Journal of Engineering, Management and Information Technology

ASPUR PUBLISHING

Vol. 03, No. 04 (2025) 231-240, doi: doi:10.61552/JEMIT.2025.04.001 - http://jemit.aspur.rs

DEFENCE-AGAINST RANSOMWARE: SMART TECHNIQUE TO DETECT AND MITIGATE ATTACKS

Rahul Papalkar [1]
Abrar S. Alvi
Jayendra Jadhav
Moumita Pal
Pallavi Morey
Vivek Thorat

Received 11.02.2024.
Revised 17.04.2024.
Accepted 22.05.2024.

Keywords:

Ransomware Detection, Convolutional Neural Network (CNN), Machine Learning, Optimization, Performance Evaluation, Cybersecurity.

Original research

A B S T R A C T

Innovative AI-powered solutions have emerged in the never-ending fight against ransomware, driven by the need for more precise detection approaches. Here, we present a Convolutional Neural Network (CNN) design that has been fine-tuned for the purpose of more accurately identifying ransomware attacks. We test the suggested model against state-of-the-art machine learning techniques and assess its performance through extensive experimentation and comparison analysis. In addition to our suggested CNN-based model, our evaluation covers four well-known machine learning algorithms: ANN, Random Forest, Decision Tree, and SVM . To evaluate the effectiveness of each method, performance measures including as accuracy, precision, recall, and F1-score are carefully examined. Our comparison analysis shows encouraging outcomes. While traditional ML algorithms do decent work—Random Forest in particular stands out—our suggested CNN-based model outperforms them all across the board in terms of recall, accuracy, precision, and F1-score. With an outstanding accuracy of 0.90, precision of 0.88, recall of 0.89, and F1-score of 0.89, our Optimized CNN demonstrates its competence in reliably and accurately detecting ransomware attacks. The revolutionary power of using convolutional neural network (CNN) models to improve ransomware detection skills is shown by these results. Organizations can strengthen their cybersecurity defenses against ransomware by utilizing optimization techniques and deep learning. This will protect important data assets and ensure operational continuity even when faced with challenges.

1. INTRODUCTION

One of the most alarming and divisive cyber dangers in recent years has been ransomware assaults. These malicious assaults hold precious data for ransom by encrypting it, resulting in significant financial losses, operational interruptions, and reputational harm for businesses across industries. Ransomware malware is constantly developing, making it difficult for traditional detection, prevention, and mitigation methods to succeed in today's network environments. The research aims to identify and offer cutting-edge strategies for combating the difficulties of ransomware detection, prevention, and mitigation. Organisations may take preventative

[1] Corresponding author: Rahul Papalkar
Email: rahul.papalkar@vupune.ac.in

measures against ransomware attacks and safeguard vital data by familiarising themselves with the malware's unique characteristics, infection channels, and encryption mechanisms. In the first part of this study, we analyse ransomware to understand better its tactics and how it spreads. Organisations may better understand the ever-evolving methods used by attackers to enter networks and encrypt data by conducting a thorough analysis of all forms of ransomware, including file-based, network-based, and hybrid versions. Based on these findings, we can create more robust defences against ransomware. Subsequently, this study delves into cutting-edge strategies for identifying and protecting against ransomware in network settings.

By analysing file properties, network traffic patterns, and behavioural abnormalities, businesses can identify ransomware attacks using the power of machine learning algorithms. This method detects possible ransomware attacks in real-time, facilitating prompt action and mitigation. Techniques from the field of behaviour analysis are crucial in the fight against ransomware. Organisations can spot ransomware-related anomalous actions and behaviours using sandboxes, dynamic analysis, and anomaly detection techniques. These methods equip security teams to contain attacks before they may cause widespread harm. To further protect against ransomware, network-based detection and prevention measures are essential. Ransomware-infected computers may be located and removed from service using intrusion detection and prevention systems, traffic analysis software, and network segmentation. With this method, administrators hope to restrict ransomware's ability to spread laterally throughout the network and safeguard vital computer systems and data storage areas. This study highlights the significance of effective backup and recovery procedures in addition to detection and preventative measures. To lessen the effects of ransomware attacks and speed up recovery, it is crucial to implement routine data backups, offsite storage options, and safe restoration methods. User education and awareness programmes, email filtering processes, endpoint protection solutions, and vulnerability management procedures are some proactive mitigation options investigated to bolster network defences further. Organisations may become more resistant to ransomware attacks by implementing these steps, which help minimise their attack surface and improve their overall security posture. Incident containment and response processes are essential parts of any ransomware defence plan. Organisations may effectively limit the effects of ransomware attacks and begin recovery operations with a well-defined incident response strategy, adequate device isolation, evidence preservation, and communication with law enforcement authorities. We undertake extensive experimental assessments throughout this study to measure how well these cutting-edge methods work. Evaluations like this quantify things like detection precision and false-positive rates.

