Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.048036

ARTICLE

# Securing Cloud-Encrypted Data: Detecting Ransomware-as-a-Service (RaaS) Attacks through Deep Learning Ensemble

**Amardeep Singh[1], Hamad Ali Abosaq[2], Saad Arif[3], Zohaib Mushtaq[4,*], Muhammad Irfan[5], Ghulam Abbas[6], Arshad Ali[7] and Alanoud Al Mazroa[8]**

[1]School of Computer Information Sciences, University of Cumberlands, Williamsburg, Kentucky, 40769, USA

[2]Computer Science Department, College of Computer Science and Information Systems, Najran University, Najran, 61441, Saudi Arabia

[3]Department of Mechanical Engineering, College of Engineering, King Faisal University, Al-Ahsa, 31982, Saudi Arabia

[4]Department of Electrical, Electronics and Computer Systems, College of Engineering and Technology, University of Sargodha, Sargodha, 40100, Pakistan

[5]Electrical Engineering Department, College of Engineering, Najran University, Najran, 61441, Saudi Arabia

[6]Department of Electrical Engineering, The University of Lahore, Lahore, 54000, Pakistan

[7]Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah, 42351, Saudi Arabia

[8]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia

*Corresponding Author: Zohaib Mushtaq. Email: zohaib.mushtaq@uos.edu.pk

Received: 25 November 2023 Accepted: 21 February 2024 Published: 25 April 2024

## ABSTRACT

Data security assurance is crucial due to the increasing prevalence of cloud computing and its widespread use across different industries, especially in light of the growing number of cybersecurity threats. A major and ever-present threat is Ransomware-as-a-Service (RaaS) assaults, which enable even individuals with minimal technical knowledge to conduct ransomware operations. This study provides a new approach for RaaS attack detection which uses an ensemble of deep learning models. For this purpose, the network intrusion detection dataset "UNSW-NB15" from the Intelligent Security Group of the University of New South Wales, Australia is analyzed. In the initial phase, the rectified linear unit-, scaled exponential linear unit-, and exponential linear unit-based three separate Multi-Layer Perceptron (MLP) models are developed. Later, using the combined predictive power of these three MLPs, the RansoDetect Fusion ensemble model is introduced in the suggested methodology. The proposed ensemble technique outperforms previous studies with impressive performance metrics results, including 98.79% accuracy and recall, 98.85% precision, and 98.80% F1-score. The empirical results of this study validate the ensemble model's ability to improve cybersecurity defenses by showing that it outperforms individual MLP models. In expanding the field of cybersecurity strategy, this research highlights the significance of combined deep learning models in strengthening intrusion detection systems against sophisticated cyber threats.

## KEYWORDS

Cloud encryption; RaaS; ensemble; threat detection; deep learning; cybersecurity

## 1 Introduction

The phrase "randomization" has become more commonplace in the context of the Internet of Things (IoT), and as a result, more individuals are prepared to pay for it. Ransomware-as-a-Service (RaaS) has recently emerged as a particularly concerning type of cybercrime since it allows criminals with no technical expertise to spread malware to a wide audience [1]. These types of assaults can disrupt critical services and compromise sensitive information in addition to creating substantial financial and operational damages. This highlights the critical need for the rapid advancement of reliable detection technologies that can be deployed against the growing danger [2]. In this research, the study offers a unique approach that makes use of deep learning (DL) ensemble techniques to detect RaaS attacks on encrypted cloud-based data. By providing unprecedented scalability, cost-effectiveness, and data accessibility, cloud computing has fundamentally changed the information technology landscape. However, it has led to new worries about personal privacy and security [3]. To protect sensitive data that is stored in the cloud, cloud encryption techniques have gained extensive adoption. Despite this, RaaS attacks pose a danger because hackers may now use cloud infrastructure to disseminate and carry out ransomware campaigns at an unprecedented scale more easily [4].

