FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 12, June, 2026, pp 85 – 93
DOI: https://doi.org/10.33003/fjs-2026-1012-5348

Few Shot Learning For Ransomware Detection Using Siamese Neural Network

***[1]Usman Ahmad Bello, [2]Abubakar Bello Tambuwal and [1]Anas Tukur Balarabe**

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

*Corresponding authors' email: usmanabello002@gmail.com

Received: 24th June 2026
Accepted: 17th July 2026
Published: 28th July 2026

ABSTRACT
Ransomware poses a threat to the availability, confidentiality and integrity of an individual's, organization, or a company's sensitive data. The attack involves locking digital data and holding its hostage until the attacker receives ransom. Due to the rapid spread of devices and interconnectedness, the increasing prevalence of ransomware attacks is concerning. Several research have been proposed, tested, evaluated and published to improve the methodology and implementation of ransomware detection methods, from behavioral, dynamic to static-based detection. Much research has been focusing on machine learning and deep learning to enhance detection accuracy. However, deep learning, with its advantage over traditional techniques, is hindered by its dependence on large number of datasets, often referred to as "data hunger". An emerging approach called few-shot learning (FSL) method is being used in various domains especially in cyber security due to its effectiveness in cases with limited data. This study investigates the usefulness of FSL in ransomware detection and explores the performance of this model with less data, utilizing its strengths to create a robust, unified model to accurately detect and classify ransomware and good wares. Utilizing the ransomware access pattern (Ransap) dataset converted into grayscale images, the proposed techniques improved the classification performance. Specifically, accuracy increased from 97.69% to 98.33%, precision from 95.71% to 97.52%, and the F1-score from 97.31% to 98.33%. In addition, the model achieved a recall of 99.16% and an AUC of 99.03%, compared with the benchmark values of 100% for both recall and AUC. This is an unprecedented achievement and a significant breakthrough in the application of FSL within the domain of ransomware detection.

Keywords: Deep Learning (DL), Few Short Learning (FSL); Machine Learning (ML); Ransomware Detection (RD)

INTRODUCTION

Cybersecurity is a critical field that protects digital devices, systems, networks, and sensitive data from unauthorized access, attacks, and damage (Davidian et al., 2024). It encompasses a broad range of practices, technologies, and strategies designed to safeguard the confidentiality, integrity, and availability of information (Davidian et al., 2024). Cybersecurity is essential for protecting personal information, financial data, intellectual property, and critical infrastructure from cyber threats in an increasingly digital world, such as hacking, phishing, ransomware, and advanced persistent threats (Sciences, 2023). One of the primary functions of cybersecurity is the implementation of robust defence attention mechanisms that help detect and prevent unauthorized access to sensitive information and mitigate potential damage from cyber incidents (Davidian et al., 2024). Approximately 75% of businesses fell prey to ransomware attacks in 2024, the study (Source, 2024) reported. This is an increase from the previous five years (2019 – 2023) and the highest figure noted so far (Source, 2024). The amount of money lost to these attacks is overwhelming, and the possibility of an increase in these attacks is concerning. This emphasizes the need for efficient methods to prevent, classify and detect ransomware attacks to secure sensitive data and facilitate decision making by companies, individual, industries, and organizations. Several research have been proposed, implemented, tested and evaluated by (Arabo et al., 2020; Cheng et al., 2019; Hampton et al., 2018; Hwang et al., 2020; Khan et al., 2020; Mercaldo, 2021; Parkar, 2021; Razaulla et al., 2023; Sreelaja, 2021; Yang et al., 2023; Yilmaz et al., 2021) to improve ransomware detection accuracy. However, there is lack of clear evaluation of which ransomware detection methods is best suited per giving detection task. Some current literature rely on large amount of dataset to improve their detection accuracy as contain in (Ale et al., 2020; Duan et al., 2021; Qiang et al., 22; Snell et al., 2017; Zhu et al., 2022). While ML models are efficient for classification and DL is useful in feature extraction in a complex pattern, they are inefficient in generalizing ransomware attacks due to limited data. Therefore, FSL proposed in this study and emerged as an effective approach for domains where data limited. The goal of this research is to study and investigate how FSL model can perform task with less data and less complexity in a low computational power environment under the constraint of a small sample dataset. These goals will achieve by exploring innovative training methods that can enhance model performance by incorporate FSL to improve detection accuracy under constraint of small dataset focusing on hyper parameter fine-turning.

The result of this research may lay the grounds to explore new gaps for researchers in the future and bring to the front the strengths and the weaknesses of these architectures. It will help them develop a FSL model tailored for ransomware detection. This finding may also establish a new benchmark in performance and contribute to the field of cyber-security.