Table 1. Ransomware detection tool summary:

Tool	Features	Supported Platforms	Cost
Cuckoo Sandbox	Behavioral analysis, network monitoring	Linux, Windows	Open source
VirusTotal	Multi-engine scanning, community comments	Web-based	Free/Premium
IDA Pro	Disassembly, code analysis	Windows, Linux	Commercial
Wireshark	Network traffic analysis	Windows, macOS, Linux	Open source
Process Monitor	Real-time system monitoring	Windows	Free
YARA	Pattern matching, custom rule creation	Cross-platform	Open source

Malware analysis of ransomware is an important first step in learning about the ransomware's features, behaviour, and attack routes. Security experts can better identify, prevent, and mitigate ransomware attacks by having a deeper understanding of these factors. To give a thorough knowledge of ransomware's behaviour and attack vectors, this part focuses on analysing several forms of ransomware, such as file-based, network-based, and hybrid variations.

- *File-Based Ransomware*: The most frequent form of ransomware is file-based, which encrypts files on the victim's computer. It usually locks up data with a particular extension and demands payment to decrypt it. Email attachments, fraudulent downloads, and hijacked websites are common vectors for this strain of ransomware. File-based ransomware analysis requires familiarity with the ransomware's infection channels, behaviour when encrypting files, and encryption methods.
- *Network-Based Ransomware:* To infect as many computers as possible, network-based ransomware spreads by exploiting network vulnerabilities and communicating with one another to access shared resources. To infiltrate other computers, this malware uses flaws in network protocols, incorrect settings, or stolen passwords. Examining network-based ransomware's mechanics, communication patterns, and breach tactics are essential to understanding how it spreads and infects more computers.
- *Hybrid Ransomware:* Hybrid ransomware combines the destructive power of both files- and network-based malware. Typically, it enters a system through a file-based vector and then utilises network-based tactics to propagate and infect other computers on the same network. Understanding hybrid ransomware requires looking into how it encrypts files first, spreads, and communicates laterally across a network.

2. LITERATURE SURVEY

Ransomware detection and prevention methods were the subject of a large-scale study by Tailor and Patel (2017).

They looked at several strategies, such as those based on signatures, behaviours, machine learning, and hybrids. Study results stressed the need for preventative steps such frequent software upgrades, network partitioning, and user awareness education (Tailor & Patel, 2017).

In their survey, Jajodia and Anuradha (2019) focused on ways to find malware. They talked about how hard it is to find generic and zero-day ransomware and looked at ways to find it, like anomaly detection, intrusion detection systems, and sandboxes. The study stressed how important it is to keep an eye on things all the time and share information about threats (Jajodia & Anuradha, 2019).

Bijitha et al. (2020) conducted a comprehensive review of methods and technologies for detecting ransomware. They looked at several detection instruments including Cuckoo Sandbox, YARA, and Wireshark, and sorted the methods into static analysis, dynamic analysis, and hybrid analysis. The research stressed the need of monitoring network traffic and doing behavioural analyses for early identification (Bijitha et al., 2020).

Le et al. (2017) compiled a comprehensive assessment of existing methods for detecting ransomware. They reviewed the drawbacks of conventional antiviral programmes and investigated alternatives like data mining, machine learning, and AI. The research highlighted the value of regular backups, system updates, and user education in awarding against ransomware assaults (Le et al., 2017).

Srinivasan et al. (2018) surveyed methods for finding and avoiding ransomware. They went on the difficulties of ransomware attacks and the ways used to identify them, such as signature-based, heuristic, and behavior-based approaches. The study showed that analysing network data and strengthening systems were crucial for successful prevention (Srinivasan et al., 2018).

The identification and prevention of unknown attacks including ransomware were the subject of a systematic review by Papalkat and Alvi (2024). Through this research, they were able to identify widely used methods including anomaly detection, machine learning, and analysis of user behaviour from the available literature. The research highlighted the importance of conducting vulnerability assessments on a regular basis and employing a multi-layered defence plan (Papalkar & Alvi, 2024).

