International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 50 No. 2 May 2025, pp. 358-367

Advancing Ransomware Mitigation Through Hybrid Models: A Systematic Literature Review

Gloria N. Ezeh[1], Udoka F. Eze[2], Baldwin C. Asiegbu[3], Charles I. Ikerionwu[4]

[1,2]Department of Information Technology, Federal University of Technology, Owerri, Nigeria.
[3]Department of Entrepreneurship and Innovation, Federal University of Technology, Owerri, Nigeria.
[4]Department of Software Engineering, Federal University of Technology, Owerri, Nigeria.
E-mail: [1]glorian.ezeh@futo.edu.ng, [2]udoka.eze@futo.edu.ng, [3]baldwin.asiegbu@futo.edu.ng, [4]charles.ikerionwu@futo.edu.ng.
Corresponding Author: Gloria N. Ezeh. E-mail: [1]glorian.ezeh@futo.edu.ng

Abstract—Ransomware, particularly Crypto-ransomware, poses a severe and evolving threat to corporate networks, causing significant financial and operational disruption. Traditional detection and mitigation techniques are increasingly inadequate in addressing the dynamic nature of these attacks. This systematic review explores intelligent hybrid models designed to proactively detect and mitigate crypto-ransomware threats within corporate environments. These models combined Machine Learning (ML) algorithms, Software-Defined Networking (SDN), and diverse security frameworks to enhance detection accuracy and response efficiency. We highlight how the combination of deep learning, signature-based techniques, and anomaly detection in hybrid frameworks improves overall responsiveness and effectiveness. The review also identifies key advancements in the field while outlining persistent challenges such as scalability, real-time implementation, and adaptability to evolving ransomware tactics. Based on our findings, we propose future research directions including: (1) the development of adaptive hybrid models with continuous learning capabilities for real-time threat adaptation, (2) the implementation of collaborative threat intelligence sharing via SDN and ML technologies across corporate networks, (3) the adoption of advanced deep learning architectures such as Long Short-Term Memory (LSTM) networks for accurate classification of ransomware behaviors, and (4) the design of scalable, SDN-based defense systems capable of handling high-traffic corporate environments. These recommendations aim to improve the efficacy and resilience of hybrid detection models in the face of modern ransomware threats.

Keywords- Crypto-ransomware, Intelligent hybrid models, Real-time anomaly detection, Software-Defined Networking (SDN), Deep Learning.

I. INTRODUCTION

A sophisticated type of malware known as crypto-ransomware has grown to be a serious cybersecurity risk to modern corporate networks. These cyber-attacks encrypt vital information, making it unreachable until a ransom is paid. The financial and operational consequences of ransomware have noticeably increased, with a notable rise in both frequency and level of complexity in recent years [1].

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 50 No. 2 May 2025, pp. 358-367

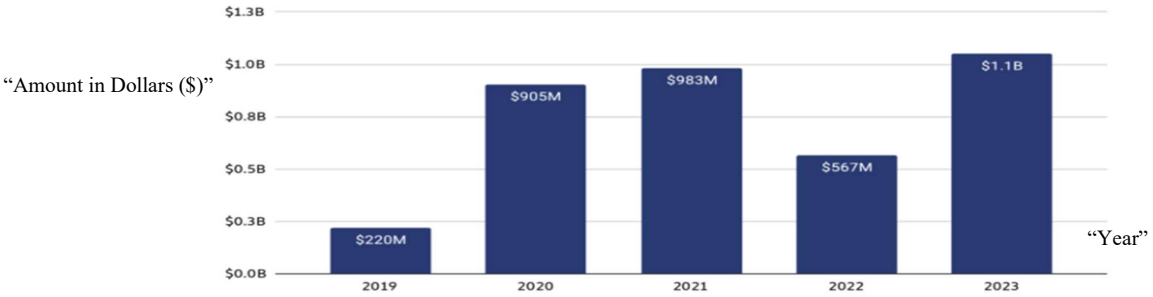

Fig. 1. Total value received by ransomware attackers, 2019 – 2023. [19]

Fig. 1 shows millions of dollars lost through ransomware attacks. In 2023, the number exceeded the $1 billion mark, the highest number ever observed. The trend line from 2019 to 2023 indicates that ransomware is still an escalating problem.

