Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 5-B, pp. 1897–1906
DOI : 10.47974/JIOS-2282

Prevention of ransomware attacks using advanced encryption and behavioral analysis

Pooja Bagane *
Sonali Kothari †
Ankur Goyal §
Ranjeet Bidwe ‡
Vaibhavi Rana @
Sanju Saji #
Sankalp Taneja $
Manya Chandiramani ^
Department of Computer Science and Engineering
Symbiosis Institute of Technology (SIT)
Symbiosis International (Deemed University)
Lavale
Pune 412115
Maharashtra
India

Abstract

In an evolving digital era, and ransomware forms are significantly increasing day by day. These attacks use encryption to lock down victims' data and ask for cash (a ransom) in turn for a decrypting key, leaving many people/organizations seriously out of pocket. Here, we will take a case study where these encryption tricks are combined with behavioral analysis and how it can be used to avoid ransomware attacks. It is based on the use of cryptographic methods to secure data and analysis of behavior monitoring in order to identify system operation practices that could cause ransomware. In it, we cover the theoretical background of this approach and how he formed these conclusions as well as the results. Look for new reports on wider implications using encryption alongside behavioral detection to protect against ransomware soon! The report also showcases the changing landscape of Ransomware

* *E-mail:* **pooja.bagane@sitpune.edu.in (Corresponding Author)**
† *E-mail:* **sonali.kothari@sitpune.edu.in**
§ *E-mail:* **ankur.goyal@sitpune.edu.in**
‡ *E-mail:* **ranjeet.bidwe@sitpune.edu.in**
@ *E-mail:* **vaibhavi.rana.btech2021@sitpune.edu.in**
# *E-mail:* **sanju.saji.btech2021@sitpune.edu.in**
$ *E-mail:* **sankalp.taneja.btech2021@sitpune.edu.in**
^ *E-mail:* **manya.chandiramani.btech2021@sitpune.edu.in**

with real-world case studies coupled with a literature review as well as documents how different methodologies proposed before adding value in mitigating these threats.

Subject Classification: *Primary 94A60, Secondary 68T05.*

Keywords: *Ransomware, File encryption, Encryption systems, Deviant behavior recognition, Security against cyber attacks, Information security principles, Malicious software, Secret key cryptography, Public key cryptography, Parameters of cyber laws, Offensive cyberspace.*

1. Introduction

Cybersecurity involves techniques that protect systems and data from unauthorized access or attacks. Ransomware, a major threat, locks victims' data until a ransom is paid, though payment doesn't guarantee recovery. According to a Novetta report, ransomware falls under broader cyber activities, employing both active and passive attack methods. This paper highlights two key preventive strategies: advanced encryption to safeguard sensitive data and behavioral analysis to detect abnormal activity and stop ransomware early. With social engineering attacks on the rise, integrating these methods is crucial for building resilient cybersecurity strategies and minimizing potential damage from ransomware threats.

2. Literature Review

Ransomware defense measures can be divided into the following two major categories: encryption protection and end user behavior analysis. Summative research, based on multiple academic papers, industry whitepapers and reports show that interest and progress is increasing in both of these areas.

2.1. *Cryptography in Cybersecurity*

Cryptography is still one of the theoretical pillars of information defense, particularly against ransomware. The goal of cryptographic methods is to protect information by encrypting it in such a way that its unauthorized use is difficult or impossible. There's symmetrical encryption and there's asymmetrical encryption. Symmetric encryption, in particular the Advanced Encryption Standard (AES), is published and widely used because of its high efficiency and strong defense security strength. The AES also works with a single shared key to implement the encryption and decryption of the elements, and therefore it can be applied in low computational capacity environments [1]. With asymmetric encryption, such as RSA (Rivest-Shamir-Adleman) encryption technique, it attempts to get around the problem of keys by using two keys – a public and a private one. It improves the secure communication substantially since there does no longer exist a shared secret key [2]. RSA is particularly powerful in stopping ransomware from eavesdropping on the go when encryption keys are exchanged back and forth. But it can be a single point of failure against well-crafted ransomware. According to Zhang, Wu, and Gupta [3], evolved malware strains are using measures to bypass or take advantage of

poor encryption implementations. This points to a necessity to complement the encryption with alternate capabilities, such as behavioral analysis, to have a strong defense to ransomware.

