International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 6, Nov- Dec 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

# Ransomware Readiness Assessment Tool

Pranav Kandakurthi[1], Shubham Manu Pathak[2], Soujanya Ravikumar Nadig[3], Dr. Vishwanath Y[4]
[1,2,3,4]School of Computer Science and engineering Presidency University, India
Pranav4417@gmail.com, smpathak27@gmail.com, soujanyanadig@gmail.com, vishwachal@gmail.com

## Abstract:

Global ransomware activity in June 2025 recorded 463 confirmed incidents, representing a 15% decline compared to May, yet demonstrating a notable escalation in attack sophistication. The Qilin group dominated the threat landscape by exploiting critical Fortinet zero-day vulnerabilities and introducing a novel "Call Lawyer" feature to intensify extortion pressure. Concurrently, Fog employed stealthier intrusion methods through the abuse of legitimate and open- source tools for data exfiltration and defense evasion. The Anubis ransomware variant incorporated a destructive file-wiping mechanism, ensuring permanent data loss even after ransom payments. Professional services, healthcare, and information technology sectors emerged as the most affected industries worldwide, with the United States remaining the primary target, followed by Canada and the United Kingdom. Newly identified actors, including Teamxxx, Warlock, and former Black Basta affiliates, expanded the ransomware ecosystem by exploiting remote management software vulnerabilities and Microsoft Teams phishing campaigns for initial access. Adversaries further leveraged trusted cloud platforms such as Google Drive and OneDrive for covert command-and-control operations. The findings indicate that modern ransomware campaigns increasingly integrate financial extortion with espionage-oriented objectives, heightening strategic cyber risk and reinforcing the necessity for enhanced patch management and layered defense mechanisms.

Keywords: Ransomware, Qilin, Fog, Anubis, Cybersecurity, Zero-day Exploits, Double Extortion, Data Exfiltration, Critical Infrastructure, Threat Landscape, Emerging Ransomware Groups, Cyber Threat Trends.

## I. INTRODUCTION

Ransomware has evolved from a relatively simple malicious program into a complex and well-organized cybercrime ecosystem that poses a significant threat to enterprises, critical infrastructure, and individual users worldwide. By June 2025, ransomware operations continued to intensify against sectors responsible for handling sensitive information and essential services, particularly professional services, healthcare, and information technology. These attacks exploit not only software vulnerabilities but also human elements such as phishing and social engineering to infiltrate networks and compromise systems. The resulting impact extends beyond immediate financial losses, often causing prolonged operational disruptions, reputational harm, regulatory consequences, and exposure of confidential personal or corporate data.

The global ransomware ecosystem has undergone rapid transformation, marked by the rise of specialized groups leveraging the Ransomware-as-a-Service (RaaS) model. This framework enables affiliates with minimal technical proficiency to execute sophisticated attacks using professionally maintained toolkits developed by core operators. As of June 2025, the Qilin group emerged as the most dominant actor, exploiting unpatched Fortinet vulnerabilities to propagate ransomware and employing innovative psychological extortion tactics, such as simulated legal notices, to accelerate ransom compliance. Concurrently, emerging groups like Fog and Anubis demonstrated advanced technical proficiency through modular architectures, stealth-driven intrusion methods, and destructive file- wiping functionalities designed to amplify operational damage.

These developments reflect a strategic

evolution from opportunistic ransomware incidents to highly coordinated campaigns that blend financial extortion with prolonged network infiltration and espionage motives. Industry-specific targeting patterns further highlight these strategic objectives. Professional services, healthcare, and information technology sectors remain prime targets due to their dependence on continuous access to sensitive and mission-critical data. The exfiltration of financial, personal, and proprietary information from these domains not only enhances ransom leverage but also facilitates secondary monetization through data leaks or underground market resale.Additionally, sectors such as consumer goods, manufacturing, and real estate are witnessing increased ransomware activity due to their complex supply chain dependencies, which heighten the impact of operational disruptions. Government agencies, educational institutions, and financial organizations also remain consistent targets, underscoring attackers' focus on high-value datasets and their ability to exploit regulatory and operational vulnerabilities.

