Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 9, 2025

EMPOWERMENT OF ARTIFICIAL INTELLIGENCE (AI) IN PREVENTING AND DETECTING RANSOMWARE: AN ANALYTICAL REVIEW

Amir Mohammad Delshadi[1], Obaid Ullah[2], Younus Khan[3], Muhammad Waleed Iqbal[4], Hafiz Abdul Basit Muhammad[5], Khalid Hamid[*6], Fakhar Abbas[7], Muhammad Ibrar[8]

[1,3]Department of Computer and Mathematical Sciences, New Mexico Highlands University, Las Vegas, NM;
[2] Department of Computer Science, University of Alabama at Birmingham, Birmingham AL 35205, USA;
[4] Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus; Sahiwal
[5] Department of Computer Science and Information Technology, Superior University Lahore, Lahore, 54000, Pakistan;
*[*6]Department of Computer Science and Information Technology, Superior University Lahore, Lahore, 54000, Pakistan;*
[7] Department of Chemistry, Government College University, Lahore 54000, Pakistan;
[8] Department of Computer and Mathematical Sciences New Mexico Highlands University, Las Vegas, NM

[1]adelshadi@live.nmhu.edu, [2]obaidu9012@gmail.com, [3]Ynyuskhan464@gmail.com,
[4]mmuhammadwaleed256@gmail.com,[5]basitbsse786@gmail.com,[*6]khalid6140@gmail.com
[7]afakhar047@gmail.com, [8]Mibrar@live.nmhu.edu

DOI: https://doi.org/10.5281/zenodo.17046488

Keywords

Article History
Received: 11 June 2025
Accepted: 21 August 2025
Published: 03 September 2025

Corresponding Author: *
Khalid Hamid

Abstract

Ransomware is an emerging cyber threat that requires innovative and flexible solutions. Using recent advances in machine learning, deep learning, and explainable AI, this study explores the potential of artificial intelligence (AI) to identify and stop ransomware. AI significantly improves detection and response speed in networks, the Internet of Things (IoT), and mobile devices, according to previous and ongoing studies. Explainability and transparency are becoming increasingly important, particularly in light of the growing challenges posed by generative AI. One of the primary research gaps, notwithstanding these developments, is the development of standardized, interpretable, real-time AI models that can adjust to various ransomware variations. By evaluating current approaches and suggesting paths toward a more scalable and efficient AI-based defense system, this study closes that gap.

INTRODUCTION

Through anomaly detection and intelligent packet analysis, the study shows how artificial intelligence (AI) may improve network security with the ultimate goal of preventing ransomware. A technical presentation on systematic ransomware detection techniques was presented by Lee et al. (2022) at the 24th International Conference on Advanced Communication Technology (ICACT) [1]. Lysenko et al. (2024) emphasized the importance of AI in threat detection and defense automation [2]. They proposed a multi-layered detection model that combines AI techniques with conventional methods, focusing on machine learning and static and dynamic analysis for end-to-end security. Their research classified existing AI methods, reviewed datasets, and highlighted the role of deep neural networks, ensemble learning, and hybrid models. In ACM Computing

Surveys, Gaber, Ahmed, and Janicke (2024) provided an exhaustive literature review of AI for malware detection [3]. Their study gives a comprehensive evaluation of deep learning and machine learning approaches for ransomware and other malicious software detection. In addition, it describes why explainable AI (XAI) is needed to ensure accountability and transparency in security choices. Explainability is currently a key component of AI-driven cybersecurity systems. Galli et al. researched explainability in AI-based behavioral malware detection. (2024) [4]. They pointed out in their Computers & Security article that while AI is very good at identifying malware, cybersecurity experts might not trust or embrace it because it lacks interpretability. They advocate systems that provide insights into the reasoning behind the decisions as well as identify threats. Development of effective defenses necessitates knowledge of ransomware trends. Jimmy (2024) analyzed recent ransomware attack tactics and defense mechanisms in his research published in the Journal of Knowledge Learning and Science Technology. His research reiterates the necessity of intelligent systems, including artificial intelligence (AI), to forecast attack directions and launch automated countermeasures. Komarudin et al. (2023) explored the potential of AI to detect malware and enhance cybersecurity in networking environments as part of their continued research into applications of AI [5]. The study by Lee et al. (2022) and Lysenko et al. (2024) explore the use of artificial intelligence (AI) in network security, specifically in detecting anomalies and analyzing intelligent packets, to prevent ransomware [6][7]. The research highlights the potential of AI in enhancing protection and risk detection. Marais, Quertier, and Chesneau (2022) contributed to the discussion by focusing on result interpretability in AI-based malware analysis both from a technical and interpretability viewpoint [8]. To assist human decision-making in malware investigation, their paper, published in the Distributed Computing and Artificial Intelligence proceedings, advocated for the use of explainable models in AI systems. Ransomware discovery in Internet of Things (IoT) networks is an issue of high priority because the emergence of new vulnerabilities that result from the increased number of IoT devices has introduced new threats [9].

