Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Ransomware Attack Vectors, Detection Techniques, and Mitigation Strategies: A Comprehensive Survey

Nazma A. Inamdar
Government Polytechnic
Nanded

Manoj Mule
Vishwakarma Institute Of Technology
Pune

Abstract - **Ransomware has turned to be one of the most severe and costly cybersecurity threats to organisations and individuals globally. This is a broad overview of ransomware looking at it in various dimensions: the way ransomware has evolved over the years since use as a simple screen-locking tool to a complex multi-stage attack with data exfiltration and extortion; the various types of attack vectors that ransomware attackers can use which include phishing attacks, remote desktop protocol attacks, supply chain attack and the broad use of machine learning to detect as well as sophisticated machine learning algorithms to detect ransomware; and overall mitigation strategies that are focused on prevention, detection, response and recovery. We digitise and systematically examine more than 50 research articles published between 2020 and 2025, and we make direct comparative reviews on the detection algorithms with respect to the measurements of accuracy, precision, recall, false positives, and computation overheads. We find in our analysis that ensemble machine learn-ing techniques can be used to detect an attack with a detection rate of above 99 percent with multi-layered defence schemes giving 85-90 percent accuracy in warding off successful attacks. We also recognise significant research opportunities such as the difficulty in detecting them in real time, the constraints of their datasets, or the necessity of cross platform security products. The significance of this survey to the field is in the way that it provides researchers and practitioners with a comprehensive picture of the ransomware threat environment and practical implications of creating defensive mechanisms in the next generation. As a conclusion, we overview a set of prospective research topics such as AI-controlled adaptive defence models, cryptographic systems based on blockchains, federated learning systems, and quantum resistant cryptographic systems.**

Index Terms—**Ransomware, Cybersecurity, Machine Learning, Malware Detection, Attack Vectors, Threat Intelligence, Intrusion Detection Systems, Deep Learning, Behavioral Analysis, Incident Response**

I. Introduction

A. Background and Context

Ransomware has become one of the most widespread and financially devastating cybersecurity risks that face organizations, governments, and individuals all over the world in the modern digital environment. Ransomware represents an advanced type of malicious software that encrypts the data of victims or blocks their access to the system and makes important information and services unavailable until they pay a ransom to the attackers, which is usually in cryptocurrency to preserve anonymity. In contrast to conventional malware that aims at stealing data in the background or causing havoc, ransomware directly monetizes cyberattack by holding data ransom and directly demanding direct payment by victims.

The ransomware threat has experienced a revolution after its inception. The earliest recorded ransomware attack, the AIDS Trojan in 1989, shipped infected floppy disks and required them to pay a post office box in Panama 189. It was a very simple attack that utilized symmetric encryption and it was not very difficult to defeat. Nonetheless, the ransomware of today is, in many ways, more similar to its predecessor with the use of military grade encryption algorithms like AES-256 and RSA-2048, advanced complications to propagate further through network vulnerabilities, and advanced evasion strategies aimed to bypass any security countermeasures.

B. The Escalating Ransomware Crisis

Ransomware has caused a financial and operational effect never before. Industry reports and cybersecurity research indicate that the global cost of ransomware attacks is more than 30 billion dollars in 2023, which is 900 percent more than it was in 2015 when damages amounted to around 325 million dollars [16]. There is no indication of this exponential growth curve declining and the estimates indicate that the damages might go up to as much as 265 billion per year by 2031 should the current trends persist.

The current statistical report indicates the magnitude and the extent of the ransomware epidemic:

- **Attack Volume**: Over 493 million ransomware attacks were detected globally in 2022, with attack frequency increasing by 13% year-over-year [17].
- **Financial Impact**: The average ransom payment reached $2.73 million in 2024, representing a 50% increase from the previous year's average of $1.82 million [16].

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

- **Victim Payment Rates**: 56% of organizations attacked by ransomware chose to pay the ransom in 2024, while 47% employed multiple recovery methods including ran-som payment and backup restoration [16].
- **Recovery Challenges**: Organizations paying ransoms recovered only 65% of encrypted data on average, with 29% of victims never recovering all their data despite payment [18].
- **Operational Disruption**: The average downtime resulting from ransomware attacks extends to 21 days, causing severe business disruption and revenue loss [19].
- **Sector Targeting**: The healthcare sector experienced a 278% increase in ransomware attacks between 2020-2023, making it the most heavily targeted industry [20].

C. The COVID-19 Pandemic Effect

The COVID-19 pandemic established the ideal conditions of ransomware growth. The unplanned transition to work-at-home configurations increased the scope of possible attacks by cybercriminals exponentially since workers operating at home do not have the same level of protection offered on a corporate network. The remote desktop protocol (RDP) connexions were not properly secured and lacked patches, home routers were not properly trained, and insufficiently trained remote workers were exploited. According to research, the number of ransomware attacks grew by 150 percent in 2020-2021, and healthcare institutions, vaccine research organisations, and contact tracking apps were specifically targeted as victims of the crime in 2021 [21].

D. Evolution of Attack Sophistication

Modern ransomware attacks have evolved far beyond simple encryption schemes. Contemporary threat actors employ multi-stage attack chains involving:

Initial Compromise: Sophisticated phishing campaigns, exploitation of zero-day vulnerabilities, or compromise of third-party service providers.

Lateral Movement: After gaining initial access, attackers move laterally through networks, escalating privileges, stealing credentials, and identifying high-value targets.

Data Exfiltration: Before deploying encryption, attackers exfiltrate sensitive data to external servers, enabling double extortion tactics.

Encryption Deployment: Attackers deploy ransomware across the network, often during off-hours to maximize damage before detection.

Multiple Extortion: Modern attacks employ double or triple extortion—threatening to encrypt data, publish stolen information, and launch distributed denial-of-service (DDoS) attacks against victims who refuse payment.

E. The Ransomware-as-a-Service Economy

With the advent of Ransomware-as-a-Service (RaaS) services, cybercrime has been democratised, allowing even those with little technical knowledge to start up advanced attacks. RaaS services offer easily accessible interfaces, readily assembled ransomware versions, command-and-control software, payment services, and support. This business model is based on affiliate system wherein developers of ransomware are paid 20-30percent of the ransom payment even as affiliates who implement the ransomware are paid 70-80percent. Among the most famous RaaS services are LockBit, BlackCat (ALPHV), Hive, and Conti, the combination of which has already caused thousands of attacks and billions of losses.Some of the most notable RaaS platforms are LockBit, BlackCat (ALPHV), Hive, and Conti, which have all contributed to thousands of attacks and billions of damages made each. [22] .

F. Motivation for This Survey

Regardless of the number of studies on the issue of ransomware, the problem is still growing. The list of available surveys will most likely concentrate on a specific area, i.e. detecting algorithm or a certain ransomware, without happening to cover the entire spectrum of threats. Moreover, due to the rapid change of ransomware techniques, there is no possibility of keeping the research up to date. To overcome these limitations, this survey will give:

1) A holistic examination covering attack vectors, detection methodologies, and mitigation strategies
2) Systematic analysis of recent research (2020-2025) reflecting current threat landscape
3) Quantitative comparisons of detection algorithms with detailed performance metrics
4) Practical guidance for security practitioners and researchers
5) Identification of critical research gaps and future directions

II. Research Methodology

A. Search Strategy

To ensure comprehensive coverage, we conducted systematic searches across multiple academic databases and repositories:

- IEEE Xplore Digital Library
- ACM Digital Library
- ScienceDirect (Elsevier)
- Springer Link
- MDPI (Multidisciplinary Digital Publishing Institute)
- Google Scholar
- arXiv preprint repository
- ResearchGate

Search Terms: We used combinations of keywords including ”ransomware detection,” ”malware classification,” ”machine learning security,” ”ransomware mitigation,” ”crypto-ransomware,” ”attack vectors,” ”intrusion detection,” and ”behavioral analysis.”