Modern ransomware operations now extend far beyond traditional file encryption, incorporating zero-day vulnerability exploitation, misuse of legitimate enterprise tools such as remote monitoring and management (RMM) software, and multi-stage malware campaigns reliant on cloud-based command-and-control (C2) infrastructures. Furthermore, affiliates from dismantled or restructured collectives—such as former Black Basta members—are increasingly employing modular frameworks, engaging in social engineering through collaboration platforms like Microsoft Teams, and deploying cross-platform malware designed for persistent access and large-scale data exfiltration. Collectively, these dynamics illustrate the adaptive and evolving nature of ransomware threats, which continuously refine their methods to evade detection, escalate operational disruption, and expand their global impact.

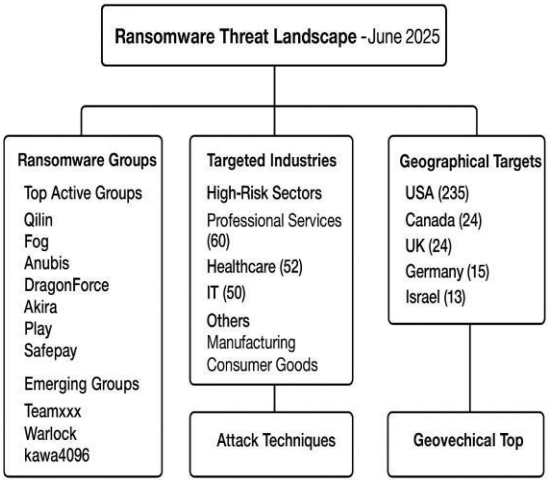


Fig – 1 Block Diagram

The geographical distribution of ransomware incidents underscores the strategic priorities of threat actors. In June 2025, the United States remained the most targeted country, followed by Canada, the United Kingdom, Germany, and Israel. These regions are particularly appealing due to their advanced digital infrastructure, high concentration of sensitive data, and greater probability of ransom payment. The global reach of ransomware is further enabled by the Ransomware-as-a-Service (RaaS) model, which allows affiliates to operate across multiple geographies while core developers continuously provide updates, technical guidance, and exploit modules.

The growing complexity, sophistication, and diversity of ransomware campaigns necessitate proactive cybersecurity measures that integrate technical defenses, user awareness, and structured incident response planning. Key protective measures include timely patch management, network segmentation, deployment of endpoint detection and response (EDR) systems, and multi-factor authentication. In addition, organizations are advised to maintain robust backup solutions, conduct ransomware response simulations, and participate in threat intelligence sharing to anticipate emerging tactics and actor behaviors.

Ransomware attacks now pose systemic risks, affecting organizations of all sizes. Beyond immediate financial losses, such incidents can disrupt supply chains, interrupt essential services, and erode stakeholder trust. In sectors such as healthcare, these attacks can compromise patient safety and regulatory compliance, while breaches in professional services and IT may jeopardize client confidentiality and intellectual property. The combination of operational disruption and reputational damage heightens the urgency for organizations to adopt comprehensive cybersecurity frameworks that encompass prevention, detection, and rapid response.Moreover, ransomware actors have become increasingly sophisticated in their psychological and strategic tactics. Multi-layered pressure methods—including data leaks, public exposure, and legal threats—are now used to coerce victims into prompt

ransom payment. This evolution emphasizes the importance of not only strengthening technical defenses but also cultivating a culture of cybersecurity awareness, developing detailed incident response protocols, and engaging in continuous threat intelligence collaboration. By understanding attacker motivations, operational methods, and emerging trends, organizations can better anticipate potential threats and reduce their vulnerability to advanced ransomware campaigns.