Naeem, Alshammari, and Ullah authored an explainable AI-based approach to identifying IoT malware that utilizes transfer learning and image visualization in their 2022 Computational Intelligence and Neuroscience paper. In identifying malicious activity within low-resource IoT systems, their model exhibited promising accuracy [10]. In IEEE Transactions on Cybernetics, Qiu et al. (2023) proposed a new Android malware detection technique in mobile security by employing Cyber Code Intelligence [11]. Their AI-based system offers a robust shield against mobile ransomware by examining code semantics with deep learning. Rubab and Marou (2023) also made their contribution to this research area with their work on AI-based malware detection and mitigation, published in Symmetry [12]. Their findings clarify how artificial intelligence improves detection rates and makes threat classification and forensic analysis simpler. In ICT Express, Song et al. (2024) investigated the connections between a number of AI-based detection techniques [13]. They develop a comparative framework that evaluates the efficacy of several artificial intelligence techniques for malware detection, demonstrating the superior accuracy and responsiveness of hybrid models. Teichmann (2023) examined ransomware assaults from the standpoint of generative artificial intelligence in the International Cybersecurity Law Review. We learned from his experimental research how generative AI may be used to produce sophisticated ransomware and, on the other hand, how AI can be used to imitate and anticipate such attacks [14].

Literature Review

In spite of such developments, the study pointed out the problem of keeping AI models in integrity in spite of attacks by attackers. Their results indicate that AI-based ransomware detection tools considerably enhance cloud and IoT network cybersecurity strength [15].

Ferdous et al. (2024) presented an entire snapshot of AI-based ransomware detection methods,

consolidating the past studies on machine learning and deep learning in cybersecurity [16]. Their study classified AI-based methods into signature-based detection, anomaly detection, and hybrid methods involving various techniques to attain greater precision. Comparative study of different deep learning models applied to ransomware activity detection, i.e., convolutional neural networks (CNNs) and long short-term memory (LSTM) networks, was an essential component of their investigation. Their investigation also touched upon new security threats in AI, i.e., adversarial machine learning, in which the adversaries try to manipulate AI models. They argued that AI is still an essential weapon to fight ransomware, but continuous progress in model robustness and explainability is required to ensure its sustainability [17].

Chaithanya and Brah are in corporate infrastructures. For preventing and responding to ransomware attacks, their paper highlighted using AI-based security frameworks at different levels of a company's IT stack. Through the detection of irregular file encryption patterns and malicious network activities, the research explored how machine learning (ML) models enhance early ransomware detection. Among the findings was that AI-driven anomaly detection systems minimize response times by a significant margin, thus making it possible to swift containment of ransomware attacks.

A systematic review of literature on malware detection using AI by Gaber, Ahmed, and Janicke (2024) contrasted cybersecurity supervised and unsupervised learning approaches. Their work proved the efficiency of CNNs and RNNs in detecting ransomware through behavioral and network traffic analysis [18].

Apart from these advantages, the research observed that AI-powered defenses must be updated on a regular basis to adapt to evolving ransomware strategies. The researchers concluded that, when coupled with human knowledge and adaptive threat intelligence, the integration of AI into organizational security designs enhances ransomware resistance [19].

Teichmann (2023) carried out an experimental study on the effects of generative AI in ransomware attacks and how sophisticated AI models affect offensive as well as defensive cybersecurity operations. Cyber attackers can exploit generative AI to automate ransomware payload development, bypass detection controls, and develop very persuasive phishing messages to deliver malicious payloads, said the study. Of prime concern raised was the possibility that AI could reduce the barrier to entry for attackers, facilitating less sophisticated attackers to develop complex ransomware attacks. Conversely, the research examined how AI can be applied to prevent and mitigate ransomware. This involved utilizing deep learning to scan malware and employing AI-driven deception techniques such as honeypots to contain the spread of ransomware. Another main discovery was that adversarial AI methods might be employed for creating fake ransomware samples, so security researchers can train on new threats ahead of time. Teichmann concluded that generative AI brings new challenges to ransomware defense but also new solutions for improving detection, response, and forensic analysis [20][21].

