*FUDMA Journal of Sciences (FJS)*
*ISSN online: 2616-1370*
*ISSN print: 2645 - 2944*
*Vol. 10 No. 21, November, 2026, pp 356 – 363*
DOI: https://doi.org/10.33003/fjs-2026-1021-6216

# Few-Shot Learning for Ransomware Detection: A Narrative Review of Machine Learning, Deep Learning and Siamese Neural Network Approaches

**[*1]Usman Ahmad Bello, [2]Abubakar Bello Tambuwal, [3]Anas Tukur Balarabe, [4]Salisu Modi and [5]Najib Hassan Adamu**

[1]Department of Computer Science, Faculty of Computing, Sokoto State University, Sokoto, P.M.B. 2134, Sokoto, Nigeria
[2]Department of Computer Science, Umaru Ali Shinkafi Polytechnic, Sokoto, Sokoto, P.M.B. 2356, Sokoto, Nigeria

*Corresponding authors' email: email: usmanabello002@gmail.com

**Received:** 15 Aug. 2026
**Accepted:** 26 Oct. 2026
**Published:** 09 Nov. 2026

**ABSTRACT**
The review examines static and dynamic analysis, binary-image representation, entropy features, transfer learning, Siamese architecture, and commonly used evaluation metrics. Findings from the reviewed studies suggest that few short learning (FSL) and Siamese neural network (SNN) based approaches may offer potential benefits for ransomware detection when labeled data are limited. However, variations in datasets, experimental configurations, few-shot settings, and evaluation procedures prevent definitive conclusions about their comparative superiority. This paper synthesizes existing research and does not present new experiments or independent experimental validation. The review identifies several research priorities, including clearly defined N-way/K-shot settings, diverse datasets, evaluation on unseen ransomware families, standardized evaluation procedures, and practical real-time assessment. Addressing these challenges may support the development of more reliable and data-efficient ransomware detection methods.

**Keywords:** Ransomware Detection, Few-Shot Learning, Siamese Neural Network, Machine Learning, Deep Learning, Meta-Learning, Malware Detection.

## INTRODUCTION

Diabetes mellitus is a chronic metabolic disorder characterized by persistent hyperglycemia resulting from impaired insulin secretion, insulin action, or both. The condition disrupts the metabolism of carbohydrates, lipids, and proteins and is associated with long-term complications affecting the cardiovascular system, kidneys, nerves, and eyes (Farzaei *et al*., 2017). Despite the availability of several synthetic antidiabetic drugs, their use is often limited by adverse effects, high cost, and reduced long-term efficacy. Consequently, there is growing interest in the development of safer, cost-effective therapeutic alternatives derived from natural products. Medicinal plants have long served as important sources of therapeutic agents due to their rich diversity of bioactive phytochemicals.

## MATERIALS AND METHODS

Ransomware is a type of malicious software that restricts access to a victim's information or system and demands payment for restoration. Its effects extend beyond the immediate loss of access to files because attacks can interrupt organizational activities, create recovery costs, and affect critical services (Davidian et al., 2024; Kumar, 2023; Sharma & Singh, 2023). The development of different ransomware variants has made the detection problem increasingly challenging (Sharma & Singh, 2023). Conventional security mechanisms can identify previously known malicious patterns, but their effectiveness may be reduced when a new variant does not match an existing signature (Sharma & Singh, 2023).

Artificial intelligence (AI), machine learning (ML), and deep learning (DL) have therefore been increasingly investigated for ransomware detection (Sharma & Singh, 2023). Machine learning approaches learn patterns from data, while deep learning uses multilayer neural networks to learn more complex representations (Aggarwal, 2019; Ferdous et al., 2024; Herbert, 2019). Research has investigated static features, dynamic behavior, network information, binary representations, and combinations of these sources (Arabo et al., 2020; Hampton et al., 2019; Khan et al., 2020; Sreelaja, 2021). However, deep learning methods are generally data hungry and may require large, labelled datasets to learn robust representations.

The limited availability of labelled ransomware samples creates a particular problem for emerging variants. Obtaining, executing, and labelling malicious software is difficult because of security, legal, technical, and operational considerations. Few-shot learning provides an alternative by attempting to learn a useful decision function from a small number of labelled examples (Ale et al., 2020; Duan et al., 2021; Qiang et al., 2022; Snell et al., 2019; Zhu et al., 2022). Siamese Neural Networks are especially relevant because they learn similarity relationships between samples rather than depending exclusively on a large number of examples for each class.

