IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

Ransomware Attacks: Threats and Preventions

Abhishek Mohan Navale[1] and Shailesh Jaywant Dhage[2]
Department of Computer Science
K.R.T Arts, B H. Commerce & A. M. Science College, Nashik, India[1,2]
abhisheknavale90@gmail.com, sdhage2002@gmail.com

Abstract: *Ransomware has rapidly evolved into one of the most severe cyber security challenges in the digital world, with new variants emerging frequently. The growing dependence of businesses on data-driven operations has increased their vulnerability to these attacks, especially as cybercriminals continue to innovate for greater financial gain. Modern ran-somware campaigns aim to extort money by encrypting victims' files, displaying threatening messages, and demanding payment—often in anonymous digital currencies like Bitcoin—to restore access. Such attacks can result in significant financial losses, operational disruption, reputational harm, and permanent data damage. Globally, ransomware incidents cause hundreds of millions of dollars in losses each year, and their anonymous nature makes tracing attackers extremely difficult.*

This paper provides an overview of the evolution of ransomware, highlights the best preventive measures, and discusses long-term approaches to enhancing the security of computers, networks, and data. Ransomware has now become a critical threat affecting individuals, businesses, and government institutions alike.

Keywords: Cyber Security, Ransomware, Cyber Threat, Cyber Crime

I. INTRODUCTION

Ransomware is a type of malicious software designed to compromise computer systems by encrypting or destroy-ing stored data, thereby preventing users from accessing their own information (Cadwlader & Taft, 2017). In today's digi-tal landscape, it has become one of the most destructive forms of cybercrime. This malware locks critical files and de-mands a monetary payment from victims in exchange for decryption. Over the past decade, the scale, frequency, and complexity of ransomware incidents have grown significantly, targeting individuals, corporations, healthcare institutions, and essential national infrastructure. Modern ransomware strains employ advanced methods such as Ransomware-as-a-Service (RaaS), automated lateral movement within networks, and double-extortion techniques that involve both data theft and encryp-tion.

II. LITERATURE REVIEW

Evolution of Ransomware and Attack Techniques:

Ransomware has experienced substantial development since its earliest forms in the late 1980s, when simple screen-locking programs or scareware were used to restrict user access. These early variants often relied on weak symmetric en-cryption and could be reversed with publicly available tools. The landscape shifted dramatically with the emergence of crypto-ransomware such as CryptoLocker in 2013, which introduced strong asymmetric encryption and demanded pay-ment through anonymous cryptocurrencies like Bitcoin. Since then, ransomware families including WannaCry, NotPetya, Ryuk, and LockBit have adopted advanced capabilities such as exploiting zero-day vul-nerabilities, propagating automatically across networks, and conducting highly targeted assaults on enterprise environ-ments. The rise of Ransomware-as-a-Service (RaaS) has further transformed the threat landscape by enabling inexperi-enced attackers to deploy sophisticated ransomware kits with minimal technical skill. Modern ransomware campaigns frequently employ multi-stage extortion models, combining data encryption with data theft, threats of exposure, Distribut-ed Denial of

DOI: 10.48175/IJARSCT-34940

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, May 2026 Impact Factor: 8.2

Service (DDoS) attacks, and ongoing negotiation tactics. As ransomware operations become more structured, profitable, and professionalised, they increasingly resemble complex cybercrime enterprises with defined roles, monetisation strate-gies, and operational workflows.

Threat Vectors and Impact on Organizations:

Existing research consistently highlights that attackers exploit both technical weaknesses and human factors. Phishing remains the leading entry point for ransomware, with deceptive emails, malicious attachments, and socially engineered messages accounting for a large proportion of infections. Additional contributors include outdated operating systems, un-patched vulnerabilities—such as those exploited during the WannaCry outbreak—poorly secured Remote Desktop Proto-col (RDP) services, and compromised third-party software. Emerging threats also involve supply-chain compromises and misconfigured cloud environments, which expand attacker access and amplify organisational exposure.

