www.ijarp.com ISSN 2456-9992
Page 1 to 8
International Journal Advanced Research Publication

Research-Article
Volume: 2
Issue: 11

RANSOMWARE DETECTION AND MITIGATION: A SYSTEMATIC SURVEY OF MACHINE LEARNING, DEEP LEARNING, AND BLOCKCHAIN-BASED APPROACHES

1Kaushal Trivedi, 1Shoaib Shaikh, and 1Chirag Sharma, *2Dr. Shashikant Mahajan

1Department of Information Technology, Vidyalankar Institute of Technology, Mumbai, India.

2Cyber Security Minor Specialization Track

Article Received	Article Revised	Published
25-09-2026	15-10-2026	04-11-2026

***Corresponding Author:** Shashikant Mahajan
Cyber Security Minor Specialization Track
DOI: https://doi-doi.org/101555/ijarp.4325

ABSTRACT

Ransomware has grown from scattered, opportunistic attacks into an organized criminal business, and the research written to counter it has grown just as quickly and in just as many directions. The result is a literature that is rich but scattered. Work on malware analysis, machine learning, blockchain forensics and healthcare security tends to be published in separate venues, and a newcomer has little help in judging which technique suits which environment. This paper surveys 18 sources published mostly between 2019 and 2026 and sorts them into six groups: machine learning detection, deep learning detection, systematic reviews, cloud and industrial detection, blockchain-based payment analysis, and healthcare and IoT studies. We compare the reviewed work by technique, dataset, strengths and weaknesses, and then draw out the gaps that keep recurring. Three stand out: detectors that struggle with zero-day and obfuscated variants, datasets that are old, scarce or synthetic, and evaluation practices that make results hard to compare. We close with five directions for future work.

KEYWORDS: *Ransomware, Malware Detection, Machine Learning, Deep Learning, Blockchain Forensics, Healthcare Security, Iot, Systematic Survey.*

1. INTRODUCTION

Ransomware is malicious software that locks a victim out of their own systems or data, most often by encrypting files, and then demands payment, usually in cryptocurrency, in exchange for restored access. Since the middle of the 2010s the threat has changed shape. Early campaigns were broad

and indiscriminate. Today the dominant model is Ransomware-as-a-Service (RaaS), in which developers lease their toolkits to affiliates and take a share of whatever ransom is collected. That arrangement removes much of the technical skill once needed to run an attack, which partly explains why incidents have become more frequent, larger and more sophisticated. Individuals, enterprises, critical infrastructure and, with growing regularity, hospitals are all targets.

The better-known families, including LockBit, BlackCat (ALPHV), BianLian, Conti and Ryuk, rely on a familiar set of tactics. They steal data before encrypting it and threaten to publish it, a practice known as double or triple extortion. They use legitimate system tools to avoid raising alarms, escalate privileges, and move laterally through cloud and on-premises networks. Defensive research has responded on several fronts: signature-based detection, behavioral and dynamic analysis, machine learning (ML) and deep learning (DL) classifiers, blockchain forensics to follow ransom payments, and sector-specific frameworks for healthcare and industrial control systems (ICS).

That breadth is also the problem. A researcher or security engineer who wants to know which method fits an endpoint, an IoT device, a cloud store or a factory network must read across several disciplines that rarely cite one another. The same goes for datasets, whose quality and age vary widely. This paper addresses that difficulty by consolidating recent work in one place. Its objectives are to review the literature on ransomware detection, classification and mitigation; to group the studies by method; to compare their techniques, datasets, strengths and limitations; to identify the gaps that remain; and to suggest where future effort would be most useful.

