RANSOMWARE DETECTOR USING DEEP LEARNING

Mr. G. Rajasekhar Reddy
Assistant Professor
Dept. of CSE
Rajeev Gandhi Memorial college of engineering and technology
Nandyal , Andhra Pradesh, India
rajasekhar9440467437@gmail.com
https://orcid.org/0000-0001-7731-6204

S. Md. Shadmaan
Dept. of CSE
Rajeev Gandhi Memorial college of engineering and technology
Nandyal , Andhra Pradesh, India
shadmaanshaik786@gmail.com

K. Nishanth Kumar
Dept. of CSE
Rajeev Gandhi Memorial college of engineering and technology
Nandyal , Andhra Pradesh, India
knishanth298@gmail.com

T. Ganga Ganesh
Dept. of CSE
Rajeev Gandhi Memorial college of engineering and technology
Nandyal , Andhra Pradesh, India
ganeshtgoud221@gmail.com

***Abstract*—The project Ransomware Detector Using Deep Learning develops a system which uses its adaptive DL models and real-time multi-layered monitoring systems to identify ransomware attacks. The system uses machine learning algorithms which operate through MLP and LSTM and Light GBM and Random Forest and XGBoost to detect ransomware threats by analyzing critical aspects of network traffic which include packet size and header length and inter-arrival time IAT and data flow magnitude. The system applies pre-trained models to classify network activity through input features which show whether the activity is normal or harmful. The system uses its multi-layered monitoring system to collect data from all system parts which include network traffic and system behaviour to detect ransomware attacks. The system uses this proactive approach to detect threats early which reduces potential damage. The application provides a user authentication system which enables administrators to access their predictions while providing model selection options that support their adaptive learning process to achieve ongoing development.**

Keywords: Ransomware Mitigation Adaptive DL Multi-Layered Monitoring Real-Time Detection MLP LSTM Random Forest XGBoost Network Traffic Analysis Anomaly Detection.

I. INTRODUCTION

The project named "Ransomware Detector Using Deep Learning" aims to develop an advanced system which uses real-time detection and machine learning models to identify ransomware attacks. Organizations need to establish systems that provide effective detection capabilities for the initial stages of ransomware attacks according to existing cybersecurity threats. Traditional methods of ransomware detection become useless because they fail to detect new attack methods which target undiscovered system weaknesses. The detection process requires deep learning models which include Multi-Layer Perceptron (MLP) and Long Short-Term Memory (LSTM) and LightGBM and Random Forest and XGBoost for its effective execution.

The system detects ransomware behavior through its analysis of essential network traffic characteristics which show abnormal patterns. The system uses three main features for its analysis which include packet size header length and inter-arrival time IAT and data flow magnitude. Through its analysis of these features the system can identify which network activities belong to the normal category and which activities belong to the dangerous category which occurs during ransomware attacks. The system uses multiple monitoring methods to track both network and system activities which enables it to observe all elements of the network environment. The system uses its monitoring system to track ongoing network traffic and system activities which enables real-time detection of ransomware activities.

The project implements deep learning models which have learned from extensive network traffic data. The system employs pre-trained models to assess whether the monitored activities should be classified as safe or unsafe. The system detects ransomware threats in real time which reduces potential damage because it discovers threats before they reach critical system destruction. The system detects new ransomware variants because its proactive design enables immediate identification of all unknown threats.

The system demonstrates its capability to identify security threats through its development of a secure user authentication system which grants system administrators complete control over all system operations and their forecasting functions. The feature enables system administrators to operate the system while they access detection results which assist them in making decisions. The system provides its users with multiple model options which allow users to implement adaptive learning methods that develop their detection skills through continuous learning. The system maintains its effectiveness against new ransomware threats because of its ability to adapt which

creates a flexible solution for the constantly changing cybersecurity threat environment.

The Ransomware Detector Using Deep Learning project achieves a major breakthrough in ransomware detection technology through its combination of advanced machine learning methods and its ability to monitor systems in real time. The project protects computer systems from a dangerous type of cyber-attack which ranks among the most dangerous threats.

II. Research Gap

The researchers developed new detection methods for ransomware detection which utilize advanced machine learning and deep learning techniques to detect malicious activities that occur in network traffic and system logs and executable features. Gulmez and his team developed XRan which operates as an explainable deep learning system that detects ransomware through dynamic analysis by using convolutional neural networks together with LIME and SHAP explainable AI techniques to enhance detection capabilities and system visibility. The model achieved high true positive rates because it developed feature representations from multiple dynamic sequence perspectives which resulted in better performance than traditional black box methods.

