen [42] model ransomware progression as a finite-state machine across multiple families. Abbasi et al. [43] improve efficiency through optimized behavioral feature selection, and Ayub et al. [44] combine dynamic analysis with prior knowledge from static ML models to improve early detection of previously unseen samples. Taken together, these studies show that pre-encryption detection is attractive because it can significantly reduce damage, but it also relies on the assumption that early-stage malicious behaviors are both observable and sufficiently distinct from benign activity. This assumption is increasingly strained by stealthy, low-and-slow, or staged ransomware.

More recent work reflects a shift from proof-of-concept detection toward operational scalability, transparency, and deployment realism. Hou et al. [45] address a longstanding weakness in the literature, namely, small and unrealistic datasets, by constructing MarauderMap, a multi-terabyte runtime dataset spanning multiple attack stages, which enables more realistic analysis of ransomware behavior across reconnaissance, tampering, exfiltration, and encryption phases. Marcinkowski et al. [46] respond to the interpretability gap by proposing MIRAD, which uses interpretable machine learning over API and registry behaviors, while Wang et al. [47] emphasize deployment practicality through CanCal, a lightweight industrial-scale pipeline that filters candidate processes before applying more expensive behavioral analysis. Compared with earlier sandbox-oriented systems, these recent approaches are less concerned with demonstrating mere detectability and more focused on *scalability, explainability, and low false-positives*. This marks an important maturation of the field.

Open Issues: Behavioral and runtime-based detection approaches fundamentally rely on the assumption that ransomware exhibits observable pre-encryption activity patterns. However, modern ransomware increasingly adopts stealthy, delayed, or low-and-slow encryption strategies that minimize detectable anomalies. Kernel- and API-level monitoring further introduces runtime overhead and scalability concerns, particularly in cloud and resource-constrained environments. Additionally, these approaches are rarely evaluated under adversarial conditions, where attackers may mimic benign processes or inject noise into behavioral traces, limiting robustness in real-world deployments. These limitations directly relate to challenges **C2** (adversarial robustness), **C5** (efficiency), and **C10** (evolving threat models).

4.1.2 Classical Machine Learning–Based Detection Approaches

Classical machine learning (ML) has been widely adopted for ransomware detection due to its ability to learn discriminative patterns from heterogeneous data while maintaining relatively low computational overhead. Across the literature, the key design differences lie in the *choice of feature modality* (static, behavioral, memory), the *degree of feature engineering*, and the *integration with system-level defenses*. These choices directly influence robustness, deployability, and generalization.

Early works explore diverse feature spaces, highlighting a fundamental trade-off between visibility and robustness. Static-analysis approaches (e.g., opcode N-grams with TF-IDF weighting [48]) are computationally efficient and easy to deploy, but are inherently fragile under packing and obfuscation. In contrast, behavioral and screen-content–based methods [49] attempt to capture runtime semantics, improving resilience to code transformation at the cost of requiring dynamic analysis environments. Memory-forensics–based approaches [50,51] provide even deeper visibility into execution artifacts and can detect fileless or previously unseen ransomware, but introduce significant monitoring overhead and deployment complexity. While these works show that carefully engineered features combined with classifiers such as Random Forest or XGBoost can achieve high reported accuracy, their effectiveness is tightly coupled to the observability and stability of the chosen feature space.

A second line of work focuses on behavioral sequence modeling and feature optimization, revealing that *feature engineering often matters more than model complexity*. Studies modeling API-call sequences and process behaviors [52–54] demonstrate that incorporating temporal structure improves detection fidelity compared to simple frequency-based features. Techniques such as Enhanced Maximum-Relevance and Minimum-Redundancy (EmRMR), Principle Component Analysis (PCA), and bio-inspired representations (e.g., digital DNA k-mers) further reduce redundancy and enhance discriminative power. Notably, works such as Jain et al. [55] show that well-designed feature-selection pipelines can allow classical models to match or even outperform deep learning methods. The key insight here is that classical ML remains competitive not because of model sophistication, but because of *efficient and domain-aware feature representations*. However,

these approaches remain vulnerable to adversarial manipulation of behavioral features and to concept drift in evolving ransomware.

Another important trend is the integration of ML with cross-layer or system-level defenses. Approaches such as the one proposed by Fernandez Maimo et al. [56] embed ML detection within SDN/NFV-enabled architectures to enable rapid isolation, while Poudyal and Dasgupta [57] and Iqbal et al. [58] combine multi-level and multimodal features (DLL, function calls, assembly, text, images) to improve detection coverage and support family attribution. Compared to standalone classifiers, these systems offer better contextual awareness and response capability, but at the cost of more complex feature pipelines and tighter integration requirements. This highlights a recurring trade-off between *detection accuracy and system complexity*.

Recent work shifts the focus from accuracy-centric evaluation to *scalability and deployment realism*. Stream-based learning approaches [59] address latency constraints in real-time environments, while comparative studies [60] demonstrate that classical ML remains competitive with deep learning when properly tuned. Expanding beyond endpoint detection, blockchain analytics [61] illustrate the applicability of ML to ransomware-related financial activity. Importantly, Rios-Ochoa et al. [62] show that models achieving near-perfect offline accuracy often degrade significantly in live deployments, exposing the gap between laboratory evaluation and operational performance. **Open Issues:** Classical ML-based approaches depend heavily on handcrafted features, which are inherently vulnerable to obfuscation, polymorphism, and feature manipulation by adaptive ransomware. Many studies rely on curated and balanced datasets, resulting in limited generalization under real-world class imbalance and evolving attack distributions. Furthermore, issues such as concept drift, feature instability, and lack of cross-dataset validation remain insufficiently addressed. Adversarial machine learning threats, including evasion and poisoning attacks, are also largely overlooked in existing evaluations. These issues highlight challenges **C1** (dataset realism), **C2** (adversarial robustness), and **C3** (generalization and drift).

4.1.3 Deep Learning–Based Ransomware Detection Approaches

In recent years, deep learning (DL) has become a prominent paradigm for ransomware detection due to its ability to automatically learn hierarchical representations from raw or minimally processed data. Unlike classical ML approaches that rely heavily on handcrafted features, DL-based methods shift the design focus toward *representation learning*, enabling models to capture complex temporal, structural, and semantic patterns. However, this shift also introduces new trade-offs related to data dependence, computational cost, interpretability, and robustness.

A dominant line of work models ransomware behavior as temporal sequences, particularly using API calls, system events, or execution traces. Hybrid CNN–RNN architectures such as DRTHIS [63] and more recent systems like RansoGuard [64] and iCNN-LSTM+ [65] demonstrate that combining spatial feature extraction (CNNs) with temporal modeling (LSTMs or attention) improves detection of both known and unseen ransomware variants. These approaches emphasize *early-stage detection* by capturing pre-encryption behaviors and adapting incrementally to evolving threats. Compared to classical ML, they offer greater expressive power and reduced reliance on manual feature engineering. However, this advantage comes at the cost of higher computational overhead, more complex training pipelines, and increased vulnerability to adversarial manipulation of event sequences. Thus, DL-based sequence models trade feature engineering effort for *data and compute dependence*.

A parallel research direction focuses on advanced representation learning from static or hybrid artifacts. Self-attention-based models (e.g., Zhang et al. [66]) address the limitations of RNNs in handling long opcode sequences by capturing global dependencies more efficiently, while image-based approaches

(e.g., RansomShield [67]) transform binaries into visual representations that CNNs can process. Hybrid systems such as SwiftR [68] combine static intermediate representations with dynamic behavioral embeddings, aiming to improve generalization to unknown families. These approaches highlight DL's flexibility in handling diverse data modalities and learning high-level abstractions. However, compared to behavioral sequence models, static and image-based methods remain more susceptible to obfuscation, packing, and adversarial perturbations, revealing a key trade-off between *representation richness and robustness*.

To address data scarcity and improve generalization, recent works incorporate generative and data-efficient learning techniques. GAN-based frameworks (e.g., TGAN-IDS [69], BGM-GAN [70]) synthesize realistic ransomware behaviors to enhance detection of early-stage or unseen attacks, while few-shot and meta-learning approaches [71] aim to reduce dependence on large labeled datasets. These methods represent a shift toward *data-centric robustness*, attempting to bridge the gap between limited training data and evolving threat landscapes. However, GAN-based systems introduce training instability and additional complexity, and their effectiveness depends on how well the generated samples reflect real-world attack distributions.

Another emerging trend is the movement toward scalable and deployment-aware DL systems. Approaches such as DeepWare [72] and VM-level monitoring frameworks [73] leverage hardware performance counters and low-level telemetry to enable efficient detection with reduced overhead. Federated learning frameworks [74] extend DL-based detection across distributed environments, addressing data privacy and heterogeneity, while large-scale empirical systems [75] demonstrate cross-domain applicability in mobile and network settings. Compared to earlier prototype models, these systems prioritize *scalability and real-world deployment*, but introduce new challenges such as communication overhead, Non-Independent and Identically Distributed (non-IID) data handling, and vulnerability to poisoning attacks.

Finally, explainability and trustworthiness have emerged as critical concerns for DL-based detection. Frameworks such as XRan [76] and recent hybrid models [77] integrate XAI techniques (e.g., SHAP, LIME) and uncertainty estimation to improve transparency and analyst trust. While these efforts address the black-box nature of DL-based models, they remain limited by the lack of standardized evaluation for explanation fidelity and by potential adversarial manipulation of explanations themselves. This reflects a broader trade-off between *model complexity and interpretability*.

Open Issues: DL-based ransomware detection methods require large volumes of labeled data and incur significant computational overhead, limiting their applicability in real-time and resource-constrained environments. These models are also susceptible to adversarial examples and traffic manipulation, which can distort learned representations. Moreover, the lack of interpretability and inconsistent evaluation of explanation fidelity raises concerns about trust and usability in operational settings. Cross-dataset generalization and robustness to evolving ransomware behaviors remain open challenges. These challenges correspond to **C2** (adversarial robustness), **C4** (explainability), and **C5** (computational efficiency).

4.1.4 Semi-Supervised/Zero-Shot/Drift-Aware Detection Approaches

Semi-supervised, zero-shot, and drift-aware ransomware detection approaches are motivated by a common limitation of supervised methods, namely, their dependence on large labeled datasets and their inability to generalize to unseen or evolving ransomware variants. While all three paradigms aim to improve adaptability, they differ in *how* they address uncertainty: semi-supervised methods leverage unlabeled data, zero-shot approaches rely on abstract representations, and drift-aware systems explicitly model temporal evolution.

Semi-supervised approaches primarily seek to bridge the gap between limited labeled dataset and abundant unlabeled observations. For example, Sharmeen et al. [78] combine unsupervised representation

learning with supervised classification to improve adaptability, whereas Urooj et al. [79] extend this idea using GAN-based augmentation to explicitly model evolving ransomware behavior over time. Compared to fully supervised methods, these approaches improve robustness to unseen variants by leveraging latent structure in data. However, their effectiveness critically depends on the *representativeness of unlabeled or synthesized data*, which is often difficult to guarantee in practice. Thus, they trade improved coverage of unknown threats for increased training complexity and potential sensitivity to distribution bias.

A complementary line of work focuses on early-stage detection under weak or sparse signals, highlighting the importance of *feature quality over model complexity*. The DPBD-FE and subsequent EMIFS/MM-EMIFS frameworks [80,81] emphasize dynamic identification of the pre-encryption boundary and adaptive feature selection tailored to early runtime behavior. Compared to generic feature extraction pipelines, these approaches detect the onset of encryption by monitoring cryptography-related API calls, demonstrating that careful feature engineering can significantly enhance performance even under limited signal conditions. However, their reliance on observable pre-encryption behavior introduces a key vulnerability: stealthy or delayed-encryption ransomware can bypass such assumptions, exposing a trade-off between *early detection and behavioral visibility*.

Zero-shot and drift-aware approaches further generalize detection to previously unseen ransomware and evolving environments, but through different mechanisms. Zero-shot methods such as Zero-Ran Sniff (ZRS) [82] abstract ransomware behavior into high-level attributes using autoencoders and attention mechanisms, enabling detection without family-specific training data. In contrast, drift-aware systems such as FeSAD [83] focus on maintaining performance over time by explicitly modeling and adapting to changes in data distribution. Moreover, FeSAD is designed to detect evolutionary ransomware under concept drift by integrating feature selection, drift calibration, and drift decision layers to enable reliable classification in non-stationary environments. While zero-shot learning emphasizes *generalization across classes*, drift-aware methods emphasize *stability across time*. Both represent a shift away from static models, yet they face a shared challenge: distinguishing benign distributional changes from adversarial evolution. Moreover, their evaluation is often limited to controlled or short-term settings, leaving long-term robustness uncertain.

Open Issues: Semi-supervised and zero-shot detection approaches aim to address data scarcity but depend heavily on the quality and representativeness of unlabeled or synthetic data. Existing attribute-based or embedding-based representations often fail to capture evolving ransomware semantics and multi-stage attack behaviors. Additionally, these methods lack long-term evaluation under realistic threat evolution scenarios, and their robustness against adversarial manipulation or poisoning of unlabeled data remains largely unexplored. These limitations relate to **C1** (dataset realism), **C3** (generalization), and **C10** (emerging threat models).

4.1.5 Network-Based and SDN-Based Detection

Network- and SDN-based ransomware detection approaches exploit visibility of data at traffic-level and centralized control to identify and contain attacks at the network layer. Unlike host-based methods, these approaches provide *global visibility and rapid response*, but offer limited insight into host-level semantics.

SDN-based frameworks (e.g., [84–86]) leverage programmable control planes to detect and block ransomware by analyzing communication patterns and dynamically enforcing flow rules. Their works focus on detecting specific ransomwares (CryptoWall, and WannaCry). Their key advantage lies in *real-time containment and network-wide enforcement*. However, they rely on the assumption that ransomware exhibits identifiable and stable communication signatures, which is increasingly invalid due to encryption, proxying, and domain fronting.

In contrast, passive traffic-analysis approaches (e.g., [87–90]) focus on statistical and flow-level features to enable scalable and lightweight detection across enterprise and IoT environments. They [88,89] also focus on specific ransomwares–Locky, LooCipher. These methods are easier to deploy and do not require SDN infrastructure, but their effectiveness degrades when malicious traffic is encrypted, tunneled, or indistinguishable from benign flows. Thus, they trade *scalability and deployability* for reduced robustness.

Some works expand the threat model by considering unconventional communication channels such as blockchain-based C&C (e.g., [91]) coordination mechanism used by the Cerber ransomware and routing-level anomalies (e.g., [92]) by analyzing routing records from the WestRock ransomware event. These approaches improve coverage against stealthy coordination strategies but introduce significant monitoring complexity and depend on infrastructure-level data that may not be available in practice.

Open Issues: Network-based detection approaches face significant visibility limitations due to the widespread use of encryption and the adoption of covert C&C channels leveraging cloud services, P2P networks, or blockchain infrastructure. Anomaly-based methods often suffer from high false positive rates and lack contextual correlation with host-level activities. SDN-based mitigation strategies further require tight integration with network infrastructure, raising deployment complexity and scalability concerns in large-scale environments. These issues reflect challenges **C6** (deployment constraints), **C7** (cross-layer coordination), and **C10** (evolving attack channels).

4.1.6 Ransomware Detection for Android and Mobile Systems

Ransomware detection in mobile environments differs fundamentally from desktop settings due to *resource constraints, limited system visibility, and strict privacy controls*. As a result, existing approaches can be broadly categorized into behavioral/runtime, static/API-based, and hybrid methods, each offering distinct trade-offs between accuracy, efficiency, and robustness.

Behavioral and runtime monitoring approaches focus on detecting anomalous system activity such as file encryption, system calls, or user–application interaction mismatches. Early systems (e.g., [93–95]) emphasize real-time detection and damage prevention by continuously monitoring processor usage, memory consumption, unauthorized encryption and I/O activity of critical processes and directories, while more recent methods (e.g., [96,97]) improve efficiency through lightweight streaming models and compiler-assisted instrumentation. These approaches provide strong semantic visibility and early detection capability, but incur runtime overhead and must carefully balance detection accuracy with battery consumption and user experience.

In contrast, static and API-based techniques (e.g., [98–100]) prioritize efficiency and scalability by analyzing permissions, API usage, and code structure prior to execution. These methods are well-suited for on-device deployment and large-scale screening, but are inherently fragile under code obfuscation, packing, and dynamic payload loading. Thus, they trade *efficiency for reduced robustness* compared to behavioral approaches.

Hybrid and traffic-based methods (e.g., [101–104]) combine static, dynamic, and network-level features to improve generalization across diverse ransomware variants. While these approaches enhance detection robustness and coverage, they introduce higher computational complexity and are less suitable for strictly resource-constrained environments. Similarly, formal and recovery-oriented solutions [105,106] extend beyond detection to provide stronger guarantees or post-attack recovery, but often require deeper system integration.

Overall, the comparison reveals a fundamental trade-off in mobile ransomware detection: *efficiency vs. robustness vs. visibility*. These challenges are further exacerbated by platform constraints such as limited energy, restricted monitoring capabilities, and rapid malware evolution, highlighting the need for lightweight, privacy-preserving, and adaptively robust detection frameworks tailored to mobile ecosystems.

Open Issues: Mobile ransomware detection remains constrained by limited resources, privacy restrictions, and restricted system visibility. Static methods struggle against obfuscation and dynamic loading, while runtime approaches incur non-trivial overhead. Encrypted traffic and evolving attack strategies further limit detection effectiveness, particularly against zero-day variants. These challenges align with **C5** (efficiency), **C6** (deployment), and **C10** (platform-specific threats).

4.1.7 Ransomware Detection for IoT/IIoT/CPS/Edge/Healthcare (ICE/IoMT) Environments

Ransomware detection in IoT/IIoT/CPS and healthcare environments differs fundamentally from traditional IT systems due to *extreme resource constraints, heterogeneity, and safety-critical requirements*. Existing approaches can be broadly categorized into lightweight behavioral detection, federated/distributed learning, and domain-specific resilience mechanisms, each reflecting different trade-offs between efficiency, scalability, and robustness.

Lightweight behavioral and hybrid approaches (e.g., [107,108]) exploit low-level telemetry (e.g., kernel activity, device signals) to enable early detection with minimal overhead. These methods are well-suited for resource-constrained IIoT edge gateways, but struggle with scalability and cross-device heterogeneity in large deployments.

Federated and distributed learning frameworks (e.g., [109,110]) address data heterogeneity and privacy constraints of IoT/IoMT networks by enabling collaborative detection across devices without centralized data collection. Compared to standalone models, they improve adaptability and coverage, but introduce communication overhead, synchronization complexity, and vulnerability to poisoning attacks.

Domain-specific approaches (e.g., [111,112]) integrate additional mechanisms such as blockchain, fog computing, and economic modeling to enhance resilience in safety-critical systems such as smart healthcare systems and vehicle ecosystems. These methods extend beyond detection to address integrity, traceability, and operational continuity, but significantly increase architectural complexity and may impact real-time performance.

Overall, the comparison reveals a fundamental trade-off in ICE/IoMT ransomware detection: *efficiency vs. scalability vs. resilience*. Lightweight methods prioritize deployability but lack global coordination, federated approaches improve adaptability but add system complexity, and domain-specific solutions enhance resilience at the cost of overhead. These challenges are further compounded by limited visibility into encrypted industrial protocols and the need to maintain safety and regulatory compliance, highlighting the importance of cross-layer, resource-aware, and deployment-specific defense strategies.

Open Issues: Detection in IoT/IIoT/CPS remains constrained by limited resources, heterogeneity, and safety requirements. Many approaches fail to scale across diverse devices and protocols, while federated methods introduce risks such as poisoning and privacy leakage. Restricted visibility into encrypted industrial traffic further limits effectiveness. These challenges align with **C5** (scalability), **C6** (deployment), and **C7** (cross-layer coordination).

4.1.8 Adversarial and Evasion Analysis of Ransomware

Ransomware evasion can be broadly categorized into *inference-time evasion* (manipulating runtime behavior to bypass detectors) and *poisoning attacks* (corrupting training data to degrade model performance). Across the literature, these strategies expose a fundamental limitation: most detection systems implicitly assume that malicious behavior remains sufficiently distinct from benign activity.

Early studies demonstrate the fragility of existing defenses. Works such as [113,114] show that both signature-based and behavioral detectors can be bypassed through carefully crafted execution patterns, including distributing malicious actions across processes. These results reveal that *behavioral distinctiveness alone does not guarantee robustness*, especially under adaptive attackers.

More recent work shifts toward intelligent and adaptive evasion. Frameworks such as RansomAI [115] and Animagus [116] demonstrate that ransomware can actively optimize its behavior, either by tuning encryption strategies or mimicking benign I/O patterns, to minimize detection probability. Compared to earlier heuristic evasion, these approaches represent a transition to *learning-driven adversaries*, significantly challenging ML/DL-based detectors.

In response to this, defensive efforts increasingly focus on identifying *invariant signals* that are difficult to conceal, such as the coupling between encryption operations and disk I/O (e.g., [117,118]). Zhao et al. [117] ERW-Radar system integrates contextual correlation, fine-grained content analysis, and adaptive optimization mechanisms, while Guo et al. [118] approach is based on the inherent temporal correlation between encryption computation and disk I/O activity. While these methods improve robustness against mimicry, they rely on assumptions about fundamental encryption behavior, which may be weakened by throttling, partial encryption, or distributed execution.

Finally, recent frameworks (e.g., Minerva [119]) integrate adversarial robustness directly into model design, moving from reactive to *proactive defense*. However, such approaches remain limited by the lack of standardized adversarial benchmarks and comprehensive evaluation under realistic attack conditions.