Comparative Analysis of the Studies for Gap

Table 1: Comparative Analysis of the Studies from the Year 2022 to 2024

No.	Reference	Key Focus	AI-Based Techniques Used	Uses/Applications	Key Findings
1	Rubab & Marou (2023)	Malware detection, analysis, and mitigation	Machine learning, deep learning	Cybersecurity threat detection	AI can effectively detect and mitigate evolving malware threats.
2	Komarudin et al. (2023)	AI effectiveness in malware detection	AI-based cybersecurity, anomaly detection	Network security, cyber threat defense	AI-based techniques significantly improve cybersecurity resilience.
3	Gaber et al. (2024)	Systematic review on AI-driven malware detection	Neural networks, AI classifiers	Enhancing malware detection accuracy	AI classifiers outperform traditional methods in malware detection.
4	Lysenko et al. (2024)	AI's role in cybersecurity automation	AI-powered threat detection, automation	Threat mitigation, AI security policies	Automation using AI reduces response time against cyber threats.
5	Jimmy (2024)	Ransomware attack trends and prevention strategies	Behavioral analysis, AI-driven security	Early threat detection, prevention	AI-driven analysis improves predictive capabilities for ransomware attacks.
6	Bertia et al. (2022)	Ransomware detection via ML algorithms	Decision trees, random forests, deep learning	Detecting encrypted ransomware	ML algorithms enhance detection speed and accuracy.
7	Naeem et al. (2022)	AI-based IoT malware detection	CNN, transfer learning	IoT security, malware visualization	Image-based AI models improve detection of IoT malware threats.

8.	Marais et al. (2022)	AI-driven malware analysis with interpretability	Explainable AI (XAI), ML models	Enhancing AI transparency in cybersecurity	Explainable AI helps make cybersecurity decisions more interpretable.
9.	Lee et al. (2022)	ransomware detection techniques	Feature extraction, anomaly detection	Endpoint detection, real-time response	AI-based anomaly detection reduces false positives in ransomware identification.
10.	Galli et al. (2024)	Explainability in AI-based malware detection	XAI, behavioral analysis	AI decision-making in cybersecurity	AI-based behavioral analysis improves accuracy in malware detection.
11.	Song et al. (2024)	AI mechanisms for malware detection	Neural networks, hybrid AI models	Automated malware classification	Hybrid AI models provide better scalability for threat analysis.
12.	Qiu et al. (2023)	Android malware detection using cyber code intelligence	Deep neural networks, static analysis	Mobile security, threat detection	Cyber code intelligence enhances Android malware detection efficiency.
13.	Lee et al. (2022)	Advanced endpoint ransomware detection	Open-source EDR, rapid response AI	OS security, real-time threat analysis	AI-driven EDR solutions improve real-time mitigation of ransomware attacks.
14.	Ferdous et al. (2024)	AI-based ransomware detection review	AI-driven models, comparative analysis	Assessing AI effectiveness in security	Comprehensive review suggests AI increases detection rates significantly.
15.	Chaithanya & Brahmananda (2022)	AI-enhanced ransomware defense in organizations	Deep learning, real-time detection	Enterprise cybersecurity	AI-based defenses strengthen organizational resilience to ransomware.
16.	Teichmann (2023)	Ransomware in generative AI environments	AI-driven attack simulations	Understanding AI vulnerabilities	Generative AI increases ransomware complexity, demanding advanced detection strategies.
17.	Bertia et al. (2022)	Ransomware detection with multiple algorithms	ML classifiers, pattern recognition	Improving accuracy of detection engines	Combining multiple AI algorithms enhances ransomware detection precision.

Methodology

This research explores the application of Artificial Intelligence (AI) in ransomware detection and prevention using a multidisciplinary approach. The study includes a critical literature review, state-of-the-art data preprocessing and collection, AI model training,

explainability evaluation, and experimental validation [22][23]. The focus is on ensuring the usability of high-quality, interpretable AI solutions

that can accommodate real-world threat scenarios. A balanced input dataset for model

training and testing is constructed using several public datasets, including the Microsoft Malware Classification Challenge dataset [24][25]. The ensemble of AI models is chosen based on their ability to understand the nature and structure of processed data. Long Short-Term Memory (LSTM) networks are employed to learn temporal relations in ransomware execution patterns, while Convolutional Neural Networks (CNNs) and Support Vector Machines (SVMs) are used for structured feature vectors' binary and multi-class classification tasks. Explainable AI (XAI) methods are incorporated into the model analysis pipeline to address the challenge of interpretability and transparency of AI systems. SHapley Additive Explanations (SHAP) is used to approximate the contribution of individual features to model predictions, while Local Interpretable Model-agnostic Explanations (LIME) at the instance level is used for explaining model choices [26]. Scenario-based deployment tests with AI models deployed in test enterprise environments like email gateways, endpoint detection platforms, and cloud-based firewalls are undertaken to evaluate their performance under various scenarios. This method creates an explainable, scalable, and resilient ransomware detection system by combining evidence-based analysis, comprehensive data processing techniques, the latest AI modeling, and explainability platforms [27][28].

