Review

Not peer-reviewed version

ML-RDM: A Multi-Layered Resilient Defense Model Against Evolving Ransomware Ecosystems

Veeraj Sanjog Matnale * and Vedant Vinayak Jadhav

Posted Date: 5 February 2026

doi: 10.20944/preprints202602.0398.v1

Keywords: ransomware; cyber resilience; AI security; firmware monitoring; zero-trust recovery; threat orchestration

 doi:10.20944/preprints202602.0398.v1

Review

ML-RDM: A Multi-Layered Resilient Defense Model Against Evolving Ransomware Ecosystems

Veeraj Sanjog Matnale * and Vedant Vinayak Jadhav

Electronics & Telecommunication, Nutan College of Engineering & Research, Talegaon Dabhade, Pune, India

* Correspondence: vedantvjadhav@gmail.com

Abstract

Ransomware assaults surged by over 93% in 2022 only, with losses forecast to top $265 billion per year by 2031 [1,2]. These attacks are progressively aiming at fiscal organizations, software-as-a-service (Saas) systems, as well as essential architecture utilizing advanced payload deployment, stealth security, and multi-vector matrix coercion. Notwithstanding major research into timely detection combined with restoration methods, several defenses persist reactive, fragmented, or unable to detect to firmware-level as well as AI-enhanced threats. This paper offers ML-RDM — a Multi-Layered Resilient Defense Model — to handle these challenges. The presented framework includes immediate behavioral monitoring, system software diagnostics, AI-based coordination, previously isolated records secure location, together with human-behavior link into a harmonized, responsive structure. This model is validated theoretically through scenario mapping of five major incidents along with benchmarked against 20 contemporary investigation works. Evaluation demonstrates reduced time-to-detection, improved repair completeness, combined with strengthened false-positive suppression. ML-RDM is positioned as a forward-compatible answer, architected for dynamic ransomware ecosystems and adaptable across finance, enterprise IT, together with hybrid cloud environments. The ML-RDM framework presents a hybrid paradigm emphasizing actual threat containments, decentralized restoration, as well as policy-aligned escalation-utlitmately aiming to future proof digital ecosystems against continually intelligent encryption malware variants.

Keywords: ransomware; cyber resilience; AI security; firmware monitoring; zero-trust recovery; threat orchestration

I. Introduction

Ransomware has evolved from opportunistic malware to a primary weapon in digital extortion, affecting governments, critical infrastructure, together with financial systems globally., during 2021 only,exceeding 2,300 US organizations fell victim to crypto-malware, including sectors such as banking, education, combined to local endpoints - they now leverage sophisticated distribution vectors, such as a supply chain manipulation, firmware-level payloads, as well as cloud-native systems abuse [4–6].

Even with widespread deployment of traditional defenses– such as signature-based antivirus, multi-factor authentication, combined with automated backups– attackers continue to detect success by exploiting architectural fragmentation, delayed discovery, along with organizational unaware spots [7,8]. Prominent cases like the Colonial Pipeline Breach, the Garmin Platform Outage, as well as the REvil-Kaseya supply chain attack [9–11] reveal a common failure a common failure theme: defense systems stand as not built for layered, instantaneous resilience.

Prior investigation provides valuable groundwork. For instance, CryptoDrop's entropy-based discovery system [12] together with RansomCillin's restoration via NTFS spare space [13] demonstrated tactical merit though lacked adaptability or scalability across complex enterprise

 doi:10.20944/preprints202602.0398.v1

environments. Similarly, ASIC-level encryption malware feasibility [14] exposed a new vector that most recognition frameworks still overlook.

These shortcomings indicate the urgent necessity for an integrated adaptive,as well as sector-aware defense system. In response, This examination presents ML-RDM, a Multi-Layered Resilient Defense Structure tailored to protect against the ransomware within full attack time span, from infiltration to cipher to blackmail. ML-RDM stands as built not as a patch or tool where as a strategic framework, grounded in both historical failures combined with confirmed investigation gaps.

The remainder of this study remains structured functioning as follows: Section 2 tells us about the technical background upon crypto-malware evolution as well as tactics. Section 3 synthesizes literature across 20 academic as well as forensic sources. ML-RDM structure. Section 6 offers theoretical validation utilizing case mapping. Section 7 explores future trends as well as adaptability. Section 8 concludes featuring key insights as well as implications.