Few-shot learning (FSL) is a machine learning paradigm designed to learn new classes or recognize patterns from a limited number of labeled examples. Rather than depending exclusively on large collections of labeled samples, FSL methods seek to develop transferable representations or learning strategies that support recognition under limited-data conditions. Meta-learning, metric-based learning, and transfer learning are among the approaches associated with this objective. In cybersecurity, these methods have been investigated for malware classification and other security tasks in which obtaining sufficient labeled examples can be difficult or costly. Nevertheless, evidence from general malware detection and intrusion detection should not automatically be interpreted as proof of effectiveness against ransomware specifically. Differences in threat characteristics, input representations, datasets, and evaluation protocols require ransomware-focused evidence to be examined separately from findings obtained in broader cybersecurity applications.

Siamese Neural Networks (SNNs) are particularly relevant to few-shot learning because they learn to compare pairs of input samples through a shared-weight architecture. By mapping samples into a feature space, these networks can estimate their similarity and support classification or verification based on learned representations. For ransomware detection, this capability may provide a basis for comparing an unfamiliar executable or its representation with known benign and malicious samples, potentially reducing dependence on large numbers of labeled examples for every ransomware family. Possible input representations include executable-file features, binary images, entropy-based features, and behavioral characteristics. However, the effectiveness of an SNN-based approach depends on factors such as the quality of the learned representations, the selection of comparison samples, the diversity of training data, and its ability to generalize to previously unseen ransomware families. Consequently, the suitability of these methods must be assessed from empirical evidence rather than assumed from their architectural design alone.

Although existing research has examined conventional malware detection methods, ML and DL based classification, and emerging data-efficient learning techniques, the literature spans different threat categories, datasets, experimental configurations, and evaluation measures. These differences make it difficult to establish how well findings from general malware classification, intrusion detection, and specific ransomware investigations methods translate across application settings. A focused synthesis is therefore needed to examine the relationship between ransomware detection and data efficient methods, particularly the potential role of FSL and SNN architectures. Such a synthesis should consider not only reported detection performance but also the availability of labeled samples, the definition of few-shot learning tasks, the treatment of unseen ransomware families, dataset diversity, and the practical requirements of real-time detection.

The aim of this paper is to review and synthesize existing research on ransomware detection, with particular emphasis on machine learning, deep learning, few-shot learning, and Siamese Neural Networks under limited-labeled-data conditions. Its distinctive contribution is a thematic examination of how these approaches relate to data scarcity in ransomware detection, bringing together relevant evidence on detection techniques, learning strategies, datasets and input representations, evaluation measures, and outstanding research gaps. The review distinguishes ransomware-specific findings from evidence drawn from broader malware detection and intrusion-detection studies, highlighting where conclusions are directly supported by ransomware research and where further validation is required. It also identifies methodological and evaluation challenges that need to be addressed to establish the practical value of few-shot and Siamese-based approaches. This paper adopts a narrative review approach, synthesizes previously published research, and does not report new experiments or independent experimental validation.

**Review Scope and Approach**

This paper presents a narrative literature review of existing research on ransomware detection and few-shot learning, synthesizing relevant studies to examine current approaches, challenges, research gaps, and emerging directions in the field. The literature was organized around five themes: ransomware detection techniques; machine learning and deep learning; few-shot and meta-learning; Siamese Neural Networks; and datasets and evaluation. Studies were considered according to their relevance to ransomware or malware detection and their contribution to data-efficient or automated detection. The review does not claim to be a systematic literature review or a meta-analysis.

The reviewed literature includes research on ransomware behavioral analysis, dynamic analysis, machine learning, hybrid analysis, few-shot learning, malware classification, Siamese Neural Networks, and ransomware datasets. Attention is given to studies that address limited samples, unknown malware, and the detection of emerging ransomware variants (Ale et al., 2020; Duan et al., 2021; Qiang et al., 2022; Snell et al., 2019; Tang et al., 2020; Tran et al., 2019; Zhu et al., 2022).

**Review Approach**

This paper adopts a narrative literature review approach to examine existing research on ransomware detection and few-shot learning, with particular emphasis on ML, DL, and SNNs. The review synthesizes relevant literature to describe current detection approaches, identify methodological challenges, examine research gaps, and highlight directions for future investigation. Rather than following a formal systematic review protocol or conducting a meta-analysis, the review uses a thematic approach to organize and interpret published research according to its relevance to data-efficient ransomware and malware detection.

The literature was organized around five themes: (i) ransomware detection techniques, (ii) machine learning and deep learning, (iii) few-shot and meta-learning, (iv) Siamese Neural Networks, and (v) datasets, representations, and evaluation. These themes provided a consistent framework for examining the reviewed studies and comparing their contributions, limitations, and relevance to ransomware detection under limited-labeled-data conditions.