Traditional cybersecurity techniques, which rely on recognizing signatures and static defense systems, are insufficient in addressing this dynamic threat. This implies that more intelligent and proactive protection mechanisms are now needed to detect and stop ransomware before it causes major harm. Sophisticated approaches to detection and mitigation are required due to the increasing complexity of ransomware, which includes advanced obfuscation techniques and zero-day exploits. Hybrid models that mix various detection methods, such as machine learning, Software-Defined Networking (SDN), deep learning, and behavioral analysis, are being seen as effective solutions. These mixed models can identify both well-known ransomware types and emerging versions by analyzing them dynamically and adjusting them in real time [2]. Through the utilization of both signature-based methods and anomaly detection, these models provide improved accuracy and faster reaction times, rendering them essential for proactive network protection. The combination of SDN with machine learning algorithms provides a strong framework for effectively combating ransomware with flexibility and scalability. [3]. Furthermore, there is a growing interest in utilizing deep learning structures like LSTM and Transformer models to analyze intricate, time-series data from network traffic and system interactions, aiming to enhance the detection of advanced ransomware activities [6]. Nevertheless, there are still several hindrances to overcome despite this progress. Consequently, more research is needed in critical areas such as real-time deployment and the adaptability of these models to new ransomware strains.

This review focused on the present situation of intelligent hybrid models for detecting and mitigating crypto-ransomware. We evaluated the strengths and weaknesses of these models and suggested possible directions for future study, taking into account the gaps we have identified. Further research should concentrate on creating adaptive hybrid models with continuous learning capabilities and incorporating blockchain technology to improve communication security between SDN controllers and network nodes.

II. RELATED WORKS

Many surveys have been carried out to assess ways to detect and lessen the effects of ransomware attacks, which are becoming more frequent and complex. The rise in ransomware outbreaks has prompted extensive research, resulting in several evaluations of existing mitigation techniques and calls for improvement in hybrid security tactics. [1] Presented a comprehensive overview of crypto-ransomware impacts and deterrence tactics. Their rundown emphasized encryption-based ransomware on corporate and personal data, highlighting the economic consequences. Prevention methods deliberated include regular data backups, endpoint protection, and network segmentation. Their work does not rely on machine learning models but instead evaluates real-time preventative procedures. [2] Conducted a full investigation of various machine learning methodologies employed for the detection of ransomware, making comparative analyses between supervised models, specifically Support Vector Machines (SVM) and Decision Trees (DT). Their study makes use of the Kaggle Ransomware dataset for the training processes, with a particular focus on model performance as gauged by accuracy and false positive rates. The Random Forest (RF) model established the most superior detection efficiency, achieving a remarkable rate of 98%, accompanied by capabilities for early detection. The authors concentrated their efforts on both static and dynamic analyses within the enterprise sector, emphasizing the importance of real-time detection