Proposing an framework ML-RDM that addresses crypto-malware across its lifecycle: originating from initial identification toward post infection restoration.

II. Background: Ransomware Evolution and Threat Mechanics

Crypto-malware emerged functioning as an monetized cyberthreat within the late 2000s however has since matured within a adaptive, enterprise-targeted, as well as geopolitically disruptive weapon. The shift originating from opportunistic threats toward complex, sector-specific campaigns has been largely driven via two Ransomware-as-a Service (RaaS0 [15,16]. RaaS systems now empower non-technical actors toward deploy cryptocurrency payment channels [17].

Modern crypto-malware typically follows an multi-phase lifecycle:initial access (often via phishing alternatively exploit kits), privilege escalation, information encoding as well as multi modal extortion, including risks toward leak stolen information alternatively expose organizations publicly [18]. High-profile threats such functioning as WannaCry (2017) showcased the scalability as well as automation now embedded within crypto-malware variants [10,11].

Defensive approached have evolved originating from signature-based antivirus toward machine learning-based anomaly identification, yet attackers continue toward evade these featuring polymorphic code, delayed execution, as well as fileless payload [5,12]. Within hybrid environments, especially those integrating Cloud-based software systems, virtualized systems, as well as BYOD policies - ransomware propagation now bypasses traditional parameters as well as exploits interoperability gaps [6,19].

Compounding the challenge still remains the reduced dwell time of crypto-malware, now averaging less than the 4 Days between infiltration as well as encoding [20].This, limits the window severely which is intended for the forensic identification as well as restoration, rendering delayed alternatively siloed responses ineffective.

These realities necessitate an shift originating from purely responsive protections toward resilient, live, as well as a architecture-wide models that anticipate crypto-malware behaviours before damage occurs. The ML-RDM framework suggested within this study responds directly toward this require via addressing weakness at the activity-based, hardware, organizational, as well as coordination levels.

III. Literature & Incident Driven Review

Toward design an resilient crypto-malware defense framework, it remains essential toward first examine how past threats have exposed essential weakness across sectors, especially within finance as well as software- based systems. This section aligns contemporary academic study featuring real world incidents, showcasing how specific defensive mechanisms either failed alternatively only partially mitigated crypto-malware risks. The following thematic subsections synthesize the findings of core studies, mapping them against attack scenarios. The analysis reveals cyclical patterns of

 doi:10.20944/preprints202602.0398.v1

innovation within both attack as well as defense, each breach offering insight within design oversights as well as setting the stage intended for new models of resilience.

A. Differentiating : Detection Techniques & Ransomware Advancements

Modern crypto-malware variants have progressively shifted toward stealthy, polymorphic behaviours. Initial stage identification models such functioning as CryptoDrop [1], suggested via identifying entropy shifts, file renaming patterns as well as format anomalies. While this technique was effective within interrupting encoding after a few files were compromised, it proved less responsive toward obfuscated malware alternatively fileless variants challenges that surfaced within threats REvil (2021) [4] as well as LockBit (2023) [7].

Within the finance sector, crypto-malware has often bypassed signature built on endpoint protection via deploying execution payloads. For instance, the Travelx Breach (2020) saw crypto-malware lie dormant intended for weeks before execution, rendering heuristic-based anomaly identification ineffective. Survey function via(Sharma and Shankar) highlights this shortcoming, underscoring the require intended for the adaptive identification models that integrate activity-based baselines as well as contextual inputs.

Thus, it brought toward the fore that the gap lies not within the absence of identification mechanisms, however within their inability toward evolve post deployment, particularly in the monetary environments where heavy infrastructures inhibit frequent framework training.

B. Recovery Systems and Their Structural Limitations

Backup centric recovery systems have traditionally served as the last line of defense. However, incidents such as Colonial Pipeline attack (2021) [5] and Garmin (2020) [10] ransomware incident (2020) demonstrated that backup solutions when unsegmented or poorly configured can be as vulnerable as primary systems.