The study by (Hwang et al., 2020) proposes a two-stage detection method for ransomware detection that focuses on controlling false negative error rates (FNR) under the nominal control of false positive error rate (FPR). This method is based on the sequential characteristic of Windows OS APIs which uses Markov and the Random Forest models, these detection methods are statistical ML techniques, to identify ransomware by looking at all the traits in addition to WOS API call. The authors used ransomware and benign wares dataset from virus share and softonic respectively for the research. The paper reports a 97.3% detection rate. The paper highlights the major challenge of mimicking the behaviour of benign ware by ransomware. Ransomware designers are smart enough to mimic the behaviour of benign ware and can even split the ransomware activity into an independent process that then aggregated later to accomplish an attack, making it harder to detect.

A proposed method of supervised learning (SL) by (Sreelaja, 2021) uses a deep learning-based detector called DeepRan. It employs a BiLSTM FC in an enterprise network using host logging data to detect ransomware attacks before they fully deployed on the victim host. The paper recorded a 99.8% detection rate using an experimental testbed for host log data collection. However, the limitation of dynamic detection related to time-consuming and only few ransomware variants can track at the time of the experiment, which cannot overlook. Therefore, the accuracy is specific to the variant that captured during the experiment only. The accuracy cannot generalize since it only uses two user data, not a particular section or department.

The study by (Qiang et al., 2022; Lo et al., 2019) have utilized meta-learning (Mle) to address the issue of classifying malware classes with only a few known samples. These models can adapt and generalize new tasks with unknown data effectively, using their learned knowledge gained during training time. The study achieved 92.4% and 95.3% accuracy in classifying malware in the Mallmg dataset using 5-way-1 shot and 5-way 4-shot method, respectively. The latter paper, which used a cosine similarity function, was able to classify novel malware families with an average accuracy of 92.52% and 93.78% on 5-shot and 10-shot, respectively. However, noise can poorly impact the performance of these models. Therefore, reducing the impact of noise and extending the idea to detect and classify ransomware could cover the way for further contributions to the public.

The study by (Zhu et al., 2022), found that there is a high demand for ransomware defence solutions that can quickly prevent, detect and classify different types of cyber-attack. However, the limited availability of cyber security datasets containing ransomware samples has identified as a major barrier to developing effective DL solutions. To address this, they proposed a FS meta-learning-based SN that uses the entropy feature directly obtained from ransomware files to retain more features associated with different ransomware attacks. The performance of the model evaluated using F1-score, and when compared to other state-of-the-art models, it achieved an F1-score of 86%.

The work of (Mercaldo, 2023) proposed a hybrid framework for detecting and preventing ransomware. The paper suggests using static analysis to limit and identify the critical processes that will be monitored by dynamic analysis during run-time. The work claims that no previous work has been done on preventing ransomware except for detection and proposes preventive measures that are already present in operating systems and might not be feasible for large organizations.

Despite the significance contribution made by the researchers of the reviewed work so far, it is evident enough less attempt has been made to use FSL including limited availability of datasets, high training costs in terms of time, significant computational and memory utilization, experimental parameters architectural complexities, and performance issues where to choose between accuracy and speed. Notwithstanding, it is impressive that researchers understand how these important architecture works as compared to other traditional ML and DL techniques in terms of detection performance. This is the gap that this research intends to fill.

Table 1: Literature Review of Existing Methods

Ref.	Objective	Methodology	Dataset Used	Features Used	Algorithms Used	Tools	Evaluation Metrics	Result	Limitations
Hwang et al. (2020)	To reduce false positive and false negative rates in ransomware detection.	Two-stage hybrid detection using API sequence modelling and machine learning.	Windows ransomware dataset (not specified).	Sequential Windows API calls.	Markov Model and Random Forest.	Windows API monitoring tools.	Accuracy, FPR, FNR.	97.3% accuracy.	High false negative rate (20%) despite good accuracy.
Mercaldo (2023)	To prevent and detect ransomware while reducing monitoring overhead.	Hybrid static and dynamic analysis framework.	Not specified.	Static process information and runtime behaviour.	Hybrid framework combining static and dynamic analysis.	Not specified.	Not specified.	Performance not reported.	Proposed prevention mechanism already exists in Microsoft OS; lacks scalability and evaluation metrics.
Zhu et al. (2022)	To classify ransomware using limited training samples.	Few-shot learning with transfer learning.	Ransomware binary dataset (not specified).	Entropy features extracted from ransomware binaries.	Siamese Neural Network with pre-trained VGG16.	VGG16 framework.	F1-score.	86% F1-score.	Accuracy not reported; limited evaluation metrics provided.
Sreelaja (2021)	To detect ransomware attacks before deployment on victim systems.	Host log analysis using deep learning.	Experimental host log data from bare-metal servers.	Host logging data.	BiLSTM-FC (DeepRan).	Experimental testbed.	Accuracy.	99.8% accuracy.	Evaluated using only two user logs; lacks validation on public datasets; limited generalizability.