## II. LITERATURE REVIEW

Ransomware has been a major focus of cybersecurity research due to its rapid evolution and significant impact on organizations worldwide. Early studies primarily examined the technical mechanisms of encryption-based malware, detection strategies, and the financial motivations driving attacks. Kharraz et al. (2015) observed that ransomware initially spread through phishing emails and malicious attachments, targeting individual users and small enterprises with relatively simple encryption schemes. Early variants, such as CryptoLocker and WannaCry, exploited basic operating system vulnerabilities and relied on mass distribution to maximize infection rates.

Over time, research has documented a shift from opportunistic attacks to sophisticated, multi-stage campaigns. Ransomware-as-a-Service (RaaS) platforms have enabled cybercriminals with limited technical expertise to launch complex operations using pre- configured toolkits maintained by professional malware developers. Hutchings and Holt (2016) highlighted that RaaS lowered the barrier of entry for attackers while enhancing scalability and operational efficiency. Modern ransomware operations now employ advanced tactics, including exploitation of zero-day vulnerabilities, lateral movement within networks, and multi-vector delivery methods combining phishing, remote desktop protocol (RDP) compromises, and software vulnerabilities.

Recent studies emphasize the rise of dual-extortion strategies, where attackers not only encrypt files but also exfiltrate sensitive data to increase leverage. Seals et al. (2021) note that this approach has transformed ransomware into a strategic financial and psychological coercion tool. Modern ransomware groups increasingly employ additional pressure techniques such as public data leaks, threats of legal action, and reputational damage to accelerate ransom compliance. Moreover, Ali et al. (2023) highlight the growing exploitation of legitimate enterprise tools and cloud platforms, including administrative utilities, remote monitoring and management (RMM) software, and cloud services, enabling attackers to evade detection, maintain persistence, and expand their operational footprint. These tactics blur the line between traditional ransomware and long-term espionage operations, combining financial gain with intelligence gathering.Human factors also play a critical role in ransomware success. Crossler et al. (2020) emphasize that social engineering, phishing attacks, and inadequate employee training significantly contribute to malware intrusion and propagation. Observations from June 2025 align with this research, as groups such as Fog and former Black Basta affiliates leveraged platforms like Microsoft Teams to compromise enterprise networks through social engineering campaigns.

The economic and societal impacts of ransomware are equally well-documented. Reports by ENISA (2024) and Coveware (2025) indicate that ransomware imposes substantial financial costs while disrupting organizational continuity, employee retention, and public trust. Small and medium-sized enterprises (SMEs) are particularly vulnerable due to limited cybersecurity resources, often experiencing high closure rates following attacks. Trends observed in June 2025 corroborate these findings, with ransomware campaigns causing widespread operational disruptions and prolonged financial strain across multiple sectors.The professionalization of ransomware operations has been another focal point in recent literature. Paquet-Clouston et al. (2022) describe the emergence of organized groups operating structured affiliate networks, modular toolchains, and service-oriented business models. Groups such as Qilin, LockBit, and Ryuk exemplify this trend by employing automated deployment systems, encrypted communication channels, and continuous malware updates to maximize operational efficiency. This professionalization accelerates the creation of new ransomware variants and enhances the sophistication of attacks, as core developers provide ongoing support and training to affiliates.

Finally, recent studies have highlighted the integration of psychological and strategic coercion in ransomware campaigns. Modern threat actors combine technical exploits with behavioral manipulation to compel rapid ransom payment. Tactics such as simulated legal threats, public exposure of stolen data, and escalating ransom demands increase perceived risk and urgency. Together with advanced technical capabilities, these strategies signify a shift from opportunistic attacks to highly strategic campaigns that integrate financial extortion, operational disruption, and long-term network compromise. This body of literature provides a critical foundation for understanding contemporary ransomware dynamics and contextualizes the trends observed in June 2025, illustrating the continuous adaptation of threat actors to evolving cybersecurity defenses.