Overall, the comparison highlights an ongoing arms race: attackers evolve from static obfuscation to adaptive, learning-driven evasion, while defenders shift from heuristic detection to invariant-based and adversarially robust models. The key insight is that robustness cannot be achieved through feature design alone; it requires adversarially aware training, cross-layer signals, and continuous adaptation.

Open Issues: Adversarial robustness remains a major gap. Detection systems are vulnerable to mimicry, temporal distribution of malicious actions, and feature manipulation. Adversarial training, robustness benchmarks, and evaluation under realistic attack scenarios remain limited, while poisoning and model-extraction threats are underexplored. These challenges correspond to **C2** (adversarial robustness) and **C3** (generalization).

Table 5 provides a summary of common ransomware evasion strategies and representative defensive countermeasures. Table 6 provides a mapping of some of the ransomware evasion studies, to adversarial ML threat models.

In contrast, semi-supervised, zero-shot, and drift-aware approaches attempt to address the limitations of static models by improving adaptability to unseen and evolving threats. However, these methods shift the challenge from feature design to *representation reliability and data realism*, and they remain sensitive to distribution bias and adversarial drift.

Table 5: Summary of common ransomware evasion strategies and representative defensive countermeasures.

Evasion Strategy	Description	Representative Defense Measures
Multi-process cooperation	Distributing malicious activities across multiple benign-looking processes to suppress strong behavioral signals	Cross-process correlation, contextual behavior aggregation
Benign behavior imitation	Mimicking I/O and execution patterns of legitimate applications to hide encryption activity	Fine-grained content analysis, invariant-based detection
Adaptive encryption scheduling	Dynamically adjusting encryption rate, duration, and algorithm to avoid triggering detectors	Temporal correlation between computation and I/O
Reinforcement learning-driven evasion	Learning optimal attack policies through feedback from detection outcomes	Robust-by-design models, adversarially trained detectors
Statistical camouflage	Producing encrypted outputs that resemble benign file modifications in size and access patterns	Byte distribution analysis, χ^2 tests
Assumption breaking	Exploiting outdated detection assumptions (e.g., single-process, burst encryption)	Adaptive thresholds, continual model updating

Table 6: Mapping ransomware evasion studies to adversarial ML threat models.

Work	Primary Technique	Threat Model	Key Insight
Beaman et al. [113] (2021)	Custom ransomware engineering	Evasion	Commercial anti-virus solutions remain vulnerable to handcrafted evasive logic
De Gaspari et al. [114] (2022)	Multi-process workload splitting	Evasion, Mimicry	Behavioral features can be neutralized via coordinated benign-looking processes
von der Assen et al. [115] (2023)	Reinforcement learning-based encryption control	Adaptive Learning	Attackers can learn optimal stealth policies against deployed detectors
Zhou et al. [116] (2023)	Imitation of benign I/O behavior	Mimicry	Behavior-based detectors fail when ransomware emulates legitimate workflows

(Continued)

Table 6 (continued)

Work	Primary Technique	Threat Model	Key Insight
Zhao et al. [117] (2025)	I/O repetitiveness and content statistics	Evasion (Defense-Oriented)	Invariant properties of encryption can expose evasive ransomware
Guo et al. [118] (2025)	Temporal correlation of encryption and I/O	Evasion (Defense-Oriented)	Temporal invariants remain effective despite behavioral camouflage
Hitaj et al. [119] (2025)	Robust-by-design architecture	Evasion, Adaptive Learning	Adversarial resilience must be embedded at model and feature levels

Overall, the comparison highlights a fundamental insight: no single approach is sufficient under realistic ransomware threat models. Instead, effective defense requires a cross-layer, adaptive framework that combines complementary strengths–early detection (behavioral), pattern learning (ML/DL), resilience (storage), and adaptability (semi-supervised/zero-shot/drift-aware)–while explicitly accounting for adversarial behavior, dataset limitations, and deployment constraints.

4.1.9 Research on Cryptocurrency Address Identification and Transaction Analysis

Ransomware operators exploit the pseudonymity of cryptocurrencies to conduct difficult-to-trace financial transactions, motivating research on identifying attacker-controlled addresses and analyzing transaction flows. Existing approaches can be broadly categorized into *heuristic/graph-based analysis*, *learning-based detection*, and *ecosystem-level studies*, each offering different trade-offs between interpretability, scalability, and attribution accuracy.

Early works (e.g., [120–122]) rely on address clustering heuristics and transaction graph analysis to quantify ransomware payments and identify attacker-controlled entities. These methods provide valuable macro-level insights into the economic structure of ransomware campaigns and are relatively interpretable, but depend on simplifying assumptions about address reuse and transaction patterns, limiting their robustness under evasion techniques.

More recent approaches adopt learning-based frameworks (e.g., [61,123]) to improve scalability and generalization. By leveraging graph-based feature aggregation and semi-supervised or imbalance-aware learning, these methods can detect both known and previously unseen ransomware-related transactions. Compared to heuristic approaches, they offer improved detection performance, but are highly dependent on labeled data quality, graph construction accuracy, and feature design, and may suffer from reduced interpretability.

A complementary line of work focuses on ecosystem-level analysis (e.g., [124]), integrating blockchain data with incident-level and economic information to study long-term trends such as payment behaviors and double-extortion strategies. While these approaches provide broader contextual understanding, they are less suited for real-time detection and rely on aggregated or delayed data.

Overall, the comparison reveals a key trade-off: heuristic methods are interpretable but brittle, learning-based methods are scalable but data-dependent, and ecosystem-level analyses are comprehensive but largely retrospective. A fundamental limitation across all approaches is the difficulty of linking pseudonymous

blockchain activity to real-world actors, particularly in the presence of mixers, cross-chain transactions, and privacy-enhancing techniques.

Open Issues: Accurate attribution remains challenging due to obfuscation techniques such as mixers, tumblers, and cross-chain transfers. The lack of high-quality labeled datasets and limited visibility into off-chain transactions further constrain detection and forensic analysis. These issues correspond to **C1** (data limitations) and **C9** (economic and policy factors).

4.1.10 Critical Insights and Lessons Learned from Research Works on Ransomware Detection

Critical Insights and Lessons Learned: A comparative analysis of existing ransomware detection approaches reveals several important trends, contradictions, and unresolved limitations across the literature. First, although many ML- and DL-based approaches report very high detection accuracy, these results are often obtained using curated, static, and highly imbalanced datasets under controlled laboratory settings. In contrast, studies that evaluate models under more realistic conditions–such as temporal drift, cross-family testing, or zero-day scenarios–typically report substantially lower robustness and generalization capability. This suggests that the apparent superiority of many learning-based methods may partly reflect dataset bias and experimental design rather than true operational effectiveness.

Second, there exists a clear contradiction between early-detection objectives and stealth-resistant detection requirements. Several behavioral and runtime-monitoring approaches assume that ransomware exhibits rapid and observable pre-encryption activities such as burst file modifications, entropy changes, or intensive API calls. However, recent ransomware families increasingly adopt delayed execution, partial encryption, intermittent encryption, and low-and-slow strategies specifically designed to evade such assumptions. As a result, approaches optimized for rapid detection may suffer from high false positives, whereas more conservative systems often detect the attack too late to prevent significant damage. This highlights a fundamental trade-off between detection speed, accuracy, and damage prevention.

Third, cross-study comparison shows that no single detection paradigm provides comprehensive coverage against the evolving ransomware threat landscape. Behavioral approaches capture runtime anomalies but are sensitive to workload variability; network-based methods can identify C&C communication but may fail against offline or encrypted attacks; memory- and storage-level techniques can detect low-level malicious activities but often incur deployment overhead; and ML/DL methods are effective at pattern recognition yet remain vulnerable to adversarial evasion, poisoning, and feature manipulation attacks. Collectively, these findings indicate that ransomware defense cannot rely on a single-layer solution and instead requires cross-layer, multi-modal, and adaptive frameworks that combine host-, network-, memory-, and storage-level visibility.

Another important insight is the growing gap between research prototypes and deployment feasibility. Many studies optimize primarily for detection performance while overlooking practical operational constraints such as latency, computational overhead, scalability, privacy concerns, explainability, interoperability, and false alarm management. This issue becomes even more pronounced in resource- constrained environments such as IoT, IIoT, CPS, and edge systems, where heavyweight monitoring and complex deep learning models may not be practical. Furthermore, explainability and analyst trust remain underexplored despite their importance in operational SOC and incident response environments.

Finally, current evaluation methodologies remain fragmented and inconsistent across studies. Different works use different datasets, feature sets, attack scenarios, and performance metrics, making direct comparison difficult. Moreover, many evaluations ignore adversarial settings, longitudinal behavior changes, and realistic deployment conditions. These inconsistencies hinder reproducibility and may inflate perceived

effectiveness. Overall, the surveyed literature suggests that future ransomware detection systems must move beyond isolated accuracy-driven designs toward robust, adaptive, deployment-aware, and explainable solutions evaluated using realistic, standardized, and continuously updated benchmarks.

Table 7 presents a classification of the ransomware detection approaches, along with the detection principle used with representative references, discussed in this subsection.

Table 7: Summary of detection-focused ransomware research.

Category	Detection Principle	Representative References
Behavioral/Runtime Detection (Host-Based)	Detect abnormal runtime behavior via file I/O, entropy, API calls, registry or kernel activity	Scaife et al. [26] (2016); Kharaz et al. [27] (2016); Chen and Bridges [28] (2017); Homayoun et al. [29] (2017); Hampton et al. [30] (2018); Kok et al. [31] (2019); Kok et al. [32] (2022); Hwang et al. [33] (2020); Ullah et al. [34] (2020); Molina et al. [35] (2021); Herrera-Silva and Hernández-Álvarez [36]; Javaheri et al. [37] (2018); Zhang et al. [38] (2024); Tang et al. [39] (2020); McIntosh et al. [40] (2021); Al Sabeh et al. [41] (2020); Ramesh and Menen [42] (2020); Abbasi et al. [43] (2022); Ayub et al. [44]; Hou et al. [45] (2024); Marcinkowski et al. [46] (2024); Wang et al. [47] (2024)
Machine Learning-Based Detection (Classical)	Supervised ML models using static, dynamic, or hybrid features	Zhang et al. [48] (2019); Su et al. [49] (2018); Cohen and Nissim [50] (2018); Ahmed et al. [52] (2020); Khan et al. [53] (2020); Arabo et al. [54] (2020); Jain et al. [55] (2025); Poudyal and Dasgupta [57] (2021); Iqbal et al. [58] (2022); Ba'abbad and Batarfi [59] (2023); Jemal and Lo [60] (2023); Rios-Ochoa et al. [62] (2025)
Deep/Representation Learning-Based Detection	CNN, RNN, LSTM, attention, and GAN-based ransomware detection	Hwang et al. [33]; Ullah et al. [34]; Molina et al. [35]; Herrera-Silva and Hernández-Álvarez [36]; Abbasi et al. [43]; Ayub et al. [44]; Aljabri et al. [51]; Fernandez Maimo et al. [56]; Dib et al. [61]; Homayoun et al. [63]; Cen et al. [64]; Ispahany et al. [65]; Zhang et al. [66]; Lachtar et al. [67]; Karbab et al. [68]; Zhang et al. [69]; Gazzan and Sheldon [70]; Zhu et al. [71]; Ganfure et al. [72]; Thummapudi et al. [73]; Lan et al. [74]; Hossain et al. [75]; Gulmez et al. [76]; Kabuye et al. [77]
Semi-supervised/Zero-shot	Detect zero-day ransomware and handle behavioral drift	Sharmeen et al. [78] (2020); Urooj et al. [79] (2023); Al-Rimy et al. [80] (2020); Al-Rimy et al. [81] (2021); Cen et al. [82] (2024); Fernando and Komninos [83] (2024)

(Continued)

Table 7 (continued)

Category	Detection Principle	Representative References
Network-Based Detection & SDN	Detect ransomware via traffic analysis	Cabaj and Mazurczyk [84] (2016); Cabaj et al. [85]; Akbanov et al. [86] (2019); Morato et al. [87] (2018); Almashhadani et al. [88] (2019); Liu et al. [89] (2020); Hernandez-Jaimes et al. [90] (2024); Pletinckx et al. [91] (2018); Li et al. [92] (2022)
Ransomware Detection for Mobile and Android Systems	Mobile-specific detection using permissions, user behavior, traffic, and lightweight ML	Song et al. [93] (2016); Chen et al. [94] (2017); Faghihi and Zulkernine [95] (2021); Chew et al. [96] (2024); Ma et al. [97] (2025); Scalas et al. [98] (2019); Alsoghyer and Almomani [99] (2019); Singh and Tripathy [100] (2024); Ahmed et al. [101] (2022); Hossain et al. [102] (2022); Albin Ahmed et al. [103] (2023); Jeremiah et al. [104] (2024); Cimitile et al. [105] (2018); Elkhail et al. [106] (2025);
IoT/IIoT/CPS/Edge/ Healthcare	Targeted ransomware detection	Fernandez Maimo et al. [56] (2019); Al-Hawawreh et al. [107] (2019); Al-Hawawreh et al. [109] (2021); Celdran et al. [108] (2023); Tariq et al. [110] (2022); Wazid et al. [111] (2022); Malik et al. [112] (2022)
Adversarial & Evasion Analysis	Study evasion strategies that bypass detection mechanisms	Beaman et al. [113] (2021); De Gaspari et al. [114] (2022); von der Assen et al. [115] (2023); Zhou et al. [116] (2023); Zhao et al. [117] (2025); Guo et al. [118] (2025); Hitaj et al. [119] (2025)
Cryptocurrency Address & Transaction Detection	Detect ransomware-related Bitcoin addresses and payments	Dib et al. [61] (2024); Conti et al. [120] (2018); Huang et al. [121] (2018); Paquet-Clouston et al. [122] (2019); Wang et al. [123] (2024); Sarabi et al. [124] (2025)

Unified Insights: Table 8 shows that no single defense paradigm is sufficient under realistic ransomware threat models. Behavioral and learning-based methods are valuable for early detection, but they often degrade under stealthy, adaptive, or distribution-shifted attacks. Network-based approaches provide broader visibility but may miss host-local encryption activity, while storage-level and backup-based mechanisms improve resilience yet often operate after some damage has already occurred. These comparisons highlight fundamental trade-offs between accuracy and latency, detection and prevention, interpretability and model complexity, and broad coverage and deployment cost. Consequently, robust ransomware defense requires cross-layer, defense-in-depth designs that combine early detection, damage containment, and recovery support.

Table 8: Comparative analysis of major ransomware defense approaches under realistic threat models.

Approach	Main Strengths	Why It Fails Under Realistic Threat Models	Fundamental Trade-Offs	Typical Best-Fit Use Cases
Behavioral/ Runtime Detection	Can detect previously unseen ransomware by monitoring file I/O, API calls, process behavior, and entropy changes; often effective against fast encryption attacks.	Assumes ransomware exhibits clear pre-encryption or early-encryption behavioral signals. Stealthy, delayed, selective, intermittent, or low-and-slow encryption can reduce detectability. Attackers may also mimic benign backup, compression, or synchronization workloads.	High sensitivity vs. false alarms; early detection vs. runtime overhead; broader monitoring vs. deployability.	Endpoint protection, host monitoring, enterprise desktops, managed servers.
Classical ML-based Detection	Efficient inference, interpretable feature sets, and suitability for tabular telemetry such as API-call counts, file activity, or registry events.	Relies on handcrafted features that may become brittle under obfuscation, polymorphism, concept drift, and feature manipulation. Performance often drops when evaluated outside the original dataset or environment.	Interpretability and lower latency vs. weaker robustness to drift and adversarial manipulation; simpler models vs. limited expressiveness.	Resource-aware endpoint monitoring, fast screening, operational settings requiring moderate interpretability.
Deep Learning-based Detection	Can learn complex temporal or structural patterns from raw or minimally processed data; useful for sequence, memory, and traffic analysis.	Requires large, representative labeled datasets and often assumes training data covers realistic future behaviors. Vulnerable to adversarial perturbations, dataset bias, and distribution shift; may be difficult to explain and validate in practice.	Potentially higher accuracy vs. higher computation cost; expressive modeling vs. explainability; robustness vs. training complexity.	High-volume telemetry analysis, cloud-scale monitoring, sequence-based detection, research prototypes with sufficient data.
Semi-supervised/Zero-shot Detection	Useful when labeled ransomware data are scarce; can improve detection of novel or rare families.	Depends heavily on the quality of unlabeled data, attribute design, or latent representations. Novel attacks that diverge from assumed semantic structure may evade detection; robustness under poisoning or adversarial drift is often unclear.	Novelty detection vs. uncertainty in decision quality; broader coverage vs. reduced reliability and interpretability.	Emerging-threat detection, environments with limited labels, exploratory threat hunting.
Network-based Detection	Can detect ransomware-related communication, lateral movement, C&C traffic, or exfiltration without relying solely on endpoint instrumentation.	Assumes malicious behavior is visible in traffic patterns. Encryption, legitimate cloud services, P2P channels, DNS tunneling, and intermittent communication reduce visibility. Host-only encryption without clear network signals may evade detection entirely.	Broader network visibility vs. weaker host context; lower endpoint overhead vs. higher false positives; detection coverage vs. limited actionability.	Perimeter monitoring, NDR/SOC pipelines, enterprise networks, exfiltration-aware monitoring.

(Continued)

Table 8 (continued)

Approach	Main Strengths	Why It Fails Under Realistic Threat Models	Fundamental Trade-Offs	Typical Best-Fit Use Cases
Storage-level/File-system Defenses	Can directly observe overwrite patterns, block changes, file versioning behavior, and abnormal access bursts; useful for limiting damage and supporting recovery.	Often assumes ransomware performs aggressive overwrite-heavy encryption. Selective encryption, partial corruption, delayed access, or backup targeting can bypass these assumptions. Some methods require kernel, firmware, or storage-stack changes.	Damage containment vs. system complexity; prevention/recovery support vs. portability; lower semantic visibility vs. strong proximity to protected data.	Backup protection, storage appliances, enterprise file servers, high-value data repositories.
Backup/Recovery-based Defenses	Essential for resilience after compromise; can restore service even when detection fails.	Often assumes backups remain intact, reachable, recent, and untampered. Modern ransomware targets backups, snapshots, and recovery workflows; exfiltration-centric attacks still cause extortion pressure even after restoration.	Recovery assurance vs. storage/management cost; resilience vs. delayed response; continuity vs. inability to prevent theft or initial disruption.	Business continuity planning, disaster recovery, critical infrastructure, regulated environments.
Deception-based Defenses	Can expose ransomware through interaction with decoys, bait files, honey shares, or controlled traps.	Effectiveness depends on realistic placement and attacker interaction. Sophisticated ransomware may detect decoys, defer execution, or use environment checks to avoid triggering traps.	Low-cost signaling vs. brittleness; early warning vs. incomplete coverage; simplicity vs. maintenance overhead.	Layered defense, early warning systems, environments where decoy placement is manageable.
Memory-based/Forensic Detection	Can reveal fileless activity, unpacked payloads, injected code, and volatile indicators invisible to static analysis.	Requires sufficient visibility into transient memory artifacts and often continuous or frequent acquisition. Fast execution, anti-forensics, and scale constraints reduce practicality in live environments.	Deep visibility vs. acquisition overhead; forensic richness vs. limited real-time scalability.	Incident response, forensic triage, memory-focused malware analysis.

4.2 Ransomware Prevention, Mitigation, and Recovery-Focused Research Works

This section systematically classifies and categorizes existing research on ransomware prevention, mitigation, and recovery strategies. For each category, we review representative approaches, provide a critical analysis of their underlying techniques and assumptions, and discuss key limitations and open research issues that remain unresolved.

4.2.1 Research Works Focusing on Storage-Level/Hardware-Assisted Ransomware Defenses

This subsection focuses on storage-level and hardware-assisted defenses against ransomware. These approaches operate below the application and operating-system layers and aim to prevent or limit data loss while enabling efficient recovery. Typical techniques leverage capabilities of solid-state drives (SSDs), block devices, storage firmware, hypervisors, or trusted hardware to detect malicious write patterns, isolate ransomware activity, and support rapid data restoration.

A substantial body of work explores embedding ransomware detection directly within storage devices, particularly SSDs, to detect malicious write patterns and enable rapid recovery. Min et al. [125] introduce Amoeba, an SSD architecture that incorporates a hardware accelerator to identify ransomware-infected pages and maintain fine-grained backup control to reduce storage overhead. Amoeba incurs negligible overhead and significantly outperforms the state-of-the-art SSD, FlashGuard, in both performance and space efficiency. Similarly, Baek et al. [126,127] propose SSD-Insider and its enhanced version SSD-Insider++, which leverage invariant behavioral features derived solely from block I/O headers to detect ransomware at the firmware level and exploit NAND flash's delayed deletion property for instant, and lossless recovery. Paik et al. [128] further demonstrate that ransomware-induced access patterns can be detected through specialized buffer management policies within flash-based storage devices. While these SSD-integrated approaches benefit from low latency and independence from the host OS, they rely on modifications to storage firmware or architecture, which may limit portability across commodity hardware platforms.

Other works explore host-level and memory-storage coordination mechanisms to prevent encrypted data from being committed to persistent storage. Elkhail et al. [129] observe that encrypted data typically passes through the OS page cache before being written to disk and propose a runtime defense that intercepts this synchronization process to prevent malicious data from reaching permanent storage; Evaluated against over a thousand ransomware samples, including advanced variants using multi-threading and boot-sector attacks, the system reliably restores affected files while incurring minimal performance overhead. In contrast, Ma et al. [130] introduce RansomTag, a hypervisor-based framework that bridges semantic gaps between storage devices and higher-level system context using a tag-based interface. This design enables accurate detection and fine-grained version recovery of overwritten or deleted files while maintaining modest backup overhead. Compared with firmware-centric SSD solutions, these approaches provide greater deployment flexibility and richer contextual information, though they introduce additional complexity in memory management and virtualization layers.