Ref.	Objective	Methodology	Dataset Used	Features Used	Algorithms Used	Tools	Evaluation Metrics	Result	Limitations
Qiang et al., (2022)	To improve classification performance on imbalanced malware image datasets.	Transfer learning using weighted loss functions.	Malware image dataset.	Malware image representations.	Convolutional Neural Network (CNN) with weighted SoftMax loss.	Pre-trained CNN model.	Accuracy.	92.4% and 95.3% accuracy	Evaluated on malware rather than ransomware; performance improvement still needed.
Lo et al. (2019)	To classify malware families using deep learning.	Transfer learning for malware image classification.	Malware samples (not specified).	Malware image features.	Xception CNN.	Xception architecture.	Accuracy.	92.52% and 93.78% on 5-shot and 10-shot	Focuses on malware classification instead of detection; dataset details and additional evaluation metrics are absent.

MATERIALS AND METHODS

This research follows a step-by-step experimental approach to achieve its aim and objectives, which structured around five (5) different key stages. Each build upon the output of the previous one, ensuring a clear and systematic methodology.

This study utilizes a publicly available dataset obtained from the kaggle.com repository, specifically the Ransap 2022 (https://www.kaggle.com/datasets/hiranomanabu/ransap-2022-ransomware-behavioral-features) ransomware behavioural features dataset. The dataset contains both ransomware and normal records derived from storage access patterns. For experimental feasibility and computational efficiency, a subset of 3,000 records selected. Furthermore, the raw tabular data transformed into image representations to enable compatibility with the FSL model. The pre-processing stage involves steps, including data cleaning, data augmentation, normalization, feature engineering, and label encoding. The dataset structured appropriately to suit the FSL model. Furthermore, the processed data randomly divided into training and testing sets using train/test split to ensure unbiased model evaluation. Model development builds an FSL-based detection model optimized with Adam optimizer, call-back function, learning rate, random seed to enhance learning efficiency and convergence. Model training and validation: Employs supervised learning with an 80:10:10 train-test-validation split and cross-validation. Performance refined based on evaluation metrics. Evaluation metrics: Five metrics used, accuracy, precision, recall, F1-score, and AUC to provide a comprehensive assessment of detection ability.

The research design focuses on the comparative analysis of FSL model. This approach selected due to its effectiveness in handling limited data and its applicability to cyber security tasks, where labelled samples often limited.

