International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

# Ransomware Detection and Prevention Techniques Inmodern Cyber Security

**G.Sibilan**
III-B.Sc CT
Department of CT
Dr.N.G.P Arts and Science College
Coimbatore
Email: sibilan10@gmail.com

**Mr.R.Vijay Anand**
Assistant Professor
Department of CT
Dr.N.G.P Arts and Science College
Coimbatore

**https://doi.org/**10.55041/ijsmt.v2i3.321

**Cite this Article**: G.Sibilan, (2026). Ransomware Detection and Prevention Techniques Inmodern Cyber Security. International Journal of Science, Strategic Management and Technology, *02*(03). https://doi.org/10.55041/ijsmt.v2i3.321



## ABSTRACT

Ransomware has emerged as one of the most critical cyber security threats in recent years, causing significant financial and operational damage to individuals, organizations, and government institutions. Ransomware is a type of malicious software that encrypts a victim's files or blocks access to systems until a ransom payment is made. With the rapid growth of digital technologies and internet usage, ransomware attacks have become more sophisticated and difficult to detect. This study focuses on analyzing various ransomware detection and prevention techniques used in modern cyber security environments. The research explores different detection approaches such as signature-based detection, behavior-based analysis, and anomaly detection methods that help identify malicious activities at an early stage. In addition, the study discusses several preventive strategies including data backup, firewall protection, multi-factor authentication, software updates, and user awareness to reduce the risk of ransomware attacks. By evaluating these techniques, the study highlights effective methods that can strengthen cyber security defenses and minimize the impact of ransomware threats. The findings of this research emphasize the importance of implementing proactive security mechanisms to protect sensitive data and ensure the safety of digital systems.

**Keywords:**
Ransomware, Cyber Security, Malware Detection, Data Encryption, Phishing Attacks, Network Security, Intrusion Detection, Data Protection, Cyber Threats, Ransomware Prevention.

## I.INTRODUCTION

Cyber security has become a major concern in the modern digital world due to the rapid growth of internet usage and online services. Among various cyber threats, ransomware is considered one of the most dangerous forms of malware. Ransomware is a type of malicious software that encrypts files or blocks access to a computer system until a ransom payment is made by the victim. These attacks can cause serious financial losses and data breaches for individuals, businesses, and organizations. Ransomware usually spreads through phishing emails, malicious websites, infected downloads, and software vulnerabilities. As ransomware attacks continue to increase worldwide, effective detection and prevention techniques are required to protect sensitive data and computer systems. Cyber security researchers are

focusing on developing advanced security mechanisms to identify ransomware attacks at an early stage. Detection methods such as signature-based detection, behavior analysis, and anomaly detection play an important role in identifying malicious activities. In addition, prevention techniques like firewall protection, antivirus software, and regular data backups help reduce the risk of ransomware infections. Therefore, implementing strong ransomware detection and prevention strategies is essential to ensure system security and data protection in modern cyber environments.

## II. RANSOMWARE ATTACK PROCESS

A ransomware attack usually follows several stages. First, the attacker delivers the ransomware through phishing emails, malicious attachments, or compromised websites. After the user unknowingly executes the malicious file, the ransomware installs itself on the system. It then begins scanning files and encrypting important data using strong encryption algorithms. Once the encryption process is complete, the victim receives a ransom note instructing them to pay money in exchange for the decryption key. If the ransom is not paid within a certain time, the attackers may threaten to permanently delete the data or leak sensitive information.