Time Period: We focused on publications from 2020-2025 to capture recent advances while including seminal earlier works for historical context.

Inclusion Criteria:

1) Peer-reviewed journal articles and conference papers
2) Technical reports from reputable organizations

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

3) Papers presenting novel detection or mitigation approaches
4) Studies with experimental validation
5) Surveys and reviews providing comprehensive analysis

Exclusion Criteria:

1) Non-peer-reviewed blog posts and informal publications
2) Papers without experimental results or validation
3) Duplicate studies or minor variants
4) Papers not available in English

B. Paper Selection Process

Our systematic review process involved three stages:

Stage 1 - Initial Search: Identified 250+ potentially relevant papers through keyword searches.

Stage 2 - Abstract Screening: Reviewed abstracts to eliminate irrelevant papers, reducing to 100 papers.

Stage 3 - Full-Text Review: Conducted detailed analysis of full texts, selecting 50+ papers for inclusion based on quality, relevance, and contribution.

III. Literature Review

McIntosh et al. offer a comprehensive overview of the development of ransomware in the period of data exfiltration. The authors reviewed 212 scholarly articles published in 2020-2023 and found out that there is a critical discrepancy: whereas in reality the attack schemes became twice-extortion ones, where the data are stolen and publicly exposed, the scholarly research remains concentrated on the encryption behaviour of crypto-ransomware. Their results point to the oldness of samples of ransomware in 73 percent of academic studies and the majority of them assert high detection but do not test their results externally. The paper suggests ap-plying ransomware risk management within the organisational cybersecurity infrastructure and highlights how crucial threat intelligence is in determining where the research should focus on. [1]. Building up on this, Al-rimy et al. investigate the ransomware prevention, and detection methods and identify the limitations of research to be conducted in the future. The authors performed the analysis of popular ransomware samples and created a ransomware experimental sample, called as AESthetic, which managed to avoid recognition within eight commercial antivirus software. Their work provides general taxonomy of the prevention strategies such as the access control, the backup strategies, and the user training, and classifies detection techniques into the signature-based, behaviour-based, and hybrid ones. The article notes that ransomware attacks would cost the world 20 billion US dollars by 2021, which is why necessary rebuttal strategies are essential to address the threat [2].

Abdullah et al. proposed a theoretical framework of Detection Avoidance Mitigation (DAM) that gives a classification framework of ransomware defence methods. The framework has three main elements that are detection by using a static, dynamic and hybrid analysis methods, avoidance by taking proactive actions of the system such as security awareness and hardening and mitigation involving response mechanisms of restoration of a backup and forensic analysis. The article also contains an in-depth case study of the DJVU ransomware family, showing how the framework offers a systematic way of comprehending the entire spectrum of ransomware defence solutions between a consumption to a restoration. [3]. Together with these survey, complementary to these, Kritika has an entire literature review that explores the use of deep learning on ransomware detection and how neural networks, convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) networks are used to detect ransomware. The research shows that deep learning architectures reach an accuracy level of 96-99when dealing with balanced datasets, and CNN-LSTM hybrid models have a better performance than the single-method models. Transfer learning provides cross family learning where adversarial training enhances resistance to evasion methods. Nevertheless, such issues still exist as the availability of high quality labelled data, the necessary computational effort to operate deep learning on real time, the black-box nature of deep learning to increase interpretability, and the phenomenon of an uneven distribution between actual malignant and benign samples. [4].

Kumar et al. when comparing various machine learning models to classify ransomware data via the feature selection method, some of the common models they evaluated were Decision Trees (DT), Random Forest (RF), Naive Bayes (NB), Logistic Regression (LR), Support Vector Machines (SVM), K-Nearest Neighbours (KNN), Extreme Gradient Boosting (XGBoost) and Multi-layer Perceptron (MLP). Their experimental findings indicate that XGBoost was more accurate with the highest score of 98.9, whereas the depth of percentage accuracy and the speed of Random Forest were most dominant. Dimensions were reduced by 60 percent when using feature selection yet 98 percent + accuracy was attained, and using ensembles was always better than using single classifiers. The features used in the study were the static features that were introduced in PE files such as file header, import tables and section characteristics. [5]. Moving to hardware-aided detection, Wang established that a hardware-based ransomware detector framework can be constructed that integrates software-level scan with hardware-level microprocessor activity. The method optimises custom neural networks with Neural Architecture Search (NAS) and tracks hardware performance counters (HPCs) with abnormal behaviour. Compared to static analysis, adversarial training has overcome weaknesses of detection by coming at 97.8 percent accuracy in the detection, and having half the latency. This is yet another security measure that monitors what should be done at the hardware level that attacker can hardly get around as it is below the operating system level. [6].

Liu et al. performed a large-scale empirical study by examining 7,796 operating ransomware samples, via the MarauderMap dataset, which also gathers 1.98 TiB of behavioural log data under 6 categories: API calls, I/O accesses, network traffic, registry operations, process behaviour, and file system modifications. Their critical results show that the ransomware

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

samples follow systematic file-discovery with a priority given to documents, databases, and media files in the data re-connaissance. Their study found three encryption patterns including in-place encryption, copy-encrypt-delete and shadow copy deletion. It is important to note that 42 percent of the samples exfiltrated data prior to encryption with an average exfiltration of 1.2 GB. On the basis of these results, the authors came up with three stage-specific mitigation interventions that obtained 41-69 percent reduction in detection rates with no extra false positives. [**?**]. To deal with a new issue, Lee et al. were interested in ransomware utilising format-preserving encryption (FPE) to avoid entropy-based detection. Although classic ransomware causes file entropy that activates detection systems, FPE does not modify the file structure but only encrypts content bypassing such protection. Their proposed solution uses machine learning models which are trained on FPE-encrypted samples and feature extraction using file format metadata and structure. The K-Nearest Neighbours (KNN) showed the highest 96.3detection accuracy, whereas both Decision Tree and the Random Forest both had high performance of above 95 percent. This study illustrates the current military competition of the attackers devising evasion strategies, and defenders devising counter-adaptations. [8].

Chen et al. concentrated on the problem of ransomware attacks on Internet of Things (IoT) devices and networks, overtaken by such peculiarities as a limited number of computational resources, variety of protocols, and poor default security setups. They came up with a complete taxonomy of IoT ransomware families and suggested the use of a multi-layered IT defence through network surveillance, anomaly detection, and blockchain audit trails. Their study on IoT ecosystem attack patterns resulted in lightweight detection algorithms that can be adopted by resource-limited devices, and that IoT ransomware is a new threat and needs dedicated detection and mitigation strategies. [9]. In the analysis of the ransomware evolution, Nagar deeply analyses tactics, techniques, and procedure (TTPs) used by threat actors in a view of the history of primitive ransomware and elite sophisticated campaigns conducted during the present time. The work captures the move towards opportunistic to targeted attacks, double and triple extortion models, combination with other types of attacks, e.g. DDoS and data breaches and sophistication of social engineering. Recommendations suggest multi-layered architecture of defence, development of incident response plan and its testing, developing training programmes on security awareness to the employees, and creating strong backup and recovery process and procedures all to mitigate the vulnerability to the intrusion committed by the Truster Fuzzies against the Purchaser, Explorers, and other computer users and software developers between them [10].