2.2. *Behavioral Analysis to Detect Anomalies*

Behavioral analysis has been found to be effective in identifying ransomware campaigns. Unlike the classical signature-based methods, the behavior analysis is aimed to detect a deviation of certain system services or user behavior from established profiles of normal activity [2].

Machine learning can be incorporated into security systems to make them more capable of early detection and respond pro-actively. Heuristic detection—a sub method under the category of behavioral based analysis— is capable of recognizing certain ransomware behaviors (e.g., new files written to more quickly, large numbers of files encrypted, ransom notes being produced). These traits have been vital for the identification of adversarial activities from well-known ransomware threats such as WannaCry, Ryuk etc. [4]. Xu, Lin, and Zhao [5] focused on behavioral analysis when using RTTIF. This deep integration significantly increases the speed and accuracy of ransomware detection so that organizations can respond more quickly and with greater accuracy.

2.3. *Combined Approaches*

By their very nature, encryption safeguards data integrity and confidentiality, but behavioral analysis enables to spot and neutralize threats before they become painful and office decide to hire you along with the IT staff. Hence, Kaspersky Lab [4] emphasizes the necessity of deploying the two strategies together for effective protection. Even if ransomware slips through the encryption, behavior monitoring can catch aberrant system performance, providing an early warning.

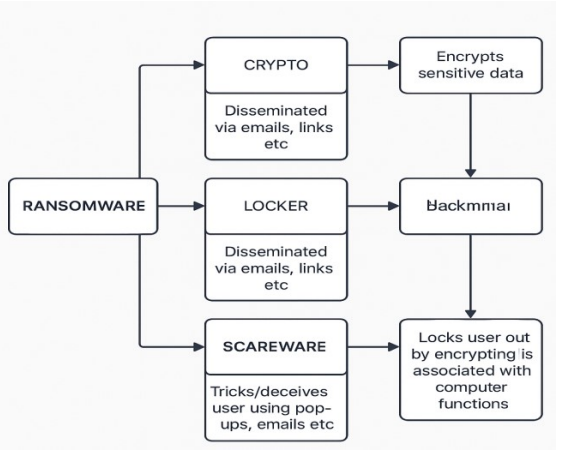

Figure 1
Types of Ransomware

Ransomware is a form of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. There are three types of ransomwares - Crypto, Locker, and Scareware. Crypto ransomware locks sensitive information with encryption and the user cannot access the data unless the decryption key is available; moreover, it is typically propagated through phishing emails and malicious links [6]. Locker ransomware also disables the essential functions of the victim's computer and the mode of dissemination is also through email and exploit kit [7]. On the other hand, scareware misleads victims using counterfeit warnings or pop-ups to give them the impression that their machine is infected and to persuade them to buy a useless or malicious application [8].

All of these ransomware themes culminate in extortion (Figure 1): the victim is forced to pay in exchange for recovering access to his files, systems or to prevent threatening alerts. These attacks are successfully launched by cyber criminals by taking advantage of user behavior and system vulnerabilities. Cyberthreat actors have turned up their ransomware levels with new tactics to pressure victims into paying for the return of their data and to enter into negotiations with victim organizations.

In [9], the issue of ethical hacking and penetration testing is addressed regarding their role in detecting vulnerability in a system. It draws attention to different tools and methodologies that are applied to make a simulation of real-world cyberattacks. The article puts importance on proactive security systems to enhance organizational defense mechanisms. The findings show that offensive security methods contribute to a high level of threat detection and mitigation. The article contributes to the idea that ethical hacking should be incorporated into the contemporary cybersecurity systems.

3. Methodology

3.1 *The Ransomware Prevention Algorithm*

The algorithm of ransomware prevention is designed to not only detect and mitigate threats, but also save you lots of headaches. To this end, it uses proactive monitoring and anomaly detection, and encryption. One key feature of the Ransomware Prevention Algorithm is that it captures critical points in the system. Activities logs, file operations by users User files or (in particular for parts of the Positive Security Architecture) as an input from the network, encryption key pairs, and pre-trained behavioral models suit these tasks in turn. Another is these components lay the foundation needed to define "normal" for the system.

The process starts with capturing System Activity Logs (Figure 2). These logs are input to the Monitoring User & File Operations modules and Machine Learning Behavioral Analysis modules. These two parts identify together what is strange data or "behavior" until it makes any sense at all using their models (like Random Forest and Decision Trees). Then they intervene with necessary caution. When an anomaly is detected, such as rapid mass encryption of files at high speed, the Anomaly Detection module is switched on. This is furthermore

linked to the AES/RSA Encryption Application for secure data handling and the Raise Alert & Response module. If an attack is detected to be in progress, alerts are sent out and corresponding actions such as killing the process or interrupting an account user taken up. AES is also used to Encrypt Private Data, with keys protected by RSA. Finally, an incident report is issued for each case detailing the threat and the system's response. This enables us to keep continually improving our detection capabilities.