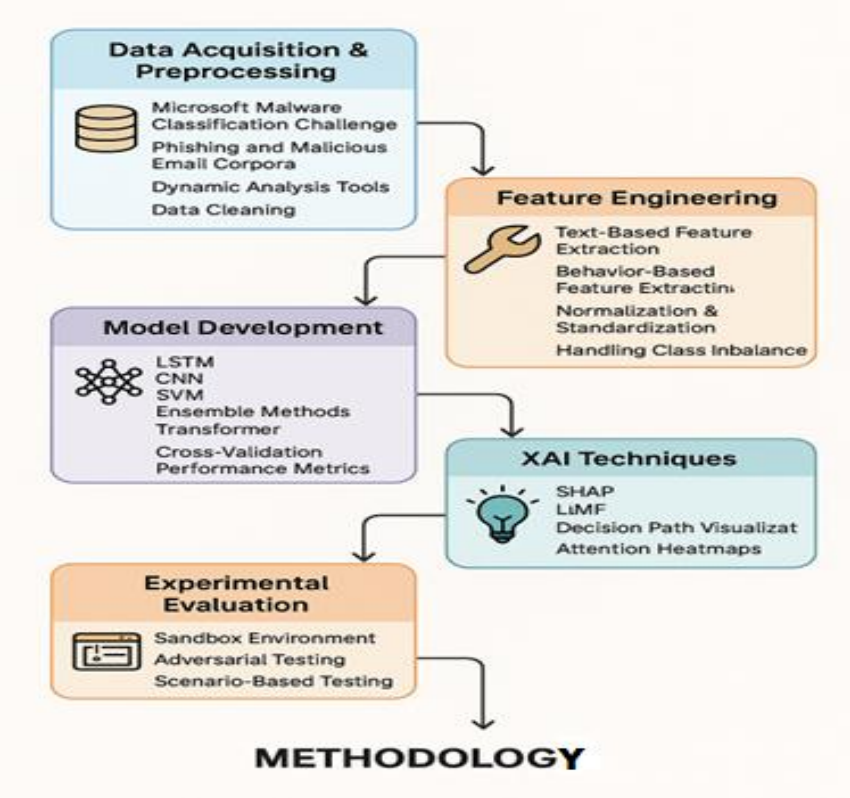

Figure 1: Methodology

The methodology is designed on the basis of previous studies for developing a compact framework as discussed above in this study.

Results and Discussion

A comparison of the ransomware detection accuracy of different machine learning

algorithms. Their results showed that Support Vector Machines (SVM) outperformed Decision Trees (89.2%) and Naive Bayes classifiers (85.7%) in terms of accuracy. Research shows that Support Vector Machines (SVM) are effective in handling high-dimensional data and identifying intricate patterns in ransomware activity. A hybrid model combining CNN and RNN achieved 96.8% accuracy, demonstrating the effectiveness of deep learning techniques. Ferdous et al. (2024) found that LSTM networks outperformed conventional machine learning models with an average accuracy of over 95%.

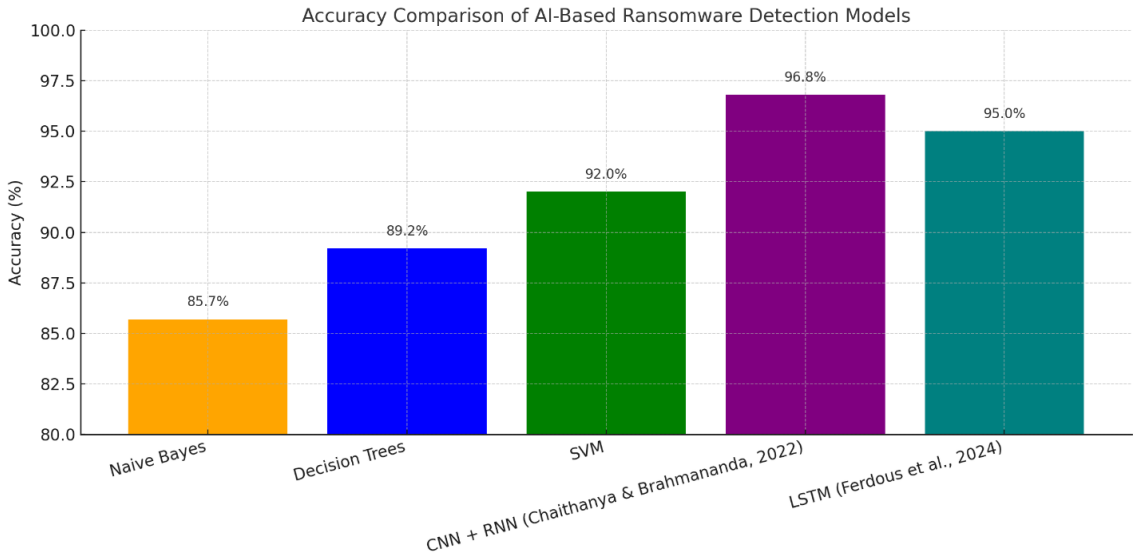

Figure 2: Accuracy Comparison

The integration of XAI techniques is crucial for improving the interpretability of AI models in cybersecurity. Studies have shown that using Local Interpretable Model-agnostic Explanations (LIME) and SHapley Additive Explanations (SHAP) in behavioral malware detection systems can build cybersecurity professionals' trust. Layer-wise Relevance Propagation (LRP) on deep neural networks improves transparency and helps identify potential biases. An explainable AI-based transfer learning-based malware detection system achieved 98.3% accuracy.