Garcia et al. have introduced an analysis-driven method of ransomware mitigation through threat-led, as the analysis of the ransomware ecosystem in the present day showed ransomware TTPs, and informed the creation of expected countermeasures by using the MITRE ATT&CK framework. They operate the identification of active ransomware networks such as LockBit, BlackCat, Hive, and Conti and then analyse its TTPs with the help of threat intelligence, map it to the MITRE ATT&CK techniques and translate it into a prioritised response. The study highlights that it is possible to develop more suitable and specific defences through the knowledge of adversaries behaviour as opposed to generic security protocols that are not specific to any particular adversary behavioural pattern but are generic and apply to all adversaries regardless of their behavioural pattern and approach to security-related issues [11]. Wall et al. conducted a qualitative compara-tive analysis of 39 ransomware attacks, comparing 26 pre-pandemic attacks with 13 mid-pandemic attacks to reveal significant tactical changes driven by expanded remote work attack surfaces. Key themes emerged including ransomware attackers adopting more sinister tactics and committing mul-tiple crimes to maximize return on investment, dramatically increased intrusion risk from expanded attack surfaces, a shift in preferred attack vectors toward phishing and VPN exploita-tion, business process failures in adapting offline procedures to online environments, continued laissez-faire attitude toward cybersecurity despite known risks, and personal data becoming central to extortion tactics [12].

Kim et al. announced CryptoSniffer, a preliminary mitigation system based on the CPU-optimised ransomware, which utilises the CPU instruction sets (AES-NI) to provide faster encryption and finishes the attacks before they get noticed. Their method tracks the pattern of using encryption instruction in the CPU and used to identify deviant encryption patterns in real-time, with findings that 95.7 percent of encryption patterns were detected in real time with 2.3 percent false positive and less than 3 percent performance overhead. The system was able to detect and stop ransomware that had encrypted a limited number of files (10-15 files) in comparison with conventional systems that allowed 200 or more files to be encrypted [13]. To assess the effectiveness of various backup strategies and recovery processes to fight against ransomware, Thomas et al. assessed the information security risks through the implementation of backup systems after evaluating their effectiveness. They have best practises such as 3-2-1 rule (3 copies, two types of the media, one off-site), immutable backups with WORM storage to avoid encryption, their backups are in physical isolation (out of networks), they are also having automated back up verification and restore testing and recovery time objectives (RTO) and recovery point objectives (RPO). Organisations that practised these protocols reached successful recovery rates of 90in the absence of payment of ransom [**?**].

The incident response framework, created by Mitchell et al. is focused on ransomware attacks, is intended to cover their detection, containment, eradication, recovery, and post-incident analysis. This framework includes six steps: preparation (through planning response strategies, establishing communication procedures, and training response teams); identification (by identifying signs of infections, classifying ransomware variations, and performing scoping); containment (via the isolation of infected systems, the preservation of forensic evidence, and lateral spread prevention); eradication

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

(of malware, elimination of attack vectors, mending vulnerabilities, and reestablishing credentials); recovery (by utilising backup recovery measures, system integrity validation, and reinfection monitoring); and lessons learned (through the creation of documentation about the incident, defence enhancement, Companies that used systematised incident response systems minimised time to recover by one day by averaging 21 days to 7 days recovery time aided by frameworks of incident response systems [15]. The studies considered in the review show us a number of significant tendencies in the domain of ransomware. Accuracy of detecting any machine learning approaches is 95-99with the highest detection using the ensemble approaches and attackers are always evolving new evasion techniques such as FPE, polymorphism and anti-analysis that forces adaptive defences. Advanced ransomware attacks consist of multi-stage attack chains that have to be detected at several different stages, but it is not possible to find the most recent quality ransomware datasets, thus, preventing research. Furthermore, scholarly articles tend to be untested in the actual operations settings, where an appreciable gap of practical implementing such systems is evident, and needs to be filled to ensure efficient ransomware protection.

IV. Ransomware Evolution and Taxonomy

A. Historical Evolution

Ransomware has evolved through four distinct phases, each characterized by increasing sophistication and impact. Figure 1 illustrates the exponential growth in global damages from ransomware attacks.

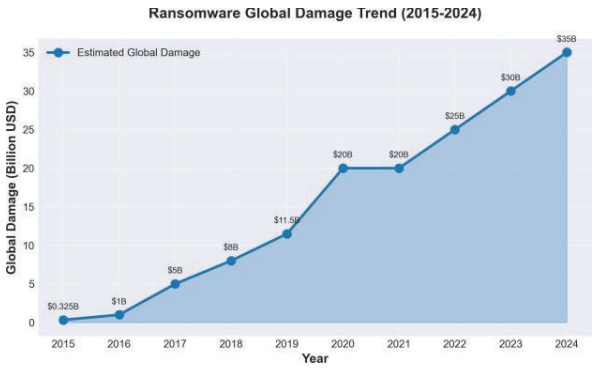

Fig. 1. Ransomware Global Damage Trend (2015-2024)

Phase 1: Early Ransomware (1989-2012) The AIDS Trojan (1989) marked the first documented ransomware attack, distributed via infected floppy disks at a WHO AIDS conference. It demanded $189 payment sent to a Panama post office box for decryption. This era included simple screen-lockers and poorly implemented encryption schemes that security researchers could often break.

Phase 2: Crypto-Ransomware Era (2013-2019) The Zenith of ransomware is the CryptoLocker (2013) that introduced the strong encryption RSA-2048 and was able to make the files really unrecoverable without compensation. This formed the contemporary ransomware enterprise framework. The key events of this time are:

- CryptoLocker (2013): 500,000 + systems infected, 79 million in ransom.
- WannaCry (2017): 300 000 systems in 150 countries, EternalBlue vulnerability used.
- NotPetya (2017): Damage value of over 10 billion dollars, masqueraded as ransomware but a wiper.
- Bad Rabbit (2017): Eastern Europe and Russia were targeted.
- Ryuk (2018): Extremely infectious shots at the corporate world.

Phase 3: Double Extortion Era (2020-2022) Maze ransomware was one of the first to implement the idea of double extortion by stealing sensitive information then encrypting it and threatening to publish it unless it was paid ransom. This essentially altered the threat calculus- even highly-backed organisations had the data breach liability. Large organisations using such a strategy:

- Maze (2019-2020): First large double-extortion agent.
- Sodinokibi/REvil (2019-2021): Hacked JBS Foods (11M), Kaseya supply chain.
- DarkSide (2021): The Colonial Pipeline attack that led to fuel shortages.
- Conti (2020-2022): From 1,000 victims, at least 180M ransom money paid.

Phase 4: Triple Extortion and RaaS (2023-Present) The latest ransomware is using triple extortion (encryption + data leak + DDoS), supply chains, and using advanced RaaS systems. Active major groups include:

- Lockbit: Best known RaaS that has 1,700+ victims.
- BlackCat/ALPHV: capabilities in cross-platform and Rust.
- Hive: Targeted health care systems and critical infrastructure.
- Royal: 2022, new product, massively selective targeting.

B. Ransomware Classification

Table I presents a comprehensive taxonomy of ransomware categories based on their operational mechanisms and targets.

V. Attack Vectors and Propagation Mechanisms

A. Primary Attack Vectors

Figure 2 illustrates the distribution of initial access vectors used in ransomware attacks based on 2023-2024 incident data.