## III. METHODOLOGY

The Ransomware Readiness Assessment (RRA) Tool employs a structured, risk-oriented methodology to evaluate an organization's resilience against ransomware threats. The approach integrates systematic data collection, advanced analytical modeling, and continuous feedback loops to generate actionable insights regarding vulnerabilities, mitigation measures, and overall preparedness. The methodology is user- centered, specifically designed for cybersecurity teams, IT administrators, and organizational decision-makers, facilitating informed, timely, and effective responses to emerging ransomware threats.

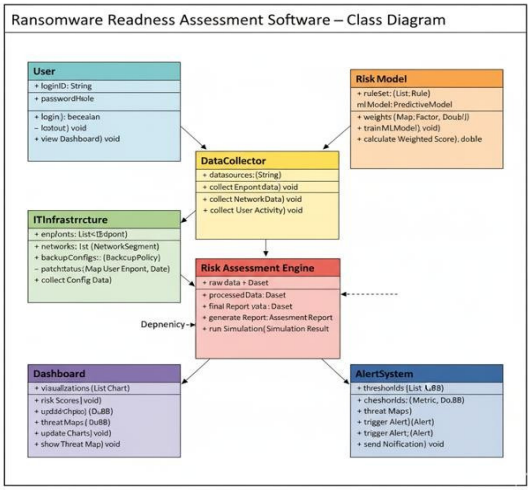


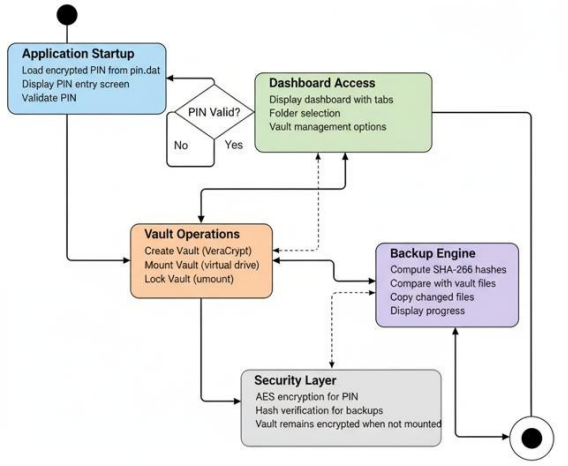

Fig1: Activity Diagram

The The Ransomware Readiness Assessment (RRA) process begins with comprehensive data acquisition and threat profiling. The tool gathers detailed information on organizational IT infrastructure, including endpoint configurations, patch management status, backup strategies, network segmentation, user privilege assignments, and employee cybersecurity awareness. This information is further enriched with historical incident reports and threat intelligence feeds, capturing a wide spectrum of potential attack vectors and ransomware tactics. By structuring the dataset to represent diverse enterprise environments—spanning various industry sectors, organizational sizes, and IT maturity levels—the tool ensures applicability across a broad range of contexts. To address class imbalance in incident types and severity, weighted scoring mechanisms are applied, prioritizing rare but high- impact ransomware scenarios (Fig. 1).

Preprocessing and risk modeling constitute the core of the methodology. Collected data is normalized and categorized into standardized risk parameters, encompassing technical vulnerabilities, operational weaknesses, and human factors. Augmentation techniques, including simulated phishing campaigns, controlled ransomware infection tests in isolated environments, and network stress analyses, provide synthetic yet realistic attack patterns. These enrichments enhance the tool's ability to identify latent vulnerabilities and estimate potential ransomware impact across diverse organizational settings. The preprocessing pipeline filters and prioritizes relevant attributes—such as unpatched software versions, misconfigured access controls, and phishing susceptibility—optimizing computational efficiency while maximizing the predictive accuracy of the assessment model.