2. RESEARCH METHODOLOGY

2.1 Sources and search terms

Searches were run across IEEE Xplore, the ACM Digital Library, SpringerLink, ScienceDirect, MDPI journals, arXiv, Google Scholar, and venues indexed by Scopus and Web of Science. Industry threat-intelligence material, notably from Health-ISAC, was consulted as well so that the academic findings could be set against real incident data. Queries paired “ransomware” with terms such as “machine learning,” “deep learning,” “blockchain,” “Bitcoin,” “healthcare,” “IoT,” “cloud,” “industrial” and “systematic literature review.” Results were limited to work from 2019 to 2026, with extra attention to the most recent five years.

2.2 Selection criteria

A paper was kept only if it met all of the following conditions.

- Relevance: it directly addresses ransomware detection, classification, forensic tracing or mitigation.
- Recency: at least ten selected papers fall within 2021–2026, although a few earlier foundational works were retained for context.
- Source quality: it appears in a recognized publisher or indexed venue, or comes from an established threat-intelligence organization.

- Accessibility: open-access papers and freely downloadable PDFs were preferred.
- Diversity: the set had to span several methodological families instead of a single narrow technique.

Eighteen papers satisfied these conditions and form the basis of the analysis that follows.

3. Literature Review

The reviewed work falls naturally into six categories. Each is discussed below, and Section 4 brings the evidence together in a single table.

3.1 Machine learning–based detection

Islam et al. [1] offer a wide-ranging review of ML approaches to ransomware detection. They cover classifiers such as Random Forest, Support Vector Machines, Decision Trees and Artificial Neural Networks, and they catalogue the features that studies most often rely on, namely API calls, file entropy and network traffic. Because it is a review, the paper produces no new experimental results, but it is useful as a map of the field. El Hariri et al. [2] move from survey to system. Their framework combines entropy and frequency analysis with several classifiers (MLP, Decision Tree, Random Forest, KNN and Logistic Regression) and is aimed at IoT ecosystems. Accuracy on their custom IoT dataset is strong, though the evaluation covers only a particular set of devices. A comparative study in JISIS [8] tests several algorithms against each other to find the most discriminative features, but its dataset is narrow, which limits how far the conclusions can be pushed.

3.2 Deep learning–based detection

Vanetik [4] applies LSTM and CNN-style models to sequences of API calls, so that ransomware is recognized by what it does rather than by a fixed signature. This is what makes the approach attractive against zero-day and previously unseen families. The price is heavier computation and the need to monitor programs while they run. RansomTrack [5] follows a similar behavioral logic but grounds it in low-level telemetry, combining ML with the RanSAP and RansMAP datasets of storage and memory access patterns. The detection signal is richer as a result, yet the method needs kernel-level instrumentation, which not every endpoint can accommodate. Kritika [9] steps back and reviews 23 papers from 2017 to 2024 on CNN, RNN and hybrid architectures. The conclusion is that hybrid models usually beat single-architecture ones, and that progress is held back by a shortage of large labeled ransomware datasets.

3.3 Systematic literature reviews

Two systematic reviews were included to capture trends at the meta level. The review in Information [3] pulls together early-detection signs, frameworks and techniques from papers published between 2020 and 2024. The review presented at ICOCI [6] looks more closely at detection methods and mitigation tooling, and it treats backup strategies and network segmentation as defenses that complement detection rather than replace it. Both are helpful for cross-checking the findings of primary studies. Being secondary sources, neither adds quantitative results of its own.

3.4 Cloud and industrial environments

Generic endpoint detectors do not always carry over to specialized settings, and two papers address this directly. Rhea [7] targets ransomware that has escalated its privileges inside cloud storage services and tries to hide, using format-aware validation to spot it. The topic is timely given how much critical data now sits in the cloud. CanCal [14] works in the opposite environment, industrial control systems, where real-time response and tight resource limits rule out heavy tools.

It proposes a lightweight detection-and-response pipeline built for those constraints. Both studies show that a design tailored to its environment can outperform a general-purpose solution there. Neither generalizes well beyond the setting it was built for.