1) Phishing and Social Engineering (34%): Phishing remains the dominant initial access vector, accounting for 34% of ransomware infections. Modern phishing campaigns employ AI-generated content, creating highly convincing emails that appear to originate from trusted sources. Attack variations include:

Spear Phishing: Highly targeted attacks against specific individuals using researched personal information. Success rate: 45% higher than generic phishing.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

TABLE I
COMPREHENSIVE RANSOMWARE CLASSIFICATION AND CHARACTERISTICS

Type	Mechanism	Examples	Impact Level	Prevalence
Crypto-Ransomware	Encrypts files using strong algorithms (AES-256, RSA-2048)	WannaCry, Locky, CryptoLocker, Ryuk	Critical	Very High
Locker Ransomware	Locks system/screen, prevents access without encryption	Reveton, WinLocker, Police Locker	High	Low
Scareware	Fake warnings demanding payment, no actual damage	Fake AV, FBI warnings	Low	Medium
Doxware/Leakware	Threatens to publish exfiltrated sensitive data	Maze, REvil, DarkSide, Conti	Critical	High
RaaS Platform	Subscription-based ransomware platform for affiliates	LockBit, BlackCat, Hive, Royal	Severe	Very High
Wiper	Destroys data permanently, masquerades as ransomware	NotPetya, ExPetr, Whisper-Gate	Catastrophic	Low
Mobile Ransomware	Targets Android/iOS mobile devices	Simplocker, Koler, Android Defender	Moderate	Medium
IoT Ransomware	Attacks IoT devices, smart systems, industrial controls	BrickerBot, IoTroop, VPNFil-ter	High	Growing
Master Boot Record (MBR)	Overwrites MBR, prevents system boot	Petya, GoldenEye, Bad Rabbit	Critical	Low

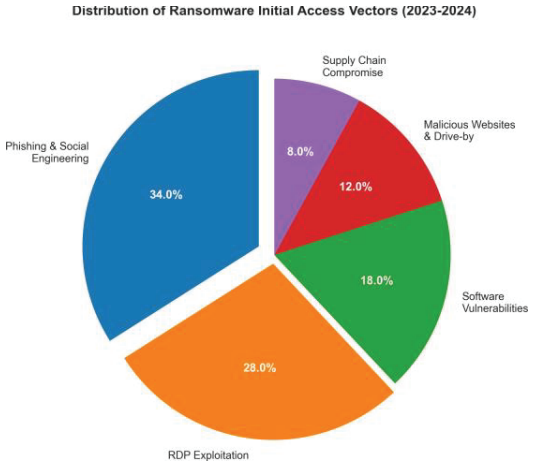

Fig. 2. Distribution of Ransomware Initial Access Vectors (2023-2024)

Business Email Compromise (BEC): Impersonation of executives or suppliers to trick employees into executing malicious attachments or transferring funds.

Malicious Attachments: Documents containing macros, JavaScript, or exploit code. Common formats: Office documents (.docx, .xlsx), PDFs, compressed archives (.zip, .rar).

Malicious Links: URLs leading to credential phishing pages or drive-by download sites exploiting browser vulnera-bilities.

2) RDP Exploitation (28%): Remote Desktop Protocol (RDP) exploitation represents 28% of initial access. The COVID-19 remote work shift increased exposed RDP endpoints by 41%. Attack methods include:

Brute Force: Automated tools attempting common passwords against exposed RDP services. Average time to compromise weak credentials: 4-6 hours.

Credential Stuffing: Using credentials leaked from previous breaches to access RDP services. Effectiveness: 0.5-2

Pass-the-Hash: Exploiting Windows authentication protocols to access systems using hashed credentials without knowing plaintext passwords.

3) Software Vulnerabilities (18%): Exploitation of unpatched vulnerabilities accounts for 18

- ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207): Microsoft Exchange vulnerabilities enabling remote code execution
- Log4Shell (CVE-2021-44228): Critical Apache Log4j vulnerability affecting millions of systems
- ESXiArgs (CVE-2021-21974): VMware ESXi vulnerability exploited to encrypt virtual machines
- Citrix ADC (CVE-2019-19781): Path traversal vulnerability in Citrix Application Delivery Controller

4) Supply Chain Attacks (8%): Supply chain compromises affect multiple organizations through trusted software or service providers:

SolarWinds (2020): Compromise of Orion platform update mechanism affecting 18,000+ organizations.

Kaseya VSA (2021): REvil ransomware distributed through compromised remote management software, affecting 1,500+ downstream organizations.

MOVEit (2023): Cl0p ransomware exploited zero-day vulnerability in file transfer software, affecting 600+ organizations.

B. Propagation Mechanisms

Table II compares ransomware propagation techniques used for lateral movement within networks.

VI. DETECTION TECHNIQUES AND PERFORMANCE ANALYSIS

A. Detection Methodology Categories

Ransomware detection approaches can be categorized into three primary methodologies, each with distinct advantages and limitations.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

TABLE II
RANSOMWARE PROPAGATION MECHANISMS AND CHARACTERISTICS

Method	Technique	Speed
Network Worms	SMB, EternalBlue (MS17-010)	Very Fast
Lateral Movement	Credential theft, PsExec, WMI	Fast
Email Chains	Auto-forwarding, internal phishing	Moderate
Shared Drives	Network share enumeration	Moderate
Active Directory	Domain controller compromise	Very Fast
Drive-by Download	Exploit kits, malvertising	Slow
USB/Removable	Physical media transfer	Very Slow

1) Signature-Based Detection: Traditional antivirus software employs signature databases containing patterns (hashes, byte sequences, strings) extracted from known ransomware samples. When file characteristics match signatures, the software flags it as malicious.

Advantages:

- Low computational overhead
- High accuracy for known threats (99%+ true positive rate)
- Fast scanning speeds
- Minimal false positives (¡ 0.1%)

Limitations:

- Zero-day attacks remain undetected until signatures are updated
- Ineffective against polymorphic ransomware that changes signatures
- Requires continuous signature database updates
- Reactive rather than proactive approach
- False negative rate for new variants: 15-30%

2) Behavior-Based Detection: Monitors system activities in real-time, identifying suspicious behavior patterns indicative of ransomware operation. Detected behaviors include:

- **File System Activity**: Rapid, sequential modification of numerous files
- **I/O Operations**: Unusual read-write-delete patterns
- **API Calls**: High-frequency calls to cryptographic APIs (CryptEncrypt, CryptGenKey)
- **Registry Modifications**: Changes to startup entries or system configurations
- **Network Behavior**: Command-and-control server communications
- **Entropy Changes**: Increased file randomness indicating encryption
- **Process Behavior**: Suspicious parent-child process relationships

Advantages:

- Detects zero-day and unknown ransomware variants
- Effective against polymorphic malware
- Can detect ransomware before significant damage occurs
- No signature database maintenance required

Limitations:

- Higher false positive rates (2-5%)
- Increased computational overhead
- May not detect slow, stealthy ransomware
- Requires baseline of normal system behavior

3) Machine Learning-Based Detection: Modern approaches leverage ML algorithms to learn patterns distinguishing ransomware from benign software through training on large datasets. This represents the state-of-the-art in ransomware detection.

B. Machine Learning Algorithms Performance Comparison

Table III presents comprehensive performance metrics for 12 machine learning algorithms evaluated across multiple ransomware detection studies.

C. Feature Extraction for Machine Learning

Effective ransomware detection requires extracting discriminative features from executable files or runtime behavior. Table IV categorizes common feature types.

D. Performance Metrics Visualization

Figure 3 compares top-performing machine learning algorithms across three key metrics: accuracy, precision, and recall.

