International Journal of Advanced Engineering and Technology
www.allengineeringjournal.com
ISSN: 2456-7655
Received: 07-03-2026, Accepted: 07-04-2026, Published: 22-04-2026
Volume 10, Issue 2, 2026, Page No. 51-53

# Ransomware attacks: Detection, prevention, and recovery strategies

**Kanchan Shah, Anoushka Vinod**
Department of Computer Science, Pillai College of Arts Commerce & Science, Panvel, Navi Mumbai, Maharashtra, India

**Abstract**
Ransomware has emerged as one of the most damaging cyber threats affecting modern digital systems. These attacks restrict access to critical data by encrypting files and demanding payment in exchange for decryption. Individuals, organizations, and even national infrastructure have increasingly become targets of such attacks. In recent years, ransomware techniques have evolved significantly with the introduction of advanced approaches such as polymorphic malware, double-extortion strategies, and ransomware-as-a-service (RaaS), which make detection and mitigation more challenging.
This study examines ransomware threats from the perspectives of detection mechanisms, preventive security practices, and recovery strategies. Various detection approaches, including signature-based methods, behavioral analysis, and artificial intelligence-driven models, are comparatively analyzed using secondary data from academic publications, cybersecurity reports, and case studies. The analysis indicates that AI-assisted detection systems provide improved adaptability and higher detection accuracy compared with traditional techniques.
The research proposes a layered cybersecurity framework integrating detection, prevention, and recovery mechanisms. Although ransomware cannot be completely eliminated, adopting a structured and proactive security strategy can significantly strengthen organizational resilience and reduce the impact of cyber incidents.

**Keywords:** Ransomware, cybersecurity, malware detection, artificial intelligence, data security, cyber threats

## Introduction
The rapid expansion of digital infrastructure has increased exposure to various cyber threats across organizations and individuals. Among these threats, ransomware has become one of the most disruptive forms of cybercrime. In a ransomware attack, malicious software prevents users from accessing important files or systems by encrypting data and demanding payment for its release.
In recent years, ransomware operations have grown more sophisticated. The emergence of ransomware-as-a-service (RaaS) platforms enables attackers with limited technical knowledge to launch advanced attacks by purchasing ready-made ransomware kits. Furthermore, modern ransomware campaigns frequently employ double-extortion techniques, where attackers not only encrypt files but also threaten to leak stolen data unless the victim pays the demanded ransom.

## Statement of the Problem
Despite improvements in cybersecurity technologies, organizations still face difficulties in detecting, preventing, and recovering from ransomware incidents. Advanced ransomware variants often use obfuscation techniques, polymorphic code, and automated attack mechanisms that allow them to bypass traditional security systems. As a result, many organizations remain vulnerable to data loss, operational disruption, and financial damage.

## Goals of the Research
- To study how ransomware attacks have changed over time
- To look at different ways to find things, such as signature-based, behavioral, and AI-based methods.
- To assess preventive cybersecurity measures
- To look at ways to recover and how to respond to situations
- To suggest a complete, multi-layered defense model against ransomware