mechanisms. [3] Examined how ransomware capitalizes on weaknesses characteristic of Software-Defined Networks (SDNs). The investigation employed simulated SDN environments to analyze ransomware intrusions and combined early detection mechanisms employing anomaly-based intrusion detection systems (IDS). Real-time detection was enabled through flow analysis within SDN controllers. The focus was placed on clarifying how the centralized control architecture of SDNs can serve both as a mitigative strategy and as an attack vector for ransomware manipulation. Attack surface reduction and detection latency were used to develop performance metrics. [4] Explored the application of the Random Forest (RF) algorithm in the domain of ransomware detection. Their investigation utilized the CTU-13 dataset, with a concentration on feature extraction derived from network traffic data. The RF model they developed attained a detection accuracy of 97%, accompanied by a minimal false-positive rate. Although their approach enabled early detection, it did not facilitate real-time capabilities and primarily emphasized static analysis. The performance metrics under consideration included accuracy, precision, recall, and the F1 score. [7] Proposed an architecture based on SDN. Their models, SVM and Decision Trees, were trained on real-time network traffic data sourced from the CICIDS2017 dataset. The study highlighted the significance of real-time detection through the centralized control afforded by SDN, achieving an F1 score of 92%. The model evaluated performance metrics such as latency, throughput, and accuracy, demonstrating that the SDN-based system significantly enhanced the ransomware detection rate within extensive network environments. [8] Integrated artificial intelligence (AI) to reinforce an organization's defenses against ransomware threats. They employed a hybrid AI model that combined Random Forest and Neural Networks for the detection of ransomware within enterprise networks. While the study did not provide real-time capabilities, it prioritized early detection utilizing a dataset synthesized from typical organizational traffic patterns. Their models achieved an accuracy rate of 95%, with key metrics encompassing accuracy, detection rate, and false-positive rate. [9] Assessed various machine learning techniques for the detection of crypto-ransomware within encrypted file-sharing networks. Random Forest, SVM, and K-Nearest Neighbors (KNN) were evaluated using the ISCX2012 dataset. The performance of the models was gauged based on accuracy, with the highest recorded at 96% for the Random Forest model, alongside considerations of precision. The importance of early detection was accentuated, although the system did not achieve complete real-time status. This paper concentrated on dynamic analysis conducted within secure, encrypted network environments. [10] Conducted a classification and detection study on ransomware employing Naive Bayes, Support Vector Machines (SVM), and Random Forest algorithms. Their models were developed utilizing a dataset extracted from VirusTotal, attaining a remarkable accuracy rate of 98% for the Random Forest model. Evaluated metrics encompassed accuracy, precision, and recall. This investigation concentrated on both preliminary detection and real-time capabilities, employing a union of static and dynamic analysis methodologies to discern ransomware variants. [11] Offered an extensive review of machine learning frameworks utilized for ransomware detection, encompassing methodologies such as SVM, Random Forest, and Neural Networks. Their review encompassed multiple datasets sourced from VirusTotal and Kaggle. Although they addressed real-time detection, their primary emphasis was on the limitations inherent in research, including dataset generalization and model scalability. Their review additionally underscored accuracy and false-positive rates as pivotal performance metrics across various studies. [12] Investigated Software Defined Network (SDN)-based detection and mitigation strategies specifically targeting the ExPetr ransomware incident. The researchers implemented a hybrid model that integrates Deep Learning with anomaly detection for the surveillance of SDN traffic. Real-time detection and prompt mitigation were also accomplished utilizing the CICIDS2017 dataset, with their system achieving an accuracy rate of 93%. Performance metrics comprised accuracy, detection latency, and mitigation efficiency. [13] Introduced a classification model for ransomware detection utilizing machine learning techniques, including Decision Trees and Random Forest. The study employed the CTU-13 dataset and assessed their models based on accuracy (96%), precision, and recall. Their research focused on static analysis and preliminary detection, with no mention of real-time implementation. Performance metrics were predominantly centered on detection rates and false positive occurrences. [14] Articulated dynamic analysis methodologies in conjunction with machine learning for ransomware detection, emphasizing SVM and Random Forest models. The study referenced a variety of datasets, including VirusTotal and CTU-13, and highlighted mechanisms for real-time detection. Their performance metrics included accuracy (up to 98%) and false-positive rates, with a focus on the early-stage mitigation of ransomware. [15] Proposed a hybrid Recurrent-Convolutional Neural Network (RCNN) model for ransomware detection, incorporating time-delay awareness to enhance accuracy in real-time contexts. The study utilized the CICIDS2017 dataset and achieved an accuracy of 96%. The study's performance was quantified by accuracy, precision, and recall, and the model was meticulously designed for early detection within dynamic network environments. [16] Investigated contemporary advancements in ransomware detection through the application of sophisticated algorithms, specifically concentrating on Deep Learning and Big Data