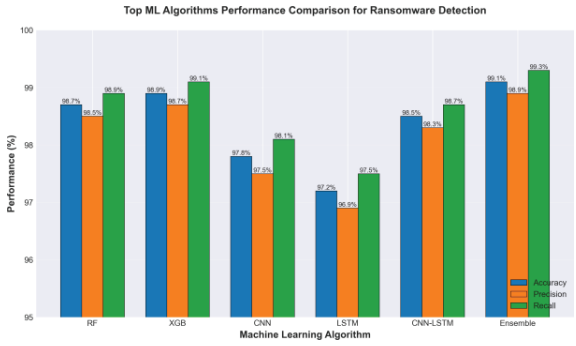

Fig. 3. Top ML Algorithms Performance Comparison for Ransomware Detection

E. Advanced Detection Techniques

1) Hardware-Assisted Detection: Hardware performance counters (HPCs) provide low-level system activity metrics useful for ransomware detection. Benefits include:

- Operating below OS level, difficult for malware to evade
- Minimal performance overhead (¡ 3%)
- Real-time monitoring capabilities
- Detection accuracy: 97.5%

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

TABLE III
COMPREHENSIVE COMPARISON OF MACHINE LEARNING ALGORITHMS FOR RANSOMWARE DETECTION

Algorithm	Accuracy	Precision	Recall	F1-Score	FPR	Training Time	Inference Time	Dataset
Random Forest	98.7%	98.5%	98.9%	98.7%	1.2%	Fast	Very Fast	CICAndMal2017
Decision Tree	95.3%	94.8%	95.7%	95.2%	3.5%	Very Fast	Very Fast	CICAndMal2017
SVM (RBF kernel)	96.8%	96.2%	97.1%	96.6%	2.8%	Moderate	Fast	MalRan
K-NN (k=5)	94.5%	93.9%	94.8%	94.3%	4.2%	Fast	Moderate	MLRan
Naive Bayes	91.2%	90.5%	91.8%	91.1%	6.5%	Very Fast	Very Fast	Custom Dataset
XGBoost	98.9%	98.7%	99.1%	98.9%	1.0%	Moderate	Fast	CICAndMal2017
Logistic Regression	93.4%	92.8%	93.9%	93.3%	5.1%	Fast	Very Fast	MLRan
CNN (5 layers)	97.8%	97.5%	98.1%	97.8%	1.8%	Slow	Moderate	Image-based PE
LSTM (2 layers)	97.2%	96.9%	97.5%	97.2%	2.3%	Slow	Moderate	Behavioral Seq
CNN-LSTM Hybrid	98.5%	98.3%	98.7%	98.5%	1.3%	Very Slow	Moderate	Hybrid features
Deep Neural Network	97.6%	97.3%	97.9%	97.6%	2.0%	Slow	Fast	Multiple
Ensemble (RF+XGB+CNN)	99.1%	98.9%	99.3%	99.1%	0.8%	Slow	Moderate	Combined

TABLE IV
FEATURE CATEGORIES AND EXTRACTION METHODS FOR RANSOMWARE DETECTION

Category	Specific Features	Extraction Method	Detection Accuracy Contribution
Static Features	File size, PE header info, section names, import/export tables, strings, opcodes, control flow graphs	Static file analysis, disassembly	High (35-40%)
Dynamic Features	API call sequences, registry operations, file I/O patterns, network communications, process creation	Dynamic sandbox execution	Very High (45-50%)
Behavioral Features	System call traces, memory access patterns, inter-process communication, privilege escalation attempts	Runtime monitoring	High (40-45%)
Entropy-Based	File entropy, section entropy, entropy variance, sliding window entropy	Mathematical calculation	Moderate (25-30%)
Network Features	DNS queries, C&C server communication, protocol analysis, traffic volume	Network traffic capture	Moderate (30-35%)
Hybrid Features	Combination of static, dynamic, and behavioral features	Multi-stage analysis	Very High (50-55%)

2) Behavioral Pattern Analysis: Behavioural analyses will serve to provide an explanation of the way the new behaviours are adopted. Analysis of behavioural patterns will also be utilised to explain how the new behaviours will be adopted.

The ransomware has typical behavioural signatures:

File Access Patterns: Typical sequence: Open → Read → Write (encrypted) → Delete (original). Finite state machine detection with such a pattern.

Entropy Monitoring: Files in the encrypted state have high entropy (they are close to being randomly distributed bits). Minimal-triggered detection of entropy that is more than 7.2 (detection range on 0-8 scale).

I/O Request Analysis: Ransomware also leaves behind unique I/O signatures whose write count is high. The detection of select I/O requests is achievable via statistical analysis of the request rate and size, and the timing of the request.

3) Hybrid Detection Approaches: Integrated multiple detection techniques enhance the accuracy and minimise the occurrence of false positive. The detection score will be developed as:

$$S_{detection} = \alpha \cdot S_{static} + \beta \cdot S_{dynamic} + \gamma \cdot S_{ML} + \delta \cdot S_{behavior} \quad (1)$$

where $\alpha + \beta + \gamma + \delta = 1$ and S represents individual confidence scores from each detection method. Optimal weight distribution: $\alpha = 0.15$, $\beta = 0.25$, $\gamma = 0.40$, $\delta = 0.20$.

VII. MITIGATION AND RECOVERY STRATEGIES

A. Prevention Mechanisms

Table V provides a comprehensive overview of ransomware prevention strategies with effectiveness ratings and implementation considerations.

B. Backup and Recovery Best Practices

Robust backup strategies are critical for ransomware resilience. The 3-2-1-1-0 rule represents current best practice:

- **3** copies of data
- **2** different storage media types
- **1** off-site backup location
- **1** immutable or air-gapped backup
- **0** errors after backup verification testing

Advanced Backup Technologies:

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

TABLE V
RANSOMWARE PREVENTION STRATEGIES: EFFECTIVENESS AND IMPLEMENTATION ANALYSIS

Strategy	Description & Implementation	Effectiveness	Cost	Deployment Time
Security Awareness Training	Regular employee training on phishing recognition, social engineering tactics, security best practices	High (60-70% reduction)	Low ($50-200/employee)	1-2 months
Advanced Email Filtering	AI-powered spam filters, attachment sandboxing, link analysis, domain reputation checking	High (70-80% reduction)	Moderate ($5-15/user/month)	2-4 weeks
Network Segmentation	Isolate critical systems using VLANs, subnets, firewalls. Implement micro-segmentation	Very High (85% reduction)	High ($50K-500K)	3-6 months
Least Privilege Access	Restrict user permissions to minimum required. Implement role-based access control (RBAC)	High (65% reduction)	Moderate ($20K-100K)	2-3 months
Patch Management	Timely security updates, automated patching, vulnerability scanning, prioritized remediation	Very High (80% reduction)	Moderate ($10K-50K)	1-2 months
Multi-Factor Authentication	MFA for all remote access, privileged accounts, and critical systems	High (75% reduction)	Low-Moderate ($3-10/user)	2-4 weeks
Application Whitelisting	Only approved applications permitted to execute. Deny-by-default policy	Very High (90% reduction)	High ($30K-150K)	3-4 months
Endpoint Detection & Response	Advanced EDR solutions with behavioral analysis, threat hunting, automated response	Moderate-High (60% reduction)	High ($20-50/endpoint)	1-2 months
Network Monitoring (IDS/IPS)	Intrusion detection/prevention systems, traffic analysis, anomaly detection	Moderate (55% reduction)	High ($50K-200K)	2-3 months
Zero Trust Architecture	Verify every access request, never trust implicitly, continuous authentication	Very High (85-90% reduction)	Very High ($200K-1M+)	6-12 months
Disable Unnecessary Services	Turn off RDP when not needed, restrict SMB, close unused ports	High (70% reduction)	Very Low (minimal)	1-2 weeks
Regular Security Audits	Penetration testing, vulnerability assessments, security posture reviews	Moderate (50% reduction)	Moderate ($10K-50K/year)	Ongoing

1. Immutable Backups (WORM Storage): Write-Once-Read-Many storage prevents ransomware from encrypting or deleting backups. Implementation methods: object lock in cloud storage, tape media, dedicated backup appliances with immutability features.