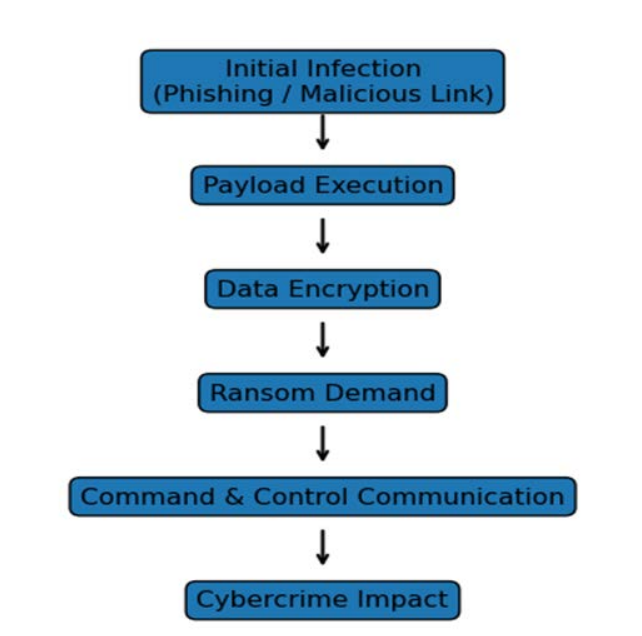


**Fig 1:** Ransomware Attack Lifecycle

## A Review of the Literature
Previous research has examined ransomware from multiple perspectives, including classification, detection techniques, and defense mechanisms. Earlier studies categorized ransomware into several forms such as crypto-ransomware, locker ransomware, and the more recent double-extortion model. Kharraz *et al.* (2015) [1] analyzed the internal functioning of ransomware and highlighted the weaknesses of traditional signature-based detection methods. Scaife *et al.* (2016) [2] proposed approaches to protect user data from malicious encryption attempts, while Brewer (2016) [3] discussed mitigation strategies for organizational environments.

More recent studies emphasize the effectiveness of behavior-based monitoring and machine learning techniques in detecting previously unknown ransomware variants. However, much of the existing literature focuses primarily on detection techniques, with limited attention given to integrating preventive and recovery strategies into a unified security framework. This study addresses that gap by examining a comprehensive multi-layer defense approach that combines detection, prevention, and recovery mechanisms.

**Methodology**

This study employs a qualitative and comparative analytical methodology.

1. **Gathering Data:** We got secondary data from:
   - IEEE and ACM journals that have been peer-reviewed
   - Reports from the cybersecurity industry
   - Published case studies of ransomware
   - Research papers for school

2. **Criteria for Evaluation:** We looked at detection and prevention strategies by using:
   - How accurate is detection?
   - Rate of False Positives
   - Time to Respond
   - How well the recovery works
   - Cost of Implementation

3. **The Process of Research:** Identifying the problem → Reviewing the literature → Comparing the results → Developing a model → Drawing a conclusion

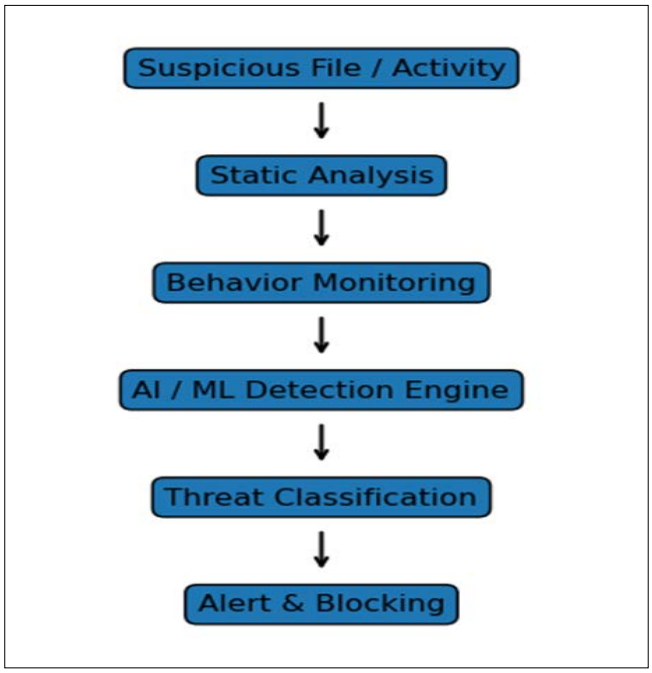


**Fig 2:** Ransomware Detection Process

**Result**

The study shows that AI-based ransomware detection systems work better than traditional signature-based systems. Regular backups and endpoint protection that aren't online greatly lessen the damage from attacks. Companies that have plans for how to respond to incidents recover faster and lose less money. The findings are displayed through comparative tables and charts that emphasize detection accuracy and recovery efficacy.

**Discussion**

The results show that ransomware threats are still changing quickly. Even though detection technologies are getting better, attackers change their methods to get around defenses. The study emphasizes the necessity for a multi-faceted security strategy that integrates technology, policies, and user awareness. Limitations encompass dependence on secondary data and absence of experimental execution. Future studies might concentrate on real-time detection and automated response mechanisms.