**Literature Search Strategy**

Relevant literature was identified through searches of scholarly databases and research platforms, including IEEE Xplore, Scopus, ScienceDirect, SpringerLink, and Google Scholar. The search covered publications from 2019 to 2026. Relevant references cited in identified publications were also considered when they provided additional information on ransomware detection, few-shot learning, or related machine learning approaches.

The search used combinations of keywords and related expressions, including:

i. “ransomware detection” and “ransomware classification”
ii. “machine learning” and “deep learning” for ransomware detection
iii. “few-shot learning” and “meta-learning”
iv. “Siamese Neural Network” and “metric learning”
v. “malware detection” and “unknown malware detection”
vi. “behavioral analysis,” “dynamic analysis,” and “hybrid analysis”
vii. “ransomware datasets,” “binary image representation,” and “entropy-based detection”

The search terms were combined in different ways to identify research addressing both ransomware-specific detection and broader malware detection techniques relevant to data-efficient learning. For example, combinations such as “ransomware detection” AND “few-shot learning” and “malware classification” AND “Siamese Neural Network” were used where appropriate. Because the review is narrative rather than systematic, these searches were intended to

identify relevant and informative studies, not to establish an exhaustive collection of every publication on the subject.




Figure 1: Literature Search Strategy

**Study Selection Criteria**

Studies were considered for inclusion based on their relevance to the review objectives, their technical contributions, and their discussion of detection under limited-data conditions. Attention was given to peer-reviewed journal articles, conference papers, and foundational publications that explain established or emerging methods.

Studies were considered relevant when they addressed one or more of the following:

i. Ransomware detection, classification, behavioral analysis, or dynamic analysis.
ii. Machine learning or deep learning methods for ransomware or malware detection.
iii. Few-shot learning, meta-learning, or other approaches designed to learn from limited labeled samples.
iv. Siamese Neural Networks and metric-learning architectures for classification or similarity-based detection.
v. Malware datasets, feature representations, evaluation measures, and generalization to previously unseen malware.

Studies focusing on general malware detection or intrusion detection were included when their methods or findings provided useful context for data-efficient cybersecurity applications. However, findings from these broader security domains were distinguished from direct evidence concerning ransomware detection.

Studies were given lower priority or excluded from the synthesis when they lacked sufficient methodological information, were not relevant to the review objectives, duplicated information already considered from the same study, or did not provide a meaningful technical contribution. These considerations guided the selection of literature without implying that a formal systematic screening procedure was conducted.

**Study Appraisal and Evidence Synthesis**

The selected studies were examined qualitatively according to their objectives, detection techniques, learning architecture, datasets, input representations, evaluation measures, and reported limitations. Attention was given to whether a study evaluated ransomware specifically or addressed malware detection more generally, whether its approach required large labeled datasets, and whether it considered previously unseen malware samples or ransomware families.

Where reported, the evaluation measures and experimental settings were examined to understand the context of the findings. However, differences in datasets, class distributions, few-shot task definitions, training configurations, and evaluation protocols limited direct comparisons between studies. Reported performance metrics were therefore interpreted in relation to each study's experimental setting rather than treated as directly comparable evidence of overall superiority.

The review did not apply a formal numerical quality-scoring system or calculate pooled performance estimates. Instead, the strength and relevance of the evidence were considered qualitatively, considering the clarity of the methodological description, the suitability of the dataset, the relevance of the evaluation procedure, and the extent to which the reported findings supported the study's conclusions. Caution was applied when interpreting findings from general malware or intrusion-detection research as evidence for ransomware-specific applications.

**Thematic Organization**

Following the identification and qualitative examination of relevant literature, the findings were synthesized into five themes:

i. Ransomware detection techniques: Signature-based, static, dynamic, behavioral, and hybrid detection approaches.
ii. Machine learning and deep learning: Learning-based classification methods and their dependence on representative training data.
iii. Few-shot and meta-learning: Approaches intended to support learning when only a small number of labeled examples are available.

iv. Siamese Neural Networks: Similarity-based learning architectures and their potential relevance to detecting previously unseen malware.

Datasets and evaluation: Dataset characteristics, input representations, evaluation measures, generalization limitations, and outstanding research gaps.

## RESULTS AND DISCUSSION

### Signature-Based and Static Detection

Signature-based detection identifies malicious files by comparing their characteristics with previously known signatures (Tran et al., 2019). It is useful for known threats but may have difficulty identifying variants that have not previously been analyzed. Static analysis examines a sample without executing it and may use features such as byte sequences, executable structures, imported functions, strings, and entropy. Static approaches are attractive because they can avoid the risks and computational cost associated with executing malicious code.