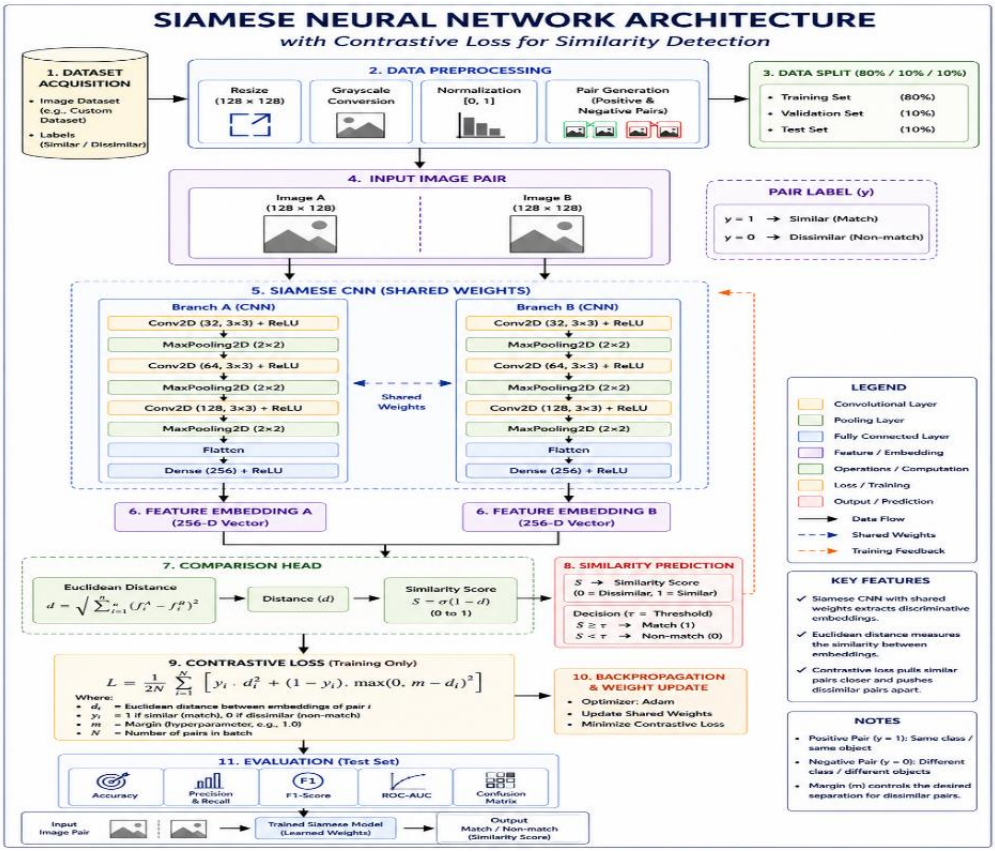

Figure 1: FSL Model System Architecture

The overall goal of this research is to study, investigate how FSL model can perform tasks with less data and complexity.

Technologies Used

Tools, and technologies have been employed in conducting the experiment and evaluating the performance of this model. For the hardware, a laptop with Intel Core i7 (11th Gen), 32GB RAM, 1TB SSD storage, Windows 11 OS, and Python as programming language was utilized. Google colab with notebook used as a programming environment. Libraries such as numpy, pandas, matplotlib, scikit-learn, scikit-image, keras and OpenCV (cv2) also used, as highlighted in the next section.

Dataset

The dataset used in this research contains 3,000 samples row data, which converted into 100 images representing both ransomware and benign files. The data processed using a custom CSV-to-image conversion function designed specifically for ransomware detection. The resulting images saved in .png format and subsequently uploaded to a Google Drive folder linked to the programming environment for further analysis. The final dataset structure consists of multiple rows, with each row representing an individual image and its corresponding label (benign or ransomware).

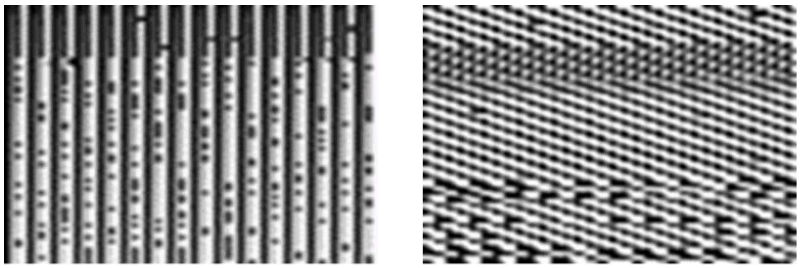

Figure 2: Sample Images for Benign

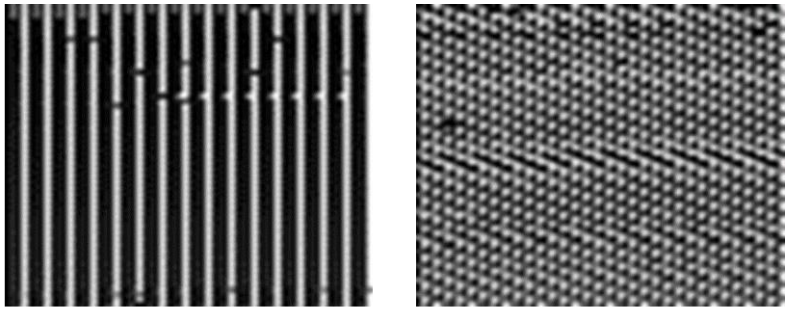

Figure 3: Sample Images for Ransomware

Evaluation Metrics

Accuracy is a fundamental evaluation metric for measuring the overall performance of a classification model (Farhadpour et al., 2024). In this dataset, accuracy measures the proportion of correctly predicted instances out of the total instances from giving samples (ransomware or benign). A high accuracy score indicates that the model is effective in making correct predictions across both ransomware and benign classes, thereby providing a reliable measure of its overall performance (Farhadpour et al., 2024).

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

Precision is an essential evaluation metric used to measure the effectiveness of a ransomware detection model in accurately identifying true positive. It defined as the ratio of correctly predicted positive instances ransomware to the total number of instances predicted as positive by the model. A high precision score indicates a low rate of false positives, meaning that benign samples rarely misclassified as ransomware, thereby enhancing the reliability of the model (Farhadpour et al., 2024).