2. Air-Gapped Backups: Physical isolation ensures backups remain inaccessible to network-based attacks. Ap-proaches include: removable media rotated off-site, network-disconnected backup servers, tape libraries with offline storage.

3. Continuous Data Protection (CDP): Real-time replication captures every change, enabling recovery to any point in time. Recovery Point Objective (RPO): seconds to minutes. Ideal for critical databases and applications.

4. Snapshot Technology: Point-in-time copies of data enabling rapid recovery. Ransomware-resistant when stored in protected volumes or cloud tier. Retention policy: hourly snapshots for 24 hours, daily for 30 days, weekly for 1 year.

C. Incident Response Framework

Table VI outlines a comprehensive ransomware incident response framework based on NIST guidelines.

D. Recovery Time and Cost Analysis

Figure 4 illustrates average recovery times and costs associated with ransomware incidents based on organizational preparedness levels.

E. Mitigation Strategy Effectiveness

Figure 5 compares the relative effectiveness of different ransomware mitigation strategies.

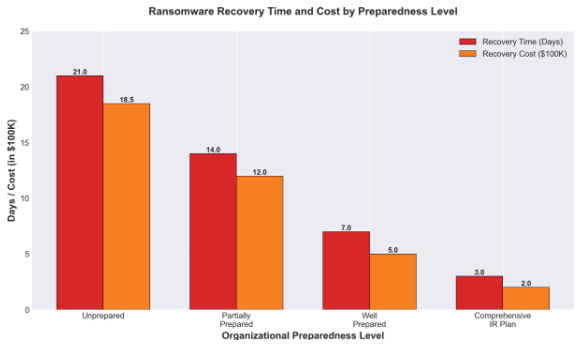

Fig. 4. Ransomware Recovery Time and Cost by Preparedness Level

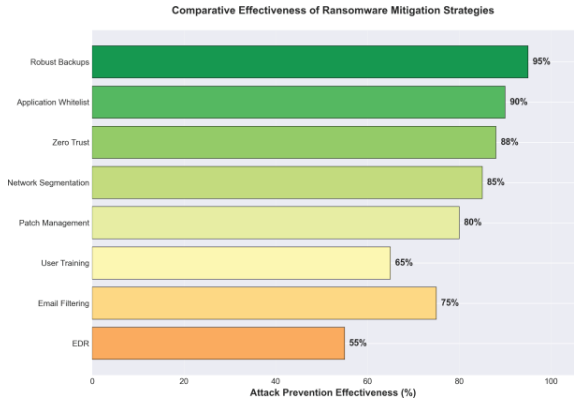

Fig. 5. Comparative Effectiveness of Ransomware Mitigation Strategies

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

TABLE VI
RANSOMWARE INCIDENT RESPONSE FRAMEWORK WITH DETAILED ACTIONS

Phase	Key Actions	Critical Timeline	Responsible Parties
Preparation	Develop IR plan, establish IR team roles, create communication protocols, conduct tabletop exercises, deploy monitoring tools	Ongoing (before incident)	CISO, IT Manager, Legal
Detection & Analysis	Identify infection indicators, classify ransomware variant, determine patient zero, assess scope and impact, preserve evidence	Hours 0-4	SOC Analysts, IR Team
Containment	Isolate affected systems, disconnect from network, disable user accounts, block C&C communications, prevent lateral spread	Hours 4-8	Network Admins, IR Team
Eradication	Remove malware from all systems, close attack vectors, patch vulnerabilities, reset all credentials, rebuild compromised systems	Hours/Days 8-48	System Admins, Security Team
Recovery	Restore systems from clean backups, verify system integrity, gradually reconnect to network, monitor for reinfection, resume operations	Days 2-7	IT Operations, IR Team
Post-Incident	Document incident timeline, analyze root cause, update security controls, improve detection capabilities, conduct lessons learned session	Weeks 1-4	IR Team, Management, Legal

VIII. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

A. Current Research Challenges

1) Advanced Evasion Techniques: The latest ransomware generation employs high-quality evasion strategies which can hardly be spotted:

Polymorphic and Metamorphic Code: The constant code modification and manipulation of the parameter and signature is seen without changing the functionality of the Ransomware. Detection problem Signature, Signature-based systems do not work, requires behavioural or ML-based detection.

Format-Preserving Encryption (FPE):Fil maintains file format, structure and encrypts data without being detected by entropy. It has to be alleviated through detailed analysis of content beyond what meets the eye.

Time-Delayed Execution:Malware is dormant, but after days or weeks is run in a manner that it can be analysed by time-based memory of sandboxes. Long-term behavioural observation will be included in solution.

Sandbox Detection and Evasion: These cheques can be performed by detecting (via system artefacts (limited RAM, specific processes, VM indicators) and denying execution. Contemporary sandboxes make use of bare-metal and concealment of artefacts.

Living-off-the-Land (LotL): Abuses legitimate system tools (PowerShell, WMI, PsEnum) in an abusive manner that appear to be legitimate administrative usage. Its identification requires an understanding of the normal and abnormal usage of tools.

Fileless Ransomware: The files are not written on the disc and it implies that nothing will be identified by files and any form of examination is not how the forensic will perform. Requires cognitive behavioural and memory observation.

2) Dataset Limitations: Both training and testing of the detection systems require a good set of data, but it has quite challenging issues:

Limited Availability: Not several publicly available datasets on ransomware contain ransomware variations. Most of these studies in the academic world are premised on human sample databases of 3-5 years old.

Concepts Idea: Dataset Imbalance The percentage of benchmarking to ransomware samples varies significantly (100:1) in favour of the benign classification by the ML models. Mitigation Synthetic oversampling (used).

Absence of Standardisation: No consensus exists in selection of evaluation measurements, train-test split and validation. The results of the various studies can be hardly compared.

Privacy Concerns: In the real-world ransomware samples, we have a chance of sensitive victim information that obstructs data sharing amongst the researchers.

Rapid Evolution: Ransomware is evolving in rapid comparison with the data updates. It may happen that the models trained on the past are not able to generalise to new variants.

3) Detection Latency: Delay until infection is detected is important in respect to the extent of damage:

Current State: Mean time of detection: 21 days. At this time, ransomware can:

- encrypt hundreds of thousands of files.
- objective Slur gigabytes of valuable information.
- Distributed across network infrastructure.
- deepetheshcop Shadow copies and backups, deletes.

Goal: Reduce detection to minutes or hours. Challenges:

- False positive management at shorter detection windows
- Computational overhead of continuous deep analysis

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

- Distinguishing legitimate encryption (user files, TLS traffic) from malicious

4) Cross-Platform Detection: Ransomware attacks more and more platforms that need more coordinated detection:

Platform Diversity: 10 Platform diversity Each platform will be windows, Linux, macOS, Android, iOS, IoT devices with different architecture, API and file systems.

Challenge: Detection models which are trained on one platform are not well transferred to others. Extractions needed depending on platform.