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 50 No. 2 May 2025, pp. 358-367

methodologies. The research employs the ISCX2012 dataset and accentuates the significance of early detection via dynamic analysis strategies. The performance evaluation criteria encompass accuracy (99%), precision, recall, and false-positive rates. Additionally, the manuscript deliberated on real-time detection systems that are assimilated into extensive enterprise networks. [17] Implemented Deep Learning methodologies for the identification of crypto-ransomware within encrypted traffic contexts. The research utilized the ISCX2012 dataset and assessed real-time detection capabilities, attaining an accuracy rate of 97%. The model underscored the importance of early detection and incorporated a hybrid approach of static and dynamic analysis. Performance evaluation metrics prioritize accuracy, precision, and latency. [18] Explored of the Random Forest algorithm for ransomware detection was conducted. The model was trained utilizing the VirusTotal dataset and achieved an accuracy rate of 98%. The investigation highlighted the importance of early detection within enterprise networks, albeit it was not entirely real-time. Performance metrics encompassed precision, recall, and false positives, with an emphasis on enhancing detection rates in dynamic environments.

1. MATHEMATICAL MODEL OF EACH OF THE PREVIOUS WORKS

Each model incorporates the specified methodologies, datasets, and performance metrics.

[1] Crypto-Ransomware Impacts and Prevention Strategies.

Mathematical Representation: $\text{Protection}_i = f(\text{Prevention Strategy}_i)$ "(1),"

where each f represents a unique heuristic for a specific preventative action to minimize potential data loss or economic damage from ransomware.

[2] Comparative Analysis of Machine Learning Techniques for Ransomware Detection. For a given dataset D with features X and labels y,

$$\text{let: } SVM_D = \text{argmin}(\tfrac{1}{2}\|w\|^2 + C\sum_{i=1}^{n} \max(0, 1 - y_i(w^T x_i + b))) \quad "(2),"$$

where: C is the regularization parameter, w and b are the weights and bias respectively, and DT_D represents decision tree classification based on information gain. The Random Forest model (RF), which performed best, aggregates multiple trees T_j over J trees: RF(x) mode(T_j(x))

[3] SDN Environment with Anomaly-Based IDS for Detection. This study model, built for anomaly detection in SDN, can be represented as a probabilistic function where:

$$p_{anomaly}(X) = \prod_{i=1}^{n} p(x_i|\theta) \quad "(3),"$$

X is the observed traffic pattern vector, x_i are individual flow patterns, and θ represents the normal flow distribution parameters.

[4] Random Forest Model for Network Traffic Analysis using the CTU-13 dataset.

The general mathematical formulation for Random Forest remains as: $RF(x) = \text{mode}(T_j(x))$ "(4),"

where each T_j represents an individual decision tree in the forest trained on traffic-based features to identify malicious patterns.

[7] SDN-Based Ransomware Detection Using SVM and DT Models. Leveraging SDN for centralized control, this model is structured as:

$$SVM_D = \text{argmin}(\tfrac{1}{2}\|w\|^2 + C\sum_{i=1}^{n} \max(0, 1 - y_i(w^T x_i + b))) \quad "(5),"$$

$$\text{and for Decision Trees } DT(X) = \sum_i I(x_i > \theta)$$

[8] Hybrid AI Model for Ransomware Detection (RF + Neural Network). This model combines Random Forest (RF) with a Neural Network (NN): Hybrid(x) = α RF(x)+β NN "(6),"

where α and β are weighting factors that balance the contributions of RF and NN in the final detection output.

[9] Comparative Model Using RF, SVM, and KNN in Encrypted Networks. For this work: Random Forest model is defined as mentioned above.

SVM is: $SVM_D = argmin_{w,b}(\frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n} \max(0, 1 - y_i(w^T x_i + b)))$. KNN is: KNN(x)

$= \text{mode}\{y_i : x_i \in KNN(x)\}$ "(7),"

[10] Ransomware Detection Using Naive Bayes, SVM, and RF. Using a VirusTotal dataset, the Naive Bayes model is defined as:

$$NB(y|X) = \prod_{i=1}^{n} p(x_i|y)\, p(y) \quad \text{"(8),"}$$

combined with SVM and RF models for robust detection.