Recent research also investigates cloud storage environments and hardware-level telemetry as alternative defense layers. Wang et al. [131] propose DeftPunk, a ransomware detection and recovery system designed for cloud block storage, combining a two-layer I/O classifier with snapshot-based recovery mechanisms to minimize data loss in multi-tenant environments. Hill et al. [132] demonstrate that ransomware activity can be detected through hardware performance counters collected from non-virtualized systems, showing that a small subset of hardware-level features can enable rapid detection with high accuracy. Zhu et al. [133] further extend storage-level defenses through their SrFTL system, which integrates semantic awareness into the flash translation layer of SSDs and leverages modified flash translation layer (FTL) with a trusted enclave to perform secure detection and recovery operations; evaluation shows SrFTL outperforms existing FTL-based solutions. Together, these approaches illustrate a shift toward cross-layer defenses that combine storage semantics, hardware telemetry, and trusted execution environments. However, their effectiveness often depends on specialized hardware support, system-level modifications, or close integration with storage infrastructure.

Open Issues: Storage- and hardware-level defenses often require modifications to firmware or system architecture, limiting deployability across heterogeneous environments. Many approaches assume write-heavy encryption behavior, which can be bypassed by ransomwares by selective or partial encryption strategies. Additionally, semantic gaps between OS, hypervisor, and storage layers hinder coordinated detection and response, particularly in multi-tenant cloud settings. These challenges correspond to **C6** (deployment) and **C7** (cross-layer integration).

4.2.2 Decoy, Honeypot, and Deception-Based Defenses

Deception-based ransomware defenses adopt a "lure-and-contain" strategy, using decoy files, honeyfolders, or deceptive environments to trigger early detection and limit damage. Unlike ML or behavioral approaches that infer malicious intent, these methods rely on *direct attacker interaction* with crafted artifacts, providing highly interpretable signals but with limited coverage.

Early works (e.g., [134,135]) demonstrate that simple decoy files can effectively expose ransomware through abnormal access patterns or blocking behavior. These methods are lightweight and enable rapid containment, but their effectiveness depends heavily on decoy placement and assumes that ransomware will interact with them.

Subsequent approaches improve robustness through adaptive and multi-functional deception. Systems such as RTrap and Ranflood [136,137] extend decoy strategies with data-driven placement of decoy files, deliberately flooding targeted disk locations with decoy files to slow ransomware progress, moving target files, while other techniques exploit system features (e.g., alternate data streams) to mislead encryption targets. Compared to basic honeypots, these methods enhance coverage and mitigation capability, but introduce higher storage and management overhead.

More recent work moves toward *active deception*, where attackers are not only detected but actively disrupted. Frameworks such as ranDecepter [138], a real-time system that isolates ransomware in a deceptive environment and feeds the ransomware with counterfeit encryption data, increasing attacker cost and delaying impact. Compared to passive approaches, these systems improve resilience but require tighter system integration and careful configuration.

Overall, deception-based defenses exhibit a key trade-off: *precision vs. coverage*. They provide low false positives and interpretable detection signals, but rely on attacker interaction and can be bypassed by ransomware that detects or avoids decoys. Consequently, they are most effective as complementary mechanisms within a broader defense-in-depth strategy rather than standalone solutions.

Open Issues: Effectiveness depends on realistic decoy placement and configuration, which sophisticated ransomware can not evade. Large-scale deployment introduces management overhead, and limited integration with behavioral or learning-based systems reduces overall robustness. These challenges correspond to **C2** (adversarial adaptation) and **C6** (deployment constraints).

4.2.3 Reverse Engineering and Decryption-Based Ransomware Analysis

Reverse engineering and cryptographic analysis focus on *understanding and breaking ransomware implementations* to enable data recovery, rather than detecting attacks in real time. Compared to behavioral or ML-based methods, these approaches provide deeper insight into malware logic and encryption mechanisms, but are largely *reactive and family-specific*.

Empirical studies (e.g., [139]) show that many existing decryption tools fail in practice, highlighting a gap between claimed and actual recovery effectiveness. In contrast, targeted reverse engineering efforts (e.g., [140]) demonstrate that detailed analysis of specific ransomware families can yield effective decryption solutions, and present tools for reverse-engineering. This contrast underscores a key trade-off: *broad applicability vs. practical effectiveness*.

Another line of work exploits implementation flaws in ransomware cryptography (e.g., [141,142]). These studies show that even ransomware using strong cryptographic primitives can be broken if key-generation or randomness mechanisms are flawed. However, such success depends on the presence of subtle vulnerabilities, making these approaches opportunistic rather than generally applicable.

More recent work integrates reverse engineering with automated detection (e.g., [143]), by extracting features through reverse engineering for static analysis and converts executable binaries into images for deep learning-based classification to support scalable ML pipelines. Compared to pure decryption approaches, these methods improve scalability and generalization, but sacrifice the ability to directly recover data.

Overall, these approaches reveal a fundamental trade-off: *depth vs. generalizability*. Reverse engineering provides strong insight and potential recovery for specific families, but does not scale across evolving ransomware variants. Unlike detection-based methods, they operate post-compromise and depend heavily on implementation weaknesses, limiting their role to complementary forensic and recovery support.

Open Issues: Effectiveness is limited by strong cryptography and advanced obfuscation, while most solutions remain family-specific and difficult to generalize. Automated analysis lacks scalability against rapidly evolving ransomware. These challenges correspond to **C10** (evolving threats) and **C5** (scalability).

4.2.4 Data Recovery via Backup Integrity and Entropy-Based Restoration

Recovery-focused approaches aim to restore data after compromise, primarily through *entropy-based identification of encrypted files* and *protection of backup integrity*. Unlike detection methods, these approaches are inherently *reactive*, emphasizing resilience rather than prevention.

Entropy-based techniques (e.g., [144,145]) identify encrypted files by detecting statistical randomness and support recovery by locating clean backup versions. While these methods are lightweight and effective for bulk encryption, their reliability depends on distinguishing encrypted data from compressed content and may degrade under selective or partial encryption. Thus, they trade *simplicity and speed* for reduced robustness.

In contrast, backup-integrity–focused approaches (e.g., [146]) target the protection of recovery mechanisms themselves by detecting attempts to delete or corrupt backup artifacts. Compared to entropy-based methods, they provide stronger *resilience guarantees* by preserving recovery points, but do not directly identify encrypted data or prevent initial damage.

Overall, these approaches highlight a key distinction: *file-level recovery vs. infrastructure-level protection*. Entropy-based methods facilitate restoration after encryption, while backup-integrity mechanisms ensure that recovery remains possible even under adversarial interference. However, both rely on a critical assumption that backups are intact and accessible, which is increasingly violated by modern ransomware employing backup targeting and data exfiltration.

Open Issues: Effectiveness of recovery is limited by compromised backups, false positives in entropy-based detection, and evasion via selective encryption. Additionally, poor integration with detection systems and lack of support for partial or semantic recovery reduce practical utility. These challenges correspond to **C8** (recovery and resilience) and **C7** (cross-layer coordination).

4.2.5 Human Factors, Organizational, and Policy Responses

Ransomware response is not purely technical; it is shaped by *economic incentives, human behavior, and policy constraints*. Existing work can be broadly grouped into *economic/strategic analyses*, *organizational and behavioral studies*, and *policy and governance frameworks*, each offering complementary but incomplete perspectives.

Economic and strategic studies (e.g., [147–149]) highlight that ransom decisions are driven by cost-benefit trade-offs under uncertainty, where organizations weigh operational disruption, financial loss, and reputational impact. Game-theoretic models (e.g., [150,151]) further show that attacker-victim interactions

are shaped by information asymmetry and strategic signaling, especially in double-extortion scenarios. While these approaches provide strong analytical insight, they often simplify real-world constraints and organizational complexity.

In contrast, organizational and behavioral studies (e.g., [152–154]) emphasize practical response challenges, including user susceptibility, communication failures, and incident coordination. These works show that effective defense requires *socio-technical integration*, combining technical controls with user awareness and response planning. However, their findings are often context-specific and less generalizable.

Policy and governance research (e.g., [155–158]) focuses on risk management, regulatory coordination, and cyber insurance. Compared to technical defenses, these approaches address systemic issues such as incentives and preparedness, but introduce trade-offs: for example, cyber insurance can improve resilience while potentially encouraging ransom payments.

Overall, the comparison reveals a central issue: *analytical optimality vs. real-world practicality*. Economic models provide decision frameworks, behavioral studies capture organizational realities, and policy approaches shape incentives, but none of these is useful as a stand alone approach. Effective ransomware response requires integrating these perspectives with technical defenses in a unified framework.

Open Issues: Decision-making remains highly uncertain, with limited guidance on ransom payment and negotiation. Misaligned incentives (e.g., insurance and payment dynamics) may encourage attackers, while Small and Medium Enterprises (SMEs) often lack resources for effective response. These challenges correspond to **C9** (economic and policy factors).

Fig. 3 illustrates a cross-layer ransomware defense architecture in which telemetry from host, network, storage, and organizational layers is analyzed both locally and jointly. Behavioral analytics, ML/DL-based scoring, and deception- or storage-oriented mechanisms feed a central correlation engine that interacts with SIEM/EDR/NDR components and an automated response orchestrator. This design reflects a defense-in-depth philosophy: host-level monitoring supports early execution-stage detection, network-level analytics improve visibility into C&C and exfiltration, storage-level defenses help contain encryption damage, and recovery mechanisms provide resilience when prevention fails. The feedback loop is critical for long-term robustness, since ransomware tactics evolve rapidly and require continuous model updates, rule refinement, and policy adaptation.

On the other hand, Fig. 4 presents a cross-layer view of ransomware defense, integrating technical, economic, and human/policy dimensions into a unified response framework. At the top layer, technical defenses–such as advanced detection mechanisms, deception detection strategies, hardware-assisted protection, and backup/recovery systems–provide the core capability for identifying and mitigating attacks. However, these mechanisms alone are insufficient, as reflected in the middle layer, where economic constraints and human/policy factors shape real-world decision-making. Organizations must balance cost-benefit considerations, cyber insurance incentives, user awareness, and regulatory requirements, often under uncertainty, as highlighted by the central "decision dilemmas" (e.g., whether to pay or resist). The bottom layer emphasizes that effective ransomware defense ultimately depends on coordinated response, combining incident management, risk mitigation, and continuous adaptation across all layers. The key insight is that ransomware defense is not purely a technical problem but a socio-technical challenge, where robust protection emerges only through tight integration of detection technologies, economic incentives, and human-centered policies.

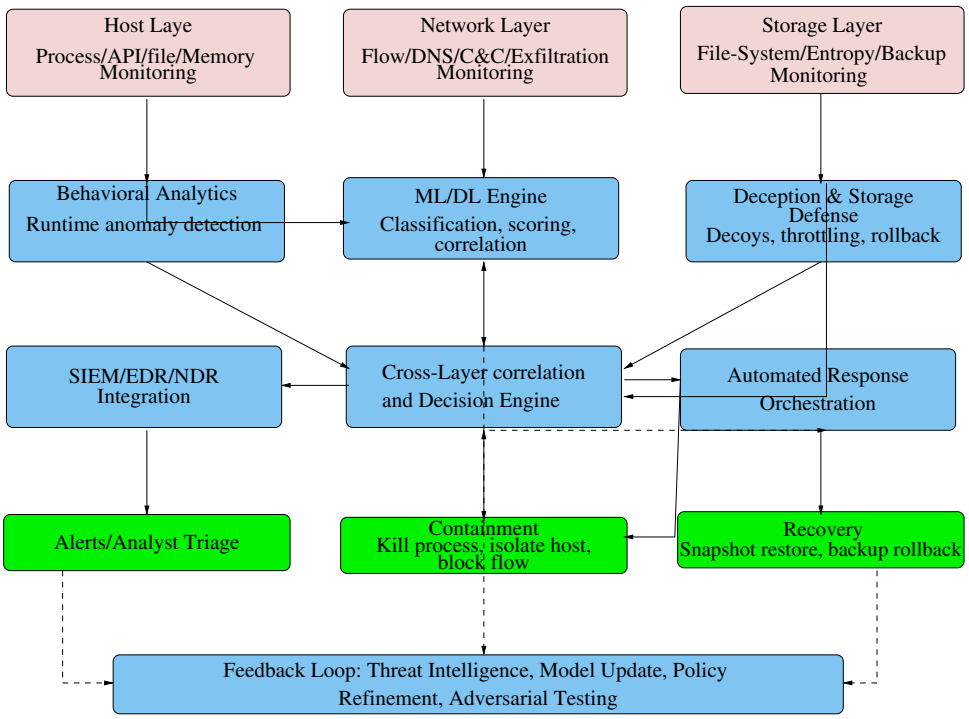

Figure 3: Cross-layer ransomware defense architecture showing how host, network, storage, and organizational defenses interact through shared analytics, correlation, response orchestration, and feedback-driven adaptation.

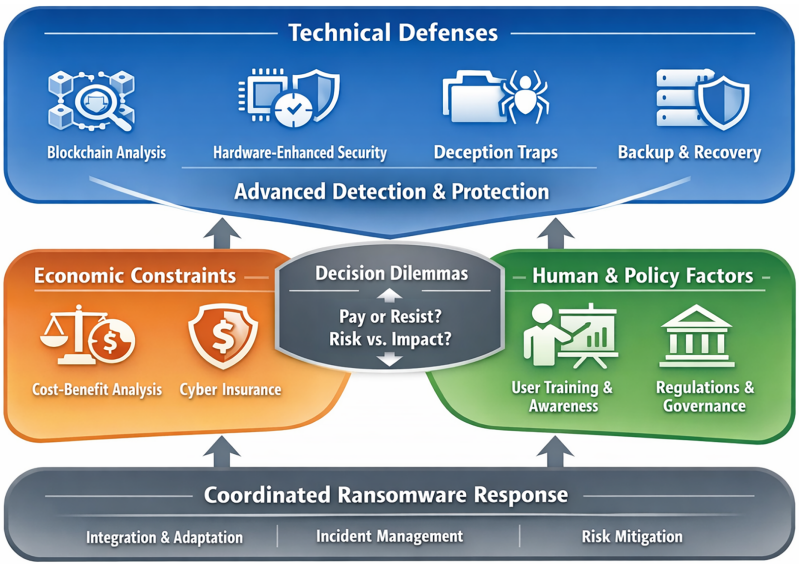

Figure 4: Cross-layer view of ransomware defense, integrating technical, economic, and human/policy dimensions into a unified response framework.

4.2.6 Game-Theoretic, Economic, and Policy Analysis of Ransomware

Ransomware can be viewed as an *economic ecosystem* driven by incentives, strategic interactions, and market structures. Existing work can be broadly grouped into *economic analyses*, *game-theoretic models*, *ecosystem/market studies*, and *policy/governance perspectives*, each capturing different facets of the ransomware economy.

Economic analyses (e.g., [159,160]) highlight that ransomware profitability is driven by weak organizational preparedness and the ability of attackers to optimize ransom pricing, including price discrimination across victims. These studies emphasize that ransomware persists because it is *economically viable*, but they often abstract away operational complexities.

Game-theoretic models (e.g., [161–163]) formalize attacker-victim interactions, showing how decisions on payment, prevention, and negotiation depend on incentives, information asymmetry, and expected losses. Compared to empirical studies, they provide analytical insights into optimal strategies, but rely on simplifying assumptions that may not capture real-world uncertainty and multi-stage attack dynamics.

Ecosystem-level studies (e.g., [164–167]) reveal that modern ransomware operates as a structured market, particularly through Ransomware-as-a-Service (RaaS) models, with affiliate-based operations, revenue sharing, and laundering mechanisms. These works provide realistic views of attacker operations, but are largely descriptive and less predictive.

Policy and governance research (e.g., [168–170]) addresses regulatory responses, attribution challenges, and the role of institutions. Compared to technical defenses, these approaches target systemic incentives, but face difficulties due to limited visibility, evolving attacker identities, and enforcement challenges.

Overall, the comparison highlights a key tension: *analytical insight vs. real-world complexity*. Economic and game-theoretic models explain incentives, ecosystem studies capture operational realities, and policy approaches shape responses, but none alone provides a complete solution. Effective mitigation requires aligning incentives across technical, organizational, and regulatory layers.

Open Issues: Existing models rely on simplified assumptions and limited empirical data, particularly for ransom payments and negotiation dynamics. The rise of RaaS further complicates incentive structures and attribution. These challenges correspond to **C9** (economic factors).

4.2.7 Foundational, Taxonomy, and Benchmarking Studies

This body of work provides cross-cutting perspectives on ransomware, including *evolution analysis, taxonomies, datasets, and benchmarking frameworks*. Unlike detection-specific studies, these efforts aim to structure the problem space, enable reproducibility, and provide broader contextual understanding.

Early studies (e.g., [171–175]) focus on the evolution of ransomware and its economic and technical drivers, highlighting why traditional defenses fail and emphasizing the need for specialized, proactive strategies. These works provide foundational insight but are largely descriptive and limited in methodological rigor.

Taxonomy-driven research (e.g., [176–178]) introduces structured models of ransomware behavior and attack lifecycles. Compared to early descriptive studies, these frameworks enable systematic analysis and mapping of defenses, but often remain static and may not fully capture rapidly evolving attack strategies.

A complementary line of work focuses on datasets and experimental platforms (e.g., [179–182]), providing benchmarks for evaluating detection methods. These contributions improve reproducibility and facilitate comparative evaluation, but their effectiveness is constrained by dataset realism and coverage of modern attack behaviors.

Other studies propose context-specific frameworks (e.g., [183–185]) tailored to particular environments such as enterprise systems or IoT, highlighting the need for domain-aware defenses. Finally, meta-analyses (e.g., [186,187]) reveal research trends, notably the dominance of detection-focused approaches and the relative lack of work on proactive and predictive defenses.

Overall, the comparison highlights a key progression: *descriptive analyses → structured taxonomies → benchmark-driven evaluation*. While these studies provide essential foundations and standardization, they remain limited by static models, outdated datasets, and insufficient alignment with evolving ransomware behaviors.

Open Issues: Existing datasets fail to capture the complexity of modern attacks, particularly regarding scale and diversity. Without standardized evaluation frameworks or longitudinal benchmarks, it remains difficult to ensure reproducibility or conduct fair performance comparisons across the field.

4.2.8 Emerging Ransomware Threat Models and Novel Attack Vectors

Recent research shows that ransomware is evolving beyond traditional file-encryption attacks toward *multi-stage, cross-layer, and non-traditional threat models*. The threat landscape encompasses hardware-level vulnerabilities, web-based infection vectors, and fileless execution techniques. Additionally, modern campaigns frequently combine encryption with data exfiltration and multi-layered extortion strategies.

Hardware- and storage-level studies (e.g., [188,189]) demonstrate that ransomware can operate below the OS layer, exploiting hardware trojans or SSD internals. Compared to software-based attacks, these approaches are more stealthy and harder to detect, but require specialized attacker capabilities, highlighting a trade-off between *attack stealth and feasibility*.

In contrast, web- and automation-based attacks (e.g., [190,191]) exploit modern browser APIs and automation frameworks to encrypt data without traditional malware installation. These methods significantly expand the attack surface, trading *ease of deployment for reduced persistence and control*.

Other works redefine ransomware threat models to account for fileless, human-operated, and exfiltration-driven attacks (e.g., [192,193]). Compared to earlier models that focus on encryption behavior, these frameworks emphasize *multi-stage attack chains and cross-layer coordination*, highlighting the limitations of detection systems built on outdated assumptions.

Finally, domain-specific studies (e.g., [194]) show that ransomware increasingly targets critical infrastructure, where attacks involve prolonged dwell time and complex system interactions. These environments require *sector-specific defenses and forensic capabilities*, rather than generic detection approaches.

Overall, the comparison reveals a fundamental shift: *from single-stage encryption attacks to adaptive, cross-layer, and hybrid threat models*. While new attack vectors improve stealth and impact, they also expose gaps in existing defenses, which remain largely focused on traditional behavioral or file-based indicators.

Open Issues: Modern ransomware combines exfiltration, fileless execution, and cross-layer techniques across cloud, browser, and hardware platforms. Existing defenses struggle to handle such hybrid, multi-stage attacks, highlighting the need for integrated and adaptive detection frameworks. These challenges correspond to **C10** (emerging threat models) and **C7** (cross-layer coordination).

4.2.9 Proactive Prevention via File Perturbation and OS Hardening

Proactive defenses aim to *prevent encryption before it occurs* by disrupting ransomware's ability to locate or access valuable data. Unlike detection-based methods, these approaches focus on *attack surface manipulation* rather than identifying malicious behavior.

File perturbation and moving-target strategies (e.g., [195–197]) randomize file extensions, hide file locations, or dynamically alter system visibility to confuse ransomware during reconnaissance and encryption phases. Compared to reactive defenses, these methods can reduce attack success without requiring detection, but rely on the assumption that ransomware uses predictable file discovery mechanisms.

Overall, these approaches highlight a key trade-off: *prevention vs. usability*. While they can significantly disrupt ransomware workflows, they may introduce compatibility issues and user overhead, and can be bypassed by adaptive malware performing deeper file-system inspection.

Open Issues: Effectiveness is limited by usability constraints and attacker adaptation. Real-world scalability remains underexplored, and integration with detection mechanisms is limited. These challenges correspond to **C6** (deployment constraints).