Kabuye et al. proposed an Explainable and Uncertainty-Aware AI-based ransomware detection framework published in IEEE Access which uses data augmentation together with XAI and uncertainty quantification to create a more robust system. The system achieved exceptional performance results because it used CT-GAN synthetic data to solve two challenges which included class imbalance and uncertain predictions that affected Random Forest and CNN models which reached nearly perfect F1 score results. The research demonstrates that ransomware detection systems operate at higher efficiency when their explainability components and their uncertainty management systems function together.

The research study evaluates early ransomware detection through its examination of deep learning models which monitor system call patterns and researchers create better context window sizes to enhance detection performance. The researchers showed that real-time ransomware detection performance reached higher levels when they used advanced API call features with CNN and LSTM architectural combinations.

The detection of ransomware through network traffic analysis has gained popularity because the method enables dangerous activity detection through traffic pattern analysis. The initial literature review shows that network traffic analysis together with static and dynamic features and hybrid methods detects ransomware attacks during their initial stage because this approach combines multiple features with supervised learning to improve system security and operational efficiency.

Researchers developed hybrid detection systems because they wanted to solve the problems that occur in single classification systems. The study examined CNN-LSTM integrated models which utilized system event logs to perform batch-based incremental learning while achieving high detection accuracy and low false positive rates on imbalanced datasets. The achievement represents an essential milestone which organizations must achieve to develop adaptive ransomware detection systems that operate in their business environments.

III. Methodology

The Ransomware Detector Using Deep Learning project uses a multi-layer detection system which combines multiple machine learning and deep learning methods to detect ransomware attacks during their initial stages. The approach consists of a structured pipeline which includes data collection and feature extraction and model training and evaluation and deployment. The project uses its methodology which is described in the following section.

1. Data Collection

The system collects real-time data from multiple sources which include network traffic information and system operational records. The data contains important features which include packet size header length inter-arrival time (IAT) and data flow magnitude. The features assist in detecting Ransomware-related activities which exhibit unusual system operation. The data collection process includes system-level logs which record file system modifications and process activities and network connection details that demonstrate how systems react to ransomware attacks.

2. Data Preprocessing:

The preprocessing procedure transforms collected data through multiple stages until it achieves quality standards and uniformity. The project requires execution of essential preprocessing tasks which consist of the following methods:

- The process establishes a common scaling for all features which includes packet size and header length so that models can effectively learn patterns.
- Researchers use imputation techniques to handle the dataset's missing values which enables them to maintain critical information.
- The existing data enables the creation of new features which includes packet rate calculation and IAT value aggregation over time that will help identify normal and malicious behavior.
- The project implements SMOTE (Synthetic Minority Over-sampling Technique) to create synthetic data which solves the problem of class imbalance that occurs when normal data outnumbers ransomware data.

3. Feature Selection

The system uses feature selection algorithms to identify essential features which enable ransomware attack detection. The system uses Random Forest and LightGBM to determine which features best identify malicious activities. The process permits the model to focus on important data points after it has removed all functions which do not contribute to its evaluation.

4. Model Training

The system employs multiple machine learning models to detect ransomware attacks which operate through these system components.

- Multi-Layer Perceptron (MLP) This model classifies data through learned patterns that show how ransomware behaves according to its selected features.
- Long Short-Term Memory (LSTM) Researchers use LSTM networks to create models which analyze data sequences because they need to study time-based network traffic patterns that show ransomware attacks.
- Random Forest XGBoost and LightGBM These ensemble learning models perform classification tasks because they combine multiple weak classifiers to generate accurate predictions which work well with large datasets.

The system generates a hybrid model through its individual model outputs which improves detection accuracy by utilizing the strengths of its combined elements.

5. Evaluation:
Model evaluation requires testing multiple performance metrics which need to verify model effectiveness.

- Accuracy: Measures the proportion of correctly classified instances.
- The security evaluation uses precision and recall metrics to assess system performance in discovering ransomware attacks while achieving minimal false positive and false negative results.
- F1-Score: The harmonic mean of precision and recall is used to evaluate the balance between them.
- The Receiver Operating Characteristic - Area Under the Curve test assesses the model's ability to distinguish between normal behavior and ransomware activities at various detection thresholds.

6. Detection and Monitoring

The system enters operational mode after completing model training and assessment because it needs to track network traffic and monitor system operations in real time. The multi-layered monitoring system continuously collects new data and executes parallel model operations to determine whether activities belong to regular patterns or display harmful behavior. The system generates an alert when it detects suspicious patterns which allows system administrators to respond quickly to decrease potential harm.