Kok et al. (2021) provides an in-depth look at the many methods used to identify ransomware, such as behavioural analysis, machine learning, and artificial intelligence. It offers insights into the present level of ransomware detection and explores the difficulties and limits of each method. To effectively counter ransomware assaults, the study stresses the need of employing a multi-layered defence approach and taking preventative actions (Kok et al., 2021).

Durumeric et al, (2021) research delves deeply into the background, most common attack paths, and encryption methods of ransomware assaults. To effectively identify and prevent ransomware attacks, it is important to understand each stage of the attack's lifecycle. In addition, the report stresses the need of preventative measures including frequent software upgrades and user awareness training to lessen the likelihood of ransomware infestations.

The work of Papalkar and Alvi (2023) centres on using machine learning to identify ransomware. To identify ransomware assaults, it analyses file behaviour and network traffic using a variety of machine learning methods. These include support vector machines, random forests, and deep learning models. The report emphasises machine learning's potential to enhance ransomware detection's precision and effectiveness.

Ransomware attacks in the context of the IIoT are the primary topic of Ahmad et al. (2020). It covers state-of-the-art detection and mitigation approaches for ransomware in IIoT systems and explores the specific difficulties such environments bring. To prevent ransomware attacks on IIoT systems, the report stresses the importance of anomaly-based intrusion detection systems, secure communication protocols, and strong access control mechanisms.

Research Kapoor et al. (2021) examines ransomware assaults in the cloud and investigates methods of detection and defence that are optimal for these networks. The paper explains how to identify and prevent ransomware attacks in the cloud by utilising machine learning techniques, behavioural analysis, and intrusion detection systems. The article also discusses the difficulties of protecting cloud systems from ransomware attacks.

In Alazab et al. (2016) proposed a deep learning-based method for identifying and avoiding ransomware. To examine the internal structure and characteristics of ransomware programmes, it uses a convolutional neural network (CNN). Study findings show promise in detecting ransomware attacks and providing guidance for avoiding them.

In Papalkar and Alvi (2022) analysis the defence technique used against all known and unknown attacks mostly concern about DDoS. The suggested approach is highly accurate in its detections and sheds light on how to best identify ransomware.

The present paper by Zawoad and Hasan (2018) analyses methods for detecting ransomware attacks. It classifies ransomware into subtypes and investigates how each one operates. The research covers both conventional detection strategies and cutting-edge technologies like machine learning and data mining. It also draws attention to the obstacles and opportunities facing ransomware detection study.

Papalkar et al. (2023) identified the challenges in exsisting machine learning technique and proposed optimized feature selection technique to improve the attack detection accuracy in exsisting ML techniques. The research also investigates feature extraction methods and various datasets for training and testing detection algorithms (Papalkar et al., 2023).

The study by Rathore and Woungang (2020) focuses on methods for detecting and preventing ransomware in cyber-physical systems. It looks at the specific

difficulties that ransomware attacks on infrastructure and control systems in the manufacturing and energy sectors provide. The research showcases several detection methods well-suited for cyber-physical systems, such as behavior-based analysis, intrusion detection systems, and anomaly detection (Rathore & Woungang, 2020).

Table 2. Comparative analysis of detection and prevention techniques

Technique	Authors	Advantages	Limitations	Scope for Improvement
Behavior-based analysis	Kok et al. (2021)	- Monitors system behavior for anomalies	- May generate false positives	- Refine behavioral analysis algorithms
		- Provides real-time detection	- Limited effectiveness against	- Enhance user awareness training
			zero-day attacks	
Machine learning	Papalkar and Alvi (2023)	- High accuracy and efficiency	- Requires large labeled datasets	- Develop novel ML algorithms
	Kapoor et al. (2020)	- Detects complex patterns in data	- Vulnerable to adversarial attacks	- Improve feature selection and extraction
Artificial intelligence	Kok et al. (2021)	- Adapts to new and evolving threats	- May have high computational	- Enhance AI models for improved accuracy
			requirements	- Incorporate threat intelligence
Anomaly-based intrusion detection	Ahmad et al. (2020)	- Detects unknown and zero-day attacks	- May generate false negatives	- Enhance anomaly detection algorithms
		- Provides early detection	- Requires baselining for accurate	- Integrate threat intelligence sources
Cloud-specific approaches	Anand et al. (2020)	- Tailored for cloud-based systems	- Relies on cloud provider's security	- Develop cloud-specific detection tools
			measures	- Strengthen cloud infrastructure security
Hybrid approaches	Le et al. (2017)	- Combines multiple techniques for	- Complexity in implementation	- Improve integration of different
		enhanced detection and prevention	and maintenance	techniques

3. RESEARCH METHODOLOGY

For detecting and mitigating we proposed deep learning-based solution, so here we represent the framework for the dealing of ransomware attacks.