4.2.10 Healthcare/Operational Impact Studies of Ransomware Attacks

Several studies examine the real-world operational and clinical consequences of ransomware attacks on healthcare organizations. Zhao et al. [198] present an early case study of a ransomware incident affecting a trauma center, demonstrating how disruptions to hospital information systems can significantly impair clinical workflows and delay patient care. Expanding this perspective, Neprash et al. [199] conduct a large-scale cohort analysis of 374 ransomware incidents affecting healthcare delivery organizations between 2016 and 2021. Their study reveals that ransomware attacks more than doubled during this period and exposed the personal health information of nearly 42 million patients, with increasingly large healthcare systems becoming primary targets. Complementing these findings, Dameff et al. [200] analyze the indirect operational consequences of a prolonged ransomware attack by examining patient flow data from two nearby emergency departments that were not directly targeted. Their analysis shows significant increases in patient volume, ambulance arrivals, wait times, emergency service diversion, and delays in critical treatments such as stroke care; These studies provide empirical evidence that ransomware attacks can cause widespread operational disruption within healthcare systems, affecting not only targeted facilities but also surrounding medical institutions and ultimately impacting patient safety and quality of care.

Open Issues: Empirical studies on ransomware impact in critical sectors remain limited, and the effects on operational continuity and patient outcomes are difficult to quantify. Inconsistent reporting and reliance on legacy infrastructure further complicate risk assessment and resilience planning. These limitations correspond to **C1** (data gaps) and **C6** (deployment challenges).

Table 9 summarizes prevention-, mitigation-, and recovery-focused ransomware research, along with their corresponding defense/recovery mechanisms and representative references. On the other hand, Table 10 provides a multi-dimensional view of ransomware research across three critical dimensions: threat models, defense layers, and adversarial capabilities.

Table 9: Summary of prevention, mitigation, and recovery-focused ransomware research.

Category	Defense/Recovery Strategy	Representative References
Storage-Level/Hardware-Assisted Defense	Prevent data loss and enable recovery using SSDs, block devices, firmware, or hypervisors	Min et al. [125] (2018); Baek et al. [126] (2018); Baek et al. [127] (2020); Paik et al. [128] (2018); Elkhail et al. [129] (2023); Elkhail et al. [130] (2023); Wang et al. [131] (2024); Hill et al. [132] (2024); Zhu et al. [133] (2025)

(Continued)

Table 9 (continued)

Category	Defense/Recovery Strategy	Representative References
Decoy, Honeypot & Deception-Based Defense	Lure and contain ransomware using decoy files, honeyfolders, and deceptive environments	Gomez-Hernandez et al. [134] (2018); Chakkaravarthy et al. [135] (2020); Ganfure et al. [136] (2023); Berardi et al. [137] (2023); Sajid et al. [138] (2025)
Reverse Engineering & Decryption	Analyze encryption schemes and recover encrypted data	Filiz et al. [139] (2021); Yuste et al. [140] (2021); Kim et al. [141] (2022); Kim et al. [142] (2025); Almomani et al. [143] (2023); Hou et al. [146] (2025)
Backup, Key Management & File Recovery	Recover encrypted data via secure backups, key escrow, or entropy-based restoration	Lee et al. [144] (2019); Davies et al. [145] (2021)
Human factors, Organizational & Policy Responses	Ransom decision-making, negotiation strategies, insurance, and governance	Everett et al. [147] (2016); Mansfield-Devine et al. [148] (2016); Connolly et al. [149] (2022); Ryan et al. [150] (2022); Meurs et al. [151] (2024); Zhang-Kennedy et al. [152] (2018); Connolly et al. [153] (2019); Thomas et al. [154] (2018); Hayes et al. [155] (2021); Bekkers et al. [156] (2023); Mott et al. [157] (2023); Bajpai et al. [158] (2023)
Game-Theoretic, Economic & Policy Analysis & RaaS Analysis	Analyze ransomware business models, payments, and underground markets	Simmonds et al. [159] (2017); Hernandez-Castro et al. [160] (2020); Cartwright et al. [161] (2019); Zhang et al. [162] (2022); Li et al. [163] (2022); Meland et al. [164] (2020); Chauhan et al. [165] (2023); Oosthoek et al. [166] (2023); Phipps et al. [167] (2025); Delgado-Mohatar et al. [168]; Adams et al. [169] (2025); van der Horst et al. [170] (2025) (2020)

(Continued)

Table 9 (continued)

Category	Defense/Recovery Strategy	Representative References
Taxonomies, Attack Evolution, Threat Landscape, and Datasets Dynamic Analysis Insights	Provide taxonomies, datasets, benchmarks, and meta-analyses	Brewer et al. [171] (2016); Furnell et al. [172] (2017); Srinivasan et al. [173] (2017); OKane et al. [174] (2018); Kharraz et al. [175] (2018); Dargahi et al. [176] (2019); Hull et al. [177] (2019); Keshavarzi et al. [178] (2020); Berrueta et al. [179] (2020); Hirano et al. [181]; Diamantopoulos et al. [182] (2024); Molina et al. [183] (2023); McDonald et al. [184] (2022); Humayun et al. [185] (2021); Razaulla et al. [186] (2023); Benmalek et al. [187] (2024)
Emerging Threat Models & Novel Attack Vectors	Study browser-based, hardware, and next-generation ransomware threats	Almeida et al. [188] (2022); Reidys et al. [189] (2022); Oz et al. [190] (2023); Rana et al. [191] (2024); McIntosh et al. [192] (2023); Raj et al. [193] (2024); Chimmanee et al. [194] (2024)
Healthcare/Operational Impact Studies	Document real-world ransomware impacts on clinical operations and patient care metrics	Zhao et al. [198] (2018); Neprash et al. [199] (2022); Dameff et al. [200] (2023)
Proactive Host Defense (Moving Target/Hardening)	Prevent encryption success via proactive file/extension perturbations or OS hardening techniques	Lee et al. [195] (2019); Lee et al. [196] (2023); Khan et al. [197] (2023)

Table 10: Multi-dimensional taxonomy of ransomware research across threat models, defense layers, and adversarial capabilities.

Category	Threat Model Dimension	Defense Layer	Adversarial Capability Level
Signature/Static Detection	Aggressive, known ransomware; predictable behavior	Host (file, API, binary)	Low—Relies on known patterns; easily evaded via obfuscation/packing
Behavioral/Runtime Detection	Moderate to stealthy; observable runtime patterns (file I/O, entropy)	Host + OS	Medium—Evades via slow encryption, mimicry, or distributed execution

(Continued)

Table 10 (continued)

Category	Threat Model Dimension	Defense Layer	Adversarial Capability Level
ML/DL-based Detection	Generalized (known + unknown variants); data-driven threat modeling	Host + Network + Hybrid	Medium–High—Vulnerable to adversarial examples, drift, poisoning
Semi-supervised/Zero-shot/ Drift-aware	Unseen, evolving, and adaptive ransomware	Cross-layer (Host + Data + Model)	High—Targets unknown threats but sensitive to distribution shift and data bias
Network/SDN-based Detection	Propagation, C&C communication, lateral movement	Network/SDN	Medium–High—Limited by encryption, tunneling, and stealth channels
Storage/Hardware-level Defenses	Aggressive encryption and overwrite-heavy attacks	Storage/Firmware/ Hardware	Low–Medium—Bypassed by selective encryption, exfiltration, or logic-based attacks
Deception/Honeypot-based	Interaction-driven attacks (file discovery, scanning)	Host + File system	Medium—Evaded via decoy detection, fingerprinting, or avoidance strategies
Proactive Prevention (MTD, OS hardening)	Reconnaissance-driven attacks; predictable file targeting	Host + OS	Medium–High—Bypassed via adaptive discovery or deeper inspection
Recovery/Backup-based	Post-compromise scenarios; encryption and data loss	Storage + Cloud	Low—Fails if backups are deleted, exfiltrated, or corrupted
Reverse Engineering/Decryption	Specific ransomware families with implementation flaws	Forensic/Post-attack	Low—Works only for vulnerable implementations; not generalizable
Blockchain/Payment Analysis	Financial flows, ransom payments, attribution	Economic/Network	Medium–High—Limited by mixers, privacy coins, cross-chain laundering

(Continued)

Table 10 (continued)

Category	Threat Model Dimension	Defense Layer	Adversarial Capability Level
Human/Organizational/ Policy	Decision-making, negotiation, socio-economic behavior	Human + Policy layer	High—Influenced by uncertainty, incentives, and incomplete information
Emerging Threat Models (Hardware, Browser, CPS)	Stealthy, cross-layer, multi-stage attacks (exfiltration, fileless, hybrid)	Cross-layer (Hardware + Cloud + CPS)	Very High—Exploits system-wide blind spots and integration gaps

4.2.11 Miscellaneous Approaches for Ransomware Detection, Prevention, and Mitigation

This category includes diverse approaches that complement traditional detection and defense mechanisms, spanning forensic analysis, learning-based detection, and analytical modeling. These methods provide valuable auxiliary capabilities but are often specialized and less integrated into end-to-end defense frameworks.

Forensic and intelligence-driven approaches (e.g., [201,202]) focus on post-incident analysis, extracting artifacts such as ransom messages and identifying common attack patterns using frameworks like MITRE ATT&CK. Compared to real-time detection methods, these approaches enhance attribution and situational awareness but are inherently reactive and do not prevent attacks. In contrast, system-level and learning-based techniques (e.g., [203,204]) emphasize efficient runtime detection using advanced models or low-level instrumentation (e.g., eBPF). These methods achieve strong detection performance with low overhead, but their effectiveness depends on environment-specific assumptions and deployment constraints.

Other works explore alternative analytical models, including statistical methods, adversarially robust heuristics, and epidemiological modeling (e.g., [145,205,206]). While these approaches broaden the analytical perspective and improve robustness in specific scenarios, they remain limited in generalizability and integration with broader defense systems.

Open Issues: These approaches are often fragmented and rely on environment-specific assumptions, limiting scalability and generalization. Integration with threat intelligence, forensic pipelines, and standardized evaluation frameworks remains limited, highlighting challenges in **C6** (integration) and **C7** (cross-layer coordination).

Overall, the above subsection-specific limitations collectively map to the cross-cutting challenges (C1–C10), providing a unified view of open research directions across the ransomware defense landscape.

4.2.12 Limitations of Existing Recovery Mechanisms

Compared to detection, ransomware recovery remains underexplored. Most existing approaches assume the availability of uncompromised backups, which is increasingly unrealistic as modern ransomware targets backup systems and incorporates data exfiltration.

Furthermore, recovery strategies often lack: (i) integration with detection systems, (ii) mechanisms for selective or partial recovery, (iii) consideration of data integrity and consistency, (iv) alignment with

organizational response workflows. Future research should focus on adaptive recovery frameworks that combine secure backups, anomaly-aware restoration, and policy-driven response mechanisms.

4.2.13 Deployment Challenges in Real-World Environments

Despite promising results, many ransomware defense techniques face significant barriers to real-world deployment. These include:

Performance overhead: Kernel-level monitoring and deep learning models introduce latency and resource consumption.

Scalability: Solutions often fail to scale across cloud-native, multi-tenant, or distributed environments.

Compatibility: Many approaches require modifications to OS, firmware, or applications, limiting adoption.

Operational integration: Limited integration with SOC workflows, SIEM systems, and incident response pipelines.

Privacy constraints: Monitoring approaches may conflict with regulatory requirements.

Addressing these challenges is essential for transitioning research prototypes into deployable solutions.

4.2.14 Challenges in Ensuring Adversarial Robustness

Ransomware detection systems are increasingly vulnerable to adversarial manipulation. Attackers can evade detection by mimicking benign behavior, injecting noise into feature space, or exploiting weaknesses in model training.

Existing work often lacks: (i) standardized adversarial evaluation benchmarks, (ii) robustness analysis across different attack models, (iii) defenses against poisoning and model extraction attacks.

Future systems must incorporate adversarial training, invariant feature design, and continuous adaptation to evolving threat strategies.

4.2.15 Evaluation Challenges and Standardization

A major weakness in current ransomware research is the lack of standardized and realistic evaluation practices. Many studies rely on small, outdated, or highly curated datasets that do not reflect modern ransomware behaviors such as selective encryption, low-and-slow attacks, data exfiltration, fileless execution, and multi-stage extortion. As a result, reported performance is often difficult to compare across studies and may overestimate real-world effectiveness. This problem is compounded by inconsistent experimental settings, different feature extraction pipelines, and limited cross-dataset or longitudinal validation.

To address these issues, the community needs benchmark datasets that are continuously updated, diverse, and representative of multiple deployment contexts, including endpoints, cloud platforms, mobile devices, IoT/IIoT systems, and critical infrastructure. Such datasets should include benign workloads, realistic user behavior, recent ransomware families, and attack traces spanning pre-encryption, encryption, exfiltration, and recovery phases. Standard evaluation protocols are also needed to improve reproducibility and fairness. These should specify train/test dataset splits, temporal validation, cross-dataset testing, ablation studies, adversarial evaluation, and reporting of computational overhead and deployment assumptions.

Equally important is the use of metrics tailored to ransomware rather than relying solely on generic ML measures such as accuracy or F1-score. Since ransomware causes progressive harm over time, metrics such as *time-to-detection*, *files protected before detection*, *damage prevented*, *recovery success rate*, *false alarm cost*, and *system overhead* are often more informative than aggregate classification accuracy. Current evaluation

practices are insufficient because they rarely capture operational impact, adversarial adaptation, or usability trade-offs, and they often ignore whether a method remains effective under realistic deployment constraints. Therefore, future work should move toward standardized, deployment-aware, and ransomware-specific evaluation frameworks that better reflect real-world defensive requirements.

4.2.16 Critical Insights and Lessons Learned from Research Works on Ransomware Prevention, Mitigation, and Recovery-Focused Research Works

Critical Insights and Lessons Learned: Research on ransomware prevention, mitigation, and recovery reveals several important insights that highlight both progress and persistent limitations in current defense strategies.

First, no single defense mechanism is sufficient. Effective ransomware protection requires a *multi-layered and defense-in-depth approach* that combines prevention (e.g., access control, patching), detection (behavioral or ML-based), mitigation (network isolation, process termination), and recovery (backup and restoration). Studies consistently show that isolated solutions fail against modern, multi-stage ransomware attacks. Second, many prevention mechanisms rely on assumptions that are increasingly invalid. Techniques such as signature-based detection or pre-encryption behavioral monitoring assume predictable attack patterns, yet modern ransomware employs stealthy execution, obfuscation, and delayed or selective encryption to evade such defenses. This highlights a fundamental gap between research assumptions and real-world adversarial behavior.

Third, mitigation strategies are often reactive and depend on timely detection. Approaches such as process termination, SDN-based traffic blocking, or access revocation can limit damage, but their effectiveness diminishes significantly if detection is delayed. As a result, mitigation alone cannot guarantee protection, particularly in fast-moving or low-and-slow attack scenarios. Fourth, recovery remains a critical yet underdeveloped component. While backup-based recovery is widely adopted, many studies assume that backups are intact and readily accessible. In practice, modern ransomware targets backup systems and incorporates data exfiltration, making recovery incomplete or insufficient for addressing extortion risks.

Fifth, there is a growing shift from prevention-centric to resilience-oriented security models. Traditional approaches prioritized preventing attacks entirely, but recent research emphasizes the importance of rapid recovery, system resilience, and operational continuity in the face of inevitable breaches. Finally, a key lesson is the need for *cross-layer and adaptive defense frameworks*. Current approaches are fragmented across host, network, storage, and organizational layers, whereas ransomware operates across all these layers simultaneously. Future solutions must integrate detection, mitigation, recovery, and policy-level responses into unified, adaptive, and adversarially robust systems.

5 Research Works Published during the Years 2022–2025, Not Discussed in This Paper

In this section, we provide references to additional relevant studies, including peer-reviewed conference papers, technical reports, and unrefereed preprints, that fall outside the primary scope of this survey and are therefore not discussed in detail. The inclusion of these works highlights the sustained and growing research activity in this area since 2022. In particular, several conference publications from 2022 onward [207–215] reflect increasing academic interest and continued methodological development.

Furthermore, a large body of technical reports and preprints published since 2022 [216–276] further demonstrates the breadth and momentum of ongoing research efforts. While many of these works are preliminary and have not yet undergone full peer review, they provide early insights into emerging directions and reinforce the observation that this research area remains active and rapidly evolving.

6 Summary of Open Issues and Research Directions

In this section, we summarize the key open issues associated with the ransomware detection, prevention, and mitigation techniques reviewed in this paper, and we further highlight critical challenges that remain unresolved across these areas. By synthesizing limitations observed in existing approaches, this section outlines promising directions for future research aimed at improving the robustness, scalability, and real-world effectiveness of ransomware defenses.

6.1 Grand Challenges in Ransomware Defense

Despite extensive research across detection, prevention, mitigation, and recovery, ransomware defense continues to face several fundamental and unresolved challenges. A primary limitation lies in the *disconnect between research and real-world deployment*. Many proposed solutions are evaluated on curated or outdated datasets under simplified threat models, leading to inflated performance claims and limited generalization to evolving ransomware behaviors. At the same time, adversarial robustness remains insufficiently addressed, as modern ransomware increasingly employs stealthy execution, adaptive strategies, and evasion techniques that undermine both machine-learning–based and behavioral detection systems.

A second major challenge is the *lack of cross-layer integration*. Existing defenses are often developed in isolation—spanning host, network, storage, and application layers—without standardized interfaces or coordinated response mechanisms. This fragmentation limits visibility into multi-stage attacks and reduces the overall effectiveness of otherwise strong point solutions. Furthermore, prevention and recovery mechanisms frequently rely on fragile assumptions, such as predictable encryption patterns or intact backups, which are increasingly violated by modern ransomware incorporating selective encryption, data exfiltration, and backup targeting.

Another critical issue is the *trade-off between security, usability, and deployability*. Lightweight and scalable solutions are needed for resource-constrained environments (e.g., IoT, edge, and cloud), yet many high-accuracy approaches require significant computational resources or system modifications. Similarly, proactive defenses such as file perturbation and deception mechanisms can impact usability and introduce operational complexity. These constraints are further exacerbated by the absence of standardized benchmarks, longitudinal datasets, and realistic evaluation frameworks that capture long-term attacker–defender co-evolution.

Finally, ransomware is inherently a *socio-technical problem*, extending beyond purely technical defenses. Economic incentives, cyber-insurance dynamics, regulatory inconsistencies, and challenges in attribution and payment tracking all influence attacker behavior and victim response. Current research often treats these dimensions independently, resulting in fragmented solutions that fail to address the broader ecosystem.

Key Insight: Addressing these grand challenges requires a shift toward *integrated, cross-layer, and adversarially robust defense frameworks* that combine technical mechanisms with economic, organizational, and policy considerations. Future solutions must emphasize realistic evaluation, adaptive learning, explainability, and seamless deployment to achieve sustainable and resilient ransomware.

Fig. 5 illustrates the key cross-layer challenges in ransomware defense, highlighting that effective protection is constrained by multiple interdependent factors. Technical limitations such as data and benchmarking gaps, adversarial robustness, and cross-layer integration issues interact with system-level concerns including scalability and usability trade-offs. These challenges are further compounded by economic, policy, and human factors that shape real-world deployment and response strategies. The figure emphasizes that ransomware defense is not a single-layer problem but a *multi-dimensional challenge* requiring coordinated solutions across technical, operational, and socio-economic domains.

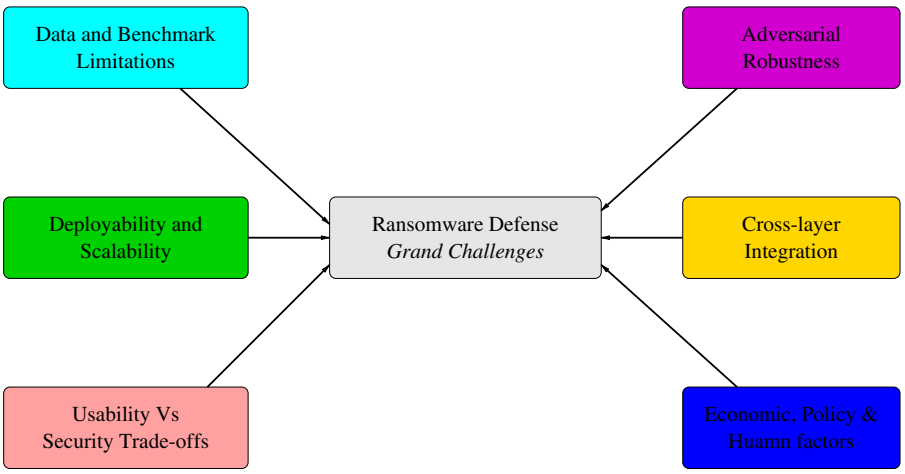

Figure 5: Grand challenges in ransomware defense: a cross-layer synthesis of technical, operational, and socio-economic limitations. Response framework.

Taxonomy Insights: Table 10 provides a multi-dimensional view of ransomware research across three critical dimensions: threat models, defense layers, and adversarial capabilities. A key observation is that low-level defenses (e.g., signature-based, storage-level) are effective against simple and aggressive attacks but fail under stealthy or adaptive threat models. In contrast, advanced approaches (e.g., ML/DL, zero-shot, and cross-layer defenses) target more sophisticated ransomware but introduce dependencies on data quality, system integration, and robustness against adversarial manipulation.

Another important insight is the increasing shift from single-layer defenses (host or network) toward *cross-layer strategies* that combine host, network, storage, and human factors. This shift is driven by the rise of high-capability adversaries who exploit multiple attack surfaces simultaneously. However, no single approach provides complete coverage, highlighting a fundamental gap between isolated defense mechanisms and real-world, multi-stage attack scenarios. Consequently, effective ransomware defense requires integrated, adaptive, and adversarially aware frameworks that align technical, economic, and organizational layers.