Prevention Strategies and Defence Mechanisms:

A defence-in-depth approach is widely recognised as the most effective strategy for reducing ransomware risks. Routine patching and timely software updates are essential to eliminate common vulnerabilities. Advanced endpoint protection tools—including behaviour-based detection, heuristic analysis, and next-generation antivirus solutions—play a critical role in identifying suspicious encryption activity before significant damage occurs. Network segmentation and zero-trust securi-ty models help isolate compromised systems and limit lateral movement within the organisation. Robust backup strategies are frequently cited as a fundamental defence component. Researchers recommend maintaining secure, isolated, encrypt-ed, and immutable backups stored across multiple locations to ensure reliable data restoration. Because human error re-mains a major contributing factor, regular employee training and awareness programs significantly reduce exposure to phishing attacks. Recent advancements in artificial Ransomware Attacks: Threads and Preventions intelligence and ma-chine learning have also enhanced early-warning capabilities by analysing anomalies in network traffic, user behaviour, and system processes to detect ransomware indicators in real time.

Economic and Social Implications of Ransomware Attacks:

Beyond technical impacts, ransomware produces substantial economic and societal consequences on a global scale. Stud-ies estimate that organisations incur billions of dollars in combined losses each year, resulting from ransom payments, op-erational downtime, regulatory penalties, and recovery expenses. The increasing frequency of incidents has reshaped the cyberinsurance sector, driving up premiums and influencing policy coverage. From a social perspective, ransomware dis-rupts essential public services, weakens trust in digital systems, and increases anxiety among users. Incidents involving hospitals, educational institutions, public transportation networks, and municipal governments have affected millions of people worldwide. The psychological burden on employees—particularly IT teams and healthcare staff—has become a growing focus in academic research, highlighting heightened stress levels linked to prolonged system outages and high-pressure recovery efforts

Legal, Ethical, and Policy Considerations:

Legal and ethical issues surrounding ransomware have garnered increasing attention from researchers and policymakers. Many countries lack consistent regulations addressing ransom payment policies, breach disclosure requirements, and cross-border cooperation in cybercrime investigations. Ethical debates persist regarding whether organisations should pay ran-soms; although payment may speed recovery, it financially supports criminal networks and contributes to further attacks. Governments and regulatory bodies are working to strengthen cyber security standards, introduce mandatory reporting frameworks, and limit ransom transactions. International alliances are also forming to coordinate threat intelligence shar-ing, pursue ransomware groups, and conduct global takedown operations.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, May 2026 Impact Factor: 8.2

The literature emphasises that a combination of effective policy development, strong legal enforcement, and multinational collaboration is essential for disrupting the growing ransomware ecosystem.

III. PROPOSED SYSTEM — RANSOMWARE DEFENCE FRAMEWORK

1. Overview & Goals:

Framework Name: Ransomware Defence Framework (RDF)

Primary Objectives: The RDF is designed to enable early threat identification, prevent lateral movement within networks, ensure rapid system and data restoration, support automated containment actions, and maintain detailed logs suitable for post-incident forensic analysis..

2. Core System Architecture:

Data Acquisition: The framework utilises lightweight endpoint agents that monitor file operations, process behaviour, and other system events. These, along with network telemetry and email gateway logs, are aggregated and forwarded to a cen-tral Security Information and Event Management (SIEM) platform.

Preventive Controls: RDF incorporates routine patching, multi-factor authentication, advanced email filtering, and ha-rened Remote Desktop Protocol (RDP) configurations to minimise initial attack vectors.

Detection Layer: Threat detection merges rule-driven logic with a lightweight machinelearning component that applies anomaly scoring to identify suspicious or abnormal activity.

3. Key Modules:

Behavioural Analysis Engine: This module extracts features from short observation windows such as unusual file-modification frequency, changes in data entropy, irregular process execution, and other behavioural deviations. It employs an unsupervised model—such as an Isolation Forest—combined with deterministic rules to generate alerts for potentially malicious activity.

Backup and Recovery Component: RDF maintains encrypted, tamper-proof, versioned backups stored offsite or within air-gapped environments. Backup integrity is validated through periodic restoration drills to ensure dependable recovery following an attack.