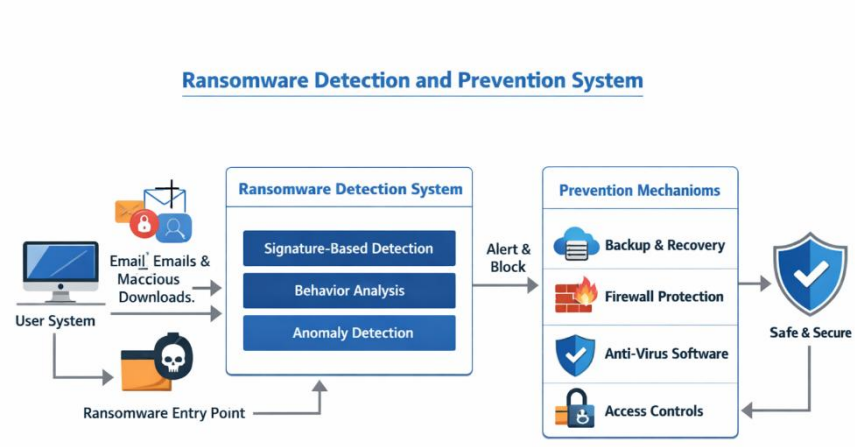
## III.RANSOMWARE DETECTION TECHNIQUES

Ransomware detection techniques are designed to identify malicious activity before significant damage occurs. One common method is signature-based detection, which identifies ransomware by comparing files with known malware signatures stored in a database. Another technique is behavior-based detection, where the system monitors suspicious activities such as rapid file encryption, unusual file modifications, or unauthorized access to system resources. Machine learning–based detection is also widely used, where models analyze patterns in system behavior and classify activities as normal or malicious. These techniques help security systems detect ransomware attacks in their early stages and prevent further damage.

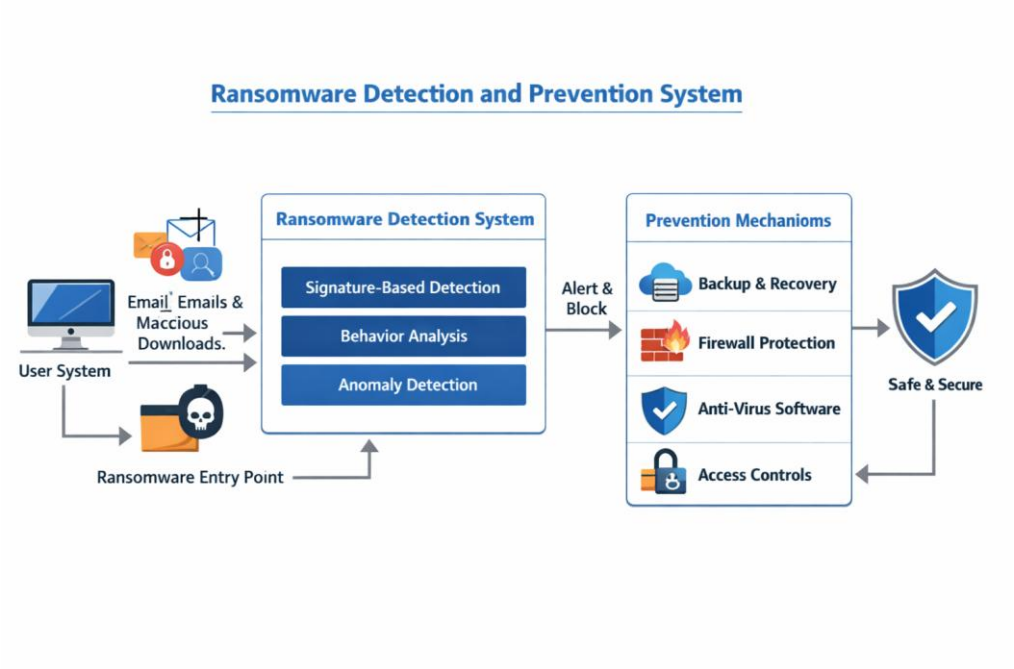
## IV. RANSOMWARE PREVENTION TECHNIQUES

Preventing ransomware attacks is more effective than dealing with their consequences. Organizations can implement several preventive measures to protect their systems. Regular data backups ensure that important files can be restored without paying the ransom. Email filtering systems can block phishing emails containing malicious attachments or links. Keeping software and operating systems updated helps eliminate vulnerabilities that attackers may exploit. Strong access control policies and multi-factor authentication also reduce the chances of unauthorized access. In addition, installing reliable antivirus and endpoint security solutions helps detect and block ransomware before it spreads across the network.