Table 11 highlights that ransomware defense remains fundamentally challenged by the gap between controlled research assumptions and the complexity of real-world attack environments. Across detection paradigms, a recurring limitation is the reliance on static datasets, handcrafted features, or high-cost models that struggle with stealthy, adaptive, and adversarial ransomware behaviors. Similarly, system-level defenses–ranging from storage and network mechanisms to deception and backup strategies–often face deployability constraints, and scalability issues in heterogeneous and resource-constrained environments such as IoT and CPS. The table also underscores that non-technical dimensions, including economic incentives, human decision-making, and policy limitations, play a critical role in shaping ransomware resilience. Overall, these observations point to the need for unified, cross-layer, and adversarially robust defense frameworks, supported by realistic datasets, standardized benchmarks, and closer integration between technical, organizational, and economic perspectives.

Table 11: Refined summary of open issues in ransomware research.

Area	Key Limitations	Implications
Behavioral Detection	Stealthy, delayed, or selective encryption weakens behavior-based assumptions; kernel/API monitoring incurs overhead; ML models remain vulnerable to adversarial manipulation; lack of realistic datasets and explainability.	Need lightweight monitoring, adversarially robust features, explainable detection models, and standardized real-world datasets.
Classical ML	Dependence on handcrafted features vulnerable to obfuscation; limited generalization due to curated datasets; dataset imbalance and concept drift; limited study of adversarial ML threats.	Need to emphasis on adaptive learning, robust feature engineering, adversarial resilience, and integration of XAI with human-in-the-loop validation.
Deep Learning	Requires large labeled datasets and high computational cost; vulnerable to adversarial examples and traffic manipulation; explanation fidelity remains uncertain.	Need development of lightweight architectures, robust training methods, trustworthy XAI, and privacy-preserving/federated learning frameworks.
Semi/Zero-shot Detection	Strong dependence on quality of unlabeled or synthetic data; difficulty capturing evolving ransomware semantics.	Need improved generative models, secure online learning, and long-term benchmarks for evolving threats.
Network/SDN Detection	Encrypted traffic reduces visibility; modern C&C channels use P2P, blockchain, or cloud services; SDN integration complexity; high false positives.	Research on encrypted traffic analytics, scalable SDN orchestration, adversarially robust traffic analysis, and cross-layer correlation.
Mobile/Android Detection	Resource constraints limit monitoring; obfuscation and dynamic loading hinder analysis; privacy restrictions limit feature extraction.	Need energy-efficient detection, hybrid static-dynamic analysis, and privacy-preserving monitoring frameworks.
IoT/IIoT/CPS Environments	Strict resource and safety constraints; heterogeneous legacy systems; federated learning risks; limited protocol visibility.	Need to focus on lightweight models, secure federated learning, interoperability, and safety-aware defense mechanisms.
Adversarial Robustness	Ransomware can mimic benign behavior, distribute workloads, or poison training data; defenses introduce overhead.	Need standardized adversarial benchmarks, invariant behavioral features, and resilient detection architectures.

(Continued)

Table 11 (continued)

Area	Key Limitations	Implications
Blockchain Analysis	Mixers and privacy services hinder attribution; cross-chain transfers reduce visibility; lack of ground-truth data.	Need improved blockchain analytics, cross-chain tracing, better datasets, and collaboration with law enforcement.
Storage/Hardware Defenses	Require firmware/hardware changes; assume overwrite-heavy behavior; cross-layer semantic gaps; cloud overhead.	Need portable defenses, cross-layer architectures, and explainable hardware-level telemetry.
Deception-based Defense	Effectiveness depends on decoy placement; advanced ransomware can detect honeypots; deployment overhead.	Need to develop adaptive deception frameworks integrated with behavioral detection.
Reverse Engineering	Strong cryptography and heavy obfuscation complicate analysis; decryption often family-specific.	Need automated reverse-engineering tools and scalable malware analysis frameworks.
Backup/Recovery	Ransomware targets backups; entropy-based detection yields false positives; storage overhead; selective encryption evasion.	Need to use tamper-resistant backups, adaptive recovery strategies, and cross-platform restoration mechanisms.
Human/Organizational Factors	Decision-making under uncertainty; misaligned incentives from ransom payments; limited SME preparedness.	Need improved governance, incident-response policies, and coordinated international strategies.
Economic Modeling	Simplified assumptions; limited empirical data; complex RaaS ecosystems.	Need better datasets, refined economic models, and policy-driven disruption strategies.
Datasets/Benchmarks	Lack of scale, realism, and diversity; absence of standardized evaluation; limited coverage of emerging systems.	Need to develop shared datasets, reproducible benchmarks, and unified evaluation frameworks.
Emerging Threats	Rise of fileless attacks, data exfiltration, and cross-layer ransomware targeting cloud and hardware.	Need integrated, multi-layer defense frameworks combining host, network, and cloud telemetry.
File Perturbation/OS Hardening	May affect usability; attackers can bypass via deeper inspection; limited real-world evaluation.	Need scalable deployment strategies integrated with detection and access control.
Miscellaneous Techniques	Reliance on environment-specific assumptions; heuristic approaches are evasion-prone; limited integration.	Need unified architectures combining detection, forensics, and predictive analytics.

(Continued)

Table 11 (continued)

Area	Key Limitations	Implications
Healthcare Impact	Limited empirical data; inconsistent reporting; difficulty quantifying patient impact.	Need longitudinal datasets, standardized reporting, and cyber-resilience frameworks for critical sectors.

Table 12 provides a higher-level, cross-cutting perspective on ransomware challenges, emphasizing systemic issues such as deployability, cross-layer coordination, assumption fragility, and economic or policy misalignment that span detection, prevention, mitigation, and recovery. In contrast to Table 11, which organizes open issues in a fine-grained, technique- and domain-specific manner (e.g., ML, DL, IoT, blockchain, storage), this table abstracts these challenges into broader thematic categories that highlight fundamental limitations affecting the entire ransomware defense lifecycle. As a result, while Table 11 is more useful for analyzing specific technical gaps within individual approaches, this table better captures system-level, operational, and cross-disciplinary challenges, underscoring the need for integrated, adaptive, and policy-aware ransomware defense strategies.

Table 12: Summary of cross-cutting open issues in ransomware detection, prevention, mitigation, and recovery.

Open-Issue Theme	Key Limitations/Gaps	Implications for Practice and Research
Deployability and Practical Adoption	Many approaches require substantial hardware/firmware/OS/browser changes, limiting retrofitting and portability across heterogeneous endpoints, cloud providers, and legacy systems; adoption is further complicated in multi-tenant and cross-VM settings.	Non-incremental solutions face high barriers to real-world adoption; defenses must be deployable, portable, and compatible with operational constraints.
Assumption Fragility and Adaptive Ransomware Behavior	Several mechanisms assume ransomwares are overwrite-heavy, support fast encryption and exhibit predictable access patterns; these assumptions are fragile against selective, slow, content-aware, logic-driven, or timing-adaptive ransomwares (e.g., partial encryption, directory traversal, staged behavior).	Defenses should be designed for strategic adversarial adaptation (not static behaviors), emphasizing robustness under adaptive and low-and-slow threat models.

(Continued)

Table 12 (continued)

Open-Issue Theme	Key Limitations/Gaps	Implications for Practice and Research
Cross-Layer Coordination and Standardization Gaps	Coordination across OS, hypervisor, storage, network, and application layers remains ad hoc; there is limited standardization of interfaces, and shared semantics for prevention and recovery.	Fragmentation reduces end-to-end visibility and weakens otherwise strong solutions; standardized interfaces and cross-layer designs are needed.
Robustness Against Adversarial Evasion	Limited evaluation under adversarial settings; resilience to evasion tactics (e.g., decoy fingerprinting, entropy manipulation, trap avoidance, similarity-metric evasion, header poisoning) is under-explored.	Without adversarially informed design and testing, attackers can systematically degrade detection, prevention, and recovery mechanisms over time.
Deception and Decoy Management Challenges	Effectiveness of placing decoy elements in the systems depends on configuration and placement; at scale, decoys introduce operational overhead, maintenance complexity, and integration challenges with other defenses.	Deception alone is brittle; it must be integrated into automated, adaptive, and coordinated defense pipelines to remain effective at scale.
Explainability, Guarantees, and Trustworthiness	Few systems provide explainable decisions, formal security guarantees, or auditable recovery logic which is problematic for regulated environments and incident response where accountability is essential.	Lack of transparency impedes trust and adoption; explainability and assurance mechanisms are needed for enterprise and critical-infrastructure use.
Data, Benchmarks, and Evaluation Limitations	Datasets are often small, platform-specific, and quickly outdated; benchmarks rarely capture modern tactics (exfiltration, living-off-the-land, multi-stage extortion); longitudinal and real-world validation is limited.	Overfitting to outdated benchmarks undermines effectiveness claims; realistic, continuously updated benchmarks and field validation are required.
Usability, Performance, and Operational Trade-offs	Preventive actions (e.g., perturbation/renaming) may harm usability and compatibility; kernel- and model-intensive defenses can add latency, energy cost, and operational fragility.	Sustainable defenses must explicitly balance security benefits against performance, reliability, and user/administrator burden.

(Continued)

Table 12 (continued)

Open-Issue Theme	Key Limitations/Gaps	Implications for Practice and Research
Recovery and Exfiltration-Centric Ransomware	Many defenses emphasize preventing encryption rather than addressing data theft, extortion pressure, and reputational harm; recovery often assumes intact backups and weakly integrates governance and response workflows.	Modern mitigation must treat exfiltration and extortion as first-class threats and integrate detection, response, governance, and recovery.
Economic, Legal, and Policy Misalignment	Ransom-payment guidance varies across jurisdictions; cyber-insurance and incentives may increase attacker profitability; attribution, smart contracts, and cross-chain laundering complicate enforcement and deterrence.	Technical mechanisms alone are insufficient; coordinated legal, economic, and policy frameworks are needed to reduce attacker incentives and impact.
Threat Intelligence Dependence and Timeliness	Many methods rely on high-quality threat intelligence or labeled data that lags emerging variants; bridging generic thresholds with organization-specific controls is unresolved.	Long-term resilience requires adaptive, intelligence-agnostic, and continuously learning systems with operationally grounded controls.
Long-Term Sustainability and Co-Evolution	Evaluations often use limited threat models and short time horizons, failing to capture attacker-defender co-evolution and sustained adaptation.	Durable defenses require continuous updating, adversarial robustness, standardized evaluation, and integration across technical and organizational domains.

Robustness Insights: Table 13 reveals that many ransomware defense approaches rely on simplifying assumptions that are increasingly invalid under modern threat models. Behavioral and storage-based methods assume observable and aggressive encryption patterns, which are bypassed by stealthy, low-and-slow attacks. Learning-based approaches, including both classical ML and deep learning, suffer from limited generalization and are vulnerable to adversarial manipulation and distribution shift. Network-based techniques are constrained by reduced visibility due to encryption and covert communication channels, while deception-based defenses are brittle against adaptive attackers. Overall, no single approach provides robust protection across evolving ransomware strategies, highlighting the need for adversarially robust, cross-layer, and deployment-aware defense frameworks.

Table 13: Robustness analysis of ransomware detection and defense approaches.

Approach	Typical Assumptions	Failure under Evasion	Robustness Limitations
Behavioral/Runtime Detection	Ransomware exhibits observable pre-encryption behaviors (e.g., rapid file writes, entropy increase).	Low-and-slow encryption, delayed execution, or selective file targeting can evade detection.	Over-reliance on short-term behavioral spikes; limited robustness to stealthy and staged attacks.
Signature-based Detection	Known ransomware patterns and signatures remain stable.	Polymorphism, packing, and code obfuscation bypass signature matching.	Completely ineffective against zero-day and rapidly evolving variants.
Classical ML-based Detection	Handcrafted features are stable and discriminative across datasets.	Feature manipulation, mimicry attacks, and adversarial perturbations degrade performance.	Poor generalization; vulnerable to evasion and concept drift.
Deep Learning-based Detection	Training data captures representative ransomware behavior; learned features generalize.	Adversarial examples, distribution shift, and unseen attack patterns reduce accuracy.	High sensitivity to data distribution; lack of interpretability limits trust and debugging.
Semi-supervised/Zero-shot Methods	Latent representations capture semantic similarity between known and unknown ransomware.	Novel ransomware with unseen behaviors or misleading feature embeddings evade detection.	Dependence on representation quality; weak guarantees under adversarial conditions.
Network-based Detection	Ransomware communication is observable via network traffic patterns.	Encrypted traffic, covert channels (e.g., DNS tunneling, HTTPS, P2P), and cloud-based C&C hide signals.	Limited visibility; high false positives; weak correlation with host-level activity.
SDN-based Mitigation	Centralized control enables timely detection and response.	Delayed detection or misclassification leads to ineffective mitigation; attackers adapt traffic patterns.	Deployment complexity; reliance on accurate upstream detection.

(Continued)

Table 13 (continued)

Approach	Typical Assumptions	Failure under Evasion	Robustness Limitations
Deception-based (Honeypots/Decoys)	Ransomware interacts with decoy files or systems.	Advanced ransomware detects and avoids decoys or delays interaction.	Brittle against adaptive attackers; effectiveness depends on placement and realism.
Storage-level/Backup-based Defense	Ransomware performs bulk overwrite encryption; backups remain intact.	Selective encryption, backup targeting, or stealthy corruption bypass protection.	Assumptions increasingly invalid; recovery fails if backups are compromised.
Memory-based Detection	Malicious artifacts are observable in volatile memory.	Memory evasion techniques (fileless malware, rapid execution) reduce detection window.	Requires continuous monitoring; high overhead; limited scalability.
Blockchain/Payment Analysis	Ransom payments can be traced via transaction patterns.	Mixers, tumblers, cross-chain transfers, and privacy coins obscure attribution.	Limited ability to link transactions to real-world actors; reactive rather than preventive.

Fig. 6 presents a taxonomy of the open issues in ransomware research detection, prevention, mitigation and recovery.

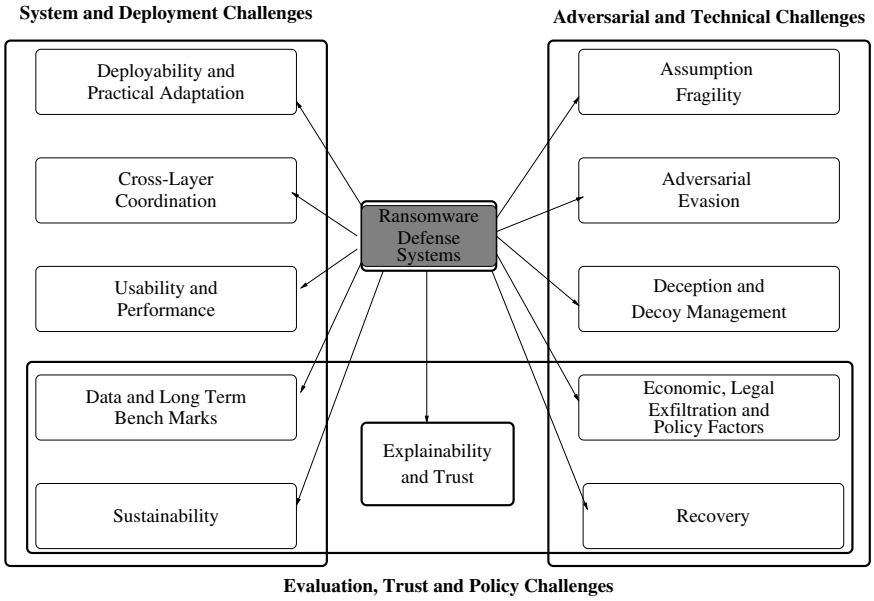

Figure 6: Taxonomy of open issues in ransomware detection, prevention, mitigation, and recovery.

Discussion: Table 14 highlights the mismatch between evolving ransomware capabilities and existing defense mechanisms. Many defenses are designed under static or simplified assumptions, whereas attackers increasingly employ adaptive, stealthy, and multi-stage strategies. The mapping emphasizes that effective ransomware defense requires adversarially robust, cross-layer, and deployment-aware solutions that integrate behavioral, system-level, and network-level insights.

Table 14: Threat model: mapping attack capabilities to vulnerable defenses and countermeasures.

Attack Capability	Vulnerable Defenses	Possible Countermeasures
Stealthy/Low-and-Slow Encryption	Behavioral detection, storage-level anomaly detection	Long-term behavioral profiling; temporal pattern analysis; cross-file and cross-process correlation; anomaly detection over extended windows
Polymorphism and Code Obfuscation	Signature-based and static analysis approaches	Behavior-based detection; dynamic analysis; invariant feature extraction; unpacking and de-obfuscation techniques
Adversarial Feature Manipulation (Evasion Attacks)	ML/DL-based detection systems	Adversarial training; robust feature selection; ensemble models; detection of adversarial inputs
Data Poisoning Attacks	Learning-based systems (ML/DL, federated learning)	Secure data pipelines; anomaly detection on training data; robust aggregation (e.g., in FL); continual validation
Encrypted and Covert Communication (C&C)	Network-based detection systems	Encrypted traffic analysis (metadata, flow features); DNS/traffic pattern analysis; cross-layer correlation with host behavior
Decoy/Honeypot Detection and Avoidance	Deception-based defenses	Adaptive and dynamic decoy placement; high-fidelity honeypots; integration with behavioral detection
Backup Targeting and Destruction	Backup and recovery-based defenses	Tamper-resistant backups; versioning; anomaly-based backup protection; distributed storage
Fileless and Memory-Resident Execution	Static analysis and file-based detection	Memory forensics; runtime monitoring; system call tracing; kernel-level visibility
Distributed/Multi-Stage Attacks	Single-layer detection approaches	Cross-layer detection (host + network + storage); attack chain correlation; SIEM integration
Use of Legitimate Tools (Living-off-the-Land)	Signature-based and rule-based detection	Behavioral baselining; context-aware anomaly detection; privilege and process monitoring

(Continued)

Table 14 (continued)

Attack Capability	Vulnerable Defenses	Possible Countermeasures
Use of Privacy Coins/Mixers (Financial Obfuscation)	Blockchain and transaction analysis	Cross-chain analytics; graph-based tracing; collaboration with financial intelligence and law enforcement
Cloud and Multi-Tenant Exploitation	Host-based and isolated detection systems	Cloud-native monitoring; tenant isolation; cross-VM detection; scalable orchestration and logging

6.2 Cross-Layer Synthesis and Integration Challenges

A key observation from this survey is that ransomware defense mechanisms are often developed in isolation across different layers, including host-based monitoring, network analysis, storage protection, and economic/policy interventions. However, modern ransomware attacks operate across these layers simultaneously.

For example, data exfiltration precedes encryption, leveraging network channels, while persistence mechanisms exploit OS-level vulnerabilities, and ransom payment relies on cryptocurrency ecosystems. As a result, single-layer defenses are insufficient.

Effective ransomware resilience requires: (i) integration of host and network telemetry, (ii) coordination between detection and recovery mechanisms, (iii) incorporation of threat intelligence and economic signals, (iv) alignment with policy and governance frameworks.

This cross-layer perspective remains underdeveloped in current research and represents a critical direction for future work.

Table 15 presents a cross-layer view of ransomware defense by aligning each attack lifecycle stage with the corresponding detection stage, representative defense mechanisms, and evaluation metrics. The framework highlights that ransomware defense cannot rely on a single technique or layer. Early-stage controls such as filtering, sandboxing, and behavioral monitoring are important for preventing execution, whereas later-stage defenses such as storage monitoring, decoy mechanisms, and backup-based recovery are essential for damage containment and resilience. The table also emphasizes that evaluation should be stage-aware: early detection methods should be judged by blocking rate and false alarms, while impact-stage defenses should be evaluated using ransomware-specific metrics such as time-to-detection, files preserved, damage prevented, and recovery success.

Table 15: Cross-layer framework mapping attack lifecycle to detection, defense, and evaluation for unified ransomware analysis.

Attack Lifecycle Stage	Detection Stage	Representative Defense Mechanisms	Relevant Evaluation Metrics
Initial Access/Delivery	Pre-compromise or early compromise	Email/web filtering, attachment scanning, URL reputation, sandboxing, user-awareness controls, patching, access control	Detection rate, false positive rate, malware blocking rate, time-to-alert, user disruption cost

(Continued)

Table 15 (continued)

Attack Lifecycle Stage	Detection Stage	Representative Defense Mechanisms	Relevant Evaluation Metrics
Execution/Payload Launch	Early execution	Static analysis, behavioral monitoring, process/API-call tracing, memory inspection, script control, privilege monitoring	True positive rate, false negative rate, time-to-detection, CPU/memory overhead, alert precision
Persistence/Privilege Escalation	Post-execution, pre-encryption	Endpoint detection and response, registry/startup monitoring, kernel hooks, credential protection, anomaly detection on privileged actions	Detection latency, persistence-blocking rate, false alarms, system overhead
Discovery/Lateral Movement	Pre-impact expansion	Network traffic analysis, SDN/NDR monitoring, authentication anomaly detection, traffic inspection, segmentation, zero-trust controls	Lateral-movement detection rate, false positive rate, response latency, containment success
Command-and-Control/Key Exchange	Pre-encryption coordination	DNS/flow analytics, encrypted traffic analysis, blockchain/CTI correlation, domain/IP reputation, sinkholing, egress control	C&C detection rate, flow-level precision/recall, time-to-block, cross-layer correlation accuracy
Encryption/File Modification	Impact stage	File-system monitoring, entropy/change-rate analysis, decoy files, storage-level defenses, process termination, I/O throttling	Time-to-detection, files protected before detection, damage prevented, false termination rate, storage overhead
Exfiltration/Double Extortion	Impact and post-impact	Data loss prevention, network exfiltration detection, access-pattern analysis, encryption-aware traffic inspection, policy-based blocking	Exfiltration detection rate, bytes/files protected, false positive rate, response time

(Continued)

Table 15 (continued)

Attack Lifecycle Stage	Detection Stage	Representative Defense Mechanisms	Relevant Evaluation Metrics
Recovery/Restoration	Post-incident	Tamper-resistant backups, immutable snapshots, rollback, key recovery, incident response orchestration, forensic triage	Recovery success rate, recovery time objective (RTO), recovery point objective (RPO), data integrity preserved, downtime
Post-Incident Learning/Adaptation	Continuous improvement	Threat intelligence updates, model retraining, rule refinement, attack replay, adversarial testing, policy revision	Model drift resilience, adversarial robustness, update latency, reproducibility, operational effectiveness over time

Fig. 3 illustrates a cross-layer ransomware defense architecture in which telemetry from host, network, storage, and organizational layers is analyzed both locally and jointly and Fig. 4 presents a cross-layer view of ransomware defense, integrating technical, economic, and human/policy dimensions into a unified response framework.