3.5 Blockchain and cryptocurrency-based detection

Since most ransom demands are paid in cryptocurrency, one line of research follows the money. Paquet-Clouston et al. [15] set out the foundational method. They analyzed Bitcoin transactions tied to 35 ransomware families to estimate a lower bound on the financial damage ransomware causes. Their data cover 2013 to 2017, so they predate the RaaS era. Mutombo [13] later applied ensemble ML, using Lazy Predict, to the UGRansome dataset in order to recognize zero-day exploits from blockchain transaction features. A 2024 study [16] used decision-tree and ensemble classifiers on Bitcoin data to separate ransom payments from ordinary transactions. More recently, a TabNet deep learning model applied to the BitcoinHeist dataset [17] reached a recall of 0.61, better than traditional ML baselines, but its F1-score was only 0.55. That gap tells us the problem is far from solved. It also leaves a blind spot: none of this work addresses privacy-preserving currencies such as Monero, which attackers increasingly favor.

3.6 Healthcare and IoT

Healthcare is among the most heavily targeted sectors, because patient data is sensitive and hospitals cannot tolerate downtime. An early survey [18] maps the ransomware risks and mitigation opportunities for healthcare IoT (HC-IoT) in the literature from 2017 onward. A scoping review published in early 2026 [10] takes a broader view of cybersecurity and privacy in healthcare and explicitly connects ransomware incidents to patient-safety risk. Elsayed et al. [11] concentrate on attacks against IoT and Internet-of-Medical-Things devices, including ransomware, DDoS and man-in-the-middle attacks, although they stop short of proposing a detection method. Finally, the Health-ISAC 2025 threat landscape report [12] anchors the academic material in real incident data, documenting campaigns by LockBit 3.0, BlackCat/ALPHV and BianLian against hospitals and blood suppliers. Because it is a vendor-produced report, it has not been through peer review, a point worth bearing in mind when weighing its statistics.

4. Comparative Analysis

Table 1 lists the technique, dataset and main limitation of each of the 18 reviewed papers. The strengths of each work are discussed in Section 3 and are not repeated here.

Table 1. Comparative summary of the reviewed papers.

Ref.	Year	Technique	Dataset	Principal limitation
[1]	2024	ML review (RF, SVM, DT, ANN)	Aggregated public datasets	No new experiments; relies on secondary data
[2]	2025	Hybrid entropy and frequency analysis with MLP, DT, RF, KNN, LR	Custom IoT ransomware traffic	Testbed limited to specific IoT devices
[3]	2024	Systematic literature review (2020–2024)	Secondary review	Excludes non-English and non-indexed sources
[4]	2024	LSTM/CNN on API call sequences	API call sequences	High computational cost; needs runtime monitoring
[5]	2025	Hybrid behavioral analysis (ML with storage and memory patterns)	RanSAP / RansMAP	Requires kernel-level instrumentation
[6]	2024	Systematic review of detection methods and tools	Secondary review	Limited quantitative cross-study comparison
[7]	2026	Format-aware validation in the cloud	Cloud storage access logs	Cloud-specific; does not transfer to on-premises
[8]	2025	Comparative ML evaluation	Public malware feature sets	Narrow dataset scope
[9]	2024	Literature review of DL (CNN, RNN, hybrid)	23 papers, 2017–2024	Notes scarcity of labeled samples
[10]	2026	Scoping review of healthcare cybersecurity	PRISMA-based review	Broad scope dilutes ransomware depth
[11]	2025	Review of IoT/IoMT attack vectors	Survey	No concrete detection methodology
[12]	2025	Industry threat-intelligence analysis	Real incident telemetry	Not peer-reviewed; vendor-produced
[13]	2024	Ensemble ML (Lazy Predict) on blockchain features	UGRansome (BTC)	Class imbalance in transaction labels
[14]	2024	Lightweight real-time detection and response	ICS traffic	Evaluated only in industrial/OT settings
[15]	2019	Blockchain transaction-graph forensics	Bitcoin, 35 families (2013–2017)	Historical data; predates modern RaaS
[16]	2024	Decision tree / ensemble classification	Bitcoin transactions	Ignores privacy coins such as Monero
[17]	2025	TabNet on transaction graph features	BitcoinHeist (2009–2018)	Moderate F1-score (0.55); dated window
[18]	2021	Survey of HC-IoT ransomware risks	Literature, 2017–2025 scope	Predates post-pandemic surge