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

Recall, also referred to as sensitivity or the true positive rate, measures the ability of a ransomware detection model to correctly identify all actual ransomware instances within the dataset. It defined as the ratio of correctly predicted ransomware cases to the total number of actual ransomware cases. A high recall score indicates that the model effectively detects most ransomware instances, minimizing the occurrence of false negatives (Maxwell et al., 2021)

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

The F1-score is a composite evaluation metric that balances both precision and recall, providing a more comprehensive measure of a ransomware detection model's performance. It defined as the harmonic mean of precision and recall, ensuring that both false positives and false negatives considered. This metric is particularly useful when there is a need to achieve a balance between accurately identifying ransomware instances and minimizing missed detections (Farhadpour et al., 2024).

$$F1 - Score = \frac{2\ X\ TP}{2\ X\ TP+FP+FN} \quad (4)$$

The Receiver Operating Characteristic - Area under the Curve (ROC-AUC) is a robust evaluation metric used to assess the ability of a ransomware detection model to distinguish between ransomware and benign classes across classification thresholds. It captures the trade-off between the True Positive Rate (TPR), also known as sensitivity, and the False Positive Rate (FPR), providing a threshold-independent measure of classification performance. A higher ROC-AUC value indicates better model discrimination, meaning the model is

more capable of correctly distinguishing ransomware instances from benign activities.

The ROC curve is a graphical representation that plots the True Positive Rate (TPR) against the False Positive Rate (FPR) at various threshold levels. The Area under the Curve (AUC) quantifies the overall performance of the model, where a value of 1.0 represents perfect classification, while a value of 0.5 indicates no discriminative ability (equivalent to random guessing).

$$TPR = \frac{TP}{TP+FN} \quad (5)$$

Table 2: Experimental Parameters Setup

Parameter	Experimental Setup
Operating System	Windows 11
Sample Size	100 images
Augmentation Techniques	Rotation, flip and zoom
Parameters	Input: 224×224; Batch size: 8 - 32; LR: 1e-2 to 1e-4; Optimizer: Adam; Epochs: 50; Layers: 3 -10 conv layers; Filters: 32 - 64 - 128; Kernel: 3×3; Dropout: 0.3-0.5; Strong data augmentation, Weight decay: 1e-4; Early stopping, batch-size: 8
Activation Function	Relu
Optimizer	Adam
Learning Rate	1e-2 - 1e-4
Number of runs	multiple to account for variance
Loss Function	Euclidean distance and contrastive loss
Train/validation/test splits	80%, 10%, 10%
Training Time	1,000 secs
Evaluation Metric	Accuracy, Precision, Recall, F1-score, AUC

RESULTS AND DISCUSSION

This section discusses the result of the entire experiment. The study utilizes a FSL based on SN for ransomware detection task. The model trained to learn similarity between pairs of samples enabling it to effectively distinguish between ransomware and benign behaviours, even with limited data.

Accuracy

As shown in Figures 4, in the first 20 epochs, the SN had already achieved accuracy of 40.00% continuing up to 70.50% at 40 epochs. The models' detection ability continued to improve, exceeding 90.00% at 45 epochs, while achieving the highest accuracy of 98.33% at 50 epochs.

The accuracy of 98.33% confirms that the model correctly classifies the vast majority of ransomware and benign samples. The precision of 97.52% indicates a low false-positive rate, meaning most instances predicted as ransomware are truly malicious. The 99.16% recall is particularly critical in ransomware detection, as it demonstrates the strong ability to correctly identify malicious samples and minimize false negatives. The F1 score of 98.33% reflects a well-balanced trade-off between precision and recall. Finally, the AUC of 99.03% demonstrates excellent separability between ransomware and benign classes, confirming that the learnt similarity space effectively distinguishes between the two categories. Overall, the SN achieves high detection performance with stable convergence, making it highly suitable for ransomware detection in few-shot learning scenarios.