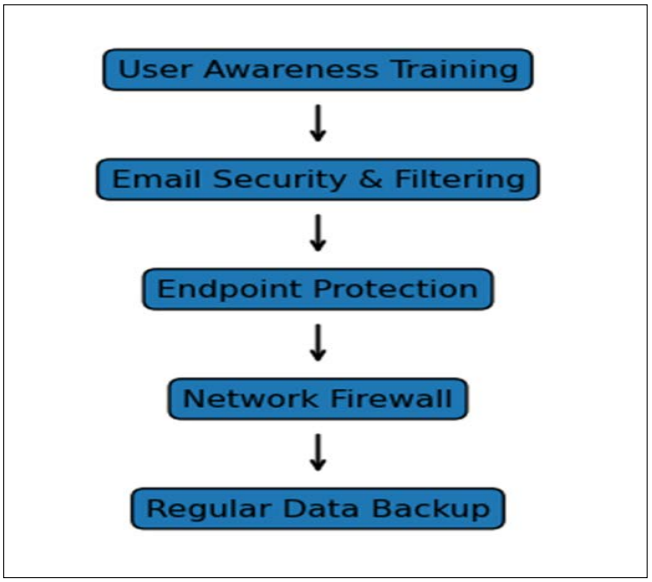


**Fig 3:** Multi-Layer Ransomware Prevention Model

**Conclusion**

Ransomware continues to pose a significant challenge to modern digital systems and organizational cybersecurity. The findings of this study indicate that effective defense against ransomware requires a combination of early detection mechanisms, preventive security practices, and well-structured recovery strategies. Implementing comprehensive cybersecurity frameworks, supported by user awareness and proactive system protection, can substantially reduce the damage caused by ransomware attacks and improve an organization's ability to respond to evolving cyber threats.

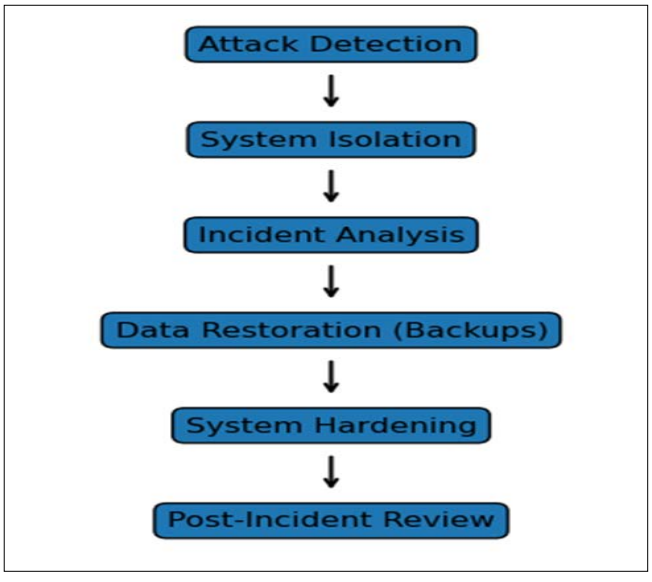


**Fig 4:** Ransomware Recovery & Response Workflow

**References**


1. Kharraz A, Robertson W, Balzarotti D, Bilge L, Kirda E. Cutting the Gordian knot: A look under the hood of ransomware attacks. IEEE Security & Privacy,2015:13(3):45–53. https://doi.org/10.1109/MSP.2015.31
2. Scaife N, Carter H, Traynor P, Butler K. Cryptolock (and drop it): Stopping ransomware attacks on user data. Proceedings of the IEEE International Conference on Distributed Computing Systems, 2016, 303–312. https://doi.org/10.1109/ICDCS.2016.46
3. Brewer R. Ransomware attacks: Detection, prevention and cure. Network Security,2016:2016(9):5–9. https://doi.org/10.1016/S1353-4858(16)30086-1
4. Kolodenker E, Koch W, Stringhini G, Egele M. PayBreak: Defense against cryptographic ransomware. Proceedings of the ACM Asia Conference on Computer and Communications Security, 2017, 599–611.
5. Sgandurra D, Muñoz-González L, Mohsen R, Lupu E. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. Proceedings of the European Symposium on Research in Computer Security, 2016, 423–441.
6. Richardson R, North M. Ransomware: Evolution, mitigation and prevention. International Management Review,2017:13(1):10–21.
7. Al-rimy B, Maarof M, Shaid S. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security,2018:74:144–166.