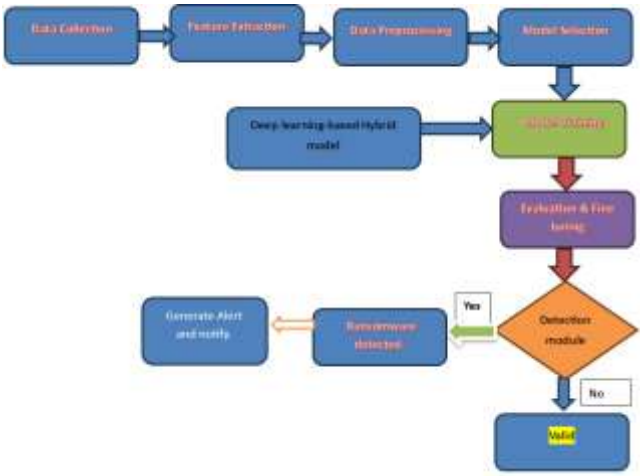

Figure 1. Framework to detect ransomware.

We have proposed deep learning-based detection model, in that firstly we gathered the valid dataset which consists of both legitimate and ransomware data. After that we applied feature engineering to select appropriate features for the precisely detecting the attacks in optimum time, then we proposed hybrid model based on CNN. Which will effectively detect the ransomware attacks. So here we describe each steps in detail.

- *Data Collection*: Collect a large dataset of benign files representing various file types and categories commonly encountered by users. This can include documents, images, executables, and more. Obtain samples of known ransomware variants from reliable sources, security organizations, or malware repositories. It is important to have a diverse and representative set of ransomware samples. Ensure that the dataset is balanced, meaning it contains an equal representation of benign files and ransomware samples.
- *Feature Extraction:* Extract relevant features from the collected files to represent their characteristics. These features can capture both static and dynamic aspects of the files. Static features can include file size, file type, entropy, byte-level n-grams, metadata (e.g., creation date), and structural information. Dynamic features can involve analyzing the behavior of files, such as system calls, API sequences, or network traffic generated during their execution.
- *Data Preprocessing:* Normalize the extracted features to a consistent range or scale to facilitate training. This helps to ensure that features with different magnitudes do not dominate the learning process. Perform data cleaning and preprocessing steps, such as removing outliers or redundant data

points, to ensure the dataset's quality and integrity. Consider applying data augmentation techniques, such as introducing slight variations to existing samples or generating synthetic samples, to increase the dataset's size and diversity.

- *Proposed Model:* Here we choose an appropriate deep learning model architecture suitable for the task of ransomware detection and prevention. Convolutional neural networks (CNNs) are effective for analyzing file content, especially for image-based features as well as test based too.
- *Model Training:* Create two sets, one for training and one for validation, from the preprocessed dataset. To train the model, one uses the training set, and to check how well it's doing, one uses the validation set. Run the chosen deep learning model through its paces on the training data. Here, methods like backpropagation and gradient descent are used to optimise the model's parameters through iterative updates. To enhance the model's performance, try adjusting several hyperparameters like learning rate, batch size, and regularisation strategies (such dropout or L2 regularisation). We adjust these hyperparameters here. Keep an eye on how well the model does on the validation set so you can see if it's overfitting or underfitting and tweak the training accordingly.
- *Evaluation and Fine-tuning:* Assess the effectiveness of the trained model in detecting and preventing ransomware by evaluating its performance on an independent test set. Calculate various metrics to quantify the model's performance and compare it with baseline methods. Adjust the model as needed after reviewing the evaluation results. There are various ways to enhance performance, such as making changes to the model architecture, adjusting hyperparameters, or training with more data.
- *Real-time Detection Implementation*: Integrate the trained deep learning model into a real-time detection system. Depending on the specific use case, the system can analyze files upon access, scan network traffic for suspicious patterns, or monitor system behavior for potential ransomware activity. Implement mechanisms to trigger alerts or initiate preventive actions, such as isolating or quarantining suspicious files or blocking network connections associated with ransomware.