For behavioral analysis, anomaly detection based on machine learning spotted abnormal system activities, and heuristic techniques pegged suspicious actions such as rapid file encryption or changes in file extensions. For encryption tasks Cryptool was used and Kali Linux was adopted to simulate attacks, indicating a strategy incorporating layers of protection against ransomware threats while under laboratory conditions.

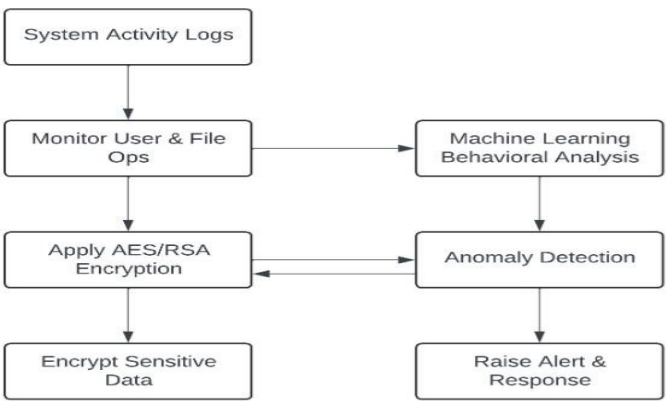

Figure 2
Ransomware Prevention Flow

Cryptool is a free software application that visualizes cryptographic algorithms and enables users to practice the use of the algorithms. The section below details the steps used to encrypt a file using the AES algorithm from Cryptool:

1. Create a Sensitive File: Prepare a file (e.g., sensitive_data.txt) containing confidential data like passwords or important documents you wish to protect.
2. Download and Open Cryptool: Install Cryptool, a tool used for encryption tasks.
3. Navigate to AES Encryption: In Cryptool, go to the Encrypt/Decrypt section and select the AES encryption option.
4. Select the File to Encrypt: Browse and upload your sensitive file (sensitive_data.txt) into the program.
5. Set the AES Key: Enter a strong and complex encryption key manually or let Cryptool generate one. This key is essential for future decryption.

6. Encrypt the File: With the file and key in place, click the Encrypt button. The program will create an encrypted version of the file (e.g., sensitive_data_encrypted.aes).
7. Store the Key Securely: Ensure the AES key is stored safely, as it is required to decrypt the file later.

3.2 *Management of Keys Using RSA:*

The Ransomware strategy usually includes an attack on the data encryption keys available for the victim to use. To avoid this situation, use of RSA (adopted encryption) can be used in managing and securing the encryption keys.

3.3 *How to protect the AES Key using RSA*

Step 1: Generate RSA Key Pair: In Cryptool, navigate to the Ensemble category and select the activity Encrypt yellow or Decrypt. Under the RSA section, choose the option to create an RSA key pair. This generates a public and private key—where the public key is used for encryption, and the private key is reserved for decryption.

Step 2: Encrypt AES Key with RSA: Use the RSA public key to encrypt the AES key, ensuring it is securely protected. This prevents unauthorized access, as only the corresponding private key can decrypt the AES key.

Step 3: Secure the Private Key: Keep the private key confidential and well-protected, such as storing it in a secure vault with biometric access. Since the AES-encrypted data can only be decrypted using this private key, ransomware cannot access or decrypt files without it.

3.4 *Using Cryptool to Decode Information*

After you have downloaded the ransomware, opened the encrypted files or retrieved your data – you can perform the following actions:

- Start program Cryptool and go to the section dealing with AES Decryption: Go to the section ‘Decrypt’ and select the option called AES Decryption.
- Now open the encrypted file: Open the sensitive data in AES encrypted file (sensitive_data_encrypted.aes) that you want to process.
- Provide the necessary field with the encryption key for AES: Provide the AES key that was utilized previously for the encryption of the file. In case the key is kept in the RSA format, you will need to decrypt the AES key possibly with the help of the RSA private key first before proceeding here.
- Decoding the File and Restoring It: The image file at the input will undergo all the processes required by Cryptool and the output will be the input sophisticated non-encrypted version demonstrating that the information you entrust can be attacked but is still possible to retrieve (sensitive_data.txt).