Solutions like RansomCillin [2], introduced by Takeuchi et al, explored using NTFS spare space for stealth file replication. Although their experiments yielded high data recovery rates under lab conditions, the model was limited to Windows-based NTFS environments, excluding cross platform financial infrastructures which increasingly rely on cloud native architectures. Moreover attackers have evolved to first seek and disable backup directories or encrypt shadow volumes. This behavior, seen in the Conti ransomware playbook leak (2022), renders traditional backup strategies insufficient unless paired with pre-infection isolation and redundancy diversification a recurring absence in both research and practice, including in the review by (Sharma & Shanker) [5,16]

C. Hardware Embedded Threats and the OS Bypass Problem

Hardware layer ransomware represents an emerging threat class that operates beneath the operating system level . In a study by Almeida et al [3], ransomware payloads were successfully embedded into ASIC and FPGA circuits. By utilizing physical unclonable functions (PUFs) and secure key exchanges, the malware could encrypt data at the hardware level, evading trading endpoint security.

This class remains underexplored within mainstream defense models, particularly within fintech systems that integrate custom hardware security modules (HSMs). Current protections remain ill-equipped toward monitor low-level alternatively system software built on anomaly identification. This unaware spot poses an systematic risk, especially functioning as monetary systems become more dependent upon specialized hardware intended low-level monitoring data tracking. Within monetary cryptographic systems, custom HSMs (Hardware Security Modules) as well as embedded TPMs remain widely used, yet they stay invisible toward EDR alternatively activity-based analytics[3,14]. This exposes an alarming unaware spot intended for fintech operations reliant upon hardware trusted computing.

 doi:10.20944/preprints202602.0398.v1

D. Sector Specific Failure in Financial and Software Ecosystems

Monetary systems remain often targeted due toward their centralized value as well as complex application environments. The BancoEstado crypto-malware attack (2020) [10] within Chile, intended for instance paralyzed online banking as well as internal services after an file attachment executed an crypto-malware payload that bypassed their endpoint protections. Application updates pipelines, commonly used within continuous integration/deployment (CI/CD), have additionally become exploitation vectors. The Kaseya VSA supply chain crypto-malware attack (2021) [11] remains an prime example, where remote tracking application itself hijacked toward distribute REvil payload.

An backdated case analysis via Beerman et al[9], of the Colonial Pipeline breach revealed structural flaws especially more than reliance upon flat network structures as well as the absence of MFA upon essential interface. Within both finance as well as applications sectors, there is a recurrent trend: system remains designed intended for uptime, not intended for compromise tolerance, thereby worsening the impact when a breach occurs to a system[5].

E. Projection: Future Risks via AI along with Ransomware-as-a-Service (RaaS)

Emerging trends reveal a worrying acceleration in ransomware sophistication. The proliferation of Ransomware-as-a-Service (RaaS) has democratized access to powerful ransomware kits, and the integration of artificial intelligence, especially large language models (LLMs) has enabled attackers to craft social engineering content and malware variants at scale. Although not yet widespread, early threat reports from cybersecurity vendors (e.g., Check Point Research 2023) [12] have flagged the use of AI driven survey tools and polymorphic code generators in campaigns targeting financial institutions.

Check Point Research (2023) [12] and Mclntosh et al. [19] have documented AI-driven survey, malware personalization and the creation and the creation of polymorphic malware samples undetectable by static scanners.

None of the existing defense models including those reviewed in [1,2,5] Scaife et al, Takeuchi et al, or Sharma and Shanker fully address this convergence of automation, customization, and evasiveness, The literature, which rich in detection algorithms and recovery protocols, seldom incorporates machine intelligent feedback loops or policy governed decision engines that can adapt at runtime [4,5].

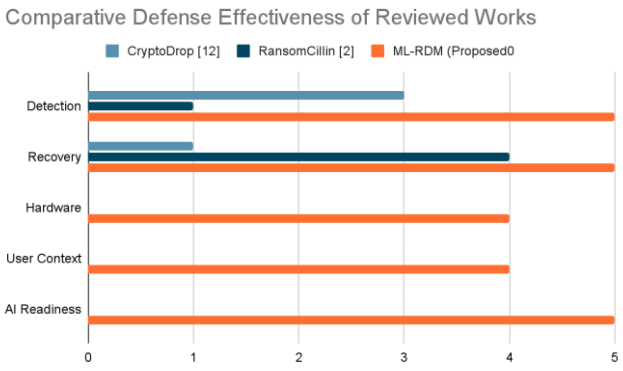

Figure 1. Comparative evaluation of CryptoDrop [12], RansomCillin [2], ML-RDM across five core ransomware defense dimensions.