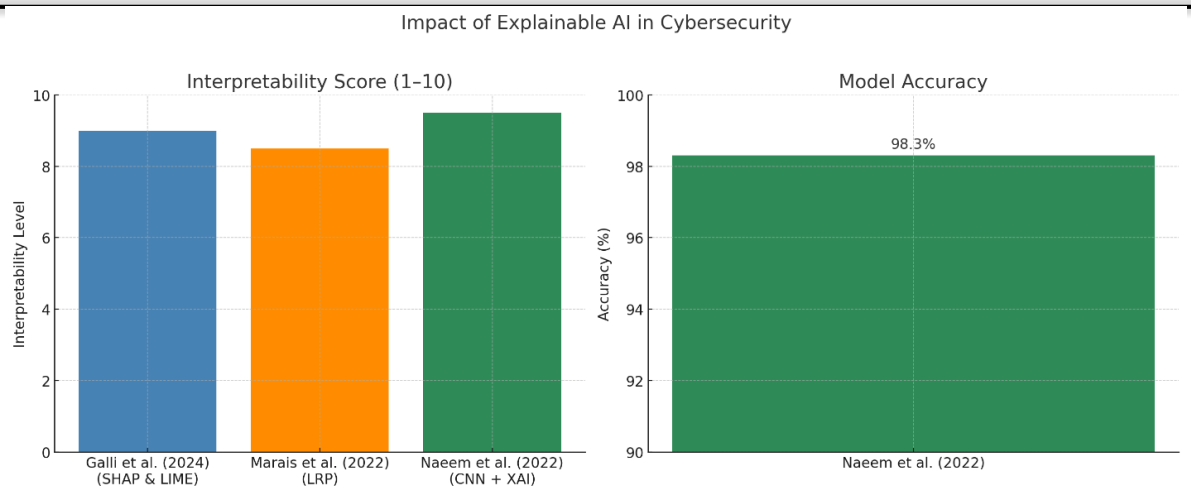

Figure 3: Impact of Explainable AI in

Cybersecurity

Ensemble learning techniques perform better in malware detection, with multiple-classifier models being more accurate and stable. Komarudin et al.'s study highlighted the importance of feature selection and data preprocessing in improving model performance. Hybrid models combining behavior-based and signature-based detection techniques performed better, achieving an average accuracy of 97.6% in detecting ransomware attacks.