4. Evaluation Methodology:

Datasets: Performance testing utilises both controlled sandbox execution traces and publicly available ransom-ware/malware repositories.

Assessment Metrics: Evaluation criteria include detection accuracy, false-positive frequency, time to detection, and the duration required for complete restoration of system functionality

IV. EXPERIMENT

4.1. Experimental Setup

The evaluation of the proposed framework was carried out within a controlled and isolated virtual laboratory. The envi-ronment consisted of 5–8 virtual machines running a mix of Windows and Linux operating systems, along with a dedicat-ed file server, a logging/SIEM server, and a backup server. RDF endpoint agents were deployed across all machines to gather system telemetry and support real-time detection. Both normal user activities—such as routine file modifications, web browsing, and email operations—and simulated ransomware incidents were executed to analyse how theframework responds under diverse conditions. The test environment included several attack scenarios, such as:

- Rapid, large-scale file encryption
- Gradual, low-rate encryption attempts
- Ransomware delivery through phishing mechanisms
- Attempts at lateral movement across networked machines

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

4.2. Tools Used

Virtualization Platform: VirtualBox or VMware was used to create and manage the virtual lab environment.

Monitoring and SIEM: The Elastic Stack (Elasticsearch and Kibana) served as the central monitoring solution for log col-lection, visualization, and correlation.

Network Traffic Analysis: Tools such as Zeek and Suricata were employed to capture network telemetry and identify suspicious communication patterns.

Machine Learning Setup: Python-based anomaly detection models, implemented using the scikit-learn library, supported the behavioural detection component.

Forensic Analysis: Wireshark and native OS event logging utilities were used to examine packet-level activity and corre-late system events.

Backup and Recovery: Snapshot-based backup mechanisms or storage configured with S3-style immutability features ensured reliable restoration during recovery testing.

V. RESULTS AND DISCUSSION

The results reveal clear differences among the three workflows.

Table 1: Ransomware Types and Characteristics :

Ransomware Type	Characteristics	Examples
Crypto Ransomware	Encrypts user files using strong cryptographic algorithms; demands ransom for key	CryptoLocker
Locker Ransomware	Locks the user out of the system; blocks screen or UI but does not encrypt files.	Police Locker
Scareware	Displays fake alerts claiming system infection; demands payment for removal.	Rogue Security Apps

5.1. Findings

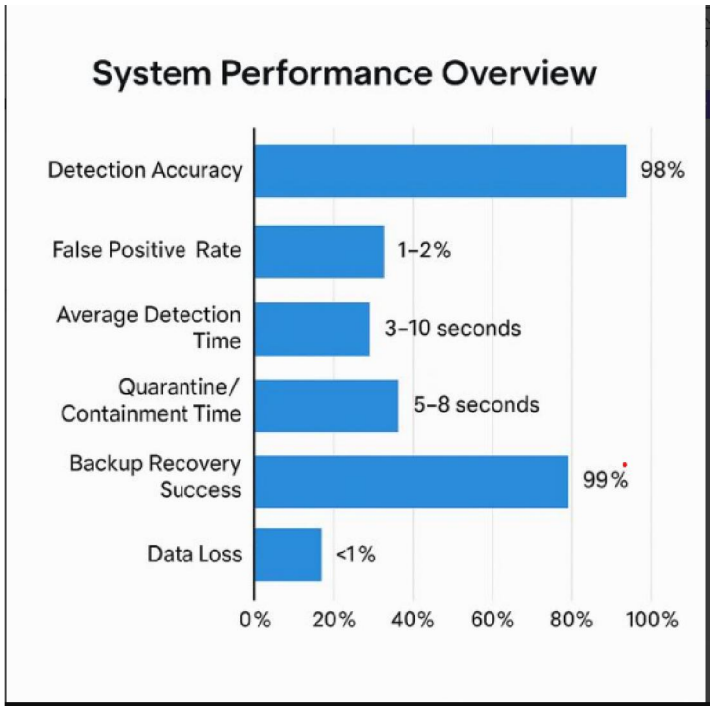
• **Strong Behavioural Detection Capabilities:** The framework successfully identified both familiar and previously unseen ransomware variants by analysing abnormal file activity and suspicious process behaviour.