The flowchart in Figure 3 illustrates a comprehensive ransomware prevention and incident response framework designed to enhance system resilience. It begins with identifying critical assets, such as sensitive files and essential systems, followed by the implementation of advanced encryption methods (e.g., AES and RSA) to secure these assets [10]. Concurrently, user education on encryption practices is essential to reduce the risk of social engineering attacks [11].

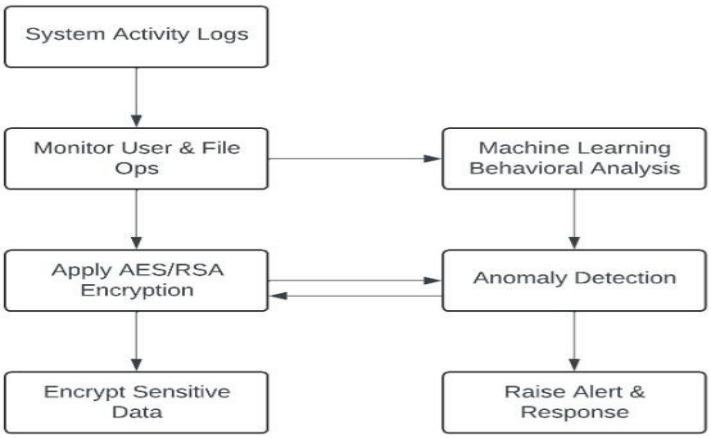

Figure 3

Prevention of ransomware attacks using advanced encryption and behavioral analysis

The next phase involves the establishment of a behavioural analysis system to understand normal user activities. By setting specific anomaly detection parameters, the system continuously monitors behaviour to detect suspicious deviations—such as unusual access times or mass file changes [12]. Upon detection of anomalies, the security team is alerted, initiating an investigation phase to determine the nature and extent of the threat. If ransomware is confirmed, an incident response is launched, including terminating malicious processes and restoring data from backups to ensure operational continuity. Post-incident, the organization updates its security measures and behavioural models based on new threat intelligence, closing the loop of continuous improvement [13]. This layered, proactive approach enables early detection, quick response, and effective recovery from ransomware attacks, thereby minimizing potential damage and enhancing long-term system protection.

A hybrid cryptographic scheme that involves recombining of AES, DES and chaotic logistic mapping is suggested in the study in [14] to transmit images securely. The chaotic map makes the initial conditions highly sensitive increasing the diffusion nature and the confusion aspect of encryption. The entropy, chi-square, and key space analysis performance evaluation are used to confirm enhanced resistance to both statistical and brute-force attacks. The relative comparison reveals that AES is the safest and chaos-based algorithms

provide lightweight randomness. The model has been shown to be applicable in cybersecurity and the field of digital forensics.

4. Results and Discussion

There is evidence to suggest that the battle with ransomware is so crucial as we move through a multi-directional defense era. For sectors like health care and finance, which are in charge of high-sensitivity data, the gap between encrypted protection and unauthorized attempts to access patient records is huge. Data that allows you to launch transactions on the spot is encrypted and behavior-checked at financial institutions. Fraudsters will thus be best equipped if they are unmasked by behavioral analysis, such as using the standard "three strikes and you're out" rule to catch them before they even have a chance. In addition, ongoing public awareness drives and staff training are important to build up resilience into an organization to enable its people to identify when someone is acting suspiciously or even in pursuit of some criminal purpose other than what their apparent appearance might suggest. At the same time, these strategies improve the overall cybersecurity footing significantly and in effect reduce both risk and impact of a ransomware attack on whole sectors deemed critical.

The authors [15] suggests a machine learning framework of identifying malware in encrypted network traffic without necessarily decrypting it. The model is able to examine the pattern of traffic and behavior characteristics to detect malicious activities, such as ransomware attacks. The findings indicate that the method is effective and scalable to real-time detection in secure communication settings. The paper emphasizes the use of AI-based detection methods in fighting emerging threats such as ransomware. It is especially applicable to the cloud and network security applications. As the ransomware is a malicious software type and an advanced malware, machine learning-based detection models in encrypted traffic settings are also critical in detecting and preventing ransomware assaults.