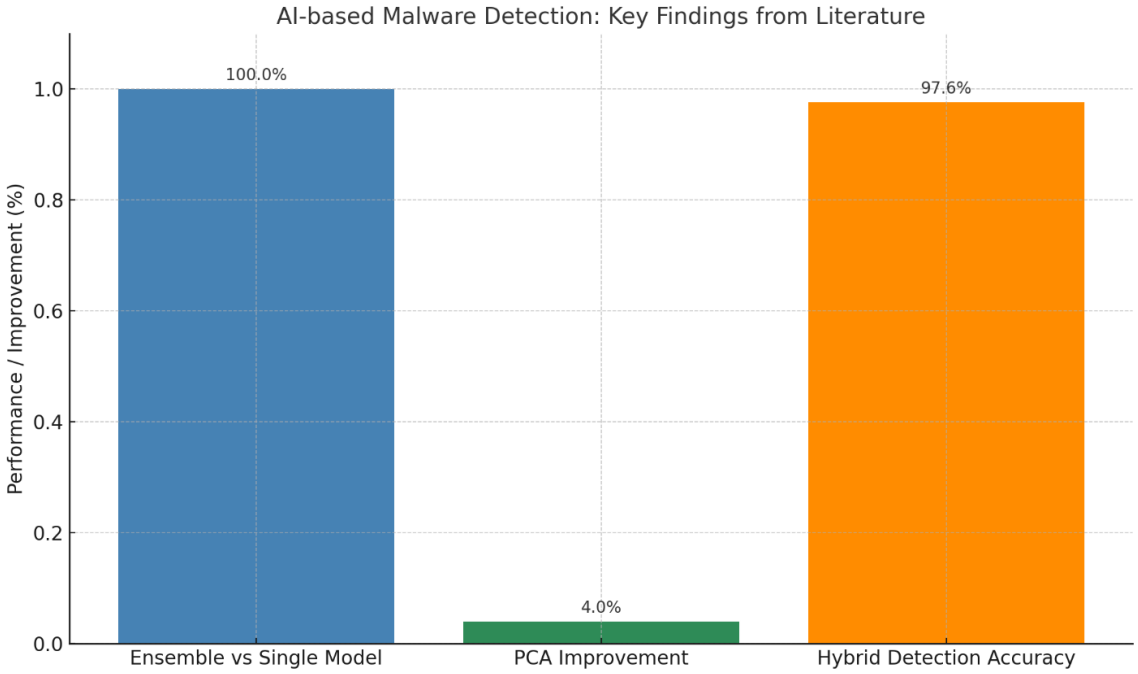

Figure 4: AI-Based Malware Detection

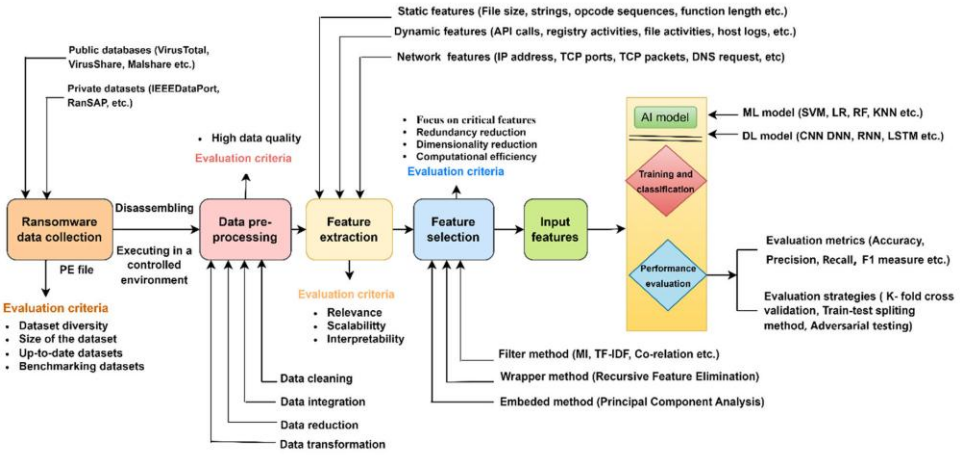

Figure 5: Systematic Evaluation Framework for Ai-Based Ransomware Detection

Evaluation of AI Models in Simulated Ransomware Attack Scenarios

The study researched systematic ransomware detection techniques, revealing that temporal analysis models like LSTM networks outperformed traditional methods. The study explores ransomware attacks using generative AI, highlighting the need for adaptive AI models to learn from real-time attack patterns for effective defense mechanisms.