7 Conclusion

This survey reviewed the evolution of ransomware from simple file-encrypting malware to a complex, adaptive, and profit-driven socio-technical threat. Research has progressed from signature- and entropy-based methods to behavior-driven, ML/XAI-based, storage-level, and deception-oriented defenses, alongside increasing focus on recovery, economics, and policy. At the same time, ransomware has expanded across new attack surfaces–including cloud, IoT, IIoT, healthcare, hardware-assisted, and cyber-physical environments–while adopting increasingly sophisticated strategies such as data exfiltration, intermittent encryption, multi-stage extortion, and ransomware-as-a-service. Although recent advances in datasets, taxonomies, and benchmarking have improved reproducibility, much of the literature remains detection-centric and continues to rely on assumptions that only partially reflect real-world attacker behavior.

Despite substantial progress, several important challenges remain unresolved. Many existing defenses are narrowly scoped, difficult to deploy at scale, or vulnerable to adversarial evasion and adaptive attack strategies. Recovery and decryption mechanisms remain largely reactive and opportunistic, while proactive and storage-level defenses often face usability, interoperability, and scalability limitations. Furthermore, economic and game-theoretic analyses provide valuable insights into attacker incentives and ransom dynamics, yet many models lack realistic operational assumptions and empirical validation. A significant gap also persists between academic research and operational practice, particularly in areas such as incident response integration, attribution, policy enforcement, cross-layer coordination, and deployment in resource-constrained environments.

Looking forward, several short-term practical priorities deserve immediate attention. These include the development of standardized and continuously updated ransomware datasets and benchmarks, realistic evaluation methodologies that account for temporal drift and adversarial behavior, deployment-aware

lightweight defenses for cloud and IoT environments, explainable detection systems suitable for SOC workflows, and faster recovery-oriented mechanisms capable of reducing time-to-detection and minimizing operational damage. Improving information sharing among academia, industry, and government agencies is also critical for enabling reproducible evaluation and coordinated response.

Beyond these immediate needs, longer-term research challenges require more fundamental advances. Future ransomware defense will likely depend on integrated, cross-layer, and adaptive frameworks that unify prevention, detection, containment, recovery, attribution, and policy mechanisms. Robustness against adversarial ML attacks, autonomous and AI-assisted ransomware, cross-platform attacks targeting hybrid cloud and cyber-physical infrastructures, and large-scale automated extortion ecosystems will become increasingly important research directions. In addition, emerging paradigms such as post-quantum cryptography, secure hardware-assisted defenses, privacy-preserving collaborative learning, and economically informed defense strategies are expected to play a significant role in next-generation ransomware resilience.

Overall, reducing the long-term impact and profitability of ransomware will require bridging the gap between theoretical research and operational deployment through realistic evaluation, interdisciplinary collaboration, standardized benchmarks, and policy-aware, human-centered defense design.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Fernando DW, Komninos N, Chen T. A study on the evolution of ransomware detection using machine learning and deep learning techniques. IoT. 2020;1(2):551–604. doi:10.3390/iot1020030.
2. Wang K, Pang J, Chen D, Zhao Y, Huang D, Chen C, et al. A large-scale empirical analysis of ransomware activities in Bitcoin. ACM Trans Web. 2021;16(2):1–29. doi:10.1145/3494557.
3. Moussaileb R, Cuppens N, Lanet J-L, Le Bouder H. A survey on windows-based ransomware taxonomy and detection mechanisms. ACM Comput Surv. 2021;54(6):1–36. doi:10.1145/3453153.
4. McIntosh T, Kayes ASM, Chen Y, Ng A, Watters P. Ransomware mitigation in the modern era: a comprehensive review, research challenges, and future directions. ACM Comput Surv. 2021;54(9):1–36.
5. Alqahtani A, Sheldon FT. A survey of crypto ransomware attack detection methodologies: an evolving outlook. Sensors. 2022;22(5):1837. doi:10.3390/s22051837.
6. Smith D, Khorsandroo S, Roy K. Machine learning algorithms and frameworks in ransomware detection. IEEE Access. 2022;10:117597–610. doi:10.1109/access.2022.3218779.
7. Aldauiji F, Batarfi O, Bayousef M. Utilizing cyber threat hunting techniques to find ransomware attacks: a survey of the state of the art. IEEE Access. 2022;10:61695–706. doi:10.1109/access.2022.3181278.
8. Oz H, Aris A, Levi A, Uluagac AS. A survey on ransomware: evolution, taxonomy, and defense solutions. ACM Comput Surv. 2022;54(11s):1–37.
9. Ispahany J, Islam MR, Islam MZ, Khan MA. Ransomware detection using machine learning: a review, research limitations and future directions. IEEE Access. 2024;12(18):68785–813. doi:10.1002/cpe.5422.
10. Alzahrani S, Xiao Y, Asiri S, Zheng J, Li T. A survey of ransomware detection methods. IEEE Access. 2025;13(2):57943–82. doi:10.1109/access.2025.3556187.
11. Anh H. Dynamic features of virusshare executables. UCI Mach Learn Repos. 2017. doi:10.24432/C50P5P.

12. Nappa A, Zubair Rafique M, Caballero J. The MALICIA dataset: identification and analysis of drive-by download operations. Int J Inf Secur. 2015;14(1):15–33.
13. Anderson HS, Roth P. EMBER: an open dataset for training static pe malware machine learning models. arXiv:1804.04637. 2018.
14. Carrier T, Victor P, Tekeoglu A, Lashkari AH. Cic-malmem-2022 dataset. 2022 [cited 2026 Jan 1]. Available from: https://www.unb.ca/cic/datasets/malmem-2022.html.
15. Sharafaldin I, Lashkari AH, Ghorbani AA. Cicids2017-dataset. 2017 [cited 2026 Jan 1]. Available from: https://www.unb.ca/cic/datasets/ids-2017.html.
16. Sharafaldin I, Lashkari AH, Ghorbani A. A realistic cyber defense dataset (CSE-CIC-IDS2018). 2017 [cited 2026 Jan 1]. Available from: https://www.kaggle.com/datasets/dhoogla/csecicids2018.
17. Moustafa N, Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS); 2015 Nov 10–12; Canberra, Australia. p. 1–6.
18. Garcia S, Parmisano A, Erquiaga MJ. IoT-23: a labeled dataset with malicious and benign IoT network traffic. 2020 [cited 2026 Jan 1]. Available from: https://www.kaggle.com/datasets/astralfate/iot23-dataset.
19. Alsaedi A, Moustafa N, Tari Z, Mahmood AN, Anwar A. TON_IoT telemetry dataset: a new generation dataset of IoT and IIoT for data-driven intrusion detection systems. IEEE Access. 2020;8:165130–50.
20. Mathur A. NATICUSdroid (android permissions) [dataset]. 2021 [cited 2026 Jan 1]. Available from: https://www.kaggle.com/datasets/budhadityadutta/naticusdroid-android-permissions.
21. Ribeiro MT, Singh S, Guestrin C. "Why should I trust you?": explaining the predictions of any classifier. In: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD'16; 2016 Aug 13–17; San Francisco, CA, USA. p. 1135–44.
22. Salzberg SL. C4.5: programs for machine learning by j. ross quinlan. Burlington, MA, USA: Morgan Kaufmann Publishers, Inc.; 1993.
23. Lundberg SM, Lee S-I. A unified approach to interpreting model predictions. In: Proceedings of the 31st International Conference on Neural Information Processing Systems (NIPS 2017); 2017 Dec 4–9; Long Beach, CA, USA. p. 4768–77.
24. Chawla NV, Bowyer KW, Hall LO, Kegelmeyer WP. SMOTE: synthetic minority over-sampling technique. J Artif Intell Res. 2002;16:321–57.
25. IBM. What is explainable AI? [cited 2023 Sep 1]. Available from: https://www.ibm.com/topics/explainable-ai.
26. Scaife N, Carter H, Traynor P, Butler KRB. Cryptolock (and drop it): stopping ransomware attacks on user data. In: Proceedings of 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS); 2016 Jun 27–30; Nara, Japan. p. 303–12.
27. Kharaz A, Arshad S, Mulliner C, Robertson W, Kirda E. UNVEIL: a large-scale, automated approach to detecting ransomware. In: Proceedings of 25th USENIX Security Symposium (USENIX Security 16); 2016 Aug 10–12; Austin, TX, USA. p. 757–72.
28. Chen Q, Bridges RA. Automated behavioral analysis of malware: a case study of wannacry ransomware. In: Proceedings of 2017 16th IEEE International Conference on machine learning and applications (ICMLA); 2017 Dec 18–21; Cancun, Mexico. p. 454–60.
29. Homayoun S, Dehghantanha A, Ahmadzadeh M, Hashemi S, Khayami R. Know abnormal, find evil: frequent pattern mining for ransomware threat hunting and intelligence. IEEE Trans Emerg Top Comput. 2017;8(2):341–51. doi:10.1109/tetc.2017.2756908.
30. Hampton N, Baig Z, Zeadally S. Ransomware behavioural analysis on windows platforms. J Inf Secur Appl. 2018;40(2):44–51. doi:10.1016/j.jisa.2018.02.008.
31. Kok SH, Abdullah A, Jhanjhi NZ, Supramaniam M. Prevention of crypto-ransomware using a pre-encryption detection algorithm. Computers. 2019;8(4):79. doi:10.3390/computers8040079.
32. Kok SH, Abdullah A, Jhanjhi NZ. Early detection of crypto-ransomware using pre-encryption detection algorithm. J King Saud Univ—Comput Inf Sci. 2022;34(5):1984–99. doi:10.1016/j.jksuci.2020.06.012.

33. Hwang J, Kim J, Lee S, Kim K. Two-stage ransomware detection using dynamic analysis and machine learning techniques. Wirel Pers Commun. 2020;112(4):2597–609. doi:10.1007/s11277-020-07166-9.
34. Ullah F, Javaid Q, Salam A, Ahmad M, Sarwar N, Shah D, et al. Modified decision tree technique for ransomware detection at runtime through API calls. Sci Program. 2020;2020(1):8845833. doi:10.1155/2020/8845833.
35. Molina RMA, Torabi S, Sarieddine K, Bou-Harb E, Bouguila N, Assi C. On ransomware family attribution using pre-attack paranoia activities. IEEE Trans Netw Serv Manag. 2021;19(1):19–36. doi:10.1109/tnsm.2021.3112056.
36. Herrera-Silva JA, Hernández-Álvarez M. Dynamic feature dataset for ransomware detection using machine learning algorithms. Sensors. 2023;23(3):1053. doi:10.3390/s23031053.
37. Javaheri D, Hosseinzadeh M, Rahmani AM. Detection and elimination of spyware and ransomware by intercepting kernel-level system routines. IEEE Access. 2018;6:78321–32. doi:10.1109/access.2018.2884964.
38. Zhang H, Zhao L, Yu A, Cai L, Meng D. Ranker: early ransomware detection through kernel-level behavioral analysis. IEEE Trans Inf Forensics Secur. 2024;19(11):6113–27. doi:10.1109/tifs.2024.3410511.
39. Tang F, Ma B, Li J, Zhang F, Su J, Ma J. RansomSpector: an introspection-based approach to detect crypto ransomware. Comput Secur. 2020;97(5):101997. doi:10.1016/j.cose.2020.101997.
40. McIntosh T, Kayes ASM, Chen YP, Ng A, Watters P. Dynamic user-centric access control for detection of ransomware attacks. Comput Secur. 2021;111(6):102461. doi:10.1016/j.cose.2021.102461.
41. Al Sabeh A, Safa H, Bou-Harb E, Crichigno J. Exploiting ransomware paranoia for execution prevention. In: Proceedings of 2020 IEEE International Conference on Communications (ICC); 2020 Jun 7–11; Dublin, Ireland. p. 1–6.
42. Ramesh G, Menen A. Automated dynamic approach for detecting ransomware using finite-state machine. Decis Support Syst. 2020;138(6):113400. doi:10.1016/j.dss.2020.113400.
43. Abbasi MS, Al-Sahaf H, Mansoori M, Welch I. Behavior-based ransomware classification: a particle swarm optimization wrapper-based approach for feature selection. Appl Soft Comput. 2022;121:108744.
44. Ayub MA, Siraj A, Filar B, Gupta M. RWArmor: a static-informed dynamic analysis approach for early detection of cryptographic windows ransomware. Int J Inf Secur. 2024;23(1):533–56.
45. Hou Y, Guo L, Zhou C, Xu Y, Yin Z, Li S, et al. An empirical study of data disruption by ransomware attacks. In: Proceedings of the IEEE/ACM 46th International Conference on Software Engineering, ICSE'24; 2024 Apr 14–20; Lisbon, Portugal.
46. Marcinkowski B, Goschorska M, Wileńska N, Siuta J, Kajdanowicz T. MIRAD: a method for interpretable ransomware attack detection. IEEE Access. 2024;12:133810–20.
47. Wang S, Dong F, Yang H, Xu J, Wang H. CanCal: towards real-time and lightweight ransomware detection and response in industrial environments. In: Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS'24; 2024 Oct 14–18; Salt Lake City, UT, USA. p. 2326–40.
48. Zhang H, Xiao X, Mercaldo F, Ni S, Martinelli F, Sangaiah AK. Classification of ransomware families with machine learning based on N-gram of opcodes. Future Gener Comput Syst. 2019;90(3):211–21. doi:10.1016/j.future.2018.07.052.
49. Su D, Liu J, Wang X, Wang W. Detecting android locker-ransomware on Chinese social networks. IEEE Access. 2018;7:20381–93. doi:10.1109/access.2018.2888568.
50. Cohen A, Nissim N. Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory. Expert Syst Appl. 2018;102(5):158–78. doi:10.1016/j.eswa.2018.02.039.
51. Aljabri M, Alhaidari F, Albuainain A, Alrashidi S, Alansari J, Alqahtani W, et al. Ransomware detection based on machine learning using memory features. Egypt Inform J. 2024;25(12):100445. doi:10.1016/j.eij.2024.100445.
52. Ahmed YA, Koçer B, Huda S, Al-Rimy BAS, Hassan MM. A system call refinement-based enhanced minimum redundancy maximum relevance method for ransomware early detection. J Netw Comput Appl. 2020;167(5):102753. doi:10.1016/j.jnca.2020.102753.
53. Khan F, Ncube C, Ramasamy LK, Kadry S, Nam Y. A digital DNA sequencing engine for ransomware detection using machine learning. IEEE Access. 2020;8:119710–9. doi:10.1109/access.2020.3003785.

54. Arabo A, Dijoux R, Poulain T, Chevalier G. Detecting ransomware using process behavior analysis. Procedia Comput Sci. 2020;168(14):289–96. doi:10.1016/j.procs.2020.02.249.
55. Jain S, Gera T, Gill R, Bhardwaj V. CrossF-Droid: integrating filter, wrapper, and regularization methods for enhanced predictive modeling to analyze android ransomware. IEEE Access. 2025;13(3):190075–92. doi:10.1109/access.2025.3624238.
56. Fernandez Maimo L, Huertas Celdran A, Perales Gomez AL, Garcia Clemente FJ, Weimer J, Lee I. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. Sensors. 2019;19(5):1114. doi:10.3390/s19051114.
57. Poudyal S, Dasgupta D. Analysis of crypto-ransomware using ML-based multi-level profiling. IEEE Access. 2021;9:122532–47. doi:10.1109/access.2021.3109260.
58. Iqbal MJ, Aurangzeb S, Aleem M, Srivastava G, Lin J. RThreatDroid: a ransomware detection approach to secure IoT based healthcare systems. IEEE Trans Netw Sci Eng. 2022;10(5):2574–83.
59. Ba'abbad I, Batarfi O. Proactive ransomware detection using extremely fast decision tree (EFDT) algorithm: a case study. Computers. 2023;12(6):121. doi:10.3390/computers12060121.
60. Jemal M, Lo D. Detection of ransomware attack using deep learning. In: Proceedings of the 2023 IEEE Conference on Dependable and Secure Computing (DSC); 2023 Nov 7–9; Tampa, FL, USA. p. 1–9.
61. Dib O, Nan Z, Liu J. Machine learning-based ransomware classification of Bitcoin transactions. J King Saud Univ Comput Inf Sci. 2024;36(1):101925. doi:10.1016/j.jksuci.2024.101925.
62. Rios-Ochoa E, Pérez-Díaz JA, García-Ceja E, Rodríguez-Hernández G. Ransomware family attribution with ML: a comprehensive evaluation of datasets quality, models comparison, and a simulated deployment. IEEE Access. 2025;13:108108–26.
63. Homayoun S, Dehghantanha A, Ahmadzadeh M, Hashemi S, Khayami R, Choo K, et al. DRTHIS: deep ransomware threat hunting and intelligence system at the fog layer. Future Gener Comput Syst. 2019;90:94–104.
64. Cen M, Jiang F, Doss R. RansoGuard: a RNN-based framework leveraging pre-attack sensitive APIs for early ransomware detection. Comput Secur. 2025;150:104293.
65. Ispahany J, Islam MR, Arif Khan M, Islam MZ. iCNN-LSTM+: a batch-based incremental ransomware detection system using sysmon. IEEE Access. 2025;13:87978–98.
66. Zhang B, Xiao W, Xiao X, Sangaiah AK, Zhang W, Zhang J. Ransomware classification using patch-based CNN and self-attention network on embedded N-grams of opcodes. Future Gener Comput Syst. 2020;110(4):708–20. doi:10.1016/j.future.2019.09.025.
67. Lachtar N, Ibdah D, Khan H, Bacha A. Ransomshield: a visualization approach to defending mobile systems against ransomware. ACM Trans Priv Secur. 2023;26(3):1–30.
68. Karbab EB, Debbabi M, Derhab A. SwiftR: cross-platform ransomware fingerprinting using hierarchical neural networks on hybrid features. Expert Syst Appl. 2023;225:120017.
69. Zhang X, Wang J, Zhu S. Dual generative adversarial networks based unknown encryption ransomware attack detection. IEEE Access. 2021;10:900–13. doi:10.1109/access.2021.3128024.
70. Gazzan M, Sheldon FT. An enhanced Minimax loss function technique in generative adversarial network for ransomware behavior prediction. Future Internet. 2023;15(10):318. doi:10.3390/fi15100318.
71. Zhu J, Jang-Jaccard J, Singh A, Welch I, Al-Sahaf H, Camtepe S. A few-shot meta-learning based siamese neural network using entropy features for ransomware classification. Comput Secur. 2022;117(7):102691. doi:10.1016/j.cose.2022.102691.
72. Ganfure GO, Wu C-F, Chang Y-H, Shih W-H. Deepware: imaging performance counters with deep learning to detect ransomware. IEEE Trans Comput. 2022;72(3):600–13.
73. Thummapudi K, Lama P, Boppana RV. Detection of ransomware attacks using processor and disk usage data. IEEE Access. 2023;11:51395–407. doi:10.1109/access.2023.3279819.
74. Lan K, Li G, Huang W, Li J. HFL-RD: heterogeneous federated learning-empowered ransomware detection via APIs and traffic features. IEEE Trans Netw Serv Manag. 2025;22(5):4096–111. doi:10.1109/tnsm.2025.3574716.
75. Hossain MA, Hasan T, Ahmed F, Cheragee SH, Kanchan MH, Haque MA. Towards superior android ransomware detection: an ensemble machine learning perspective. Cyber Secur Appl. 2025;3:100076.