Sreelaja (2021) investigated signature matching for ransomware filtering, while other studies have used binary or image representations for malware classification. Binary-to-image conversion allows conventional image-processing and convolutional architectures to be applied to malware data. However, visual representations may not capture every characteristic of ransomware behavior and can be sensitive to how binary information is transformed.

### Dynamic and Behavioral Detection

Dynamic analysis observes a program during execution and can capture system calls, file operations, process behavior, registry modifications, and network activities. The research (Hampton et al., 2019) examined ransomware behavioral analysis on Windows platforms, while (Hwang et al., 2020) investigated two-stage ransomware detection using dynamic analysis and machine learning. The author in (Arabo et al., 2020) also considered process behavior for ransomware detection.

Dynamic analysis can provide information that is difficult to obtain from a static representation. However, it requires execution of the sample and may therefore introduce scalability and security challenges. Malware can also use anti-analysis techniques that reduce the amount of useful behavior observed in a sandbox. These limitations have motivated researchers to investigate combinations of static and dynamic information (Mercaldo, 2021).

### Early and Zero-Day Ransomware Detection

Early detection attempts to identify ransomware before extensive encryption or other damaging activities occur. The study by (Mercaldo, 2021) investigated pre-encryption detection of crypto-ransomware, while the author (Zuhair & Selamat, 2020) proposed a multi-tier streaming analytics model for 0-day ransomware detection. Other approaches have investigated machine learning and deep learning methods for detecting unknown or previously unseen ransomware (U. Z oora, M. Rajarajan, 2022), (Shashikant et al., 2021).

The challenge of zero-day detection is closely related to the limited-data problem. A new ransomware family may not have sufficient labelled samples for conventional supervised training. Consequently, methods capable of learning from small samples or transferring knowledge from related classes are important research directions.

### Machine Learning and Deep Learning for Ransomware Detection

Machine learning can be divided into supervised, unsupervised, and semi-supervised learning. Supervised learning uses labelled examples to learn a classification function. Unsupervised learning attempts to discover patterns without predefined labels, while semi-supervised learning combines labelled and unlabeled data. These approaches have been applied to malware and ransomware detection (Neal, 2007; Sutton & Barto, 2012).

Random forest, anomaly detection, clustering, finite-state modelling, and other machine learning methods have been investigated. The study (Khammas, 2020) for example, examined ransomware detection using random forest, while (Ramesh & Menen, 2020) investigated an automated dynamic approach based on a finite-state machine. The study in (Khan et al., 2020) proposed a digital DNA sequencing engine for ransomware detection using machine learning.

Deep learning extends machine learning through multilayer neural network architectures. CNNs have been applied to malware images and other representations because they can learn spatial and hierarchical patterns (Krizhevsky et al., 2012; Liu & Deng, 2015). The study (Catak et al., 2021) investigated data augmentation for malware detection using CNNs, while other studies have examined transfer learning and deeper CNN architectures. Deep learning can reduce the need for manually engineered features, but its performance is commonly associated with the quantity and diversity of training data.

Transfer learning attempts to address data limitations by adapting a model that has already learned useful representations from another dataset. Architectures such as VGG, AlexNet, ResNet, and Inception have been used in image and malware classification research (He & Xiangyu, 2022; Krizhevsky et al., 2012; Liu & Deng, 2015; Szegedy et al., 2014). Nevertheless, the effectiveness of transfer learning depends on the similarity between the source and target domains.

### Few-Shot Learning and Meta-Learning

Few-shot learning is a learning setting in which a model is required to make reliable predictions from a small number of labelled examples. Instead of assuming that a large training set is available for every class, FSL attempts to learn representations or decision functions that can be adapted to new classes using limited samples. The study in (Duan et al., 2021) reviewed few-shot learning for intrusion detection, while the study (Song et al., 2022) discussed the evolution, applications, challenges, and opportunities of few-shot learning.

Meta-learning is closely associated with few-shot learning. A meta-learning system learns information across multiple tasks so that it can adapt to a new task using only a small number of examples. In cybersecurity, this property can be useful when new attack types appear and only a limited amount of labelled data is available (Yang et al., 2023) (Mohammadi et al., 2020).

Prototypical Networks provide one example of metric-based few-shot learning (Snell et al., 2019). The approach represents examples in an embedding space and uses class prototypes for classification. Similar ideas are applicable to malware and ransomware because samples can be represented in a feature space where similarity and dissimilarity are learned rather than relying only on conventional class-specific classifiers.