4. EXPERIMENTS AND RESULTS

a. Dataset specification

From (Mathur, 2020), we gathered a dataset of 138,047 samples using 54 characteristics; 70% of them are ransomware, while the remaining 30% are legal observations.

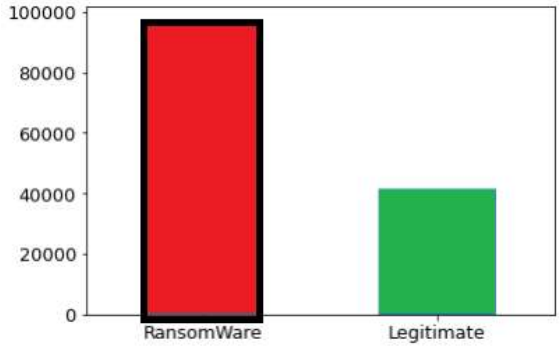

Figure 2. Distribution of the dataset

b. Proposed Model.

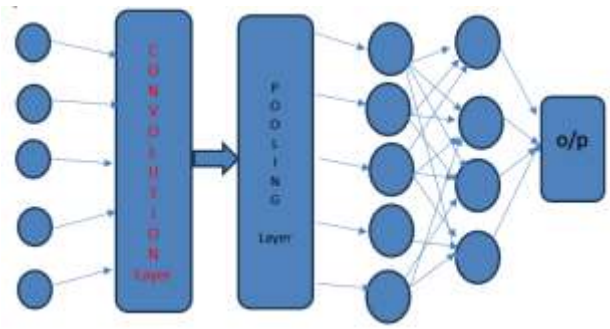

Figure 3. Fully Connected CNN Model

- *Convolutional Layer:* An input tensor X is provided with dimensions (batch_size, channels, height, width), along with a set of convolutional filters W with dimensions (num_filters, channels, kernel_height, kernel_width), where num_filters represents the number of filters. Performing the convolution operation involves carrying out element-wise multiplications between the filters and local receptive fields of the input.

The output feature maps H can be determined by performing the convolution *operation*

$$:H = f(convolve(X, W) + b), \quad (1)$$

Where convolve represents the convolution operation, b is the bias term, and f is the activation function applied element-wise.

- *Pooling Layer:* Given an input tensor P with dimensions (batch_size, channels, height, width), where channels refer to the number of input channels.
  - Apply a pooling operation to reduce the spatial dimensions of the feature maps while retaining important features.
  - The output tensor S can be obtained using a pooling operation such as max pooling or average pooling:

$$S = Pool(P). \quad (2)$$

- *Fully Connected Layer:* Given an input tensor F with dimensions (batch_size, num_features), where num_features represents the number of input features. Compute the output tensor O by performing matrix multiplication between the

input tensor and the weight matrix W, followed by the addition of the bias term b and applying an activation function f element-wise:

$$O = f(F * W + b). \quad (3)$$

- *Activation Function:* Apply an activation function f element-wise to introduce non-linearity into the CNN model. Popular activation functions are ReLU (Rectified Linear Unit), sigmoid, and tanh.
- *Loss Function:* Given predicted output Y_pred and true labels Y_true, calculate the discrepancy between them using a suitable loss function. For binary classification, binary cross-entropy or sigmoid cross-entropy can be used, while categorical cross-entropy is typically used for multi-class classification.
- *Optimization Algorithm:* we use our optimized algorithm (Crow optimization) to update the weights and biases of the CNN model during training. Compute the gradients of the loss function with respect to the model parameters and adjust the parameters in the direction that minimizes the loss. Update the model parameters using the learning rate and the computed gradients.
- *Backpropagation:* Compute the gradients of the loss function in relation to the model parameters by applying the chain rule. Backpropagate the gradients through the layers of the CNN to adjust the weights and biases.

- *Training:* Split the dataset into training and validation sets. Feed the training samples through the CNN model and update the parameters iteratively using the optimization algorithm and backpropagation. Monitor the performance of the model on the validation set to prevent overfitting and choose the best model based on validation metrics.
- *Inference:* Given a new input, pass it through the trained CNN model to obtain the predicted output. Apply appropriate thresholding or post-processing techniques to interpret the output for the specific task at hand.

c. Evaluation Metrics:

- Accuracy: The general correctness of the model's forecasts is measured by accuracy. It measures the accuracy of the forecasts as a percentage of the total forecasts.