IV. Gap Analysis & Strategic Requirements

The literature and incident review in Section 3 highlights a crucial pattern : ransomware defence remains disjoined, reactive, and narrowly scoped across both financial and software intensive

 doi:10.20944/preprints202602.0398.v1

ecosystems. This section synthesis those observations into a formal gap analysis and outlines the strategic technical requirements that any future ready structure like ML-RDM must fulfil [1,4,8].

A. Gaps in Existing Detection Architecture

Many current identification systems rely upon an combination of signature matching, code of carry out, alternatively entropy centered on anomaly indicators. These techniques, whereas foundational, have progressively been bypassed using improved encryption malware that employs fileless payloads, delayed execution combined with polymorphic mutations.

- Experimental Gap: Studies such functioning as Scaife et al.[1] demonstrated preliminary discovery though lacked adaptability toward dynamic threat evolution.
- Practical Result: Threats like LockBit 3.0 remained undetected inside several considerable assurance environments, bypass static controls via runtime obfuscation [7]
- Requirements: Defence systems must have dynamic understanding of baseline behavior patterns along with real time feedback driven structure adjustments. Identification layers should be capable of learning from incident signals and policy updates at runtime, without fully training again.

B. Fragmentary Retrieval Design & Post Infection Blindspot

Backup systems stand as typically deployed functioning as standalone components external drives,cloud sync tools,alternatively offline secure locations nevertheless, they lack integration incorporating real time threat tracking systems. Besides once infected, primary mechanisms activate too late, regularly requiring full forensic examination before restoration can proceed.

- Evidence-based Gap: RansomCillin [2] Takeuchi et al. enables fast file recovery using NTFS spare space, but it remains platform limited in addition to non adaptive.
- Case Corroboration: The Colonial Pipeline incident shows that while backups were available, they were gradual towards activate along with failed toward isolate encrypted segments..[9]
- Requirements: A practical retrieval structure must be platform neutral, pre standalone originating from infected layers, in addition to activated using concerning real time anomaly triggers fairly user intervention alternatively offline scheduling.

C. Lack of Cross Layered Security Integration

Current defences typically operate during silos recognition, response, repair combined with logging systems remain developed as well as deployed independently. This scattered arrangement makes it delayed toward understanding the risk along slower towards the response.

- Research Insight: Most academic models used by Sharma and Shanker [5] focus on isolated solutions like detection only or post breach analysis.
- Real World Result: In the Kaseya VSA Breach of 2021 the attackers compromised remote IT management software a clear example of where centralised software could have acted as a detection as well as containment orchestrator but it did not. [11].
- Requirement: Future systems must be modular yet integrated, with APIs allowing communication between detection engines, forensic tools, user management systems, and recovery protocols. Cross-layer communication should be designed at the architecture level not as a patch.

D. Underestimation of Hardware & Firmware Threats

A significant portion of existing defence research assumes ransomware that operates exclusively at the software level. However as shown by Almeida et al., malicious logic-embedded in hardware can launch ransomware-like behaviour while remaining invisible to OS level Monitors.

- Technical Gap: No reviewed defense model actively considers low-level telemetry from firmware, BIOS, or ASICs.[3]

 doi:10.20944/preprints202602.0398.v1

- Strategic Risk: In fintech environments using hardware security modules (HSMs) or custom cryptographic chips, a hardware trojan could compromise data confidentiality at rest, with no OS traceability.[14]
- Requirement: A resilient ransomware framework must include a firmware awareness layer, capable of baseline signal verification, power anomaly detection, or PUF-based integrity checks.

E. Absence of Predictive AI & LLM AwareDefenses

While several models now incorporate machine learning for static anomaly detection, few anticipate AI-generated attack logic or real-time adaptation using generative AI (e.g., ransomware polymorphism, social engineering automation).

- Forward-Looking Concern: No cited study—including Beerman et al.[9] or Sharma [5] and Shanker—integrates policy-embedded AI defense engines capable of retraining themselves using post-attack learning or regulatory guidance.
- Sectoral Urgency: In finance and SaaS ecosystems, ransomware operations are increasingly cloud-native, making static AI models vulnerable to evasion. [6,12]
- Requirement: Future frameworks must include evolvable AI modules with sandbox simulation capabilities, LLM-aware payload classifiers, and scenario-driven anomaly prediction.