Reading down the table, a few patterns appear. First, the evidence base is lopsided. Seven of the 18 entries are reviews or reports with no experimental component of their own ([1], [3], [6], [9], [10], [11] and [12]), so the number of papers that actually test a detection method is smaller than the headline count suggests. Second, nearly every method comes with a dependency that narrows its use: kernel-level access, runtime monitoring, a particular device testbed, or a particular platform. Third, datasets recur. BitcoinHeist, UGRansome and the Bitcoin transaction collections underpin most of the blockchain work, and the age of that data matters, as discussed below.

5. DISCUSSION

Taken together, the studies show that behavioral and hybrid ML/DL approaches can now detect both known and zero-day ransomware with encouraging results. Blockchain forensics has made it possible to put numbers on the scale of the ransomware economy, and domain-specific

frameworks now exist for cloud, industrial and healthcare settings. Those are real advances.

They sit alongside a persistent tension between accuracy and cost. The behavioral methods that cope best with unseen variants [4], [5] are also the ones that demand runtime monitoring or kernel instrumentation. That overhead may be acceptable on a server and is much harder to justify on a medical device or an industrial controller. The environment-specific systems [7], [14] avoid some of that cost by narrowing their scope, but they pay for it in portability. No reviewed approach delivers generalizability, low overhead and high precision at the same time.

The blockchain thread raises a different concern. Moderate scores such as the 0.55 F1 reported in [17] suggest that separating ransom payments from legitimate transactions is difficult, and the reliance on Bitcoin leaves open what happens when payments move to privacy-preserving coins. Meanwhile the healthcare literature [10], [11], [18] documents the risk well but offers little in the way of tested detection. Industry reporting [12] shows that the families actually active in hospitals are the same ones the academic datasets often fail to represent.

6. Research Gaps

6.1 Technical gaps

- Most ML and DL detectors are tested against known families and lose accuracy on zero-day or heavily obfuscated variants, especially those that use legitimate system tools.
- Cloud and ICS/OT detectors stay tied to their own platforms and do not extend to hybrid or multi-cloud deployments.
- Payment classifiers such as the TabNet approach in [17] focus on Bitcoin and ignore privacy coins like Monero.
- API-sequence and behavioral methods [4], [5] often need kernel-level or runtime instrumentation, which may be impractical on constrained IoT and IoMT devices.

6.2 Dataset limitations

- Widely used datasets such as BitcoinHeist and UGRansome reflect activity from 2009 to 2020 and miss the tactics of modern RaaS operators such as LockBit 3.0 and BlackCat.
- Public, labeled behavioral datasets, including storage and memory traces and API call sequences, are scarce. This restricts reproducibility and cross-study comparison, a point stated explicitly in [9].
- Healthcare and IoT datasets are mostly synthetic or testbed-generated [2], which limits confidence in real-world performance.

6.3 Performance and evaluation limitations

- Reported performance varies widely and is hard to compare, because studies use different metrics, data splits and evaluation protocols.
- Several blockchain classifiers report only moderate F1-scores (0.55 in [17]), pointing to an unresolved balance between recall and precision.
- The systematic reviews [3], [6] note that false-positive rates for production-grade deployments are rarely reported, which makes operational viability difficult to judge.

7. Future Research Directions

The gaps above point toward five priorities.