Table 1: Performance Metrics Results

Performance Metrics	Result (%)
Accuracy	98.33
Precision	97.52
Recall	99.16
F1-Score	98.33
AUC	99.03

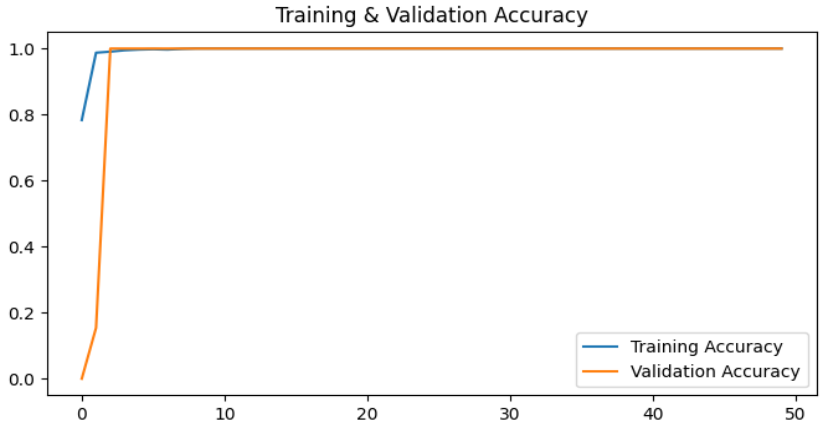

Figure 4: SN Training Accuracy Curve for 50 epochs

Figure 5 gives insight into the SN model training loss. At first 20 epochs, the loss dropped to 10.20%. The same trend was maintained at the 35th epochs, where the model dropped to 3.00% at the 50 epoch, standing at 0.5%. The consistency suggests robust training and prediction irrespective of the epochs used; the model learned to reduce error as the epochs increased.

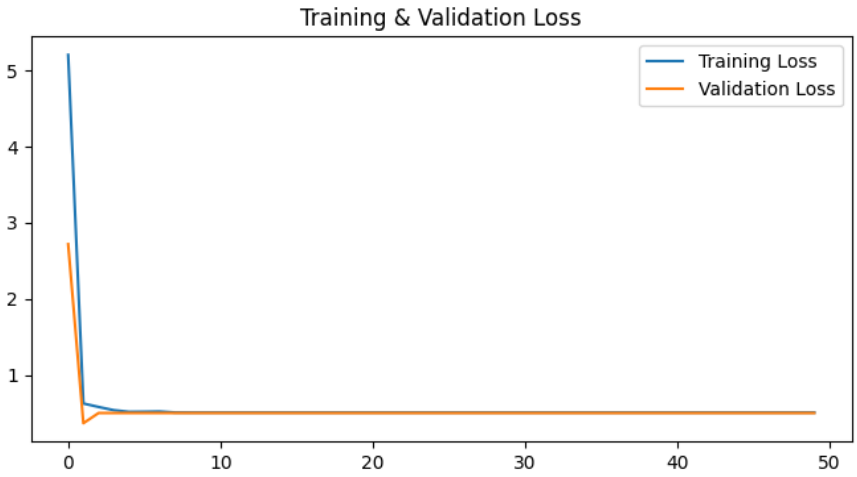

Figure 5: SN Training Loss Curve for 50 epochs

Similarly, influenced by the complexity of its dual-branch architecture the SN training time is because of the computational cost of processing paired inputs for similarity learning. By comparing feature embeddings extracted from two identical networks with shared weights, this model learns patterns which introduces additional computation during training, which may also affect overall performance and efficiency of the trained model. The SN took approximately 1,000 seconds to train. This training time reflects the computational demand of distance-based similarity computation and pairwise feature extraction. Despite this, the model demonstrated stable learning behavior and effective discrimination between similar and dissimilar ransomware and benign.