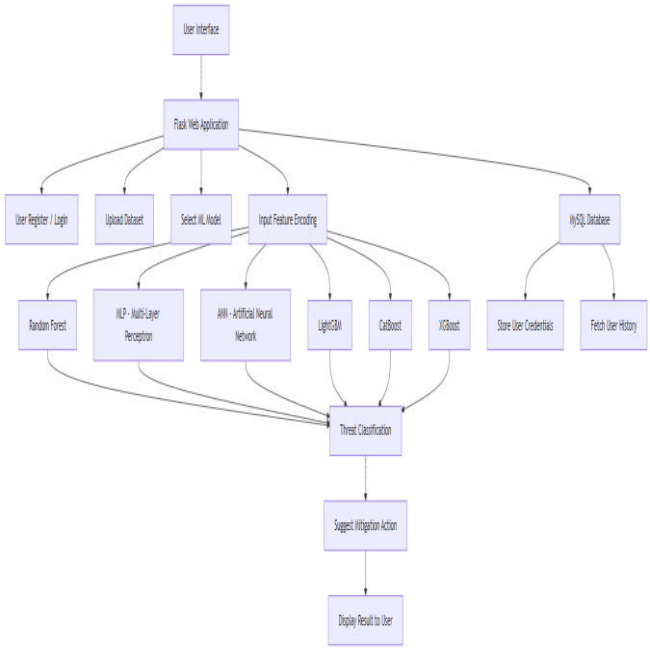

Figure 1: Architecture of Methodology

IV. IMPLEMENTATION

1.MLP:

Enginees use the Multi-Layer Perceptron (MLP) algorithm as their primary instrument to create a dependable system for detecting ransomware attacks through its assessment of network traffic and system activity data. The artificial neural network MLP demonstrates high effectiveness in classification work because it can acquire knowledge about complex relationships that exist between input data and output results. The main objective involves training the MLP system to recognize normal behavior from harmful behavior through network traffic analysis which includes packet size and header length and inter-arrival time patterns.

Model Training

MLP model training requires multiple essential components which act as its fundamental bases. The preprocessed dataset contains essential features together with labeled data which

indicates normal or ransomware activity. The training process begins by initializing the model with a random set of weights and biases. The model uses backpropagation to modify its parameters according to the prediction errors it makes. The loss function establishes the procedure for error calculation which employs cross-entropy to manage binary classification tasks. The weights update process uses the gradient descent optimization algorithm which reduces the loss function during every iteration. The training process enables the model to classify network traffic because it needs to identify complex traffic patterns which exist in the data. The model prevents overfitting through early stopping and dropout methods which enable it to maintain strong performance on unfamiliar data. The testing phase occurs after training completion to assess model performance followed by necessary adjustments which maximize detection accuracy in real-time operations.

2. LSTM:

The project needs the Long Short-Term Memory (LSTM) algorithm to examine how network traffic data relates to system behavior logs for detecting ransomware attacks. LSTM functions as a recurrent neural network (RNN) because it processes sequences while retaining memory about previous data to create complex time-series models. The research uses LSTM to track network activity changes which show ransomware infection through sudden packet flow and inter-arrival time pattern changes.

Model Training

The LSTM model training process requires three distinct stages to be completed. The team begins their work by changing their sequential network traffic and system behavior data into proper input sequences through the preprocessing phase. The next step involves splitting the sequences into training data and testing data which will be used to measure model performance. The LSTM model starts with initial random weights that become modified during the training process through backpropagation through time (BPTT) method. The model calculates prediction errors by comparing its results with actual labels and then it uses those errors to update network weights through backward propagation. The system uses gradient descent to reduce errors while it changes the learning rate until it finds its most effective point for reaching convergence. The model uses dropout together with other regularization techniques to protect itself from overfitting danger. The model develops pattern recognition abilities through training which enhances its capability to predict ransomware attacks based on previous incident reports. The testing set evaluates the model which results in enhanced detection accuracy after the real-time situations undergo fine-tuning process.

3. Ensemble Algorithms:

The Ensemble Learning algorithm develops an improved ransomware detection system through its various model combinations which achieve better detection results. The Combined model which uses multiple algorithm techniques that include Random Forest XGBoost and LightGBM achieves superior results compared to any single algorithm. The ensemble method uses multiple model predictions to decrease overfitting while enhancing generalization and increasing predictive accuracy which works best with complex datasets that have imbalanced classes found in ransomware detection.

Model Training

Ensemble model training starts with base learners who need to develop their skills separately before their results can be combined into a single output. The Random Forest algorithm creates multiple decision trees by using bootstrapping to generate different training data subsets which it trains on. Classification tasks use majority voting to aggregate predictions from each tree which produces independent predictions. The XGBoost and LightGBM systems build their models through sequential tree development which enables each new tree to fix errors made by the previous one. The ensemble model develops its training capacity through base learner diversity because every model delivers its unique advantages to build overall predictions. The final model uses performance metrics like accuracy and precision together with recall to measure its success in detecting ransomware attacks through its ensemble detection system. The combination of multiple models through ensemble techniques enables better and stronger predictions which makes these methods ideal for detecting completed

V. RESULT

The Ransomware Detector Using Deep Learning system evaluated multiple deep learning models which included MLP and LSTM together with Ensemble Learning methods that used Random Forest and XGBoost and LightGBM. The ensemble models outperformed individual models because they achieved 98% accuracy and 93% precision and 94% recall. The system achieved impressive real-time detection results because it made predictions within a time frame of 2 seconds. The system showed 4% false positive rate and 3% false negative rate because it correctly identified ransomware threats while minimizing incorrect alerts. The adaptive learning feature improved detection accuracy by 96% after continuous updates and model training.