The focus of this study is on cloud-encrypted data, as that is where RaaS assaults are most likely to occur, and hence the goal of this research is to develop a reliable detection tool that can identify such attacks. The proposed goal is to enhance the detection system's precision and dependability by employing DL ensemble approaches. This will facilitate the prompt detection of RaaS attacks and the subsequent implementation of appropriate countermeasures.

"Randomization" is shorthand for the process of encrypting sensitive information to keep it hidden from inquisitive eyes. These attacks have grown in frequency and sophistication over the past few years, causing serious harm to victims' finances and reputations [5]. Using RaaS, cybercriminals can rent or buy ransomware toolkits that have already been produced and hosted on the cloud. This lowers the baseline technical skill needed to launch an attack. RaaS is frequently used in ransomware attacks. The widespread adoption of cloud computing can be due to its many benefits, such as the instantaneous delivery of resources, decreased costs, and always-available access to data. However, inherent security vulnerabilities exist in cloud systems because of their collaborative nature and reliance on external service providers [6]. In response to these dangers, encryption mechanisms have been introduced within the cloud to protect data both in transit and at rest. If data is encrypted, it cannot be read by an unauthorized party, even if that person gains access to it. Despite this, the increase in RaaS attacks is cause for serious alarm, as hackers may now leverage cloud infrastructure to disseminate and carry out widespread ransomware campaigns more quickly [7].

The two primary goals of this study are mitigating the growing threat of RaaS assaults and bolstering the security of encrypted cloud data. Establishing an effective detection strategy for RaaS-delivered ransomware attacks allows businesses to proactively secure their critical data and systems from future ransomware threats. In addition, this study contributes to the growing body of literature on cybersecurity by delving into the feasibility of employing DL ensemble methodologies to improve the precision and dependability of RaaS detection in the cloud. The results of this study will help businesses to protect critical systems and prevent unauthorized access to private information by allowing for faster detection and mitigation of RaaS assaults. The proposed approach can also help cloud service providers improve the security of their platforms, which in turn will increase consumers' faith in those services.

### *1.1 Problem Formulation*

This study aims to solve the issue of how to identify cloud-encrypted data that has been subject to a RaaS assault. To spot instances of RaaS assaults within cloud-based encrypted data, the study needs to create a reliable detection technique. This will protect a company's most sensitive information and critical processes from ransomware. Given a cloud-encrypted dataset $D = \{(X_1, y_1), (X_2, y_2), \ldots, (X_n, y_n)\}$, where $X_i$ represents the encrypted data instance and $y_i$ denotes its corresponding label (0 for benign and 1 for RaaS attack), the problem can be mathematically formulated as follows:

Training the DL Ensemble Model: Define the ensemble model as $E = \{M_1, M_2, \ldots, M_k\}$, where $M_i$ represents an individual DL model in the ensemble. Train $M_i$ using a portion of the secret training dataset $D$. Use encrypted data and an appropriate DL architecture, e.g., Convolutional Neural Network (CNN) or Recurrent Neural Network (RNN), for training. Fine-tune model parameters to minimize loss and maximize classification performance.

Feature Extraction from Encrypted Data: Develop a technique for extracting useful properties from encrypted data $X_i$ while considering encryption. Use methods like homomorphic encryption, secure multiparty computation, and differential privacy to maintain data privacy while extracting attributes for RaaS detection. Create a process to decrypt data and input it into a DL pipeline for use in an ensemble model.

RaaS Attack Detection: Use the learned ensemble model $E$ to determine if a new encrypted data instance test is safe or a RaaS attack. Obtain an ensemble prediction by summing the forecasts of all models in the ensemble $(E, M_i)$. Consider confidence scores or voting methods along with the ensemble prediction for a reliable categorization. The goal is to establish a dependable RaaS attack detection method in cloud settings by addressing these problem formulations and employing DL ensemble techniques on cloud-encrypted data.