Ale et al., (2020) investigated few-shot learning for Android malware classification, while (Tran et al., 2019) investigated

image-based unknown malware classification with few-shot learning models. The author (Qiang et al., 2022) examined incremental malware classification using few-shot learning. These studies indicate that limited-data learning is relevant to malware detection beyond ransomware alone.

**Siamese Neural Networks for Ransomware Detection**

A Siamese Neural Network contains branches that share parameters and process two or more inputs to learn a similarity relationship. Instead of directly learning a conventional class boundary, the network learns whether input samples are similar or different. This property makes SNNs suitable for few-shot settings because a new sample can be compared with a small number of reference samples.

Zhu et al., (2022) proposed a few-shot meta-learning based Siamese Neural Network using entropy features for ransomware classification. Their approach used entropy information obtained from ransomware binaries together with image-based information and a pre-trained network. The study evaluated ransomware classification using 1,046 samples across 11 classes and reported a weighted F1-score above 86% (Zhu et al., 2022).

The use of entropy features is relevant because entropy can capture statistical characteristics of binary regions. Such characteristics may contain information associated with packed, encrypted, or otherwise transformed malware content. Combining entropy with learned image features can therefore provide a representation that differs from using visual information alone.

Ahmad Bello et al., (2026) investigate a non-hybrid Siamese Neural Network for ransomware detection under limited-data conditions. Its motivation is to determine whether strong detection performance can be obtained without combining AlexNet and VGG architecture. The experimental work used the RanSAP dataset and evaluated accuracy, precision, recall, F1-score, and AUC. The reported results were 98.33% accuracy, 97.52% precision, 99.16% recall, 98.33% F1-score, and 99.03% AUC.

Dauda et al., (2024) also investigated ransomware detection using a Siamese neural network, reporting 97.67% accuracy, 95.71% precision, 100% recall, 97.31% F1-score, and 100% AUC. Although these results demonstrate the potential of similarity-based learning, the evaluation remains dependent on the dataset and experimental setup, and the extent to which the model generalizes to unseen ransomware samples requires further investigation.

**Datasets and Data Representation**

Dataset selection is a major factor in ransomware detection research. A model can only learn patterns that are represented in its training data. Public malware repositories provide access to malicious samples, but researchers must still address sample diversity, labelling quality, duplication, family distribution, and safe handling.

RanSAP is particularly relevant to the reviewed research. The author (Hirano et al., 2022) introduced RanSAP as an open dataset of ransomware storage access patterns for training machine learning models. The source dissertation uses the Ransap dataset after conversion into grayscale images. This representation permits a Siamese CNN-based model to learn similarity between samples.

Other studies use executable bytes, entropy, API calls, process behaviour, network characteristics, or combinations of these representations. Each representation captures a different aspect of ransomware. Consequently, the choice of representation should be related to the intended detection objective and evaluation environment.

Dataset imbalance and data leakage are additional concerns. If related samples from the same ransomware family appear in both training and test sets, the measured performance may overestimate generalization. Studies should therefore clearly report their splitting strategy and, where possible, evaluate performance on families or variants that are not represented in the training set.

**Evaluation Measures**

Accuracy, precision, recall, F1-score, and AUC are commonly used to evaluate ransomware classification. Accuracy measures the proportion of correctly classified observations as shown in equation 8.1. Precision measures the proportion of predicted ransomware samples that are ransomware as shown in equation 8.2. Recall measures the proportion of actual ransomware samples that are correctly detected as shown in equation 8.3. F1-score provides a combined measure of precision and recall as shown in equation, while AUC describes classification separability across decision thresholds.

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \quad (1)$$

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

$$F1-Score = 2x\ \frac{Recall\ x\ Precision}{Recall+\ Precision} \quad (4)$$

No single metric provides a complete description of a ransomware detector. High accuracy can be misleading when classes are imbalanced. Recall is particularly relevant because a false negative can allow ransomware to remain undetected. Precision is also important because excessive false positives can interfere with legitimate activities. Confusion matrices provide additional information by showing true positives, true negatives, false positives, and false negatives.

Computational performance should also be considered. A model that achieves strong classification performance but requires excessive processing resources may be difficult to deploy in resource-constrained environments. Therefore, execution time, model complexity, hardware requirements, and memory consumption can provide useful complementary information.