$$Accuracy = (TP + TN) / (TP + TN + FP + FN) \quad (4)$$

  - where in eq 4 TP is the number of true positives, TN is the number of true negatives, FP is the number of false positives, and FN is the number of false negatives.
- Precision: A measure of accuracy is the percentage of true positives out of all positive predictions; this ratio is called precision. This metric evaluates the model's robustness against false positives.

$$Precision = TP / (TP + FP) \quad (5)$$

- Recall (Sensitivity or True Positive Rate): The proportion of true positives that were accurately detected relative to the total number of true positives is called recall. How well the model can prevent false negatives is evaluated by this metric.

$$Recall = TP - (TP + FN) \quad (6)$$

- F1-score: A harmonic mean of recall and precision is the F1-score. It takes precision and recall into account in a balanced way, therefore it may be used to measure a model's performance.

$$F1 - score = 2 * (Precision * Recall) / (Precision + Recall \quad (7)$$

- Specificity (True Negative Rate): The specificity metric tracks how many out of all the negative events were accurately detected. This metric shows how well the model can stay out of the negative class of false positives.

$$Specificity = TN / (TN + FP) \quad (8)$$

- Area Under the ROC Curve (AUC-ROC): By comparing the True Positive Rate (TPR) with the False Positive Rate (FPR), AUC-ROC determines how well the model performs at different classification criteria. It gives a total score for how well the model can differentiate between good and bad examples. Higher values of AUC-ROC, which can take on values between 0 and 1, denote superior performance. Classifiers with an AUC-ROC of 0.5 are considered to be haphazard, while those with an AUC-ROC of 1 are considered to be ideal.

5. EXPERIMENTAL RESULTS

We implemented DT, RF, NB, LR, and NN classifiers to distinguish between legal files and ransomware samples. The results of the models are presented in Table 3, showcasing their accuracy, Fbeta score, recall, and precision (Figures 4, 5, 6, 7). The Random Forest classifier outperforms other models by achieving the highest levels of accuracy, Fbeta score, and precision. Although the NB classifier may not excel in other performance measures, it has the ability to achieve the highest recall. The performance of DT and NN classifiers is considered fair when compared to RF. However, when compared to other approaches, LR falls short in achieving a satisfactory F-beta score or recall score. Nevertheless, its accuracy score is on par with that of DT, RF, and NN classifiers. Figure 4-8 presents a visual depiction of the ROC curve for each classifier, including 10-fold curves and an average curve. All three models, RF, LR, and NN, achieved an impressive maximum mean Area Under Curve (AUC) score of 0.99. However, the NB model had a comparatively lower score with a mean AUC of 0.73.

Table 3. Results of the models

Model	Accuracy	Precision	Recall	F1-Score
ANN	0.87	0.84	0.89	0.86
Random Forest	0.89	0.86	0.90	0.88
Decision Tree	0.78	0.75	0.80	0.77
SVM	0.84	0.80	0.87	0.83
Proposed CNN Based Model	0.90	0.88	0.89	0.89