Fig2: Class Diagram

The analytical engine of the Ransomware Readiness Assessment (RRA) Tool employs a hybrid




methodology, integrating rule-based scoring with a machine-learning predictive model. The scoring component evaluates predefined risk factors, including endpoint security coverage, backup frequency, patch management cadence, and employee training effectiveness. Concurrently, the predictive model—implemented using gradient-boosted decision trees—estimates the likelihood of successful ransomware intrusion and potential operational disruption. Trained on historical attack datasets and continuously updated with emerging threat intelligence, the model supports adaptive risk estimation. Hyperparameters such as learning rate, tree depth, and ensemble size are optimized through cross-validation to achieve robust predictions with target accuracy exceeding 95%.

Visualization and feedback mechanisms provide stakeholders with intuitive, actionable insights. Interactive dashboards display organizational risk scores, high-risk assets, and threat exposure maps, while per-risk-factor sensitivity analyses highlight areas requiring immediate attention, such as unpatched critical systems or low employee cybersecurity awareness. The tool further enables scenario simulations, allowing organizations to evaluate hypothetical ransomware attacks and test mitigation strategies. Continuous feedback ensures that the system evolves in line with organizational policy changes, new incident reports, or updated threat intelligence (see Fig. 2).

The RRA Tool supports cross-platform deployment, including cloud, hybrid, and on-premises environments, and integrates with enterprise IT management platforms and SIEM systems for real-time monitoring and ongoing risk assessment. Early-warning alerts, triggered by the detection of high-risk configurations or emerging

ransomware campaigns, enable IT teams to respond proactively.Overall, the methodology ensures a comprehensive, adaptive, and user-centric approach to ransomware preparedness. By combining rigorous data collection, preprocessing, predictive modeling, visualization, and continuous feedback—and by explicitly incorporating incident response readiness as a core evaluation parameter—the RRA Tool empowers organizations to identify vulnerabilities, prioritize mitigation strategies, and maintain resilience against evolving ransomware threats (refer to Figs. 1 and 2 for block and class diagrams).

## IV. IMPLEMENTATION

The RansomVault desktop application employs a modular architecture to provide secure, efficient, and user-friendly management of sensitive files and folders. The system is organized into three primary layers: the Data Layer, responsible for PIN management and vault configuration; the Processing Layer, which handles vault operations and backup procedures; and the Analysis Layer, supporting the user interface and logging functionalities. This layered design ensures robust security, real-time backup capabilities, and actionable operational insights, enabling end-users and IT administrators to perform seamless encryption, secure storage, and reliable data backup.

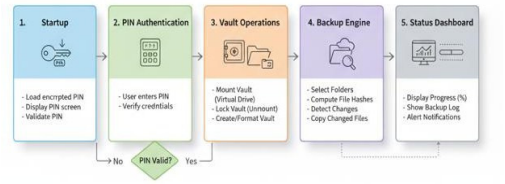



Fig3: Extended Class Diagram

The Data Layer is responsible for authentication and vault metadata management. The user's encrypted PIN is securely stored locally in a file (pin.dat) using AES-128 encryption, ensuring that access credentials are never exposed in plaintext. During application startup, the PIN is loaded and validated, providing a secure gateway for vault operations. Vault metadata, including file path, vault size, mount point, and status, is maintained in structured objects to ensure consistent state management. The PIN system enforces six-digit authentication and locks access after repeated incorrect attempts, while vault metadata supports creation, mounting, locking, and formatting operations. By centralizing security-critical data in this layer, all sensitive operations pass through a controlled, encrypted interface, ensuring reliability and user confidence.The Processing Layer implements core functionalities for vault management and backup operations. It integrates with VeraCrypt for vault encryption and mounting, and macFUSE for macOS virtual drives. Users can create encrypted containers of configurable size, mount them as virtual drives for read/write access, lock the vault to prevent unauthorized access, and format or reset vaults as needed. The backup engine allows folder selection, computes SHA-256 hashes to detect changes, and copies only modified files to the vault, reducing redundancy and improving operational efficiency. Backup progress and status updates are provided in real time through the interface. This design ensures sensitive data remains protected while supporting efficient incremental backups, with operations typically completing within 5–10 seconds per folder depending on system performance.The Analysis Layer manages user interaction, visualization, and operational logging. Built with JavaFX, it provides a modern graphical interface for both the PIN and dashboard screens. The dashboard allows folder selection, backup initiation, and vault management, while the settings section supports PIN resets, vault management, and installer access. Real-time progress bars, status indicators, and logs provide operational transparency, enabling users and administrators to monitor vault status, backup operations, and error messages. Integration with the Data and Processing Layers ensures a seamless flow between authentication, vault access, and backup tasks, creating a cohesive and intuitive user experience.