**Table 1: Literature Review Table**

| Study | Approach | Research Focus | Dataset / samples | N-way/K-shot setting | Performance metric and evaluation protocol | Limitation/Issue |
|---|---|---|---|---|---|---|
| (Hampton et al., 2019) | Behavioral analysis | Windows ransomware behavior | 14 ransomware families + benign apps (>36M API calls across 30 runs) | Traditional dynamic API frequency analysis | Contingency tables, Chi-Square test, API call frequency distributions | Dynamic analysis requires execution |
| (Arabo et al., 2020) | Process behavior | Ransomware detection | 7 ransomware, 34 malware, 41 benign samples | Rule-based/supervis | Precision, Recall, False Positive Rate (FPR), Latency | Behavior-dependent observations |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | ed process metrics | | |
| (Khan et al., 2020) | Machine learning | Digital DNA representation | Real-world ransomware & goodware samples (VirusTotal/MalwareDB) | Supervised classification with Active Learning | Accuracy, Precision, Recall, F1-Score, Execution time | Feature/data dependence |
| (Hwang et al., 2020) | Dynamic + ML | Two-stage detection | Windows ransomware & normal software API call sequences | Two-stage Markov + Random Forest model | Accuracy (97.3%), FPR (4.8%), FNR (1.5%) via cross-validation | Requires dynamic analysis |
| (Mercaldo, 2021) | Hybrid analysis | Detection and prevention | Static PE features + Dynamic API trace logs | Hybrid static/dynamic classifier | Detection Accuracy, False Positive Rate, Mitigation Response Time | Higher system complexity |
| (Duan et al., 2021) | Few-shot learning | Intrusion detection | CIC-IDS2017 & CSE-CIC-IDS2018 datasets | 5-way 1-shot / 5-way 5-shot | Accuracy, F1-score, Precision, Recall under few-shot support sets | Broad IDS scope |
| (Snell et al., 2019) | Prototypical networks | Few-shot classification | Omniglot & miniImageNet benchmark datasets | 5-way 1-shot / 5-way 5-shot / 20-way 1-shot | Classification Accuracy on unseen query sets across episodes | Requires suitable embeddings |
| (Ale et al., 2020) | Few-shot learning | Android malware | Android APK static opcode / API permission features | 5-way 1-shot / 5-way 5-shot | Accuracy, F1-score across few-shot Android malware families | Different malware domain |
| (Zhu et al., 2022) | FSL + SNN | Ransomware classification | Ransomware entropy graphs from PE binaries | 5-way 1-shot / 5-way 5-shot (Meta-learning episodic setup) | Weighted F1-score (>86%), Precision, Recall, Accuracy | Limited ransomware samples |
| (Qiang et al., 2022) | Few-shot learning | Incremental malware classification | Standard malware benchmarks (e.g., BIG 2015 / VirusShare) | 5-way 1-shot / 10-way 5-shot | Accuracy, Incremental Learning Recall across novel malware classes | Malware rather than ransomware only |
| (Hirano et al., 2022) | RanSAP dataset | Ransomware access patterns | RanSAP: 7 primary ransomware families, 21 variants, 5 benign apps | Not reported | Feature importance analysis, Storage I/O classification accuracy | Dataset scope and representation |
| (Dauda et al., 2024) | Siamese network | Ransomware detection | Public image-converted ransomware binary dataset (130 samples) | 2-way 1-shot / 2-way 5-shot (Pairwise distance comparison) | Accuracy, F1-Score, AUC-ROC under Siamese metric learning | Experimental setting dependent |

**Research Gaps and Future Directions**

The reviewed literature identifies several research gaps. First, many ransomware and malware detection methods depend on relatively large, labelled datasets. This can limit their usefulness for newly emerging variants for which only a few labelled samples are available. Few-shot learning addresses this problem conceptually, but more experiments are needed under clearly defined and reproducible few-shot settings.

Second, studies differ in how they define limited data. Future work should explicitly report N-way/K-shot configurations, support and query sets, pair construction, episodic training procedures, and the number of examples used for each class. Without these details, it is difficult to compare different few-shot models fairly.

Third, evaluation of unseen ransomware families remains important. A model may perform strongly when training and testing samples come from closely related distributions, but this does not necessarily demonstrate its ability to detect a new family. Future studies should therefore include family-level separation or other protocols designed to measure generalization.

Fourth, datasets should become larger and more diverse while preserving the limited-data objective. Ransomware families, goodware categories, collection sources, and time periods should be represented carefully. RanSAP provides a useful dataset for storage access patterns (Hirano et al., 2022) but broader evaluation can strengthen the evidence.

Finally, practical deployment requires consideration of detection speed, computational cost, continuously changing ransomware behavior, and real-world data. Future research should evaluate few-shot ransomware detection in operational environments and investigate whether models can adapt when new variants appear.