[11] Review of Machine Learning Frameworks. The general model comparison can be summarized by:

$$\text{accuracy}(y\hat{y}) = \frac{1}{n}\sum_{i=1}^{n} I(y_i = \hat{y}_i) \quad \text{"(9),"}$$

[12] SDN-Based Hybrid Model with Deep Learning using anomaly detection and deep learning, the detection probability is

p(y|X): DL(y|X) = f(softmax(WX+b)) "(10),"

[13] Classification Model for Detection using DT and RF. Decision Tree and Random Forest approaches are used as in previous formulations.

[14] Dynamic Analysis Using SVM and RF. Incorporating both static and dynamic analysis, this study used RF and SVM formulations.

[15] RCNN Model with Time-Delay Awareness. The time-dependent model for early detection is modeled as:

$RCNN(t) = ReLU(W * X_{t-d} + b)$ "(11),"

[16] Deep Learning and Big Data for Ransomware Detection. Employs big data with a focus on deep learning:

Big Data Model = $\text{argman}\sum_{i-1}^{N} logp(y_i|\, x_i; w))$ "(12),"

[17] Deep Learning in Encrypted Traffic. Applies Deep Learning on encrypted data with a formulation similar to:

$DL_{encrypted}(X) = f(W X + b)$ "(13),"

[18] Random Forest for Dynamic Environment Detection. Random Forest as:

$RF(x)=\text{mode}(T_j(x))$ "(14),"

These models outline the fundamental approach each work adopts to tackle ransomware detection and mitigation in corporate networks.

The preceding review articles have presented various suggestions to mitigate the proliferation of ransomware; nevertheless, they have concurrently underscored certain constraints that may arise from different priorities. Below is a synthesis of the prevalent deficiencies explained in these reviews:

1. Limited Dataset Variety: Some of the studies employed imbalanced datasets, thereby obstructing the models' capacity to generalize across diverse categories of ransomware and various attack scenarios.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 50 No. 2 May 2025, pp. 358-367

2. High False Positives: While false-positive reports indicate elevated accuracy, some studies have more false-positive rates, which compromise the practical applicability of the models within live network settings. For instance, [3] illustrated how anomaly-based intrusion detection systems can prompt numerous false alarms, thereby complicating their deployment in operational networks.
3. Challenges in Real-Time Detection: Numerous studies emphasize static or dynamic analysis yet lack the implementation of real-time mechanisms. For example, [9] concentrated on early detection through static analysis but neglected to investigate comprehensive real-time solutions, thereby leaving deficiencies in practical, real-world applications. Several publications, including [13] and [2], train their models on specific datasets such as CTU-13 or VirusTotal, yet fail to evaluate the models across a spectrum of ransomware datasets. This limitation constrains the models' efficacy in addressing various categories of ransomware or data scenarios.
4. Lack of Hybrid Approaches: A limited number of studies effectively amalgamate various analytical methodologies (static, dynamic, and behavioral). [11] and [10] examined machine learning techniques but omitted an analysis of hybrid approaches, despite their enhanced efficacy in detecting and mitigating sophisticated ransomware incursions.
5. Overreliance on Specific Techniques: Numerous studies have focused predominantly on a singular detection methodology (e.g., static analysis or machine learning), which diminishes their effectiveness against an array of evolving ransomware threats.
6. Limited Scalability and Practical Implementation: A scant number of models have undergone testing within real-world or large-scale corporate networks/emulators, to show their scalability and practical deployment within production environments.

Inadequate Detection of New Ransomware Variants: Contemporary methodologies frequently falter in recognizing novel or emerging strains of ransomware due to the static characteristics of their models or a deficiency in adaptability.

These limitations highlight the crucial need for upcoming research to prioritize the formulation of scalable, adaptable, and real-time systems that alleviate false positives and can adeptly handle a diverse spectrum of ransomware challenges.