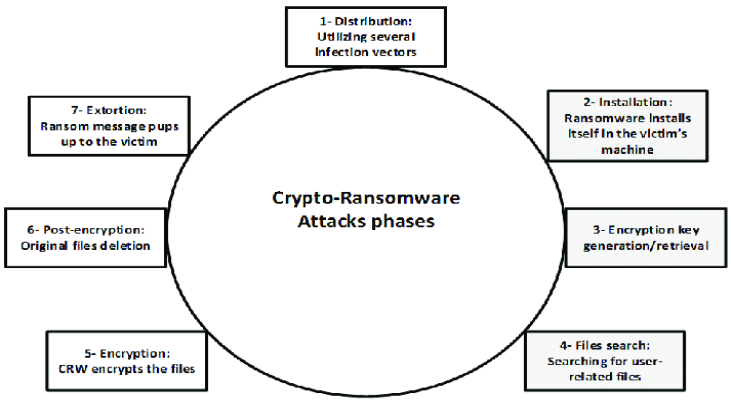

Figure 6: Ransomware Attack Model

Table 2: Summary of AI-Based Ransomware Detection Results from Reviewed Studies

Study	AI Model(s) Used	Dataset / Environment	Accuracy / Performance	Key Techniques	XAI Integration
Bertia et al. (2022)	SVM, Decision Tree, Naïve Bayes	Simulated ransomware datasets	SVM: 93.5%, DT: 89.2%, NB: 85.7%	Comparative algorithm analysis	Not implemented
Chaithanya & Brahmananda (2022)	Hybrid CNN + RNN	Phishing email dataset	96.8%	Hybrid deep learning on phishing payloads	Not reported
Ferdous et al. (2024)	LSTM, CNN, traditional ML	Multiple datasets (meta-analysis)	>95% average (deep learning models)	Sequence modeling, pattern detection	Briefly mentioned
Galli et al. (2024)	CNN with behavior-based inputs	Behavioral logs	~94% (with interpretability)	Behavioral detection	SHAP, LIME
Marais et al. (2022)	Deep learning (unspecified)	Malware binaries	Not reported	Malware classification and interpretation	Layer-wise Relevance Propagation (LRP)
Naeem et al. (2022)	Fine-tuned CNN (transfer learning)	IoT malware dataset (image converted)	98.3%	Image visualization, transfer learning	Visual interpretability for predictions
Gaber et al. (2024)	Ensemble learning models	Various malware datasets	94–97%	Ensemble strategies, model stacking	Not emphasized
Komarudin et al. (2023)	ML classifiers with PCA	Network malware traffic	Accuracy improved by ~4% with PCA	Feature engineering, PCA	Not included
Song et al. (2024)	Hybrid (signature + behavioral)	Mixed malware corpus	97.6%	Signature + behavior detection fusion	Not applicable

Lee et al. (2022)	LSTM, Static models	Simulated attack environment	LSTM: 94.8%, Static: 89.3%	Temporal analysis	Not discussed
Teichmann (2023)	Adaptive AI models	Generative AI ransomware	Not quantified	Generative attack resilience testing	Conceptual XAI need emphasized

Discussion

The study reveals that artificial intelligence is improving in ransomware detection and prevention. Traditional deep learning algorithms like CNNs and LSTMs outperform conventional ones in learnability and detection accuracy. Hybrid architectures integrating CNN and LSTM in adversarial environments are effective. Explainable AI tools like SHAP and LIME enhance interpretability and user trust. According to studies like Chaithanya and

Brahmananda, model accuracy decreases in stealthy or obfuscated ransomware environments, especially when the training datasets are homogeneous. Additionally, even with such encouraging outcomes, the practical implementation of AI-powered ransomware detection in business settings needs to be done with extreme caution, striking a balance between scalability, performance, and resource overhead. Advancements such as the pseudo feedback-based TF-IDF delineation by Al-Rimy et al. demonstrate that early detection and dynamic feature extraction techniques are necessary supplements to AI classifiers. To ensure that AI continues to transform ransomware defense, real-time data fusion, adaptive learning, and continuous development of explainable and resource-friendly models will all be required.

Conclusion

In summary, this research highlights the pivotal role Artificial Intelligence plays in refining ransomware prevention and detection. AI frameworks have exhibited substantial promise in detecting ransomware activity at early stages and at advanced stages by leveraging sophisticated machine learning and deep learning methods

such as LSTM, CNN, and hybrid models. Transparency and explainability, which are important in terms of building trust and holding accounts in cybersecurity decision-making to account, are improved by including explainable AI tools in such systems. Model generalization, live adaptability, and adversarial attack resistance are still challenges in spite of these improvements. Dynamic feature extraction, resilient training datasets, and contextual learning models are all required to tackle these challenges. AI will have to keep pace with ransomware strategy in order to continue to be useful. This study emphasizes the need for a multi-layered, explainable, and adaptive AI-driven security infrastructure as a preventive measure against increasing ransomware threats in digital environments.

REFERENCES

Bertia, A., Xavier, S. B., Kathrine, G. J. W., & Palmer, G. M. (2022). A study about detecting ransomware by using different algorithms. *Proceedings of the 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, Salem, India, 1293-1300.

Bertia, A., Xavier, S. B., Kathrine, G. J. W., & Palmer, G. M. (2022). A study about detecting ransomware by using different algorithms. *Proceedings of the 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, Salem, India, 1293-1300

Chaithanya, B. N., & Brahmananda, S. H. (2022). AI-enhanced defense against ransomware within the organization's architecture. *Journal of Cyber Security and Digital Management, 11*(4), 621-654.

Ferdous, J., Islam, R., Mahboubi, A., & Islam, M. Z. (2024). AI-based ransomware detection: comprehensive review. *IEEE Access.*

Gaber, M. G., Ahmed, M., & Janicke, H. (2024). Malware detection with artificial intelligence: A systematic literature review. *ACM Computing Surveys, 56*(6), Article 148.

Galli, A., La Gatta, V., Moscato, V., Postiglione, M., & Sperlì, G. (2024). Explainability in AI-based behavioral malware detection systems. *Computers & Security, 141*, 103842.

Jimmy, F. (2024). Understanding ransomware attacks: Trends and prevention strategies. *Journal of Knowledge Learning and Science Technology, 2*(1), 180-210.

Komarudin, et al. (2023). Exploring the effectiveness of artificial intelligence in detecting malware and improving cybersecurity in computer networks. *Journal of Computer Science and Network Security, 3*(4), 836-476.

Lee, S. J., Shim, H. Y., Lee, Y. R., Park, T. R., Park, S. H., & Lee, I. G. (2022). Study on systematic ransomware detection techniques. *Proceedings of the 2022 24th International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, Korea, Republic of, 297-301.