## CONCLUSION

Ransomware remains a significant cybersecurity problem, and automated detection continues to require methods that can identify malicious samples efficiently. ML and DL have

provided important improvements in automated detection, but their dependence on large, labelled datasets remains a challenge. Learning a few-shots provides a data-efficient alternative by enabling models to learn from a limited number of examples.

Siamese Neural Networks are particularly relevant because they learn similarity relationships and can compare new samples with a small set of reference examples. Existing research has demonstrated the potential of few-shot and Siamese approaches for malware and ransomware detection. However, differences in datasets, representations, few-shot configurations, and evaluation procedures limit direct comparison between studies. Future research should therefore emphasize standardized few-shot experiments, diverse datasets, and evaluation on unseen ransomware families, computational efficiency, and real-world validation. These directions can strengthen the evidence for data-efficient ransomware detection and support the development of models capable of adapting to emerging threats.

**REFERENCES**

Aggarwal, C. (2019). Advanced Topics in Neural Networks and Deep Learning. https://doi.org/doi.org/10.1007/9783319944630

Ahmad Bello, U., Bello Tambuwal, A., & Tukur Balarabe, A. (2026). Few Shot Learning For Ransomware Detection Using Siamese Neural Network. Fudma Journal of Sciences, 10(12), 85–93. https://doi.org/10.33003/fjs-2026-1012-5348

Ale, L., Li, L., Kar, D., Zhang, N., Palikhe, A., & Christi, C. (2020). Few-Shot Learning to Classify Android Malwares. 1001–1007. https://doi.org/10.1109/ICSIP49896.2020.9339429

Arabo, A., Dijoux, R., Poulain, T., & Chevalier, G. (2020). Detecting Ransomware Using Process Behavior Analysis Detecting Ransomware Using Process Behavior Analysis. Procedia Computer Science, 168(2019), 289–296. https://doi.org/10.1016/j.procs.2020.02.249

Catak, F. O., Ahmed, J., Sahinbas, K., & Khand, Z. H. (2021). Data augmentation based malware detection using convolutional neural networks. 1–26. https://doi.org/10.7717/peerj-cs.346

Dauda, M. K., Ahmad, I., & Alassafi, M. O. (2024). ENHANCING RANSOMWARE DETECTION USING SIAMESE NETWORK. April. https://doi.org/10.59018/022438

Davidian, M., Kiperberg, M., & Vanetik, N. (2024). Early Ransomware Detection with Deep Learning Models. Future Internet. https://doi.org/doi.org/10.3390/fi16080291

Duan, R., Li, D., Tong, Q., Yang, T., Liu, X., & Liu, X. (2021). A Survey of Few-Shot Learning : An Effective Method for Intrusion Detection. 2021. https://doi.org/10.1155/2021/4259629

Ferdous, J., Islam, R., Mahboubi, A., & Islam, Z. (2024). AI-Based Ransomware Detection : A Comprehensive Review. IEEE Access, 12(October), 136666–136695. https://doi.org/10.1109/ACCESS.2024.3461965

Hampton, N., Baig, Z., & Zeadally, S. (2019). Journal of Information Security and Applications Ransomware behavioural analysis on windows platforms. 40, 44–51. https://doi.org/10.1016/j.jisa.2019.02.008

He, K., & Xiangyu, Z. (2022). Deep Residual Learning for Image Recognition. Computer Vision Foundation, 1–9.

Herbert, F. (2019). An Introduction to Neural Networks - Thou shalt not make a machine to counterfeit a human mind. https://doi.org/doi.org/10/1007/9783319944630

Hirano, M., Hodota, R., & Kobayashi, R. (2022). Forensic Science International : Digital Investigation RanSAP : An open dataset of ransomware storage access patterns for training machine learning models. Forensic Science International: Digital Investigation, 40, 301314. https://doi.org/10.1016/j.fsidi.2021.301314

Hwang, J., Kim, J., Lee, S., & Kim, K. (2020). Two - Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques. Wireless Personal Communications, 112(4), 2597–2609. https://doi.org/10.1007/s11277-020-07166-9

Khammas, B. M. (2020). Ransomware Detection using Random Forest Technique. ICT Express, 6(4), 325–331. https://doi.org/10.1016/j.icte.2020.11.001

Khan, F., Ncube, C., Ramasamy, L. K., Kadry, S., & Nam, Y. (2020). A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning. IEEE Access, 8, 119710–119719. https://doi.org/10.1109/ACCESS.2020.3003785

Krizhevsky, B. A., Sutskever, I., & Hinton, G. E. (2012). ImageNet Classification with Deep Convolutional Neural Networks. https://doi.org/10.1145/3065386