76. Gulmez S, Kakisim AG, Sogukpinar I. XRan: explainable deep learning-based ransomware detection using dynamic analysis. Comput Secur. 2024;139:103703.
77. Kabuye H, Issac B, Yumlembam R, Neera J. Explainable and uncertainty aware AI-based ransomware detection. IEEE Access. 2025;13(3):106573–89. doi:10.1109/access.2025.3581424.
78. Sharmeen S, Ahmed YA, Huda S, Koçer B, Hassan MM. Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. IEEE Access. 2020;8:24522–34. doi:10.1109/access.2020.2970466.
79. Urooj U, Al-Rimy BAS, Zainal AB, Saeed F, Abdelmaboud A, Nagmeldin W. Addressing behavioral drift in ransomware early detection through weighted generative adversarial networks. IEEE Access. 2023;12:3910–25. doi:10.1109/access.2023.3348451.
80. Al-Rimy BAS, Maarof MA, Alazab M, Alsolami F, Shaid SZM, Ghaleb FA, et al. A pseudo feedback-based annotated TF-IDF technique for dynamic crypto-ransomware pre-encryption boundary delineation and features extraction. IEEE Access. 2020;8:140586–98. doi:10.1109/access.2020.3012674.
81. Al-Rimy BAS, Maarof MA, Alazab M, Shaid SZM, Ghaleb FA, Almalawi A, et al. Redundancy coefficient gradual up-weighting-based mutual information feature selection technique for crypto-ransomware early detection. Future Gener Comput Syst. 2021;115(5):641–58. doi:10.1016/j.future.2020.10.002.
82. Cen M, Deng X, Jiang F, Doss R. Zero-Ran Sniff: a zero-day ransomware early detection method based on zero-shot learning. Comput Secur. 2024;142:103849.
83. Fernando DW, Komninos N. FeSAD ransomware detection framework with machine learning using adaption to concept drift. Comput Secur. 2024;137(7):103629. doi:10.1016/j.cose.2023.103629.
84. Cabaj K, Mazurczyk W. Using software-defined networking for ransomware mitigation: the case of CryptoWall. IEEE Netw. 2016;30(6):14–20. doi:10.1109/mnet.2016.1600110nm.
85. Cabaj K, Gregorczyk M, Mazurczyk W. Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. Comput Electr Eng. 2018;66(1):353–68. doi:10.1016/j.compeleceng.2017.10.012.
86. Akbanov M, Vassilakis VG, Logothetis MD. Ransomware detection and mitigation using software-defined networking: the case of WannaCry. Comput Electr Eng. 2019;76(3):111–21. doi:10.1016/j.compeleceng.2019.03.012.
87. Morato D, Berrueta E, Magaña E, Izal M. Ransomware early detection by the analysis of file sharing traffic. J Netw Comput Appl. 2018;124(4):14–32. doi:10.1016/j.jnca.2018.09.013.
88. Almashhadani AO, Kaiiali M, Sezer S, O'Kane P. A multi-classifier network-based crypto ransomware detection system: a case study of locky ransomware. IEEE Access. 2019;7:47053–67.
89. Liu T-M, Kao D-Y, Chen Y-Y. Loocipher ransomware detection using lightweight packet characteristics. Procedia Comput Sci. 2020;176(2):1677–83. doi:10.1016/j.procs.2020.09.192.
90. Hernandez-Jaimes ML, Martínez-Cruz A, Ramírez-Gutierrez KA, Guevara-Martínez E. Enhancing machine learning approach based on nilsimsa fingerprinting for ransomware detection in IoMT. IEEE Access. 2024;12(2):153886–97. doi:10.1109/access.2024.3480889.
91. Pletinckx S, Trap C, Doerr C. Malware coordination using the blockchain: an analysis of the cerber ransomware. In: Proceedings of 2018 IEEE Conference on Communications and Network Security (CNS); 2018 May 30–Jun 1; Beijing, China. p. 1–9.
92. Li Z, Rios ALG, Trajković L. Machine learning for detecting the WestRock ransomware attack using BGP routing records. IEEE Commun Mag. 2022;61(3):20–6. doi:10.1109/mcom.001.2200215.
93. Song S, Kim B, Lee S. The effective ransomware prevention technique using process monitoring on android platform. Mob Inf Syst. 2016;2016(1):2946735. doi:10.1155/2016/2946735.
94. Chen J, Wang C, Zhao Z, Chen K, Du R, Ahn G-J. Uncovering the face of android ransomware: characterization and real-time detection. IEEE Trans Inf Forensics Secur. 2017;13(5):1286–300. doi:10.1109/tifs.2017.2787905.
95. Faghihi F, Zulkernine M. RansomCare: data-centric detection and mitigation against smartphone crypto-ransomware. Comput Netw. 2021;191:108011.
96. Chew C, Kumar V, Patros P, Malik R. Real-time system call-based ransomware detection. Int J Inf Secur. 2024;23(3):1839–58. doi:10.1007/s10207-024-00819-x.

97. Ma B, Zhou L, Liao C, Zhou Y, Li J, Ma J. RansomSentry: Runtime detection of android ransomware with compiler-based instrumentation. IEEE Trans Dependable Secur Comput. 2025;22(4):3354–70. doi:10.1109/tdsc.2025.3529119.
98. Scalas M, Maiorca D, Mercaldo F, Visaggio CA, Martinelli F, Giacinto G. On the effectiveness of system API-related information for Android ransomware detection. Comput Secur. 2019;86(7):168–82. doi:10.1016/j.cose.2019.06.004.
99. Alsoghyer S, Almomani I. Ransomware detection system for Android applications. Electronics. 2019;8(8):868. doi:10.3390/electronics8080868.
100. Singh N, Tripathy S. It's too late if exfiltrate: early stage android ransomware detection. Comput Secur. 2024;141:103819.
101. Ahmed U, Lin J, Srivastava G. Mitigating adversarial evasion attacks of ransomware using ensemble learning. Comput Electr Eng. 2022;100(3):107903. doi:10.1016/j.compeleceng.2022.107903.
102. Hossain MS, Hasan N, Samad MA, Shakhawat HM, Karmoker J, Ahmed F, et al. Android ransomware detection from traffic analysis using metaheuristic feature selection. IEEE Access. 2022;10:128754–63. doi:10.1109/access.2022.3227579.
103. Albin Ahmed A, Shaahid A, Alnasser F, Alfaddagh S, Binagag S, Alqahtani D. Android ransomware detection using supervised machine learning techniques based on traffic analysis. Sensors. 2023;24(1):189. doi:10.3390/s24010189.
104. Jeremiah SR, Chen H, Gritzalis S, Park JH. Leveraging application permissions and network traffic attributes for android ransomware detection. J Netw Comput Appl. 2024;230:103950. doi:10.1016/j.jnca.2024.103950.
105. Cimitile A, Mercaldo F, Nardone V, Santone A, Visaggio CA. Talos: no more ransomware victims with formal methods. Int J Inf Secur. 2018;17(6):719–38.
106. Elkhail AA, Bacha A, Malik H. Sniper: countering locker ransomware attacks through natural language processing. IEEE Trans Dependable Secur Comput. 2025;22(4):4160–75.
107. Al-Hawawreh M, Den Hartog F, Sitnikova E. Targeted ransomware: a new cyber threat to edge system of brownfield industrial Internet of Things. IEEE Internet Things J. 2019;6(4):7137–51.
108. Celdrán AH, Sánchez PMS, Von der Assen J, Shushack D, Gómez ÁLP, Bovet G, et al. Behavioral fingerprinting to detect ransomware in resource-constrained devices. Comput Secur. 2023;135:103510. doi:10.1016/j.cose.2023.103510.
109. Al-Hawawreh M, Sitnikova E, Aboutorab N. Asynchronous peer-to-peer federated capability-based targeted ransomware detection model for industrial IoT. IEEE Access. 2021;9:148738–55. doi:10.1109/access.2021.3124634.
110. Tariq U, Ullah I, Yousuf Uddin M, Kwon SJ. An effective self-configurable ransomware prevention technique for IoMT. Sensors. 2022;22(21):8516. doi:10.3390/s22218516.
111. Wazid M, Das AK, Shetty S. BSFR-SH: blockchain-enabled security framework against ransomware attacks for smart healthcare. IEEE Trans Consum Electron. 2022;69(1):18–28. doi:10.1109/tce.2022.3208795.
112. Malik AW, Anwar Z, Rahman AU. A novel framework for studying the business impact of ransomware on connected vehicles. IEEE Internet Things J. 2022;10(10):8348–56. doi:10.1109/jiot.2022.3209687.
113. Beaman C, Barkworth A, Akande TD, Hakak S, Khan MK. Ransomware: recent advances, analysis, challenges and future research directions. Comput Secur. 2021;111:102490.
114. De Gaspari F, Hitaj D, Pagnotta G, De Carli L, Mancini LV. Evading behavioral classifiers: a comprehensive analysis on evading ransomware detection techniques. Neural Comput Appl. 2022;34(14):12077–96.
115. von der Assen J, Celdrán AH, Luechinger J, Sánchez PMS, Bovet G, Pérez GM, et al. RansomAI: AI-powered ransomware for stealthy encryption. In: Proceedings of 2023 IEEE Global Communications Conference; 2023 Dec 8–12; Kuala Lumpur, Malaysia. p. 2578–83.
116. Zhou C, Guo L, Hou Y, Ma Z, Zhang Q, Wang M, et al. Limits of I/O based ransomware detection: an imitation based attack. In: Proceedings of 2023 IEEE Symposium on Security and Privacy (SP); 2023 May 21–25; San Francisco, CA, USA. p. 2584–601.
117. Zhao L, Zhang Y, Wang Z, Yuan F, Hou R. ERW-Radar: an adaptive detection system against evasive ransomware by contextual behavior detection and fine-grained content analysis. In: Proceedings of NDSS; 2025 Feb 24–28; San Diego, CA, USA.
118. Guo L, Hou Y, Zhou C, Zhang Q, Jiang Y. Ransomware detection through temporal correlation between encryption and I/O behavior. Proc ACM Softw Eng. 2025;2(FSE):197–218. doi:10.1145/3715725.

119. Hitaj D, Pagnotta G, De Gaspari F, De Carli L, Minerva MLV. A file-based ransomware detector. In: Proceedings of the 20th ACM Asia Conference on Computer and Communications Security, SEC'25; 2025 Aug 25–29; Hanoi, Vietnam. p. 576–90.
120. Conti M, Gangwal A, Ruj S. On the economic significance of ransomware campaigns: a Bitcoin transactions perspective. Comput Secur. 2018;79(1):162–89. doi:10.1016/j.cose.2018.08.008.
121. Huang D, Aliapoulios MM, Li VG, Invernizzi L, Bursztein E, McRoberts K, et al. Tracking ransomware end-to-end. In: Proceedings of 2018 IEEE Symposium on Security and Privacy (SP); 2018 May 21–23; San Francisco, CA, USA. p. 618–31.
122. Paquet-Clouston M, Haslhofer B, Dupont B. Ransomware payments in the Bitcoin ecosystem. J Cybersecur. 2019;5(1):tyz003. doi:10.1093/cybsec/tyz003.
123. Wang K, Tong M, Pang J, Wang J, Han W. XRAD: ransomware address detection method based on Bitcoin transaction relationships. ACM Trans Web. 2024;18(4):1–33.
124. Sarabi A, Huang Z, Wang C, Karir T, Liu M. The ransomware decade: the creation of a fine-grained dataset and a longitudinal study. In: Proceedings of 34th USENIX Security Symposium (USENIX Security 25); 2025 Aug 13–15; Berkeley, CA, USA. p. 4799–818.
125. Min D, Park D, Ahn J, Walker R, Lee J, Park S, et al. Amoeba: an autonomous backup and recovery SSD for ransomware attack defense. IEEE Comput Archit Lett. 2018;17(2):245–8.
126. Baek S, Jung Y, Mohaisen A, Lee S, Nyang D. SSD-insider: internal defense of solid-state drive against ransomware with perfect data recovery. In: Proceedings of 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS); 2018 Jul 2–5; Vienna, Austria. p. 875–84.
127. Baek S, Jung Y, Mohaisen D, Lee S, Nyang D. SSD-assisted ransomware detection and data recovery techniques. IEEE Trans Comput. 2020;70(10):1762–76. doi:10.1109/tc.2020.3011214.
128. Paik J-Y, Choi J-H, Jin R, Wang J, Cho E-S. A storage-level detection mechanism against crypto-ransomware. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security; 2018 Oct 15–19; Toronto, Canada. p. 2258–60.
129. Elkhail AA, Lachtar N, Ibdah D, Aslam R, Khan H, Bacha A, et al. Seamlessly safeguarding data against ransomware attacks. IEEE Trans Dependable Secur Comput. 2023;20(1):1–16. doi:10.1109/tdsc.2022.3214781.
130. Ma B, Yang Y, Li J, Zhang F, Shen W, Zhou Y, et al. Travelling the hypervisor and SSD: a tag-based approach against crypto ransomware with fine-grained data recovery. In: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS'23; 2023 Nov 26–30; Copenhagen, Denmark. p. 341–55.
131. Wang Z, Song Y, Xu E, Wu H, Tong G, Sun S, et al. Ransom access memories: achieving practical ransomware protection in cloud with DeftPunk. In: Proceedings of 18th USENIX Symposium on Operating Systems Design and Implementation (OSDI 24); 2024 Jul 10–12; Clara, CA, USA. p. 687–702.
132. Hill JE, Walker TO, Blanco JA, Ives RW, Rakvic R, Jacob B. Ransomware classification using hardware performance counters on a non-virtualized system. IEEE Access. 2024;12(4):63865–84. doi:10.1109/access.2024.3395491.
133. Zhu W, Hernandez G, Garcia W, Tian D, Rampazzi S, Butler KRB. SrFTL: leveraging storage semantics for effective ransomware defense in flash-based SSDs. ACM Trans Storage. 2025;21(4):1–42.
134. Gómez-Hernández JA, Álvarez-González L, García-Teodoro P. R-Locker: thwarting ransomware action through a honeyfile-based approach. Comput Secur. 2018;73:389–98.
135. Sibi Chakkaravarthy S, Sangeetha D, Cruz MV, Vaidehi V, Raman B. Design of intrusion detection honeypot using social leopard algorithm to detect IoT ransomware attacks. IEEE Access. 2020;8:169944–56. doi:10.1109/access.2020.3023764.
136. Ganfure GO, Wu C-F, Chang Y-H, Shih W-K. Rtrap: trapping and containing ransomware with machine learning. IEEE Trans Inf Forensics Secur. 2023;18:1433–48.
137. Berardi D, Giallorenzo S, Melis A, Melloni S, Onori L, Prandini M. Data flooding against ransomware: concepts and implementations. Comput Secur. 2023;131:103295.
138. Sajid MSI, Wei J, Al-Shaer E. ranDecepter: real-time identification and deterrence of ransomware attacks. In: Proceedings of 2025 IEEE Conference on Communications and Network Security (CNS); 2025 Sep 8–11; Avignon, France. p. 1–9.

139. Filiz B, Arief B, Cetin O, Hernandez-Castro J. On the effectiveness of ransomware decryption tools. Comput Secur. 2021;111(3):102469. doi:10.1016/j.cose.2021.102469.
140. Yuste J, Pastrana S. Avaddon ransomware: an in-depth analysis and decryption of infected systems. Comput Secur. 2021;109:102388.
141. Kim G, Kim S, Kang S, Kim J. A method for decrypting data infected with Hive ransomware. J Inf Secur Appl. 2022;71(1):103387. doi:10.1016/j.jisa.2022.103387.
142. Kim G, Kang S, Baek S, Kim K, Kim J. How to decrypt files encrypted by Rhysida ransomware without the attacker's private key. J Inf Secur Appl. 2025;151(10):104340. doi:10.1016/j.cose.2025.104340.
143. Almomani I, Alkhayer A, El-Shafai W. E2E-RDS: efficient end-to-end ransomware detection system based on static-based ML and vision-based DL approaches. Sensors. 2023;23(9):4467.
144. Lee K, Lee S, Yim K. Machine learning based file entropy analysis for ransomware detection in backup systems. IEEE Access. 2019;7:110205–15. doi:10.1109/access.2019.2931136.
145. Davies SR, Macfarlane R, Buchanan WJ. Differential area analysis for ransomware attack detection within mixed file datasets. Comput Secur. 2021;108(8):102377. doi:10.1016/j.cose.2021.102377.
146. Hou Y, Guo L, Zhou C, Zhang Q, Liu W, Sun C, et al. Preventing disruption of system backup against ransomware attacks. Proc ACM Softw Eng. 2025;2(ISSTA):229–49. doi:10.1145/3728880.
147. Everett C. Ransomware: to pay or not to pay? Comput Fraud Secur. 2016;2016(4):8–12. doi:10.1016/s1361-3723(16)30036-7.
148. Mansfield-Devine S. Ransomware: taking businesses hostage. Netw Secur. 2016;2016(10):8–17. doi:10.1016/s1353-4858(16)30096-4.
149. Connolly AY, Borrion H. Reducing ransomware crime: analysis of victims' payment decisions. Comput Secur. 2022;119:102760.
150. Ryan P, Fokker J, Healy S, Amann A. Dynamics of targeted ransomware negotiation. IEEE Access. 2022;10:32836–44. doi:10.1109/access.2022.3160748.
151. Meurs T, Cartwright E, Cartwright A, Junger M, Abhishta A. Deception in double extortion ransomware attacks: an analysis of profitability and credibility. Comput Secur. 2024;138:103670.
152. Zhang-Kennedy L, Assal H, Rocheleau J, Mohamed R, Baig K, Chiasson S. The aftermath of a crypto-ransomware attack at a large academic institution. In: Proceedings of 27th USENIX Security Symposium (USENIX Security 18), SEC'18; 2018 Aug 15–17; Baltimore, MD, USA. p. 1061–78.
153. Connolly LY, Wall DS. The rise of crypto-ransomware in a changing cybercrime landscape: taxonomising countermeasures. Comput Secur. 2019;87(5):101568. doi:10.1016/j.cose.2019.101568.
154. Thomas J. Individual cyber security: empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. Int J Bus Manag. 2018;12(3):1–23.
155. Hayes K. Ransomware: a growing geopolitical threat. Netw Secur. 2021;2021(8):11–3.
156. Bekkers L, van't Hoff-De Goede S, Misana-ter Huurne E, van Houten Y, Spithoven R, Leukfeldt ER. Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. Comput Secur. 2023;127(2):103099. doi:10.1016/j.cose.2023.103099.
157. Mott G, Turner S, Nurse JRC, Mac Coll J, Sullivan J, Cartwright A, et al. Between a rock and a hard (ening) place: cyber insurance in the ransomware era. Comput Secur. 2023;128:103162.
158. Bajpai P, Enbody R. Know thy ransomware response: a detailed framework for devising effective ransomware response strategies. Digit Threat Res Pract. 2023;4(4):1–19.
159. Simmonds M. How businesses can navigate the growing tide of ransomware attacks. Comput Fraud Secur. 2017;2017(3):9–12. doi:10.1016/s1361-3723(17)30023-4.
160. Hernandez-Castro J, Cartwright A, Cartwright E. An economic analysis of ransomware and its welfare consequences. R Soc Open Sci. 2020;7(3):190023. doi:10.1098/rsos.190023.
161. Cartwright E, Hernandez Castro J, Cartwright A. To pay or not: game theoretic models of ransomware. J Cybersecur. 2019;5(1):tyz009.

162. Zhang C, Luo F, Ranzi G. Multistage game theoretical approach for ransomware attack and defense. IEEE Trans Serv Comput. 2022;16(4):2800–11. doi:10.1109/tsc.2022.3220736.
163. Li Z, Liao Q. Preventive portfolio against data-selling ransomware—A game theory of encryption and deception. Comput Secur. 2022;116(2):102644. doi:10.1016/j.cose.2022.102644.
164. Meland PH, Bayoumy YFF, Sindre G. The Ransomware-as-a-Service economy within the darknet. Comput Secur. 2020;92(2):101762. doi:10.1016/j.cose.2020.101762.
165. Chauhan PS, Kshetri N. Ransomware as a service kit: a novel cybercrime strategy to monetize victims' data. Computer. 2023;56(10):102–6.
166. Oosthoek K, Cable J, Smaragdakis G. A tale of two markets: investigating the ransomware payments economy. Commun ACM. 2023;66(8):74–83.
167. Phipps A, Nurse JRC. Inside ransomware groups: an analysis of their origins, structures, and dynamics. Comput Secur. 2026;160:104705.
168. Delgado-Mohatar O, Sierra-Cámara JM, Anguiano E. Blockchain-based semi-autonomous ransomware. Future Gener Comput Syst. 2020;112(6):589–603. doi:10.1016/j.future.2020.02.037.
169. Adams M, Moore T. How informative are cybersecurity risk disclosures? Empirical analysis of firms targeted by ransomware. Comput Secur. 2025;159(5799):104626. doi:10.1016/j.cose.2025.104626.
170. van der Horst M, Kho R, Gadyatskaya O, Mollema M, Van Eeten M, Zhauniarovich Y. High stakes, low certainty: evaluating the efficacy of high-level indicators of compromise in ransomware attribution. In: Proceedings of the 34th USENIX Security Symposium (USENIX Sec), SEC'25; 2025 Aug 13–15; Seattle, WA, USA.
171. Brewer R. Ransomware attacks: detection, prevention and cure. Netw Secur. 2016;2016(9):5–9.
172. Furnell S, Emm D. The ABC of ransomware protection. Comput Fraud Secur. 2017;2017(10):5–11. doi:10.1016/s1361-3723(17)30089-1.
173. Srinivasan CR. Hobby hackers to billion-dollar industry: the evolution of ransomware. Comput Fraud Secur. 2017;2017(11):7–9.
174. O'Kane P, Sezer S, Carlin D. Evolution of ransomware. IET Netw. 2018;7(5):321–7. doi:10.1049/iet-net.2017.0207.
175. Kharraz A, Robertson W, Kirda E. Protecting against ransomware: a new line of research or restating classic ideas? IEEE Secur Priv. 2018;16(3):103–7.
176. Dargahi T, Dehghantanha A, Bahrami PN, Conti M, Bianchi G, Benedetto L. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. J Comput Virol Hacking Tech. 2019;15(4):277–305. doi:10.1007/s11416-019-00338-7.
177. Hull G, John H, Arief B. Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Sci. 2019;8(1):1–22.
178. Keshavarzi M, Ghaffary HR. I2CE3: a dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion. Comput Sci Rev. 2020;36:100233.
179. Berrueta E, Morato D, Magaña E, Izal M. Open repository for the evaluation of ransomware detection tools. IEEE Access. 2020;8:65658–69. doi:10.1109/access.2020.2984187.
180. Hirano M, Hodota R, Kobayashi R. RanSAP: an open dataset of ransomware storage access patterns for training machine learning models. Forensic Sci Int Digit Investig. 2022;40:301314.
181. Hirano M, Kobayashi R. RanSMAP: open dataset of ransomware storage and memory access patterns for creating deep learning based ransomware detectors. Comput Secur. 2025;150:104202.
182. Diamantopoulos D, Pletka R, Sarafijanovic S, Narasimha Reddy AL, Pozidis H. WannaLaugh: a configurable ransomware emulator—learning to mimic malicious storage traces. In: Proceedings of the 17th ACM International Systems and Storage Conference, SYSTOR'24; 2024 Sep 23–24; Virtual. p. 118–31.
183. Molina RMA, Bou-Harb E, Torabi S, Assi C. RPM: ransomware prevention and mitigation using operating systems' sensing tactics. In: Proceedings of 2023-IEEE International Conference on Communications (ICC); 2023 May 28–Jun 1; Rome, Italy. p. 1–6.
184. McDonald G, Papadopoulos P, Pitropakis N, Ahmad J, Buchanan WJ. Ransomware: analysing the impact on Windows active directory domain services. Sensors. 2022;22(3):953.