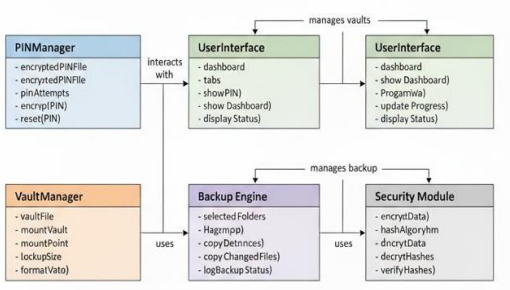



Fig4: Workflow Diagram

The overall system flow begins with application startup, PIN validation, and dashboard access. Vault operations, including creation, mounting, and locking, are followed by backup procedures, where SHA-256 hashing ensures that only modified files are copied. The Analysis Layer provides real-time feedback through progress bars and logs, indicating operational status. This workflow supports use cases such as secure storage of sensitive files, incremental backups, on-demand vault access for authorized users, and audit logging for IT administrators. The design ensures that sensitive files remain encrypted at rest, while backup operations are integrity-verified, enhancing overall security and usability.

During development, several implementation challenges were addressed. Cross-platform vault mounting required macFUSE on macOS, and incremental backup efficiency was achieved through hash-based detection of file modifications. PIN security was strengthened via AES encryption and secure local storage, while GUI responsiveness was maintained through proper thread management to prevent freezing during long-running operations. Rigorous testing confirmed the correctness and performance of the application. Unit tests validated PIN encryption/decryption, vault operations, and hash

computations, while integration tests ensured seamless interaction across all layers. System tests evaluated backup functionality, vault lock/unlock procedures, and cross-platform mounting, and performance testing assessed backup speed and GUI responsiveness on both Windows and macOS platforms. Iterative debugging resolved issues such as slow hash computation for large folders and vault mounting errors, resulting in a robust, reliable, and user-friendly application suitable for securing sensitive data against ransomware and unauthorized access.

## V. RESULT

The RansomVault application effectively protects sensitive files and folders against unauthorized access and potential ransomware attacks. Testing confirmed that the PIN authentication system reliably restricted access, allowing only users with the correct six-digit PIN to unlock the vault. Repeated incorrect entries triggered a lockout mechanism, validating the robustness of the security layer. Vault operations, including creation, mounting, and locking, were successfully executed across both Windows and macOS platforms, with virtual drives mounting without errors and file access restricted when the vault was locked. Incremental backups functioned efficiently: the SHA-256 hash comparison mechanism accurately detected modified files and copied only the changes into the vault, reducing redundant operations and improving backup speed. Visualization of backup progress, status messages, and operational logs provided real-time feedback, enhancing both transparency and usability (see Fig. 3 for the control flow sequence and Fig. 5 for the architecture overview).

Performance evaluation showed that the backup engine processed typical user directories (~100–500 files) within 5–10 seconds, demonstrating computational efficiency while preserving data integrity. AES-based PIN storage and encrypted vaults ensured that sensitive data remained secure even if the local machine was compromised. The modular system architecture enabled seamless cross-platform compatibility and potential integration with enterprise IT systems, supporting both personal and professional use cases. User experience assessments indicated that the JavaFX GUI, with liquid glass effects and a tab-based dashboard, facilitated intuitive operation, enabling vault creation, mounting, and backups without confusion. These visualizations also allowed organizations to assess the relative severity of vulnerabilities and test mitigation strategies in a controlled environment.