Kumar, I. (2023). Emerging Threats in Cybersecurity: A Review Article. 1–9. http://bluemarkpublishers.com/index.php/IJANS%0A%7C

Liu, S., & Deng, W. (2015). Very Deep Convolutional Neural Network Based Image Classification Using Small Training Sample Size. https://doi.org/doi.org/15/978-1-4799-6100-9/15/

Mercaldo, F. (2021). A framework for supporting ransomware detection and prevention based on hybrid analysis. Journal of Computer Virology and Hacking Techniques, 17(3), 221–227. https://doi.org/10.1007/s11416-021-00388-w

Mohammadi, F. G., Amini, M. H., & Arabnia, H. R. (2020). An Introduction to Advanced Machine Learning : Meta Learning Algorithms , Applications and Promises.

Neal, R. M. (2007). Pattern Recognition and Machine Learning. Technometrics, 49(3), 366–366. https://doi.org/10.1198/tech.2007.s518

Qiang, Q., Cheng, M., Hu, Y., Zhou, Y., Sun, J., Ding, Y., Qi, Z., & Jiao, F. (2022). An Incremental Malware Classification Approach Based on Few-Shot Learning. ICC 2022 - IEEE International Conference on Communications, 2682–2687. https://doi.org/10.1109/ICC45855.2022.9838295

Ramesh, G., & Menen, A. (2020). Automated dynamic approach for detecting ransomware using finite-state machine. Decision Support Systems, 138(July), 113400. https://doi.org/10.1016/j.dss.2020.113400

Sharma, S., & Singh, S. (2023). Ransomware Threat , Attack , Prevention and Cure on Window Platform Texture-Based Automated Classification of Ransomware. Journal of The Institution of Engineers (India): Series B, 102(1), 131–142. https://doi.org/10.1007/s40031-020-00499-w

Shashikant, Y., Harsh, J., Sumedh, M., Joshi, N., Pradeep, K., Aarti, G., & Agarkar, A. (2021). Signature-less ransomware detection and mitigation. Journal of Computer Virology and Hacking Techniques, 0123456789. https://doi.org/10.1007/s11416-021-00384-0

Snell, J., Swersky, K., & Zemel, R. (2019). Prototypical Networks for Few-shot Learning. 31st Conference on Neural Information Processing Systems (NIPS 2019), Long Beach, CA, USA., Nips.

Song, Y., Wang, T., Mondal, S. K., & Sahoo, J. P. (2022). A Comprehensive Survey of Few-shot Learning : Evolution , Applications , Challenges , and Opportunities. 1–24.

Sreelaja, N. K. (2021). Ant Colony Optimization based Light weight Binary Search for efficient signature matching to filter Ransomware. Applied Soft Computing, 111, 107635. https://doi.org/10.1016/j.asoc.2021.107635

Sutton, R. S., & Barto, A. G. (2012). Reinforcement learning_Peter. Learning, 3(9). http://incompleteideas.net/sutton/book/the-book.html%5Cnhttps://www.dropbox.com/s/f4tnuhipchpkgoj/book2012.pdf

Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., Erhan, D., Vanhoucke, V., & Rabinovich, A. (2014). Going Deeper with Convolutions.

Tang, F., Ma, B., Li, J., Zhang, F., Su, J., & Ma, J. (2020). Computers & Security RansomSpector : An introspection-based approach to detect crypto ransomware. Computers & Security, 97, 101997. https://doi.org/10.1016/j.cose.2020.101997

Tran, T. K., Sato, H., & Kubo, M. (2019). Image-based Unknown Malware Classification with Few-Shot Learning Models.

U. Z oora, M. Rajarajan, Z. P. A. K. (2022). Zero-day ransomware attack detection using deep contractive autoencoder and voting based ensemble classifier. 52, 13941–13960. https://doi.org/10.1007/s10489-022-03244-6

Yang, A., Lu, C., Li, J., Huang, X., Ji, T., & Li, X. (2023). Application of meta-learning in cyberspace security : a survey. Digital Communications and Networks, 9(1), 67–78. https://doi.org/10.1016/j.dcan.2022.03.007

Zhu, J., Jang-Jaccard, J., Singh, A., Welch, I., AL-Sahaf, H., & Camtepe, S. (2022). A few-shot meta-learning based siamese neural network using entropy features for ransomware classification. Computers and Security, 117. https://doi.org/10.1016/j.cose.2022.102691

Zuhair, H., & Selamat, A. (2020). applied sciences A Multi-Tier Streaming Analytics Model of 0-Day Ransomware Detection Using Machine Learning.

©2026 This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International license viewed via https://creativecommons.org/licenses/by/4.0/ which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is cited appropriately.