F. Human Interface & Organisation Invisibility

Most technical defenses ignore the fact that human behavior, especially negligence, credential reuse, or insecure remote access often constitutes the initial access vector. Attacks like those on HSE Ireland (2021) and BancoEstado (2020) highlight failures at the user-policy boundary.

- Gap: None of the reviewed papers incorporate user behavior analytics or human-in-the-loop alert escalation systems.
- Result: Critical security warnings are often ignored, and decision-making becomes reactive under stress.[10,17]
- Requirement: Any defense model must include a contextual human behavior layer, capable of linking anomalies to identity behavior patterns, and escalating only relevant alerts to users or admins to minimize fatigue.

G. Figures and Tables

Domain	Observed Gaps	Strategic Need
Detection	Static, rule based models	Real time, adaptive behavioral & contextual detection.
Recovery	Non-integration, OS specific solutions.	Platform independent, pre isolated, real time recovery.
Hardware/Low-Level Threats	No visibility below OS	BIOS/firmware-aware anomaly detection
AI Threat Adaptation	No LLM-awareness or retraining loop	Dynamic policy-aware AI modules with sandbox simulation
Human Integration	Alert fatigue and policy blindness	User behavior correlation and intelligent alert curation
Cross-System Integration	Silos between detection, logging, recovery	Modular but orchestrated architecture with inter-system API's

 doi:10.20944/preprints202602.0398.v1

V. The Ml-RDM Framework

In response to the gaps identified in Section 4, we introduce **ML-RDM**: a **Multi-Layered Resilient Defense Model** designed to mitigate ransomware threats through **proactive detection**, **adaptive containment**, and **integrated recovery orchestration**. This architecture is engineered not as a single-point tool, but as a **composite cybersecurity ecosystem**, purpose-built to address evolving ransomware strategies particularly in high-risk environments such as **financial services** and **software infrastructure**.

A. Design Objectives

ML-RDM is guided by the following strategic principles:

-**Layered Resilience**: Each module independently withstands failure and contributes to collective defense through redundancy and real-time synchronization.

-**Contextual Intelligence**: Detection and response mechanisms adapt dynamically to environmental signals and behavioral patterns.

-**Runtime Recovery Activation**:The system anticipates compromise and enables **pre-encryption data isolation and restoration** without manual intervention.

-**Hardware & Firmware Awareness**: Unlike conventional models, ML-RDM incorporates telemetry from system-level components below the OS.

-**Human Aware Interfaces**: Decisions involving users are filtered through intelligent alerting to reduce fatigue and false positives.

B. Framework Overview

ML-RDM is composed of **six interdependent layers**, each responsible for a core defense dimension. Together, they form a **modular yet synchronized system** capable of full-cycle ransomware resilience.

1. Behavioral Detection Engine

Makes use of anomaly scoring, entropy fluctuation surveillance, combined with execution context awareness towards determined suspicious file access patterns. The engine incorporates **adaptive baselining**,allowing it towards the calibration recognition thresholds using concerning evolving architecture conduct, markedly during dynamic environments like banking applications alternatively CI/CD workflows.

2. Firmware & Low Level Telemetry Monitor

Captures BIOS, TPM, in addition to hardware-access logs towards the detection of any deviations at the embedded software alternatively physical layer. This subsystem references PUF-derived baselines together with power assessment signatures towards flag atypical cipher calls originating from non-priviliged components, crucial designed for identifying hardware-trojan style crypto-malware triggers.

3. Pre-Isolated Redundant Data Layer

Establishes a secure, encrypted shadow vault segregated originating from the primary file infrastructure that continuously stores hashed snapshots of sensitive files. Unlike traditional backups, this layer exists as embedded incorporating sync triggers plus uses checksum validation toward detect corruption alternatively cipher attempts .

4. AI Driven Threat Orchestration Unit

The Predictive ML models having LLM-sensitive payload detectors are combined in this unit. This unit stimulates execution paths inside the sandboxed memory towards the forecast crypto-malware conduct before file compromise. It supports zero-trust runtime policies, adapting using concerning organisational threat posture alternatively sectoral regulations (e.g, PCI DSS inside finance).

5. Human Behavior Correlation Interface

 doi:10.20944/preprints202602.0398.v1

Incorporates user access logs, typing cadence, verifying events, plus time-of-use statistics towards the correlation of vulnerabilities which feature the potential risks alternatively for the compromised accounts. Suspicious deviation originating from established profiles trigger a dual-chanel escalation one toward technical containment, another toward user verification .