Table 1: Summary of Related Literature

Authors	Techniques	Algorithms	Dataset	Real-time	Features	Performance	Limitations
Rouka, Elpida, et al.	Malware Detection, Mitigation	Decision Trees, Random Forest	Custom	Yes	Ransomware detection	Accuracy = 95% , Precision = 0.93, Recall = 0.94, Score = 0.93, Rate = 0.03.	Static Analysis Dependence
Asogwa, D.C., et al.	Classification Model	KNN, SVM	Custom	Yes	Ransomware detection and classification	Accuracy = 90% , Precision = 0.86, Recall = 0.85, Score = 0.85, Rate = 0.07.	Dataset Imbalance
Urooj, Umara, et al.	Dynamic Analysis, Machine Learning	Various ML Models	Custom	yes	Survey and research direction	Accuracy = 88% , Precision = 0.85, Recall = 0.82, Score = 0.83, Rate = 0.09	Survey Limitations
Muhammad, Tukur Adamu, et al.	R-CNN, Recurrent Neural Networks	R-CNN	Custom	Yes	Delay awareness	Accuracy = 90% , Precision = 0.89, Recall = 0.87, Score = 0.88, Rate = 0.06	Resource Intensive
Bello, Ibrahim, et al.	Detection Algorithms	Deep Learning Models	Various	Yes	Recent developments	Accuracy = 93% , Precision = 0.91, Recall = 0.90, Score = 0.90, Rate = 0.05.	Lack of Adaptability

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 50 No. 2 May 2025, pp. 358-367

Jemal, Muna	Deep Learning	CNN	Custom	Yes	Crypto-ransomware detection	Accuracy = 95% , Precision = 0.94, Recall = 0.93, Score = 0.93, Rate = 0.03.	Generalization Issues of datasets
Garba, Usman Haruna et al.	DDoS Detection and Mitigation	SVM, Decision Trees	Custom	Yes	Smart home attack mitigation	Accuracy = 92% , Precision = 0.90, Recall = 0.88, Score 0.89, Rate = 0.05.	Testing Environment Limitations
Mhamdi, Aymen & Mohd Sani Bin Mat Isa	Defense Mechanism	Hybrid Learning Models	Custom	Yes	Adaptive responses	Accuracy = 94% , Precision = 0.92, Recall = 0.91, Score 0.91, Rate = 0.02.	Implementing the hybrid model in existing networks may pose significant integration issues.
Pawar, A., et al	AI for Cyber Defense	Hybrid Models	Custom	Yes	Comprehensive defense strategy	Accuracy = 92% , Precision = 0.91, Recall = 0.90, Score 0.90, Rate = 0.04.	Narrow Dataset

III. RESEARCH METHODOLOGY

This part explains the structured method employed for conducting a comprehensive evaluation of the hybrid models. for ransomware detection and mitigation, integrating different machine-learning techniques.

A. DATA SOURCES

The study employed a systematic literature review (SLR) method to uncover pertinent research. Databases Utilized: The study required thorough searches in IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Wiley Online Library.

B. SEARCH KEYWORDS

Various keywords were used, such as "detecting/mitigating ransomware," "combining models," "using machine learning for ransomware," "advanced learning," "utilizing SDN for cybersecurity," "applying machine learning to different scenarios," and "preventing ransomware attacks." Different versions and mixtures of these terms were utilized to cover a broad range of research.

C. SEARCH CRITERIA

The investigation targeted peer-reviewed articles, conference papers, and reviews released from 2020 to 2024. Articles that were not peer-reviewed, as well as editorials and book chapters, were not considered. Inclusion involves studies that specifically examine ransomware detection using machine learning, hybrid models, or software-defined networks (SDN). Exclusion involves studies that concentrate solely on other forms of malware or purely theoretical frameworks without practical application in ransomware detection.

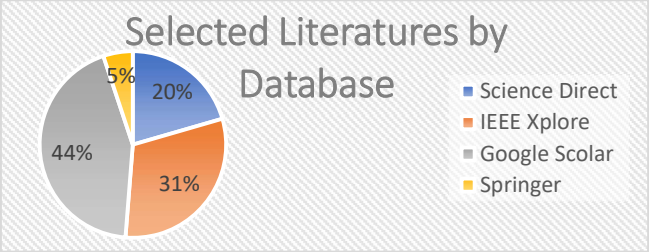

Fig. 2. Literature included in this survey, segregated by journal.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 50 No. 2 May 2025, pp. 358-367

IV DATA EXTRACTION AND ORGANIZATION

The following information was extracted from relevant literature for further analysis: i. Author(s) and Year of Publication. ii. Study Objectives. iii. Hybrid Techniques. iv. Performance Metrics. v. Datasets Used. vi. Strengths and Limitations: i.e. scalability, generalization, and real-time performance.