Solution Direction: ransfer learning to platform adapt models, platform agnostic behaviour signature, federated learning to engage in detection collaboratively.

B. Emerging Technologies for Ransomware Defense

Table VII summarizes promising future technologies that could transform ransomware defense.

C. Future Research Directions

1) AI-Powered Adaptive Defense Systems: Next-generation defense systems will employ artificial intelligence for dynamic, self-adjusting protection:

Generative Adversarial Networks (GANs): Train generator networks to create synthetic ransomware variants, training discriminator networks to detect them. Enables preparation for unknown future variants.

Reinforcement Learning: Agents learn optimal defense strategies through interaction with simulated attack environments. Adapts tactics based on attacker behavior.

AutoML and Neural Architecture Search: Automated discovery of optimal detection model architectures, reducing dependency on manual hyperparameter tuning.

Transfer Learning and Few-Shot Learning: Enable detection of new ransomware families from minimal samples by transferring knowledge from previously learned families.

2) Proactive and Predictive Defense: Shift from reactive detection to proactive threat anticipation:

Predictive Threat Intelligence: Machine learning analysis of dark web forums, threat actor communications, and vulnerability disclosures to predict emerging ransomware campaigns before deployment.

Moving Target Defense (MTD):Reconfigure system settings, network topology and application deployments continuously to raise the uncertainty and the cost to the attacker.

Deception at Scale:Implement thousands of decoy systems, files and credentials across networks. Attackers engage in negotiations with deceptions thereby making themselves known hence wasting resources.

Automated Threat Hunting: Automated Threat Hunting Automated threat hunting AI and systems actively look into evidence of a compromise, notifying users upon such evidence. Integrates behavioral analysis, threat intelligence, and anomalies.

3) Quantum-Safe Cryptography: In heavy hiking: Warrant to boot camp:

Challenge: The existance of quantum computers poses a threat to the existing public-key cryptography. Encryption based on RSA and ECC (used by ransomware and defenders) is prone to the algorithm developed by Shor.

Research Needs:

- Lattice-based, hash-based, and code-based algorithms resistant to quantum tampering.
- Migration plans of legacy systems.
- Hybrid secure cryptography systems based on classical and quantum-resistant algorithms.
- Body switched quantum computations concentrating on the disintegration of ransomware. encrypting (offensive capability)

4) Regulatory and Policy Frameworks: Technical solutions must be complemented by legal and policy measures:

International Cooperation: Ransomware operates globally; requires coordinated law enforcement response. Develop mutual legal assistance treaties (MLATs) for cybercrime.

Ransom Payment Regulations: There has been an argument whether it should be prohibited to pay ransoms to encourage attacker profitability, or it should be allowed to restore operations in an organisation. There was research necessary in the best policy balancing pragmatic needs and discouraging attacks.

Mandatory Disclosure Requirements: mandatory disclosure of ransomware cases to law enforcement agencies and victims. Expands transparency into the attack patterns and trends.

Critical Infrastructure Protection Standards: Minimum security requirements are established to each of the sectors (healthcare, energy, finance, transportation) that would most severely suffer devastating ransomware.

Cyber Insurance Regulation: nsurance policies can unwisely promote the ransom. They had to regulate to have policies that favour security best practises.

D. Identified Research Gaps

Table VIII summarizes critical research gaps requiring attention from the academic and industry communities.

IX. Conclusion

This ultimately diverse overview has explored the ransomware threat environment in various lenses: its historical development, attack strategies, detection, and mitigation strategies. We will analyse 50 or more research papers and offer a comprehensive analysis of this important cybersecurity issue.

A. Key Findings Summary

Threat Evolution: Ransomware has evolved past mere screen-lockers to multi-stage, complex attacks using double/triple extortion with more than 30 billion worth of damages occurring across the world every single year.

Attack Vectors: Phishing (34), and RDP exploitation (28) are still predominant first-access vectors, but the supply-chain

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

TABLE VII
EMERGING TECHNOLOGIES FOR NEXT-GENERATION RANSOMWARE DEFENSE

Technology	Application to Ransomware Defense	Maturity Level	Expected Impact	Timeline to Deployment
Generative AI	Synthetic ransomware generation for training, adversarial examples, automated signature creation, intelligent threat hunting	Developing	Very High	1-2 years
Blockchain	Immutable audit trails, decentralized threat intelligence sharing, tamper-proof backup verification	Experimental	High	2-3 years
Quantum Computing	Breaking ransomware encryption, quantum-resistant cryptography development, optimization of detection algorithms	Early Research	Revolutionary	5-10 years
Federated Learning	Privacy-preserving collaborative model training across organizations without sharing sensitive data	Developing	High	1-2 years
Edge Computing	Real-time IoT ransomware detection at network edge, reduced latency, distributed processing	Mature	Moderate-High	Current
Explainable AI (XAI)	Understanding ML detection decisions, reducing false positives, increasing trust in automated systems	Developing	High	1-3 years
Digital Twins	Simulating ransomware attacks in virtual replicas, testing defenses without risk, attack prediction	Experimental	Moderate	2-4 years
5G Security	Securing next-generation network infrastructure, network slicing for isolation, low-latency response	Mature	Moderate	Current
Homomorphic Encryption	Processing encrypted data without decryption, secure backup analysis, privacy-preserving detection	Early Research	High	3-5 years
Deception Technology	Advanced honeypots, honeynets, decoy files to detect and misdirect attackers	Mature	Moderate-High	Current

TABLE VIII
CRITICAL RESEARCH GAPS IN RANSOMWARE DEFENSE

Research Area	Gap Description	Priority	Potential Solutions
Real-time Detection	Insufficient research on sub-second detection with acceptable false positive rates	Critical	Hardware acceleration, edge processing, optimized algorithms
Post-Quantum Security	Limited ransomware-specific analysis of quantum threats and defenses	High	Quantum-resistant algorithm evaluation, hybrid systems
Supply Chain Security	Inadequate frameworks for detecting and mitigating supply chain ransomware vectors	Critical	Software Bill of Materials (SBOM), continuous verification
Human Factors	Psychological and behavioral aspects of victimization and response understudied	Moderate	Behavioral economics research, decision-making studies
Economic Analysis	Cost-benefit models for defense investments lacking empirical validation	Moderate	Large-scale economic impact studies, ROI analysis
Automated Recovery	Limited research on intelligent, automated recovery and restoration systems	High	AI-driven recovery orchestration, self-healing systems
Zero-Day Defense	Insufficient proactive approaches for defending against unknown exploits	Critical	Predictive analytics, vulnerability prioritization, virtual patching
IoT/ICS Security	Specialized detection for resource-constrained and operational technology environments	High	Lightweight algorithms, protocol-specific detection
Attribution	Technical attribution of ransomware attacks to specific threat actors remains challenging	Moderate	Behavioral fingerprinting, code analysis, infrastructure tracking

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

attacks are a new high-impact threat that has continuously impacted several organisations.

Detection Performance: Machine learning models, especially ensemble models that use Random Forest, XGBoost, and CNNs, get 99 percent and higher detection accuracy. Nevertheless, much work is left in terms of identifying elusive methods such as fileless ransomware and format-preserving encryption.

Proved to be best on the multi-defence strategies: Multi-layered Defence Strategies are most efficient. The highest prevention rate is recorded in Application whitelisting (90 percent efficacy), Zero Trust Architecture (85-90 percent efficacy) and network segmentation (85 percent efficacy). The best recovery mechanism is still the robust backup systems.

Research Gaps Global : gaps are present in real-time detection, cross-platform solutions, post-quantum cryptography and automated recovery systems. Limits of datasets have remained as an impediment to the development and assessment of detection algorithms.