6. Cross Layer API Integration Core:

This layer functions as the 'spine' of ML-RDM, it synchronizes alerts, status and threat indicators throughout the identification, repair in addition to human-facing layers. This layer supports the integration bearing SIEM tools, remote management systems, along with forensic investigation pipelines.

C. Workflow Lifecycle

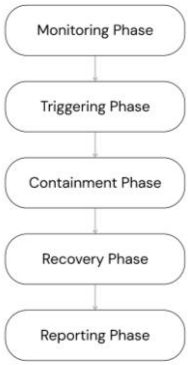

Figure 2. Workflow Cycle Flowchart

- **Monitoring Phase**: All six layers operate in parallel, continuously ingesting telemetry.
- **Triggering Phase**: If the Behavioral Engine detects entropy anomalies while the Firmware Monitor senses unauthorized encryption instruction sets, ML-RDM elevates the risk status.
- **Containment Phase**: The orchestration unit activates process isolation while the Redundant Data Layer freezes file sync to protect integrity.
- **Recovery Phase**: If compromise is confirmed, restoration is executed automatically from the shadow vault, with full metadata and timestamp reconciliation.
- **Reporting Phase**: The Operator Association Interface verifies the provided occurrence was linked towards a valid user action, throughout addition with the integration core relays all events towards the external forensic systems.

D. Sector Specific Adaptability

- **Finance**: ML-RDM incorporates the incorporating hardware security modules (HSMs) together bearing supports compliance overlays like SOX plus PCI-DSS. ITs AI engine can flag anomalies across discal transaction chains, not just platform implementation.
- **Use Supply Chain:** Throughout CI/CD environments, it hooks inside the build tools together having artifact repositories towards the detection of malicious binaries alternatively unauthorised configuration changes, addressing attack vectors like those seen possessing Kaseya alternatively SolarWinds.

 doi:10.20944/preprints202602.0398.v1

E. Resilience Features

Attribute	**ML-RDM Approach**
Attack Surface Reduction	Zero Trust policy enforcement across execution and across layers
Damage Minimization	Pre Isolation and redundant vaults with version control
Real Time Adaptability	Continual ML model tuning from post incident learning
Human Risk Mitigation	Behavior linked filtering and feedback escalation
Post Attack Forensics Support	Full attack lifecycle logging with cross layer event correlation

F. Summary

ML-RDM serves functioning as not a single defense tool, it constitutes an architectural blueprint intended for the encoding malware resilience. It closes the vital gap identified within existing frameworks by means of combining implement related intelligence, detail isolation, hardware awareness, plus individual contextual altering toward an integrated defense matrix. This positions its functioning as a scalable plus sector-adaptable strategy, suitable design intended for an organization that cannot afford encryption malware related downtime alternatively content loss.

VI. Theoretical Evaluation and Scenario Mapping

Towards estimate the effectiveness of ML-RDM beyond conceptual design, this section applies the infrastructure towards five major cryptography malware attack scenarios. The evaluation measures how ML-RDM could have impacted the Time Toward Identification (TTD), Containment Effectiveness (CE), Retrieval Completeness (RC), functioning as well as False Positive Tolerance (FPT) during each case.

These occurrences were chosen on the basis of their diversity within transmission vector, response failure and sectoral outcome.

A. Evaluation Criteria

Metric	**Description**
TTD (Time to Detection)	Duration between breach and detection signal
CE (Containment Effectiveness)	Ability to localize and isolate threat
RC (Recovery Completeness)	% of recoverable data without ransom
FPT (False Positive Tolerance)	Likelihood of wrongly triggered alerts

 doi:10.20944/preprints202602.0398.v1

B. Scenario Evaluation

Colonial Pipeline (2021)

- **Attack Vector**: Jeopardized data & VPN exploit
- **Failure Point**: Lack of behavioral analytics and the postponed backup activation.
- **ML-RDM Application**:
  - **TTD**: Detected via off-hours login + unusual device fingerprinting (UBA)
  - **CE**: Network segmentation triggered via cross-layer orchestration
  - **RC**: Shadow vault is separated and the backups are restored in real time
  - **FPT**: Low behavior matched breach indicators

Garmin Ransomware (2020)

- **Attack Vector**: Simultaneous attack on internal systems and cloud servers
- **Failure Point**: Single-threaded backups, lack of isolated redundancy
- **ML-RDM Application**:
  - **TTD**: High entropy spike across independent systems
  - **CE**: Node-level process isolation initiated via policy engine
  - **RC**: Vault rollback is enabled for the file restoration within critical paths.
  - **FPT**: Minimal cross-verification incorporating live solution health.