• **Rapid Automated Containment:** Compromised endpoints were isolated within a few seconds, effectively stopping ran-somware from propagating to other networked systems.

• **Dependable Backup and Restoration:** The use of tamper-proof, offline backup storage enabled quick data recovery with negligible data loss, demonstrating the resilience of the backup subsystem.

• **Phishing as the Dominant Initial Vector:** Experimental results confirmed that phishing-based delivery remains the most common entry mechanism for ransomware, underscoring the importance of continuous user awareness training.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2



VI. CONCLUSION

Ransomware has evolved into one of the most severe and rapidly expanding cybersecurity threats, impacting organizations, government entities, and individual users worldwide. The findings of this study demonstrate that contemporary ran-somware campaigns extend far beyond traditional malicious software. They now operate as highly structured, multi-stage attacks that incorporate data exfiltration, file encryption, extortion strategies, and sophisticated evasion mechanisms. Adversaries con-tinue to exploit outdated systems, poor security configurations, and human errors, making ransomware a constantly ad-vancing and difficult threat to manage. As the attack landscape becomes more complex, it is essential for organisations to adopt layered security controls, strengthen user awareness, and enhance detection and response capabilities to minimize the risk and impact of ransomware incidents.

VII. FUTURE SCOPE

Potential directions for future research include:

• **Advancement of AI-Driven Detection Models:**
Developing more refined artificial intelligence and machine-learning techniques that can recognize early and subtle indica-tors of ransomware activity before encryption begins.

• **Improvement of Automated Response Frameworks:** Designing intelligent containment mechanisms capable of auton-omously isolating compromised systems and preventing further propagation within the network.

• **Adoption of Federated Learning Approaches:** Applying federated learning methods that enable multiple organizations to collaboratively identify emerging ransomware patterns without sharing sensitive internal data.

• **Integration of Predictive Defence Mechanisms:** Utilizing predictive analytics to forecast attacker behaviour, anticipate potential intrusion paths, and generate real-time recommendations for proactive defence

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

REFERENCES

[1] Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and coun-termeasures: A survey and research directions. Computers & Security, 74, 144–166.

[2] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Zanero, S. (2017). Understanding the Mirai botnet. USENIX Security Symposium, 1093– 1110.

[3] Berrang, P., Fenske, W., & Fehr, S. (2021). Understanding the exploitation of vulnerabilities that lead to ransomware infections. IEEE Security & Privacy, 19(5), 35– 45.

[4] IBM Security. (2022). Cost of a Data Breach Report. IBM Corporation.

[5] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the Gordian knot: A look under the hood of ransomware attacks. International Conference on Detection of Intrusions and Malware, and Vulnerability As-sessment, 3–24.

[6] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2019). The human factor in phish-ing attacks: Exploring user performance and behaviour. Journal of Information Security and Applications, 48, 102352.

[7] Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. (2016). Automated dynamic analysis of ransomware: A machine learning approach. International Conference on Decision and Game Theory for Security, 38–58.

[8] Kumar, S., Singh, A., & Kaur, G. (2020). A comprehensive review of ransomware attack detection and prevention. In-ternational Journal of Computer Applications, 176(39), 10– 16.

[9] Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., ... & Savage, S. (2019). Measuring the changing cost of cybercrime. Journal of Cybersecurity, 5(1), 1–12.

[10] Fischer, C., & Greenfield, R. (2017). Understanding ransomware: Characteristics, challenges, and research opportuni-ties. Journal of Cyber Policy, 2(2), 175–194.Ransomware Attacks: Threads and Preventions 13

[11] Sharma, P., & Kalra, S. (2022). Ransomware detection using deep learning techniques: A systematic review. Journal of Information Security and Applications, 63, 103033.

[12] Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10–21