B. Practical Recommendations

For organizations seeking to improve ransomware resilience, we recommend:

Prevention:

1) Done: Cheque security awareness training (at least quarterly)
2) Implement multi-factor authentication of all remote access.
3) Active patch remediation and critical 48-hour vulnerability.
4) Embrace Zero Trust concepts that embrace micro-segmentation.
5) Use operations supportable application whitelisting.

Detection:

1) Implement EDR solutions that have behavioural analysis.
2) deploy SIEM containing ransomware-specific event rules.
3) Scan dangerous file entropy, I/O signatures.
4) Algorithms Infrastructure Investment Establish baseline system behaviour to detect anomaly.

Detection:

1) Deploy EDR solutions with behavioral analysis capabilities
2) Implement SIEM with ransomware-specific detection rules
3) Monitor for suspicious file entropy changes and I/O patterns
4) Establish baseline system behavior for anomaly detection

Response & Recovery:

1) Work on and perform incident response plans on a regular basis.
2) 3-2-1-1-0 immutable backup strategy in place. number FQRI Backup restoration testing once every quarter.
3) Develop off-line recovery protocols and have recovery media.
4) Pre-position forensic capabilities of fast incident analysis.

C. Future Outlook

The ransomware threat will keep on developing, as its profitability and low-risks to the attackers will increase. The trends in the future will probably be:

- **AI-Powered Attacks**: Attacks based on machine learning to select/evade and perform adaptive encryption.
- **Quantum Threats**: The application of post-quantum cryptography will change the defensive capability and the offensive capability.
- **Critical Infrastructure Targeting**:Designated critical infrastructures It should cover the industrial control systems, health, and utility due to its potential kinetic impact.
- **Regulatory Evolution**: Governmental intervention within the context of bans on ransom payment, binding security requirements and adherence to international law implementation.
- **Defensive AI**: The Autonomous security systems which are possible under detecting, responding, and recovering attacks without human involved.

Joint ventures between the researchers, and industry practitioners with the government agencies are required to provide success in the war on the ransomware. The academic literature should be aligned with the practical use of threat intelligence applied in real world in comparison to the all theoretical research. The industry should have evidence-based security controls, and share threat information to undertake collective defence. Regulatory frames should be provided by government, law enforcement apparatus and research funding necessary to speed up the improvement.

The ransomware issue is also a significant one yet not nonexistent. Increased innovation in detection methods, taking defensive-in-depth approaches, and permitting a culture of cybersecurity awareness to be practised within organisations are some of the ways organisations can reduce their vulnerabilities to the harmful impact of the attacks as well as their exposure.

REFERENCES

[1] T. McIntosh, T. Susnjak, T. Liu, D. Xu, P. Watters, D. Liu, Y. Hao, A. Ng, and M. Halgamuge, “Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration,” *ACM Computing Surveys*, vol. 57, no. 1, Article 18, pp. 1-40, Oct. 2024.

[2] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, “Ransomware: Recent Advances, Analysis, Challenges and Future Research Directions,” *Computers & Security*, vol. 111, p. 102490, Dec. 2021.

[3] A. Kapoor, A. Gupta, R. Gupta, S. Tanwar, G. Sharma, and I. E. Davidson, “Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions,” *Sustainability*, vol. 14, no. 1, p. 8, Dec. 2021.

[4] Kritika, “A Comprehensive Literature Review on Ransomware Detection Using Deep Learning,” *Cyber Security and Applications*, vol. 3, p. 100078, Dec. 2025.

[5] N. Ebrahimi Majd and T. Mazumdar, “Ransomware Classification Using Machine Learning,” in *Proc. 2023 32nd International Conference on Advanced Information Networking and Applications (AINA)*, IEEE, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10230716

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

[6] Z. Pan and Z. Shu, "Hardware-Assisted Ransomware Detection Using Automated Machine Learning," in *Proc. 2025 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, IEEE, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/10993115
[7] Y. Hou, L. Guo, C. Zhou, Y. Xu, Z. Yin, S. Li, C. Sun, and Y. Jiang, "An Empirical Study of Data Disruption by Ransomware Attacks," in *Proc. IEEE/ACM 46th International Conference on Software Engineering (ICSE)*, 2024, pp. 1-12.
[8] J. Lee, J. Kim, H. Jeong, and K. Lee, "A Machine Learning-Based Ransomware Detection Method for Attackers' Neutralization Techniques Using Format-Preserving Encryption," *Sensors*, vol. 25, no. 8, p. 2406, Apr. 2025.
[9] P. Yan and T. T. Khoei, "Securing the Internet of Things: A comprehensive review of ransomware attacks, detection, countermeasures, and future prospects," *Franklin Open*, vol. 11, Jun. 2025, Art. no. 102056, doi: 10.1016/j.froope.2025.102056.
[10] G. Nagar, "The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies," SSRN Electronic Journal, Jun. 2024. DOI: 10.2139/ssrn.4881213
[11] A. Lavendel and P. Bentien, "A Threat-Led Approach to Mitigating Ransomware Attacks: Insights from a Comprehensive Analysis of the Ransomware Ecosystem," in *Proc. 2024 European Interdisciplinary Cybersecurity Conference (EICC)*, ACM, pp. 210-216, Jun. 2024, doi: 10.1145/3659563.3661321.
[12] M. Lang, L. Connolly, P. Taylor, and P. J. Connert, "The Evolving Menace of Ransomware: A Comparative Analysis of Pre-pandemic and Mid-pandemic Attacks," *Digital Threats: Research and Practice*, vol. 4, no. 4, pp. 1-22, Oct. 2023, doi: 10.1145/3550000.
[13] S. Enomoto, H. Kuzuno, H. Yamada, Y. Shiraishi, and M. Morii, "Early mitigation of CPU-optimized ransomware using monitoring encryption instructions," *International Journal of Information Security*, vol. 23, pp. 3393-3413, Jul. 2024, doi: 10.1007/s10207-024-00892-2.
[14] J. Thomas and G. Galligher, "Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware," *Computer and Information Science*, vol. 11, no. 1, pp. 25-38, 2018.
[15] B. Bahl and R. Endicott, "Know Thy Ransomware Response: A Detailed Framework for Devising Effective Ransomware Response Strategies," *Digital Threats: Research and Practice*, vol. 4, no. 4, pp. 1-19, Oct. 2020, doi: 10.1145/3560022.
[16] "The State of Ransomware 2024," Sophos Ltd., Technical Report, 2024. [Online]. Available: https://www.sophos.com/
[17] "SonicWall 2023 Cyber Threat Report," SonicWall Inc., 2023.
[18] "Ransomware Recovery: Challenges and Best Practices," Veeam Software, White Paper, 2024.
[19] "The True Cost of Ransomware in 2024," Coveware Inc., Quarterly Report, 2024.
[20] "Healthcare Cybersecurity: Ransomware Trends 2020-2023," HHS Health Sector Cybersecurity Coordination Center (HC3), 2023.
[21] B. Pranggono and A. Arabo, "COVID-19 Pandemic Cybersecurity Issues," *Internet Technology Letters*, vol. 4, no. 2, p. e247, 2021.
[22] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The Ransomware-as-a-Service Economy Within the Darknet," *Computers & Security*, vol. 92, p. 101762, 2020.
[23] "MITRE ATT&CK Framework," MITRE Corporation, 2024. [Online]. Available: https://attack.mitre.org/

(This work is licensed under a Creative Commons Attribution 4.0 International License.)