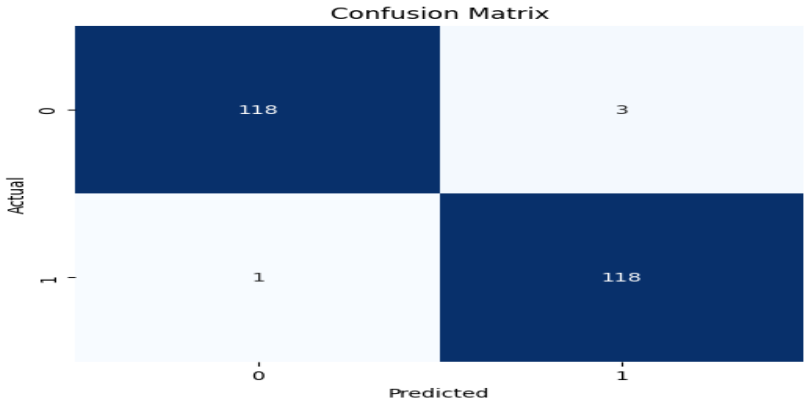

Figure 6: Confusion Metrics for SNNs Model

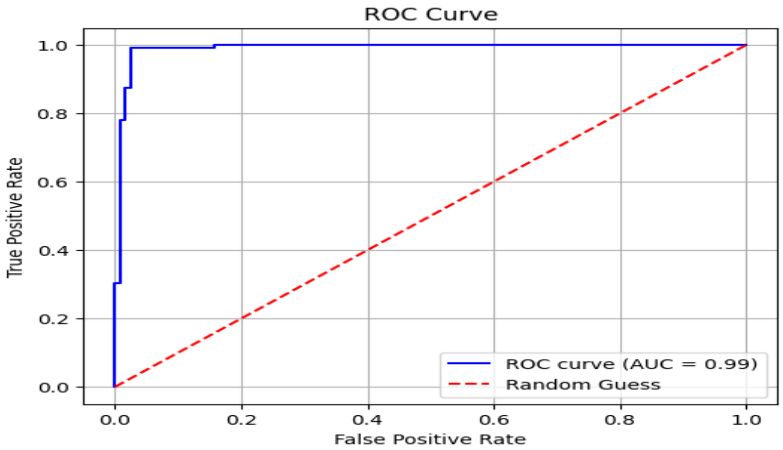

Figure 7: AUC Metrics for SNNs Model

Comparison between Benchmark study and Proposed Research

This section compares an existing benchmark system with the proposed research experiment, focusing on dataset characteristics, domain specific, training parameters configurations, computational environment, and model performance results.

The benchmark system (Dauda et al., 2024) used a public dataset with 130 images. It employed SN with hybrid architectures combining AlexNet and VGG family. Although the hardware, experimental parameter, OS version, and execution time not reported, the model achieved peak accuracy of 97.67%, 95.71% (precision), 100% (recall), 97.31% (F1-score) and 100% (AUC), with Precision and AUC delivering the best results among the evaluated metrics. In comparison, our proposed work used a public dataset converted from row data to images comprising 100 images under controlled experimental conditions. The images were also resized to 224 × 224 to match the experimental setup. The model trained in a low-computational environment. The model demonstrated consistent performance and trained for 50 epochs at random search, recording distinct execution times: 1,000 seconds. Despite limited computational resources and a smaller dataset, the proposed approach outperformed the benchmark. Specifically, the accuracy of 98.33%, 97.52% (precision), 98.33% (F1-score) and acceptable execution time, considering the dataset and hardware constraints.

Table 3: Comparison between Benchmark study and Proposed Research

Parameter	Benchmark Study (Dauda et al., 2024)	Proposed Research
Dataset Type	Public dataset	Public dataset
Dataset Size	130 images	100 images
Image Resolution	Not specified	224 × 224
Model Architectures	Siamese Network Combined with VGG and Alexnet	Siamese Network
Training Strategy	From scratch	From scratch
Hardware Configuration	Not specified	Intel Core i7 (11th Gen), 32GB RAM, 1TB SSD storage
Operating System	Not reported	Windows 11
Number of Epochs	100	50
Batch Size	86	8
Training Time	Not reported	1,000 secs
Loss Function	Contrastive loss	Euclidean distance and contrastive loss
Evaluation Metric	Accuracy, Precision, Recall, F1-score, AUC	Accuracy, Precision, Recall, F1-score, AUC
Best Result Achieved	97.67% (Acc), 95.71% (precision), 100% (recall), 97.31% (F1-score) and 100% (AUC)	98.33 % (Acc), 97.52% (precision), 99.16% (recall), 98.33% (F1-score) and 99.03% (AUC)

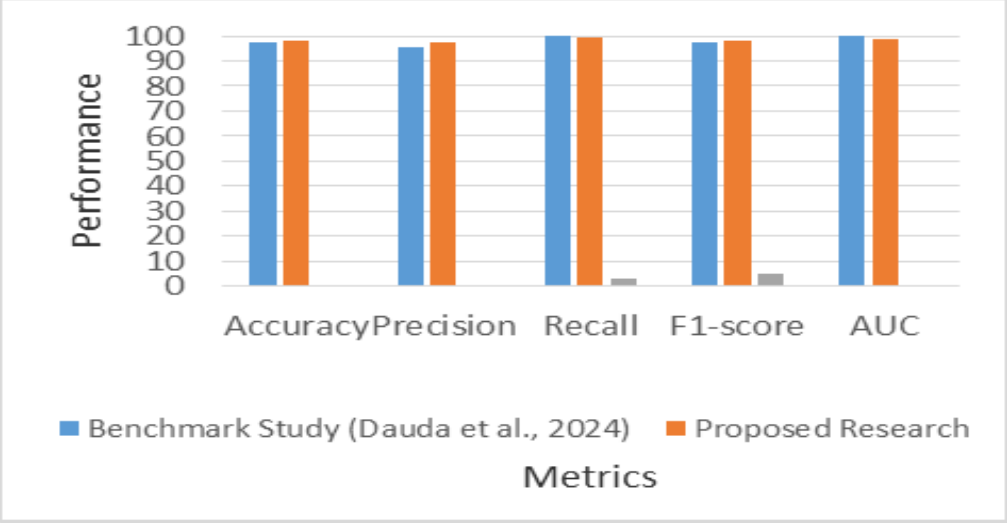

Figure 8: Comparison Results between Benchmark and Proposed Research

Contribution

The following points outline the unique and impactful contributions of this study to the field ransomware detection cyber security.