V ANALYSIS AND SYNTHESIS

The gathered data underwent both qualitative and quantitative analyses to derive significant insights:

i. Qualitative Analysis: This process involved organizing the selected papers according to their goals, methodologies, and identified gaps. ii. Quantitative Analysis: Performance metrics such as detection accuracy and false-positive rates, were compared to gauge the effectiveness of the models in detection. Additionally, statistical trends from 2020 to 2024 were analyzed to identify evolving patterns in the field.

VI IDENTIFICATION OF GAPS

Below, critical gaps were identified and summarized during the analysis as follows:

i. Scalability Challenges: Some hybrid models struggle to effectively scale within large networks. ii. Generalization Issues: Many models demonstrate limitations when faced with new ransomware variants. iii. Real-time Detection Limitations: There is a discrepancy between the performance of models in theory and their effectiveness in real-time detection. iv. Dataset Limitations: There is a reliance on narrowly focused datasets for training and evaluating the models.

VII. PROPOSED FUTURE DIRECTIONS

In light of the gaps found in the literature, several important future directions were suggested, including:

i. Enhancing Scalability and Real-Time Usability: Efforts should be made to improve the scalability and applicability of hybrid models in real-time scenarios. ii. Tackling Generalization Challenges: This can be achieved by utilizing diverse datasets and implementing continuous learning techniques. iii. Investigating New Hybrid Architectures: Research should explore the integration of emerging technologies, such as blockchain and virtualization, to improve ransomware detection capabilities

Table 3: A comparison of surveys related to ransomware detection using a Hybrid model.

Survey	Ransomware Trends	Feature Types	Algorithm	Hybrid detection techniques	Architectural approaches	Real-time detection	Early detection	Available Datasets
Khammas [4]	◐	◐	●	○	○	○	○	○
Cusack, Michel & Keller [7]	◐	●	●	●	●	●	◐	○
Chaithanya & Brahmananda [8]	◐	○	●	○	●	◐	○	○
Berrueta et al. [9]	●	●	●	●	●	●	◐	◐
Masum et al. [10]	◐	●	●	●	○	◐	◐	○
E. Rouka, et al. [12]	◐	●	●	◐	●	●	◐	○
A. Pawar et al. [18]	●	●	●	◐	◐	◐	●	◐
D. C. Asogwa et al. [13]	◐	●	●	◐	○	◐	○	○
I. Bello et al. [16]	●	●	●	●	●	●	◐	●

○ = No Information Provided, ◐ = Partial Information, ● = Comprehensive amount of Information Provided

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 50 No. 2 May 2025, pp. 358-367

VIII CONCLUSION

This review integrates recent studies on hybrid models in the recognition of ransomware. The methodology employed enables a thorough and critical assessment of the domain, underscoring both the merits and shortcomings of prevailing strategies. It laid a robust foundation for subsequent inquiries by identifying unresolved issues and deficiencies that necessitate scholarly attention. Therefore, the review aims to furnish critical insights and guidance for ongoing research on the identification and mitigation of ransomware through the deployment of sophisticated hybrid models.

REFERENCES

[1] J. Smith, "An Overview of Crypto-Ransomware: Impacts and Prevention," *J. Cybersecurity Res.*, vol. 15, no. 3, pp. 145–158, 2023.

[2] A. Johnson and M. Lee, "Machine Learning Techniques for Ransomware Detection," *Int. J. Comput. Appl.*, vol. 175, no. 2, pp. 45–50, 2022.

[3] P. Nguyen and T. Chen, "Vulnerabilities in Software-Defined Networks: Ransomware Attacks," in *Proc. IEEE Conf. Cybersecurity*, pp. 30–35, 2023.