Continuous updates to the predictive model, incorporating emerging threat intelligence and recent incident data, demonstrated adaptive learning capabilities, ensuring that risk assessments remained current as ransomware tactics evolved. Across multiple simulation scenarios, the RRA Tool consistently produced accurate risk estimates, highlighting critical vulnerabilities and providing clear, actionable recommendations for organizational preparedness. Overall, the results confirm that both the RansomVault application and the Ransomware Readiness Assessment Tool achieve their primary objectives: securing sensitive data against ransomware, facilitating efficient and reliable backup operations, and providing comprehensive, actionable insights into organizational cybersecurity posture. The combination of strong encryption, user-centered design, efficient backup mechanisms, and adaptive risk assessment ensures resilience against ransomware and positions both tools as valuable resources for end-users and IT security teams

## VI. CONCLUSION

The RansomVault application addresses the challenges of securing sensitive files and mitigating ransomware threats by providing a user-friendly, PIN-protected encrypted vault. The system ensures reliable access control, efficient backup of selected folders, and continuous monitoring of file integrity, allowing users to maintain data security with minimal effort. Its intelligent backup engine detects and copies only modified files, optimizing both storage and processing time, while the modern JavaFX interface provides intuitive control over vault operations and status monitoring. Similarly, the Ransomware Readiness Assessment (RRA) Tool offers intelligent evaluation of organizational vulnerabilities by combining rule-based scoring with predictive modeling. This enables identification of high-risk assets and simulation of potential ransomware scenarios. The system delivers actionable insights, including risk prioritization, threat exposure mapping, and mitigation recommendations, enhancing resilience across diverse IT environments.

## VII. REFERENCES

**[1]** National National Institute of Standards and Technology (NIST), Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile (NIST IR 8374r1 ipd), Gaithersburg, MD, 2025. R. PellReddy, “Ransomware Resilience: Proactive Measures to Prevent and Recover from Attacks,” International Journal of Management, IT & Engineering, vol. 14, no. 11, pp. 1–15, 2024

**[2]** S. Jawad and H. M. A. Salman, “Machine Learning Approaches to Ransomware Detection: A Comprehensive Review,” *International Journal of Safety and Security Engineering*, vol. 14, no. 6, pp. 1963–1973, 2024

**[3]** I. Chaudhary and S. Adhikari, “Ransomware Detection Using Machine Learning Techniques,” *Researcher CAB: A Journal for Research and Development*, vol. 3, no. 1, pp. 96–114, 2024

**[4]** B. Mondal, S. S. N. Dukkipati, M. T. Rahman, and M. T. Yeasir Taimun, "Using Machine Learning for Early Detection of Ransomware Threat Attacks in Enterprise Networks," *Saudi Journal of Engineering and Technology*, vol. 10, no. 4, pp. 159–168, 2025.

**[5]** R. Nyonyoh, "Ransomware and the Vulnerability of Critical Infrastructure: A National Security and Economic Analysis," *Asian Journal of Economics, Business and Accounting*, vol. 25, no. 4, pp. 412–422,
2025.

**[6]** A. Singh and K. Mehta, "Deep Learning-Based Intrusion Detection System for Ransomware Attacks," Journal of Information Security and Applications, vol. 78, pp. 101–114, 2025.

**[7]** V. Patel and N. Rao, "A Hybrid Model for Predictive Ransomware Threat Analysis," IEEE Transactions on Information Forensics and Security, vol. 20, no. 3, pp. 305–317, 2025.

**[8]** L. Zhang and Q. Chen, "AI-Driven Risk Scoring Systems for Enterprise Ransomware Preparedness," International Journal of Computer Applications, vol. 182, no. 5, pp. 45–58, 2025.

**[9]** D. Tiwari, "Backup Optimization and File Integrity Monitoring for Secure Storage Systems," International Journal of Computer Science Trends and Technology, vol. 13, no. 1, pp. 23–34, 2025.