Our research developed a specialised pipeline to convert the dynamic behavioural applications of seven distinct ransomware families into specialized image representations using CSV to image function. This contribution bridges the gap between behavioural analysis and computer vision, allowing for the use of DL spatial detection techniques to identify malicious execution patterns.

Another core contribution of this work is the successful implementation of a SN architecture tailored for small-scale datasets. Using a dual-stream architecture to learn similarity metrics rather than simple classification, we demonstrated that high-accuracy detection is achievable even when limited samples from a specific ransomware family are available focusing on hyperparameter optimization.

Lastly, we provided a comprehensive framework of experimental parameters specifically tuned for ransomware detection. Through rigorous optimization of critical hyper parameters including Euclidean distance, contractive loss, learning rate, optimizer, data augmentation, callback function, train/test/validation split, batch size, and execution time, we achieved a model state that balances sensitivity and specificity, ensuring robust performance in detecting evolving threats.

CONCLUSION

Through careful hyperparameter fine-tuning and architectural configuration, the proposed model achieved strong ransomware detection performance despite operating on a small dataset and modest hardware. The results further show that a simpler SN architecture can perform competitively compared to more complex hybrid models that developed by incorporating the architectural principles of AlexNet and features of the VGG configuration from the benchmark research. This indicates that increased structural complexity does not necessarily guarantee superior performance which balance between the speed and accuracy allowing the researcher to choose among. Overall, the findings confirm that proper selection of models, systematic optimization, and rigorous evaluation are key factors in achieving reliable and efficient ransomware detection.

REFERENCES

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). ScienceDirect ScienceDirect ScienceDirect 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

Cheng, G., Guo, C., & Tang, Y. (2019). dptCry : an approach to decrypting ransomware WannaCry based on API hooking. CCF Transactions on Networking, 0123456789. https://doi.org/10.1007/s42045-019-00024-8

Davidian, M., Kiperberg, M., & Vanetik, N. (2024). Early Ransomware Detection with Deep Learning Models.

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

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

Hampton, N., Baig, Z., & Zeadally, S. (2018). Journal of Information Security and Applications Ransomware behavioural analysis on windows platforms. 40, 44–51. https://doi.org/10.1016/j.jisa.2018.02.008

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

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

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

Parkar, P. (2021). A Survey on Cyber Security IDS using ML Methods. ICICCS.

Qiang, Q., Cheng, M., Hu, Y., Zhou, Y., Sun, J., Ding, Y., Qi, Z., & Jiao, F. (n.d.). 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

Raza, D. M., & Victor, D. B. (2021). Crime Using Random Forest. Proceedings of the International Conference on Artificial Intelligence and Smart Systems (ICAIS-2021), 7, 980–987.

Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Member, S., Mansoor, W., & Member, S. (2023). The Age of Ransomware : A Survey on the Evolution , Taxonomy , and Research Directions. IEEE Access, 11(April), 40698–40723. https://doi.org/10.1109/ACCESS.2023.3268535

Sciences, N. (2023). Emerging Threats in Cybersecurity: A Review Article. 1–9.

Snell, J., Swersky, K., & Zemel, R. (2017). Prototypical Networks for Few-shot Learning. Nips.

Source, S. (2024). Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023. 1–4.

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

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

Xin, C., Liu, Z., Zhao, K., Miao, L., Ma, Y., Zhu, X., Zhou, Q., Wang, S., Li, L., Yang, F., Xu, S., & Chen, H. (2024). An improved transformer network for skin cancer classification. Computers in Biology and Medicine, 149(June), 105939. https://doi.org/10.1016/j.compbiomed.2022.105939

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

Yilmaz, Y., Cetin, O., Arief, B., & Hernandez-castro, J. (2021). Journal of Information Security and Applications Investigating the impact of ransomware splash screens.

Journal of Information Security and Applications, 61(July), 102934. https://doi.org/10.1016/j.jisa.2021.102934

Zhang, H., & Zhang, S. (2024). Focaler-IoU: More Focused Intersection over Union Loss. 1–4.

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