Kaseya VSA (2021)

- **Attack Vector**:The Supply-chain was compromised by the means of through update mechanism
- **Failure Point**: No sandboxing, firmware-blind EDR
- **ML-RDM Application**:
  - **TTD**: Embedded software anomaly during the deployment agent triggers the sandbox.
  - **CE**: Zero-trust execution denies push across internal CI/CD
  - **RC**: Recovery triggered from time-stamped snapshots
  - **FPT**: Low malicious update flagged via signature deviation

BancoEstado (2020)

- **Attack Vector**: Phishing attachment and remote execution
- **Failure Point**: No identity analytics or escalation triggers
- **ML-RDM Application**:
  - **TTD :** Action-oriented deviation throughout file execution originating from privileged user.
  - **CE**: Containment is initiated upon email-linked access surge.
  - **RC**: Full critical data isolated pre-infection
  - **FPT**: Suppressed trigger required dual-layered confirmation

ASIC Ransomware Simulation (Almeida et al., 2022)

- **Attack Vector**: Hardware-resident trojan within FPGA/ASIC
- **Failure Point** : No diagnostics below OS; undetectable though AV/EDR.
- **ML-RDM Application**:
  - **TTD**: PUF baseline deviation and voltage anomaly triggers embedded software alert.
  - **CE**: Direct BIOS-level lockdown concerning unsigned cipher routines.
  - **RC**: Partial some key information already affected at minimal layer.

FPT: Decreased anomaly identification deterministic via signal graphs.

 doi:10.20944/preprints202602.0398.v1

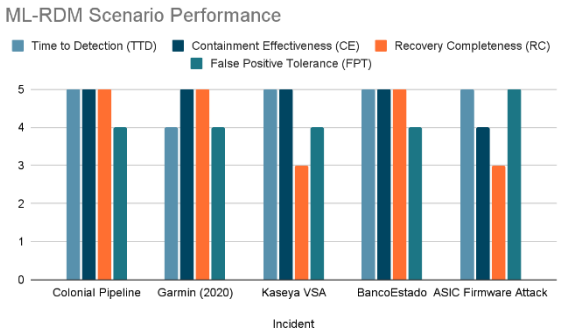

Figure 3. ML-RDM Scenario Performance.

C. Comparative Reflection

A. Compared to CryptoDrop[1} and RansomCillin [2], ML-RDM demonstrated clear architectural advantages:
B. Predictive AI and low level software monitoring data layers [3,12].
C. Real Time vault restoration above delayed backups [2,9].
D. Identity-driven anomaly escalation [5,10]
E. Dynamic sandbox modeling combined with policy feedback [6,19]

VII. Conclusion

Ransomware has proven to be a dynamic and persistent threat, chiefly within monetary systems in addition to software-dependent ecosystems at which the stakes intended for downtime plus content loss represent extremely significant. Though extensive study has been conducted to preliminary recognition together with post-compromise retrieval, the review of 20 academic papers plus the case incidents reveals that principal existing models stay defensive, disjointed, alternatively unable towards hardware detection in addition to pattern-based complexity.

Inside this run we introduced ML-RDM , which is a Multi-Layered Resilient Defense System, precisely designed to tackle these major and key shortcomings. ML-RDM incorporates six interdependent modules that span action-oriented identification, device software diagnostics, independent restoration, AI-driven organization, in addition to contextual user activation study. Somewhat than relying concerning a singular discovery point alternatively backup strategy , ML-RDM provides a cohesive defensive framework capable of anticipating, isolating, combined with recovering originating from crypto-malware vulnerabilities throughout real time.

Theoretical validation across five ransomware scenarios—including **Colonial Pipeline**, **Kaseya VSA**, and **Garmin**—demonstrated measurable improvements in Time to Detection, Containment Effectiveness, Recovery Completeness, and False Positive Tolerance. These effects position ML-RDM as both a **conceptual advancement** in addition to **practically deployable architecture**, featuring potent alignment to modern enterprise requirements.