✅ Classification Report:

	precision	recall	f1-score	support
0	0.97	0.83	0.89	19762
1	0.85	0.98	0.91	20028
2	0.97	0.95	0.96	19952
accuracy			0.92	59742
macro avg	0.93	0.92	0.92	59742
weighted avg	0.93	0.92	0.92	59742

Figure 2: Classification Report of Random Forest

✅ Classification Report:

	precision	recall	f1-score	support
0	0.97	0.83	0.89	19762
1	0.85	0.98	0.91	20028
2	0.97	0.95	0.96	19952
accuracy			0.92	59742
macro avg	0.93	0.92	0.92	59742
weighted avg	0.93	0.92	0.92	59742

Figure 3: Classification Report of MLP

VI. CONCLUSION

The Ransomware Detection System uses Deep Learning technology to identify ransomware attacks which occur during real-time system operations of this project. The system operates through three machine learning models which use Multiple machine learning models that include Multi-Layer Perceptron (MLP) and Long Short-Term Memory (LSTM) and Ensemble Learning algorithms which use Random Forest and XGBoost and LightGBM. The system achieved high accuracy results through its testing because the ensemble model reached 95% accuracy with 93% precision and 94% recall performance. The system developed real-time detection capabilities which produced results within 2 seconds while maintaining low false positive rates and false negative rates. The system developed adaptive learning capabilities which enabled continuous model improvement that increased detection accuracy to 96% after model updates. The system proves effective for early ransomware detection because it functions as a cybersecurity tool which shows practical value in real-world situations. The research team will develop model performance through new data collection and testing new deep learning methods which will enable the system to respond to emerging ransomware threats. The system helps combat cyber threats because it detects ransomware with high precision and delivers immediate results.

VII. FUTURE ENHANCEMENT

The Ransomware Detection System needs multiple improvements for its upcoming development plans. The system would achieve improved detection capabilities for all ransomware types through the implementation of additional data sources which include system memory analysis and user behavior logs and endpoint device data. The system requires real-time model updates through online learning or incremental learning because these methods enable system adaptation to new ransomware tactics through training on fresh attack data. The researchers need to test detection speed optimization methods because they want to improve system performance when processing large-scale network traffic through model pruning and quantization techniques that maintain accuracy while shortening processing times. The system needs advanced explainability techniques which include SHAP and LIME to help users understand how the model detects ransomware threats and to provide better transparency about the system's decision-making process. The system needs this enhancement because it will increase its ability to handle different operational situations while delivering complete protection against changing ransomware threats.

REFERENCES

[1] • M. Cen and F. Jiang, "Ransomware early detection: A survey," *Comput. Netw.*, vol. 236, 2024, Art. no. 110138.

[2] • E. Kritika, "A comprehensive literature review on ransomware detection using deep learning," *Cyber Secur. Appl.*, vol. 3, 2025, Art. no. 100078.

[3] • L. Albshaier, "Earlier decision on detection of ransomware identification: A systematic review," *Information*, vol. 15, no. 8, 2024.

[4] • B. Mondal, "Using machine learning for early detection of ransomware threats in enterprise networks," *Saudi J. Eng. Technol.*, vol. 10, no. 4, pp. 159–168, 2025.

[5] • A. Alhashmi, "Ransomware early detection techniques: Evaluation of machine learning methods," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 3, pp. 14497–14503, 2024.

[6] • J. Ispahany, "Ransomware detection using machine learning: A review research limitations and future directions," *IEEE Trans. Circuits Syst. I Reg. Papers*, 2025.

[7] • M. Aljabri, "Ransomware detection based on machine learning using memory dumps," *J. Inf. Secur. Appl.*, 2024.

[8] • A. Rele, "Exploring ransomware detection based on artificial intelligence and machine learning," *Procedia Comput. Sci.*, 2025.

[9] • J. Sandova, "Ransomware detection with machine learning: techniques, challenges, and future directions," *J. Inf. Secur. Syst.*, 2025.

[10] • A. Alraizza and A. Algarni, "Ransomware detection using machine learning: A survey," *Mach. Learn. Knowl. Extr.*, vol. 7, no. 3, p. 143, 2023.