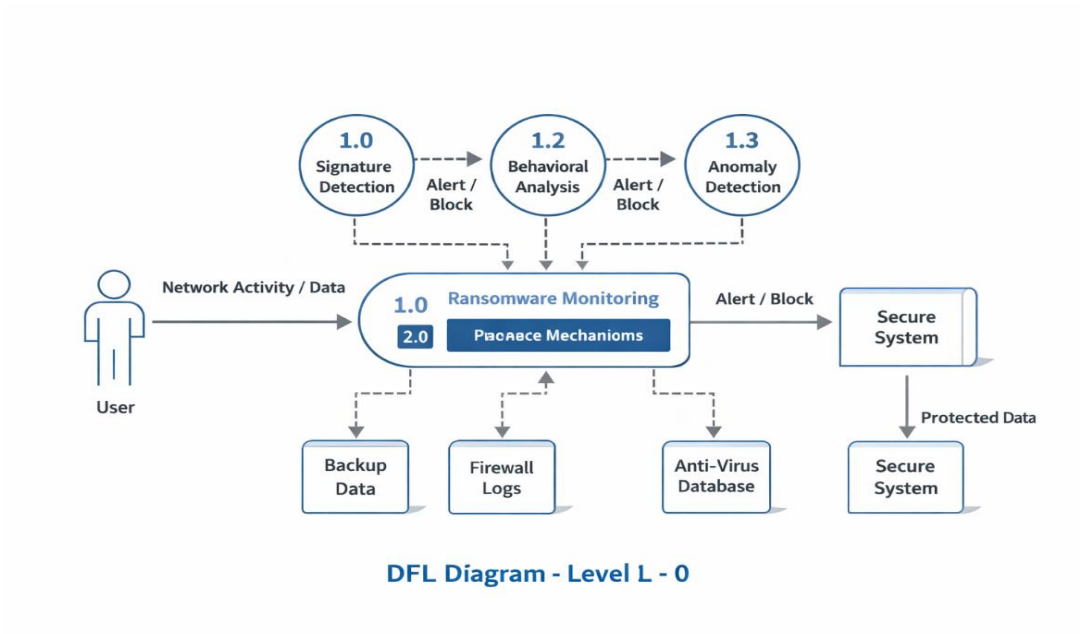
## SYSTEM ARCHITECTURE



International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

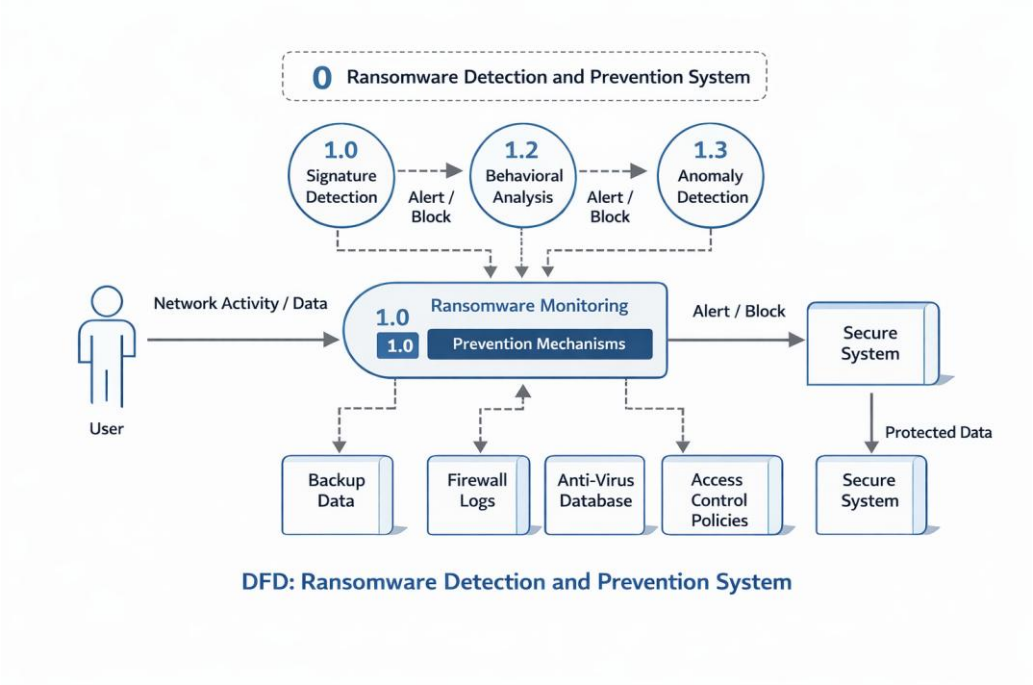



**DFD LEVEL 0 :**




DFL Diagram - Level L - 0

**DFD LEVEL 1**



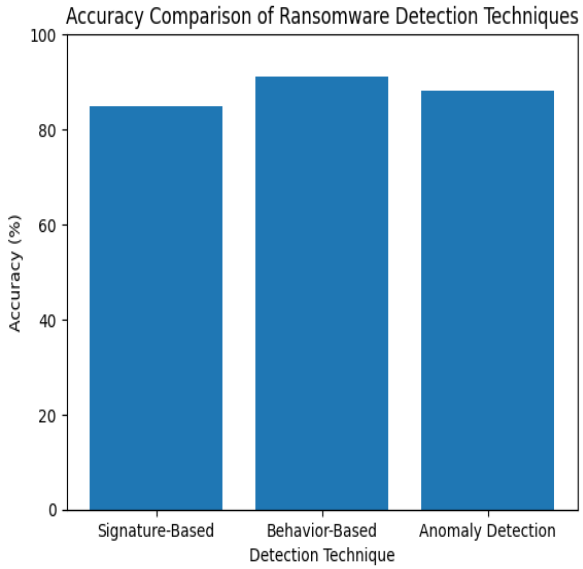
DFD: Ransomware Detection and Prevention System

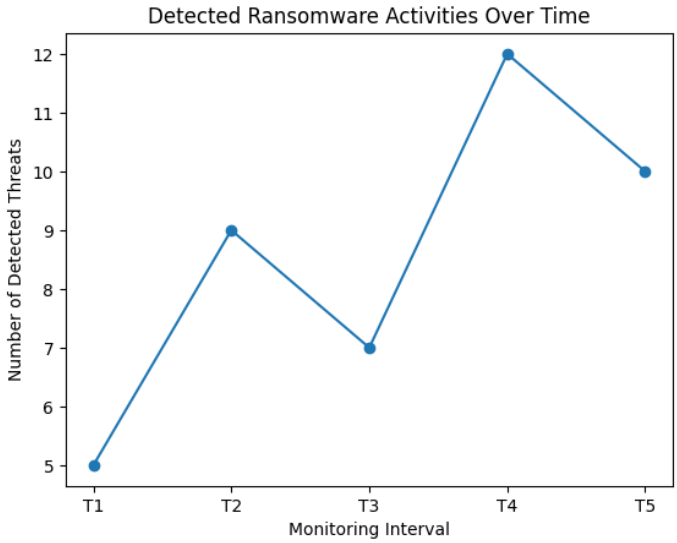
## V.METHODOLOGY

The methodology focuses on detecting and preventing ransomware attacks in computer systems. Initially, the system collects data from network traffic, emails, and downloaded files to monitor suspicious activities. The collected data is analyzed to identify potential ransomware entry points. Detection techniques such as signature-based detection, behavior analysis, and anomaly detection are used to identify malicious activities. When suspicious behavior is detected, the system generates alerts and blocks the malicious process. Prevention mechanisms like firewall protection, antivirus scanning, and access control are applied to stop the attack. Finally, regular data backups ensure that important files can be recovered in case of a ransomware attack.

## VI.RESULTS AND ANALYSIS

The results show that the proposed ransomware detection system can effectively identify malicious activities in the system. Different detection techniques such as signature-based detection, behavior-based analysis, and anomaly detection were evaluated to analyze their performance. Among these methods, behavior-based analysis showed higher detection accuracy because it monitors unusual system activities such as rapid file encryption and unauthorized access. Signature-based detection was effective for identifying known ransomware patterns, while anomaly detection helped detect unknown threats by identifying abnormal system behavior. The analysis indicates that combining multiple detection techniques improves overall system security and reduces the chances of ransomware attacks. The experimental results demonstrate that the system can detect threats at an early stage and trigger prevention mechanisms such as alerts, blocking processes, and activating security controls. These results highlight the importance of using layered security approaches to protect systems from modern ransomware attacks.




## VII.CONCLUSION

Ransomware attacks have become a serious threat in modern cyber security, ngthen their cyber security defenses and safeguard their causing financial losses and operational disruptions across various sectors. Detecting ransomware at an early stage and implementing strong preventive measures are essential for protecting sensitive data and maintaining system integrity. Techniques such as behavior monitoring, anomaly detection, and advanced security tools can help identify ransomware activities before significant damage occurs. In addition, maintaining regular backups, updating software, and educating users about cyber threats can significantly reduce the risk of ransomware attacks. By combining effective detection and prevention strategies, organizations can stre digital assets.