185. Humayun M, Jhanjhi NZ, Alsayat A, Ponnusamy V. Internet of things and ransomware: evolution, mitigation and prevention. Egypt Inform J. 2021;22(1):105–17. doi:10.1016/j.eij.2020.05.003.
186. Razaulla S, Fachkha C, Markarian C, Gawanmeh A, Mansoor W, Fung BCM, et al. The age of ransomware: a survey on the evolution, taxonomy, and research directions. IEEE Access. 2023;11:40698–723.
187. Benmalek M. Ransomware on cyber-physical systems: taxonomies, case studies, security gaps, and open challenges. Internet Things Cyber Phys Syst. 2024;4:186–202.
188. Almeida F, Imran M, Raik J, Pagliarini S. Ransomware attack as hardware trojan: a feasibility and demonstration study. IEEE Access. 2022;10:44827–39.
189. Reidys B, Liu P, Huang J. RSSD: defend against ransomware with hardware-isolated network-storage codesign and post-attack analysis. In: Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems; 2022 Feb 28–Mar 4; La Jolla, CA, USA. p. 726–39.
190. Oz H, Aris A, Acar A, Tuncay GS, Babun L, Uluagac S. RØB: ransomware over modern web browsers. In: Proceedings of 32nd USENIX Security Symposium (USENIX Security 23); 2023 Aug 9–11; Anaheim, CA, USA. p. 7073–90.
191. Rana MU, Shah MA, Al-Naeem MA, Maple C. Ransomware attacks in cyber-physical systems: countermeasure of attack vectors through automated web defenses. IEEE Access. 2024;12:149722–39.
192. McIntosh T, Kayes ASM, Chen YPP, Ng A, Watters P. Applying staged event-driven access control to combat ransomware. Comput Secur. 2023;128(1):103160. doi:10.1016/j.cose.2023.103160.
193. Raj A, Narayan V, Muskan V, Sani A, Sharma P, Sarma SS. Modern ransomware: evolution, methodology, attack model, prevention and mitigation using multi-tiered approach. Secur Priv. 2024;7(6):e436.
194. Chimmanee K, Jantavongso S. Digital forensic of maze ransomware: a case of electricity distributor enterprise in ASEAN. Expert Syst Appl. 2024;249:123652.
195. Lee S, Kim HK, Kim K. Ransomware protection using the moving target defense perspective. Comput Electr Eng. 2019;78(66):288–99. doi:10.1016/j.compeleceng.2019.07.014.
196. Lee S, Lee S, Park J, Kim K, Lee K. Hiding in the crowd: ransomware protection by adopting camouflage and hiding strategy with the link file. IEEE Access. 2023;11:92693–704.
197. Khan MM, Hyder MF, Khan SM, Arshad J, Khan MM. Ransomware prevention using moving target defense based approach. Concurr Comput Pract Exp. 2023;35(7):e7592. doi:10.1002/cpe.7592.
198. Zhao JY, Kessler EG, Yu J, Jalal K, Cooper CA, Brewer JJ, et al. Impact of trauma hospital ransomware attack on surgical residency training. J Surg Res. 2018;232:389–97. doi:10.1016/j.jss.2018.06.072.
199. Neprash HT, McGlave CC, Cross DA, Virnig BA, Puskarich MA, Huling JD, et al. Trends in ransomware attacks on us hospitals, clinics, and other health care delivery organizations, 2016–2021. JAMA Health Forum. 2022;3(12):e224873. doi:10.1001/jamahealthforum.2022.4873.
200. Dameff C, Tully J, Chan TC, Castillo EM, Savage S, Maysent P, et al. Ransomware attack associated with disruptions at adjacent emergency departments in the US. JAMA Netw Open. 2023;6(5):e2312270. doi:10.1001/jamanetworkopen.2023.12270.
201. Villalba LJG, Orozco ALS, Vivar AL, Vega EAA, Kim T-H. Ransomware automatic data acquisition tool. IEEE Access. 2018;6:55043–52. doi:10.1109/access.2018.2868885.
202. Song Z, Tian Y, Zhang J. Similarity analysis of ransomware attacks based on ATT&CK matrix. IEEE Access. 2023;11:111378–88. doi:10.1109/access.2023.3322427.
203. John TC, Abbasi MS, Al-Sahaf H, Welch I, Jang-Jaccard J. Evolving malice scoring models for ransomware detection: an automated approach by utilising genetic programming and cooperative coevolution. Comput Secur. 2023;129:103215.
204. Anand PM, Charan PVS, Chunduri H, Shukla SK. LARM: linux anti ransomware monitor. Comput Secur. 2025;159:104700.
205. Venturini M, Freda F, Miotto E, Conti M, Giaretta A. Differential area analysis for ransomware: attacks, countermeasures, and limitations. IEEE Trans Dependable Secur Comput. 2025;22(4):3449–64.
206. Cevallos-Salas D, Estrada-Jiménez J, Guamán DS, Urquiza-Aguiar L. Ransomware dynamics: mitigating personal data exfiltration through the SCIRAS lens. Comput Secur. 2025;157:104583.

207. Gray IW, Cable J, Brown B, Cuiujuclu V, McCoy D. Money over morals: a business analysis of conti ransomware. In: Proceedings of 2022 APWG Symposium on Electronic Crime Research (eCrime); 2022 Nov 30–Dec 2; Virtual. p. 1–12.
208. Falco G, Thummala R, Kubadia A. WannaFly: an approach to satellite ransomware. In: Proceedings of the 2023 IEEE 9th International Conference on Space Mission Challenges for Information Technology (SMC-IT); 2023 Jul 18–21; Pasadena, CA, USA. p. 84–93.
209. Beerman J, Berent D, Falter Z, Bhunia S. A review of colonial pipeline ransomware attack. In: Proceedings of 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW); 2023 May 1–4; Bangalore, India. p. 8–15.
210. Zou S, Zhang J, Jiang S, Cheng Y, Ji X, Xu W. OutletGuarder: detecting darkside ransomware by power factor correction signals in an electrical outlet. In: Proceedings of 2022 IEEE 28th International Conference on Parallel and Distributed Systems (ICPADS); 2023 Jun 10–13; Nanjing, China. p. 419–26.
211. Mofidi F, Hounsinou SG, Bloom G. L-IDS: a multi-layered approach to ransomware detection in IoT. In: Proceedings of 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC); 2024 Jan 8–10; Las Vegas, NV, USA. p. 0387–96.
212. Lawall A, Beenken P. A threat-led approach to mitigating ransomware attacks: insights from a comprehensive analysis of the ransomware ecosystem. In: Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference, EICC'24; 2024 Jan 5–6; Xanthi, Greece. p. 210–6.
213. Hansen P, Henry WC, Reith MG, Thummala R, Falco G. Guarding the galaxy: satellite ransomware and countermeasures. In: Proceedings of 2024 IEEE Aerospace Conference; 2024 Mar 2–9; Big Sky, MT, USA. p. 1–6.
214. Holmström A. Managing a ransomware attack: the resilience of a swedish municipality—A case study. In: Proceedings of International Conference on Information Systems Security and Privacy; 2024 Feb 26–28; Lisbon, Portugal.
215. Dhumal A, Ghaleb M, Abdelsalam S, Moldovan A-N, Hamdan M. Zero trust architecture for ransomware defense in virtualized environment. In: Proceedings of the IEEE/ACM 12th International Conference on Big Data Computing, Applications and Technologies; 2025 Dec 1–4; Nantes, France. p. 1–7.
216. Barker WC, Fisher W, Scarfone K, Souppaya M. Cybersecurity framework profile for ransomware risk management. Natl Inst Stand Technol. 2022. doi:10.6028/NIST.IR.8374-draft.
217. Zhu T, Li X, Zhang W. Applying ChatGPT-powered game theory in ransomware negotiations. TechRxiv. 2023. doi:10.36227/techrxiv.170244324.48846520/v1.
218. Fujima H, Kumamoto T, Yoshida Y. Using ChatGPT to analyze ransomware messages and to predict ransomware threats. Res Sq. 2023. doi:10.21203/rs.3.rs-3645967/v1.
219. Kumamoto T, Yoshida Y, Fujima H. Evaluating large language models in ransomware negotiation: a comparative analysis of ChatGPT and claude. Res Sq. 2023. doi:10.21203/rs.3.rs-3719038/v1.
220. Zhang W, Li X, Zhu T. Entropy and memory forensics in ransomware analysis: utilizing LLAMA-7B for advanced pattern recognition. TechRxiv. 2023. doi:10.36227/techrxiv.24742389.v1.
221. Hyslip TS, Burruss GW. Ransomware. In: Handbook on crime and technology. Cheltenham, UK: Edward Elgar Publishing; 2023. p. 86–104.
222. Möller DPF. Ransomware attacks and scenarios: cost factors and loss of reputation. In: Guide to cybersecurity in digital transformation: trends, methods, technologies, applications and best practices. Berlin/Heidelberg, Germany: Springer; 2023. p. 273–303.
223. Kang Q, Gu Y. Enhancing ransomware detection: a windows API min max relevance refinement approach. Preprints. 2023. doi:10.20944/preprints202311.1004.v1.
224. Liu S, Chen X. Applying moving target defense against data theft ransomware on windows OS. Preprints. 2023. doi:10.20944/preprints202312.0948.v1.
225. Horduna M, Lăzărescu S-M, Simion E. A note on machine learning applied in ransomware detection. 2023 [cited 2026 Jan 1]. Available from: https://ia.cr/2023/045.
226. Takeuchi K, Kumamoto T, Yoshida Y, Fujima H. Decentralized identity verification system for data access to prevent data exfiltration ransomware. TechRxiv. 2022. doi:10.36227/techrxiv.24732729.v1.

227. Altais B, Arkwright B, Ashbourne T, Middleham E. Novel algorithmic framework for high-fidelity ransomware detection using entropy-based behavioural signatures. Preprints. 2024. doi:10.31219/osf.io/sdkfj.
228. Panaras A, Silverstein B, Edwards S. Automated cooperative clustering for proactive ransomware detection and mitigation using machine learning. TechRxiv. 2024. doi:10.36227/techrxiv.172684422.25967523/v1.
229. Sarewap R, Muller P, Baker T, Dupont M, Steinberg W. Efficient ransomware detection through dynamic file system traffic analysis: a methodological approach. Preprints. 2024. doi:10.31219/osf.io/xju6w.
230. Miranem V, Petrescu G, Schelling D, Vasiliev A. Ransomware detection on Windows systems using file system activities and a hybrid machine learning approach. Preprints. 2024. doi:10.31219/osf.io/27neh.
231. Moritaka H, Komuro D. Enhanced ransomware detection using dual-layer random forest on opcode sequences. Preprints. 2024. doi:10.22541/au.172193050.02354794/v1.
232. Ozturk M, Yilmaz B, Arslan Z, Demirbas A. An effective strategy for ransomware mitigation on android devices via android OS file system API. Res Sq. 2024. doi:10.21203/rs.3.rs-4299415/v1.
233. Wiles A, Colombo F, Mascorro R. Ransomware detection using network traffic analysis and generative adversarial networks. Preprints. 2024. doi:10.22541/au.172659907.77469627/v1.
234. Gong W, Zha Y, Tang J. Ransomware detection and classification using generative adversarial networks with dynamic weight adaptation. Preprints. 2024. doi:10.31219/osf.io/5vju7.
235. Wang Y, Li Z, Zhang Y. Optimized ransomware detection through reverse bayer analysis of file system activities. Preprints. 2024. doi:10.31219/osf.io/du74g.
236. Eisenwer S, Berenyi S, Zaharoff A, Montrose J, Solberg E, Grimaldi F. Automated detection of ransomware using dynamic code sequence mapping. TechRxiv. 2024. doi:10.36227/techrxiv.173014814.48823875/v1.
237. Stastne S, Johansson S, Laurent S, Kruger T, Fitzgerald G. Dynamic signal-based ransomware detection with temporal-pattern profiling technique. Preprints. 2024. doi:10.22541/au.173083395.56558646/v1.
238. Axali J, Devereaux L, Spencer A, Vasilev F. A multicriteria decision-making approach for ransomware detection using Mitre ATT&CK mitigation strategy. Preprints. 2024. doi:10.22541/au.172591117.70081883/v1.
239. Limer A, Abramovich R, Devereux G, Ziemniak P, Dubois F. Automated ransomware detection using dynamic behavior trace profiling. TechRxiv. 2024. doi:10.36227/techrxiv.173030558.85237080/v1.
240. Neweva W, Fitzwilliam O, Waterbridge J. Forensic analysis of live ransomware attacks on linux-based laptop systems: techniques and evaluation. Res Sq. 2024. doi:10.21203/rs.3.rs-4900486/v1.
241. Zhang R, Liu Y. Ransomware detection with a 2-tier machine learning approach using a novel clustering algorithm. Res Sq. 2024. doi:10.21203/rs.3.rs-4567706/v1.
242. Lowev T, Fisher C, Collins J. Advanced ransomware detection and classification via semantic analysis of memory opcode patterns. Preprints. 2024. doi:10.31219/osf.io/5cfvp.
243. Tariq U. Combatting ransomware in ZephyrOS-activated industrial IoT environments. Heliyon. 2024;10(9):e29917. doi:10.1016/j.heliyon.2024.e29917.
244. Alzonem F, Albrecht G, Castellanos D, Vandermeer M, Stansfield B. Ransomware detection using convolutional neural networks and isolation forests in network traffic patterns. Res Sq. 2024. doi:10.21203/rs.3.rs-5278706/v1.
245. Blaas N, Winterbourne J, Beauregarde W, Heathcote E. Ransomware detection through contextual behavior mapping and sequential dependency analysis. Res Sq. 2024. doi:10.21203/rs.3.rs-5527159/v1.
246. Baston P, Lacroix E, Jackson T, Maitland L, Lehmann E, Shulman M. Hierarchical ransomware detection with adaptive anomaly clustering and threat signature prediction. TechRxiv. 2024. doi:10.36227/techrxiv.173203458.80683063/v1.
247. Bennett E, Ellington J, Blackstone G, Whitfield H, Ashcroft L. Enhanced vectorized ransomware detection: a novel spectral segmentation approach using nonlinear frequency patterns. 2024 [cited 2026 Jan 1]. Available from: https://osf.io/preprints/osf/qd253_v1.
248. Hurley R, Kruger P, Nascimento H, Keller S. Real-time ransomware detection through adaptive behavior fingerprinting for improved cybersecurity resilience and defense. Preprints. 2024. doi:10.31219/osf.io/7d2y5.

249. Loaiza C, Becker J, Johansson M, Corbett S, Vesely F, Demir P. Dynamic temporal signature analysis for ransomware detection using sequential entropy monitoring. TechRxiv. 2024. doi:10.36227/techrxiv.173091147.70647129/v1.
250. Bai H, Hu Y, Liu Q, Zhang J, Xu L, Lin H. Ransomware detection on Windows systems using file system activity monitoring and a hybrid XGBoost-isolation forest approach. Preprints. 2024. doi:10.22541/au.172893916.67101182/v1.
251. Schmaltz K, Thompson S, Mendes D, Carvalho J. Robust defense mechanisms against adversarial ransomware attacks: implementing a universal network-level detection filter. Res Sq. 2024. doi:10.21203/rs.3.rs-5123680/v1.
252. Xu B, Wang S. Examining windows file system IRP operations with machine learning for ransomware detection. Res Sq. 2024. doi:10.21203/rs.3.rs-4032456/v1.
253. Lummen D, Gruber S, Schmidt A, Abramov J, Anderson C. Opcode-based ransomware detection using hybrid extreme gradient boosting and recurrent neural networks. TechRxiv. 2024. doi:10.36227/techrxiv.172962886.67904740/v1.
254. Brinkley Y, Thompson D, Simmons N. Machine learning-based intrusion detection for zero-day ransomware in unseen data. Preprints. 2024. doi:10.22541/au.172685266.62026194/v1.
255. Blue E, Campbell G, Stokes A, Thompson L, Clarke J. Ransomware detection on linux operating system using recurrent neural networks with binary opcode analysis. Preprints. 2024. doi:10.31219/osf.io/vzk3d.
256. Feyal J, Matthews R. Quality evaluation of true random bit-streams in ransomware payload bytecode. TechRxiv. 2024. doi:10.36227/techrxiv.172651853.33813035/v1.
257. Keyogeg B, Thompson M, Dawson G, Wagner D, Johnson G, Elliott B. Automated detection of ransomware in windows active directory domain services using log analysis and machine learning. Preprints. 2024. doi:10.22541/au.172779663.36925703/v1.
258. Li G, Wang S, Chen Y, Zhou J, Zhao Q. A hybrid framework for ransomware detection using deep learning and monte carlo tree search. OSF. 2024. doi:10.31219/osf.io/cjyvb.
259. Olabim M, Greenfield A, Barlow A. A differential privacy-based approach for mitigating data theft in ransomware attacks. Preprints. 2024. doi:10.22541/au.172625434.48862692/v1.
260. Hagerty S, Huxley D, Fiennes A, Hartwell L, Pembroke M. Ransomware detection using network traffic patterns: a hybrid approach with isolation forest and gradient boosting. Res Sq. 2024. doi:10.21203/rs.3.rs-5297735/v1.
261. Pavica C, Swanson G, Whitaker R, Johansson S. A feedback controlled optimization approach to minimize ransomware propagation in internet of things networks. Preprints. 2024. doi:10.31219/osf.io/8qkva.
262. Argene M, Ravenscroft C, Kingswell I. Ransomware detection via cosine similarity-based machine learning on bytecode representations. Preprints. 2024. doi:10.22541/au.172348750.00074165/v1.
263. Ozturk M, Demir A, Arslan Z, Caliskan O. Dynamic behavioural analysis of privacy-breaching and data theft ransomware. Res Sq. 2024. doi:10.21203/rs.3.rs-4097219/v1.
264. LaRocque A, Gross G, Lindholm F, Greco P, Dupont B, Kruger J. Effective ransomware detection using autonomous patternbased signature extraction. Preprints. 2024. doi:10.22541/au.173016272.26231350/v1.
265. Koike S, Tanaka H, Maeda M. Federated learning-based ransomware detection via indicators of compromise. Res Sq. 2024. doi:10.21203/rs.3.rs-4585988/v1.
266. Azugo P, Venter H, Nkongolo MW. Ransomware detection and classification using random forest: a case study with the UGRansome2024 dataset. arXiv:2404.12855. 2024.
267. Matae T, Fentiman K, Kingsleigh S, Antonovich J. Introducing adaptive sequence embedding for effective ransomware detection. Preprints. 2024. doi:10.22541/au.173161592.25153018/v1.
268. Wasoye S, Stevens M, Morgan C, Hughes D, Walker J. Ransomware classification using BTLS algorithm and machine learning approaches. Res Sq. 2024. doi:10.21203/rs.3.rs-5131919/v1.
269. Jabid T, Masum S, Shams RA, Chowdhury A, Islam MM, Ferdaus MH, et al. A brief history of ransomware. In: Ransomware evolution. Boca Raton, FL, USA: CRC Press; 2024. p. 3–17.
270. Long J, Liang H. Ranaway: a novel ransomware-resilient refs file system. Res Sq. 2024. doi:10.21203/rs.3.rs-3960276/v1.

271. Gihavo D, Ivanovich O, Harrison A, Merritt L, Schneider V. Automated file trap selection using machine learning for early detection of ransomware attacks. TechRxiv. 2024. doi:10.36227/techrxiv.172840476.68122495/v1.
272. Guo J, Liang H, Long J. Leveraging file system characteristics for ransomware mitigation in linux operating system environments. Res Sq. 2024. doi:10.21203/rs.3.rs-4308346/v1.
273. Williams M, Morales R, Johnson K, Martinez G, Bennett J. Entropy-based network traffic analysis for efficient ransomware detection. TechRxiv. 2024. doi:10.36227/techrxiv.172840776.66718131/v1.
274. Wu Y, Chang Y. Ransomware detection on linux using machine learning with random forest algorithm. TechRxiv. 2024. doi:10.36227/techrxiv.171778770.06550236/v1.
275. Gupret E, Turner A, Evans C, Morgan R, Richardson M. Dual-layer ransomware classification using opcode and network traffic similarity. Preprints. 2024. doi:10.22541/au.172719839.91919526/v1.
276. Schuetz SW, Chen Y, Forderer J, Ma Y. Does ransomware make investors "WannaCry?" on investors' divergent reactions to ransomware hits and near misses. MIS Q. 2025;49(3):1153–68. doi:10.25300/misq/2024/18509.