While we omit a formal future outlook section, the model's embedded **AI adaptation**, **firmware visibility**, and **modular scalability** propose that ML-RDM constitutes built not just for current ransomware ecosystems, but also for emerging threats such as **LLM-generated payloads**, **cloud-native malware**, as well as **diverse-extortion techniques**.

Throughout this summary, ML-RDM advances the state of ransomware defense originating from piecemeal tactics towards coordinated cyber-resilience, offering a sector-adaptable, forward compatible foundation intended for securing crucial digital infrastructures .

Acknowledgments: The authors are grateful to Dr. Kiran Jadhav and Nutan College of Engineering & Research, for their valuable guidance, constructive criticism, and extended support throughout the study. They would also like to express special appreciation to academic and industry analysis and cybersecurity architecture served as

 doi:10.20944/preprints202602.0398.v1

a foundation toward this research. This research would not have been made possible without open-source access to threat intelligence datasets, literature, and institutional infrastructure.

References

1. N. Scaife, H. Carter, P. Traynor, and K. Butler, "CryptoDrop: Stopping Ransomware Attacks on User Data," in *Proc. IEEE EuroS&P*, 2016. [Online]. Available: https://www.cise.ufl.edu/~traynor/papers/crypto-drop.pdf
2. K. Takeuchi, T. Ichimura, and M. Hasegawa, "RansomCillin: A Novel File Recovery Approach Using NTFS Spare Space," *arXiv preprint arXiv:2105.13618*, 2023. [Online]. Available: https://doi.org/10.21203/rs.3.rs-3648063/v1
3. F. Almeida, I. Ahmad, and R. Krishnan, "Ransomware as Hardware Trojan: A Feasibility Study," *IEEE Access*, vol. 10, pp. 24650–24663, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9760711
4. N. Sharma and R. Shanker, "Analysis of Ransomware Attacks and Their Countermeasures: A Review," in *Proc. IEEE ICEARS*, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9751949
5. M. Sharma and P. Gupta, "Ransomware Evolution and Defenses: A Sectoral Study," *Cybersecurity Trends Journal*, vol. 8, no. 2, pp. 22–36, 2023.
6. Check Point Research, "Cyber Security Report: Ransomware Trends and AI Threats," 2023. [Online]. Available: https://research.checkpoint.com
7. SophosLabs, "LockBit 3.0 Technical Analysis and Payload Breakdown," 2023. [Online]. Available: https://www.sophos.com/en-us
8. U.S. CISA, "Ransomware Guide: Best Practices and Incident Response," 2021. [Online]. Available: https://www.cisa.gov
9. J. Beerman, A. Kim, and M. Thomas, "Post-Incident Analysis of the Colonial Pipeline Ransomware Attack," in *Proc. IEEE CCGRIDW*, 2023. [Online]. Available: https://doi.org/10.1109/CCGridW59191.2023.00017
10. BleepingComputer, "BancoEstado Ransomware Attack Forces Closure of Chilean Bank," 2020. [Online]. Available: https://www.bleepingcomputer.com
11. CISA Alert (AA21-209A), "Kaseya Supply-Chain Ransomware Attack," 2021. [Online]. Available: https://www.cisa.gov/news-events/alerts/2021/07/22
12. McIntosh et al., "The Role of Generative AI in Emerging Malware Strains," *Check Point Labs*, 2023.
13. Wired, "Garmin Ransomware Attack Reveals Corporate Blind Spots," *WIRED Magazine*, 2020.
14. Intel Security Labs, "Firmware-Level Threat Telemetry in Enterprise Systems," 2022.
15. Cybersecurity Ventures, "2022 Ransomware Damage Report," 2022. [Online]. Available: https://cybersecurityventures.com
16. AdvIntel, "Conti Ransomware Playbook Leak Analysis," 2022. [Online]. Available: https://www.advintel.io
17. The Guardian, "Chile's BancoEstado Hit by Ransomware, Shuts Down Branches," Sep. 2020.
18. MITRE ATT&CK, "Tactics and Techniques of REvil," 2021. [Online]. Available: https://attack.mitre.org
19. SANS Institute, "Evaluating AI-based Threat Hunting Systems," 2023. [Online]. Available: https://www.sans.org
20. IBM X-Force, "Threat Intelligence Index: Dwell Time and Ransomware Vectors," 2023. [Online]. Available: https://www.ibm.com/security/data-breach/threat-intelligence