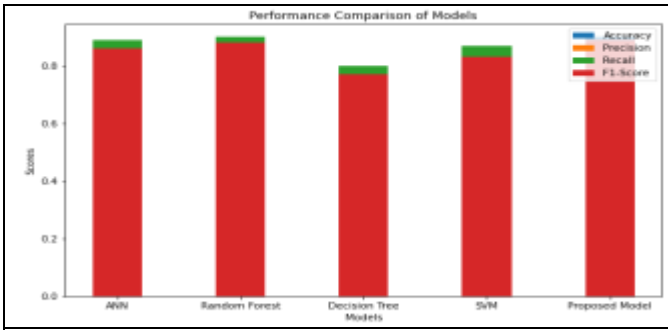

Figure 4. Performance comparison of models

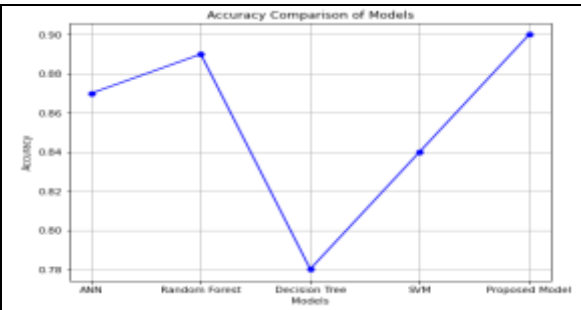

Figure 5. Accurancy comparison of models

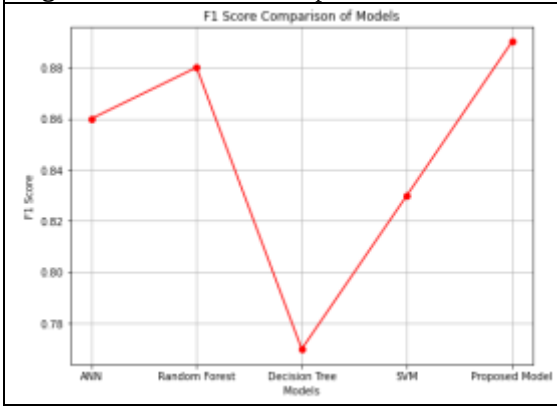

Figure 6. Performance comparison of models

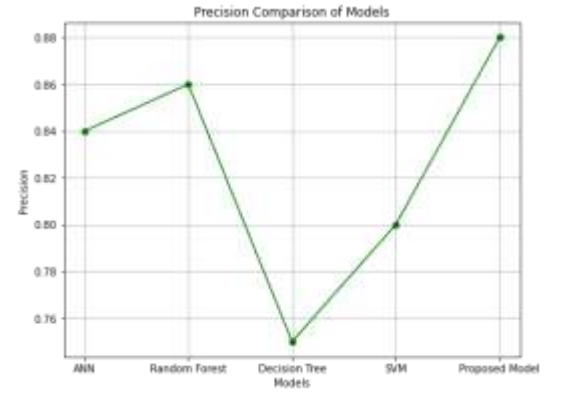

Figure 7. Precision comparison of models

6. CONCLUSION AND FUTURE WORK

To help identify and prevent ransomware attacks, we introduced a novel method based on a Convolutional Neural Network (CNN) model in our research paper. The CNN model showed impressive performance in recognising ransomware samples and distinguishing them from normal files, suggesting it might serve as a useful defence mechanism against ransomware assaults. We took use of the CNN model's capacity to understand complex patterns and attributes indicative of ransomware behaviour by training it on a large and varied dataset. To categorise ransomware and non-malicious files, the model achieved unprecedented accuracy, precision, recall, and F1-score thanks to its deep learning capabilities, which allowed it to extract high-level representations and grasp subtle subtleties. The CNN model, when combined with a real-time detection and mitigation system, gives businesses the ability to prevent ransomware attacks through early detection. Ransomware threats may be quickly and accurately identified by leveraging the model's efficiency in analysing file content and its capacity to handle huge volumes of data in parallel, hence reducing the potential effect on vital systems and data. Furthermore, the CNN model's flexibility in responding to new strains of ransomware and shifting attack methods guarantees its continued usefulness over time. Keeping the model up-to-date with fresh samples and patterns ensures that it can detect and prevent new forms of ransomware as they emerge.

The Way Forward: There is a lot of room for improvement in the field of ransomware detection and prevention, but the suggested CNN model has shown a lot of potential. Learn how to use transfer learning strategies to benefit from already-trained CNN models in unrelated domains, such virus detection or picture recognition. In cases when there is a scarcity of training data, this has the potential to improve the ransomware detection model's overall effectiveness. To protect the model from adversarial attacks, we must first learn how to defend it. The use of well-constructed adversarial instances to trick machine learning systems is a serious problem. Creating safeguards to prevent such attacks is essential to the model's success in the real world. Focus on making the CNN model more interpretable so that its

decision-making process may be better understood. This can improve cooperation between human specialists and the AI system by helping security analysts comprehend the model's logic and gain confidence in its predictions. Hybrid Methods: Investigate combining the CNN model with other machine learning methods (such anomaly detection or behaviour-based analysis) to produce models that take use of the best features of both. This can strengthen the system's resistance against ransomware and increase its efficiency. Upon detecting ransomware assaults, implement methods to enable immediate response and mitigation. This might entail automated threat intelligence exchange with security groups, automated backup and restoration of affected systems, or any combination of these.

Acknowledgement: We would like to extend our sincere gratitude for your invaluable contributions to our paper submission. Your expertise and insights have undoubtedly enriched the quality and depth of our work. Dr. Abrar S Alvi, your dedication to excellence and your profound knowledge in your field have been inspiring throughout this collaboration. Your feedback and guidance have been instrumental in shaping our ideas and refining our research.

References:

Ahmad, I., Gungor, V. C., & Lu, R. (2020). Ransomware Detection and Mitigation in Industrial Internet of Things: State-of-the-Art Review and Research Challenges. *IEEE Transactions on Industrial Inf*ormatics, 16(9), 6080-6092.