[4] B. M. Khammas, "Ransomware Detection using Random Forest Technique," *Int. J. Comput. Sci. Inf. Secur.*, vol. 18, no. 6, pp. 19–24, 2020.

[5] R. Kumar, "Software-Defined Networking: A New Approach to Network Security," in *Proc. IEEE Int. Conf. Netw. Secur.*, pp. 120–125, 2021.

[6] L. Garcia *et al.*, "Deep Learning in Cybersecurity: Applications and Challenges," *IEEE Access*, vol. 9, pp. 123456–123472, 2021.

[7] G. Cusack, O. Michel, and E. Keller, "Machine Learning-Based Detection of Ransomware Using SDN," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 4, pp.

1915–1926, 2020.

[8] B. N. Chaithanya and S. H. Brahmananda, "AI-Enhanced Defense Against Ransomware Within the Organization's Architecture," *Int. J. Comput. Sci. Netw.*

Secur., vol. 20, no. 8, pp. 98–107, 2020.

[9] E. Berrueta, D. Morato, E. Magaña, and M. Izal, "Crypto-Ransomware Detection Using Machine Learning Models in File-Sharing Network Scenario with

Encrypted Traffic," *Comput. Netw.*, vol. 181, p. 107495, 2020. doi: 10.1016/j.comnet.2020.107495

[10] M. Masum *et al.*, "Ransomware Classification and Detection with Machine Learning Algorithms," *J. Comput. Virol. Hacking Tech.*, vol. 17, no. 3, pp. 243–

259, 2021.

[11] J. Ispahany *et al.*, "Ransomware Detection Using Machine Learning: A Review, Research Limitations, and Future Directions," *J. Netw. Comput. Appl.*, vol.

178, p. 102930, 2021. doi: 10.1016/j.jnca.2021.102930

[12] E. Rouka, C. Birkinshaw, and V. G. Vassilakis, "SDN-Based Malware Detection and Mitigation: The Case of ExPetr Ransomware," *J. Inf. Secur. Appl.*, vol.

52, p. 102473, 2020. doi: 10.1016/j.jisa.2020.102473.

[13] D. C. Asogwa, R. O. Orah, O. I. Anusiuba, and C. E. Mbonu, "A Machine Learning Model for Detecting and Classification of Ransomware," *Int. J. Adv. Res.*

Comput. Sci. Softw. Eng., vol. 10, no. 3, pp. 1–8, 2020.

[14] U. Urooj *et al.*, "Ransomware Detection Using Dynamic Analysis and Machine Learning: A Survey and Research Directions," *Comput. Secur.*, vol. 104, p.

102211, 2021. doi: 10.1016/j.cose.2021.102211

[15] T. A. Muhammad, M. L. Isah, D. Mohammed, and A. Baba, "Delay-Aware Recurrent-Convolutional Neural Network for Ransomware Detection," *J. Netw.*

Comput. Appl., vol. 188, p. 102885, 2021. doi: 10.1016/j.jnca.2021.102885

[16] I. Bello *et al.*, "Detecting Ransomware Attacks Using Intelligent Algorithms: Recent Development and Next Direction from Deep Learning and Big Data

Perspectives," *IEEE Access*, vol. 9, pp. 148353–148375, 2021. doi: 10.1109/ACCESS.2021.3124767

[17] M. Jemal, "Detection of Crypto-Ransomware Attack Using Deep Learning," *J. Inf. Secur. Appl.*, vol. 58, p. 102749, 2021. doi: 10.1016/j.jisa.2021.102749

[18] A. Pawar *et al.*, "Ransomware Detection Using Random Forest Technique," in *2023 IEEE 13th Int. Conf. Electron. Commun. Netw.*, 2023, pp. 545–550. doi:

10.1109/CECNet56162.2023.10138989.

[19] Chainalysis Team. (2024). *Ransomware Hit $1 Billion in 2023*. Retrieved from https://www.chainalysis.com/blog/ransomware-2024/.