- Large, public and regularly updated behavioral datasets that reflect current RaaS tactics, so that models are trained and tested against threats that exist today.
- Lightweight detection architectures that can run on resource-constrained IoT, IoMT and OT devices without a serious loss of accuracy.
- Extension of blockchain forensics to privacy-preserving cryptocurrencies, so that analysis does not stop where payments become harder to trace.
- Standardized metrics and evaluation protocols, including routine reporting of false-positive rates, so that studies can be compared fairly.
- Closer ties between academic detection research and live threat-intelligence sources such as Health-ISAC [12], to keep proposed solutions aimed at the families that are active in the wild.

8. CONCLUSION

This survey examined 18 papers on ransomware detection and mitigation, grouped into machine learning, deep learning, systematic reviews, cloud and industrial detection, blockchain payment forensics, and healthcare and IoT research. Most of them were published within the past five years. The field has matured: hybrid behavioral models handle many unseen variants, blockchain analysis exposes the scale of ransom payments, and tailored frameworks exist for specialized environments. Even so, the comparison shows that no single method yet combines generalizability, low overhead and high precision. Outdated or synthetic datasets, inconsistent evaluation and limited reporting of false positives make progress harder to measure than it should be. Addressing these weaknesses, as outlined in Section 7, would do much to improve the resilience of individuals, organizations and critical infrastructure against a threat that continues to change.

REFERENCES

1. M. R. Islam, M. Z. Islam, and M. A. Khan, “Ransomware detection using machine learning: A review, research limitations and future directions,” IEEE Access, vol. 12, pp. 68785–68806, May 2024.
2. A. El Hariri et al., “Realtime ransomware process detection using an advanced hybrid approach with machine learning within IoT ecosystems,” Eng. Res. Express, vol. 7, no. 1, art. 015211, Jan. 2025.
3. “Earlier decision on detection of ransomware identification: A comprehensive systematic literature review,” Information, vol. 15, no. 8, art. 484, Aug. 2024.
4. N. Vanetik, “Early ransomware detection with deep learning models,” Future Internet, vol. 16, art. 291, Aug. 2024.
5. “RansomTrack: A hybrid behavioral analysis framework for ransomware detection,” arXiv:2604.08739, 2025.
6. “A systematic literature review of ransomware detection methods and tools for mitigating potential attacks,” in Proc. Int. Conf. Comput. Inform. (ICOCI), CCIS vol. 2001, pp. 80–95, 2024.
7. “Rhea: Detecting privilege-escalated evasive ransomware attacks using format-aware validation in the cloud,” arXiv:2601.18216, 2026.

8. “Ransomware detection with machine learning,” J. Internet Serv. Inf. Secur. (JISIS), vol. 15, no. 1, Feb. 2025.
9. E. Kritika, “A comprehensive literature review on ransomware detection using deep learning,” Cyber Secur. Appl., art. 100078, 2024.
10. “A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems,” Appl. Sci., vol. 16, no. 3, art. 1511, Feb. 2026.
11. N. Elsayed et al., “Cybersecurity and frequent cyber attacks on IoT devices in healthcare: Issues and solutions,” arXiv:2501.11250, Jan. 2025.
12. Health-ISAC, “2025 health sector cyber threat landscape,” Health-ISAC Annu. Threat Rep., 2025.
13. E. N. Mutombo, “Blockchain security for ransomware detection,” arXiv:2407.16862, 2024.
14. S. Wang, F. Dong, H. Yang, J. Xu, and H. Wang, “CanCal: Towards real-time and lightweight ransomware detection and response in industrial environments,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), pp. 2326–2340, 2024.
15. M. Paquet-Clouston, B. Haslhofer, and B. Dupont, “Ransomware payments in the Bitcoin ecosystem,” J. Cybersecur., vol. 5, no. 1, art. tyz003, 2019.
16. “Machine learning-based ransomware classification of Bitcoin transactions,” J. King Saud Univ. Comput. Inf. Sci., 2024.
17. “Ransomware transaction detection on the blockchain with the TabNet model,” in Proc. IEEE Conf., 2025.
18. “A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research,” IEEE Access, vol. 9, pp. 121395–121417, 2021.