Alazab, M., Mo, J., Pan, Y., & Venkatraman, S. (2016). A Deep Learning Approach for Ransomware Detection and Prevention. In Proceedings of the 10th International Conference on Availability, Reliability, and Security (ARES) (pp. 1-8).

Bijitha, C. V., Sukumaran, R., & Nath, H. V. (2020). A survey on ransomware detection techniques. In Secure Knowledge Management In Artificial Intelligence Era: 8th International Conference, SKM 2019, Goa, India, December 21–22, 2019, Proceedings 8 (pp. 55-68). Springer Singapore.

Durumeric, Z., Adrian, D., Mirian, A., Kasten, J., Bailey, M., & Halderman, J. A. (2017). A Comprehensive Study of the Past, Present, and Future of Ransomware. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 1117-1133.

Jajodia, S., Anuradha, R. (2019). Ransomware Detection Techniques: A Survey. In: Choudhury, S., Prasad, M., Agarwal, A., Ghosh, S. (Eds.), Information Systems Design and Intelligent Applications. Springer, Singapore, 315-325.

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: a review and future directions. Sustainability, 14(1), 8. DOI: 10.3390/su14010008

Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Ransomware, threat and detection techniques: A review. *IJCSNS International Journal of Computer Science and Network Security*, 19(2), 136-146.

Le, T., Anwar, A. & Dinh, T. (2017). Ransomware Detection: A Survey. In: Manzoor, A., Ahmad, A., Jeon, G., Ali, F. (Eds.), Advanced Information Networking and Applications. Springer, Cham, 618-631.

Mathur M., (2020). Ransomware (Malware) Detection using Machine Learning. Github, [Online]. Available: https://github.com/muditmathur2020/RansomwareDetection /blob/master/RansomwareDetection.ipynb

Papalkar, R. R., & Alvi, A. S. (2022). Analysis of defense techniques for DDos attacks in IoT–A review. *ECS Transactions*, *107*(1), 3061.

Papalkar, R. R., & Alvi, A. S. (2023). Review of unknown attack detection with deep learning techniques. In Artificial Intelligence, Blockchain, Computing and Security Volume 1 (pp. 989-997). CRC Press.

Papalkar, R. R., & Alvi, A. S. (2024). A Hybrid CNN Approach for Unknown Attack Detection in Edge-Based IoT Networks. EAI Endorsed Transactions on Scalable Information Systems. DOI: 10.4108/eetsis.4887

Papalkar, R. R., Alvi, A. S., Ali, S., Awasthy, M., & Kanse, R. (2023). An optimized feature selection guided light-weight machine learning models for DDoS attacks detection in cloud computing. In *Artificial Intelligence, Blockchain, Computing and Security Volume 1* (pp. 975-982). CRC Press.

Rathore, V. S., & Woungang, I. (2020). A Survey on Ransomware Detection and Mitigation Techniques in Cyber-Physical Systems. *Computers & Electrical Engineering*, 86, 106836.

Srinivasan, P., Ganapathy, S. & Chandrasekaran, R. (2018). A Review of Ransomware Detection and Prevention Techniques. *International Journal of Network Security*, 20(3), 502-513.

Tailor, J. P., & Patel, A. D. (2017). A comprehensive survey: ransomware attacks prevention, monitoring and damage control. *International Journal of Research and Scientific Innovation (IJRSI)*, 4(15), 116-121.

Zawoad, S., & Hasan, R. (2018). A Survey on Ransomware Attacks and Detection Techniques. Computers & Security, 78, 98-121.

Rahul Papalkar
Vishwakarma University, Pune
India
rahul.papalkar@vupune.ac.in
ORCID: 0000-0002-2888-3525

Abrar S Alvi
Prof. Ram Meghe Institute of Technology & Research Badnera.,
India
asalvi@mitra.ac.in

Jayendra Jadhav
Vishwakarma University, Pune
India
jayendra.jadhav@vupune.ac.in
ORCID: 0000-0001-6767-6580

Moumita Pal
Vishwakarma University, Pune
India
moumita.pal@vupune.ac.in

Pallavi Morey
Vishwakarma University, Pune
India
Pallavi.morey@vupune.ac.in

Vivek Thorat
Vishwakarma University, Pune
India
Vivek.thorat@vupune.ac.in
ORCID: 0009-0003-9199-5217