5. Conclusion

Innovations in encryption technology paired with new behavior detection systems provide a proactive, multi-layered approach to defense against ransomware attacks. When used in combination with user education and real-time anomaly detection, these measures significantly reduce vulnerabilities. Future developments in machine learning and AI will further enhance our ability to protect systems from emerging forms of ransomware threats.

6. Future Scope

The next generation of ransomware prevention systems based on the combination of the sophisticated encryption and behavioral analysis can be developed. Recent articles in the Journal of Discrete Mathematical Sciences and Cryptography acknowledge the usefulness of machine learning-based solutions to malware detection in encrypted network traffic based on behavioral patterns,

and not inspection of the payload [15]. The same techniques can be applied to detect cases of ransomware in real-time and respond to their actions.

Moreover, cryptography-based architecture, especially one based on decentralized networks like blockchain has shown a robust potential to secure data integrity and avoid unauthorized access [16]. They can also alleviate the effects of ransomware attacks significantly by having tamper-proof data storage and assuring transactions validation.

The multi-layered approach to a defense against the changing ransomware threats can be attained by implementing a combination of strong encryption methods with real-time behavioral detection in future systems. The integration may result in the creation of scalable, secure, and intelligent cybersecurity solutions that would be used in the contemporary distributed and cloud-based settings.

References

[1] J. Smith and R. Doe, "Advanced Encryption Strategies for Ransomware Defense," *Cybersecurity Review Journal*, vol. 14, no. 2, pp. 89–97 (2022).

[2] M. Johnson, "Secure Communication and Anomaly Detection in Cyber Defense," *Journal of Information Security Technologies,* vol. 19, no. 1, pp. 45–53 (2021).

[3] Y. Zhang, L. Wu, and A. Gupta, "Limitations of Cryptography in Malware Mitigation: A Case Study on Ransomware," *Proceedings of the International Conference on Cyber Threat Intelligence*, pp. 102–110 (2020).

[4] Kaspersky Lab, "Heuristic Detection and Behavioral Analysis in Ransomware Defense," *Kaspersky Research Report*, pp. 33–41 (2021).

[5] X. Xu, J. Lin, and C. Zhao, "Behavioral Threat Intelligence and Ransomware Detection," *International Journal of Cybersecurity Research*, vol. 17, no. 3, pp. 124–131 (2019).

[6] A. Kharraz, S. Arshad, C. Mulliner, W. Robertson, and E. Kirda, "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks," in *Proc. of the 12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment* (DIMVA) (2015).

[7] M. Conti, A. Gangwal, and S. Ruj, "On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective," *Computers & Security*, vol. 92 (2020).

[8] Symantec Corporation, *Internet Security Threat Report,* vol. 21 (2016).

[9] A. Godbole, R. Dhabliya, and V. Tiwari, "Ethical hacking and penetration testing: Strengthening cybersecurity posture through offensive security measures," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 4, pp. 1295–1305 (2024), doi: 10.47974/JDMSC-1983

[10] M. Bishop, Computer Security: Art and Science, 2nd ed., Addison-Wesley (2019).

[11] C. Tankard, "Advanced persistent threats and how to monitor and deter them," *Network Security,* vol. 2011, no. 8, pp. 16-19 (2011).

[12] S. Shone, P. J. D. Williams, D. N. S. Parekh, and Q. Liu, "A hybrid genetic algorithm for feature selection to improve data mining classification," *Information Sciences*, vol. 177, no. 18, pp. 3782–3792 (2007).

[13] NIST, "Guide for Cybersecurity Event Recovery," NIST Special Publication 800-184 (Dec. 2016).

[14] P. Bagane, S. Kothari, A. Goyal, K. Joshi, M. Garg, N. Namboodiri, and P. Karthik Krishna, "CyberCraft: Encryption and decryption tool for images using AES, DES, and chaotic logistic map," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 29, no. 2-B, pp. 797–806 (2026), DOI: 10.47974/JDMSC-2526

[15] A. Pratap Singh and M. Singh, "Real time malware detection in encrypted network traffic using machine learning with time based features," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 3, pp. 841-850 (2023), DOI: 10.47974/JDMSC-1760

[16] V. Ramachandran, H. M. A. Ghanimi, B. Marapelli, N. Kaur, M. Rajya Laxmi, R. Kumar Bommisetti, S. Sengan and Pankaj Dadheech, "An enterprise blockchain model: A reliable cryptography-based cyber-physical systems for securing user data, *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-B, pp. 2103–2114, (2025), DOI: 10.47974/JDMSC-2368

Received April, 2025