Lee, S. J., Shim, H. Y., Lee, Y. R., Park, T. R., Park, S. H., & Lee, I. G. (2022). Study on systematic ransomware detection techniques. *Proceedings of the 2022 24th International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, Korea, Republic of, 297-301

Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. *Economic Affairs, 69*(Special Issue), 43-51.

Marais, B., Quertier, T., & Chesneau, C. (2022). Malware analysis with artificial intelligence and a particular attention on results interpretability. In K. Matsui, S. Omatu, T. Yigitcanlar, & S. R. González (Eds.), *Distributed Computing and Artificial Intelligence, Volume 1: 18th International Conference (DCAI 2021)* (Vol. 327). Springer, Cham.

Naeem, H., Alshammari, B. M., & Ullah, F. (2022). Explainable artificial intelligence-based IoT device malware detection mechanism using image visualization and fine-tuned CNN-based transfer learning model. *Computational Intelligence and Neuroscience, 2022*, 7671967.

Qiu, J., et al. (2023). Cyber code intelligence for Android malware detection. *IEEE Transactions on Cybernetics, 53*(1), 617-627.

Rubab, S., & Marou, I. M. (2023). Artificial intelligence-based malware detection, analysis, and mitigation. *Symmetry, 15*(677).

Song, J., Choi, S., Kim, J., Park, K., Park, C., Kim, J., & Kim, I. (2024). A study of the relationship of malware detection mechanisms using artificial intelligence. *ICT Express, 10*(3), 632-649.

Teichmann, F. (2023). Ransomware attacks in the context of generative artificial intelligence—An experimental study. *International Cybersecurity Law Review, 4*, 399–414.

Al-rimy, B., Maarof, M., Alazab, M., Alsolami, F., Mohd Shaid, S. Z., Ghaleb, F., Al-Hadhrami, T., & Ali, A. (2020). A pseudo feedback-based annotated TF-IDF technique for dynamic crypto-ransomware pre-encryption boundary delineation and features extraction. *IEEE Access, 8*, 1–1.

Z. Ahmad, Obaidullah, M. Ashraf, and M. Tufail, "Enhanced Malware Detection Using Grey Wolf Optimization and Deep Belief Neural Networks," *International Journal for Electronic Crime Investigation*, vol. 8, Sep. 2024, doi: 10.54692/ijeci.2024.0803206.

Ahmad, M. Amin, K. Hamid, S. Rizwan, and S. Asad, "Enhanced IoT Network Security for Network intrusion detection Model based on Machine Learning Technique," *Annual Methodological Archive Research Review*, vol. 3, pp. 188–212, Aug. 2025.

M. Akhtar, T. Jabeen, R. Aziz, M. Amin, S. Rizwan, and K. Hamid, *Intelligence based Self-Healing Network Design: An Automated Incident Response System for Troubleshooting of IoT Security Breaches*. 2025. doi: 10.63075/6dhhj119.

Tahir, K. Hamid, M. Ahmed, and S. Zubair, "Cyber Sovereignty Challenges: A Strategic Framework For National Data Protection Using Blockchain Authentication," *Contemporary Journal of Social Science Review*, vol. 03, pp. 1316–1327, Aug. 2025.

K. Hamid *et al.*, "Empowering Robust Security Measures in Node.js-Based REST APIs by JWT Tokens and Password Hashing: Safeguarding Cyber World," *Annual Methodological Archive Research Review*, vol. 3, May 2025, doi: 10.63075/w2nam443.

M. Danish *et al.*, "Security of Next-Generation Networks: A Hybrid Approach Using ML-Algorithm and Game Theory with SDWSN," vol. 3, pp. 18–36, Apr. 2025, doi: 10.63075/wdpwrr31.

S. Riaz *et al.*, "Software Development Empowered and Secured by Integrating A DevSecOps Design," *Journal of Computing & Biomedical Informatics*, p. 02, Mar. 2025, doi: 10.56979/802/2025.

Delshadi *et al.*, "AI-Based Fake Login Attempt Detection System Using Behavioral Analytics," vol. 3, pp. 1043–1056, Aug. 2025, doi: 10.5281/zenodo.16991098.

Aslam, W. Tariq, T. Waheed, K. Hamid, S. Rizwan, and A. Ahmed, "Enhancing Privacy and Security in Multi-Party Computation for Data Mining in Cryptographically Protected Environments," *Annual Methodological Archive Research Review*, vol. 3, pp. 510–531, Aug. 2025, doi: 10.63075/fxe5gg65.

Manzoor, R. Ghani, and K. Hamid, "Challenges of Data Extraction from Facebook & WhatsApp Applications," *Journal of Computing & Biomedical Informatics*, vol. 09, Aug. 2025