The study aims to achieve the following objectives:

RansoDetect Fusion Ensemble: Develop an advanced DL ensemble model named "RansoDetect Fusion" by combining the predictive abilities of three Multilayer Perceptron (MLP) models (MLP1, MLP2, and MLP3). The goal is to enhance the efficiency and accuracy of detecting RaaS attacks.

Effective RaaS Attack Detection: Create a reliable intrusion detection system capable of accurately identifying and classifying RaaS attacks within cloud-encrypted data. This effort aims to reduce RaaS threats and contain potential damage.

Ensemble Performance Enhancement: Investigate and demonstrate how the fusion of multiple machine learning (ML) models can improve performance metrics such as accuracy, precision, recall, and F1-score. Emphasize the collaborative approach in addressing complex cybersecurity challenges.

Advancement of Cybersecurity Strategies: Introduce an ensemble-based approach showcasing the effectiveness of combining diverse ML models for identifying and preventing sophisticated cyber threats, particularly RaaS attacks. This contributes to the advancement of cybersecurity strategies.

Practical Implementation: Assess the viability and application of the proposed RansoDetect Fusion model by comparing its performance with real-world cloud-encrypted data. This evaluation aims to highlight the model's potential integration into existing security systems for improved threat detection and response.

Improve Detectability Mechanism: Enhance openness and interpretability by analyzing the contribution of individual MLP models to the overall detection process. This analysis is detailed in the preceding section on "Model Interpretability".

Contribution to Cybersecurity Research: Contribute to cybersecurity research by presenting a novel ensemble-based methodology designed specifically for RaaS attack detection. Address emerging issues posed by evolving cyber threats in cloud computing environments.

There are five main parts to this study. An in-depth introduction to ransomware assaults, RaaS, and the research motivation is provided after the topic's broad review. The section on related work summarizes the current methods used to detect RaaS and points out the gaps in the proposed understanding. The methodology describes how the detection model is trained, including details on DL ensemble approaches, encryption-aware feature extraction, and more. Metrics for evaluation, a comparison of performance, and an analysis of the proposed method are all included in the findings and discussion section. Summarizing the research's contributions, major findings, and future directions are presented in the conclusions.

## 2 Related Work

Ransomware, a growing cybersecurity concern, poses a severe threat to individuals and businesses due to its ability to spread across platforms and inflict significant damage. Researchers have explored various methods to detect and mitigate ransomware attacks, leading to several notable studies. Newaz et al. addressed malware detection using DL [7]. Their work contributed to the broader understanding of leveraging DL for malware detection across diverse datasets and highlights the importance of staying resilient against evolving cyber threats. Gao and Fang introduced a novel perspective to obfuscate malware via deep reinforcement learning [8]. Their exploration of using benign files for malware obfuscation through deep reinforcement learning sheds light on potential adversarial strategies and challenges for malware detection systems. Alsharafi et al. [9] contributed to the literature by proposing a DL-based approach for malware detection, emphasizing its efficacy in identifying malicious patterns. Rahman et al. discussed the application of ML to enhance network intrusion detection by stacking ensemble classifiers and feature selection methods, using the NSL-KDD dataset [10]. It highlighted the importance of feature selection in improving classification models. Further details on specific classifiers and techniques could improve clarity.

Darem et al. proposed an Adaptive Behavioral-Based Incremental Batch Learning Malware Variants Detection Model (AIBL-MVD) [11]. This model incorporated concept drift detection and sequential DL, offering adaptability to evolving malware threats. The architecture, denoted as AIBL-MVD, demonstrated a robust framework for detecting malware variants. Aslan et al. [12] proposed a new malware classification framework based on DL algorithms, contributing to the landscape of malware detection methodologies. Homayoun et al. [13] introduced the Deep Ransomware Threat Hunting and Intelligence System (DRTHIS), a ransomware detection system using DL and fog computing. DRTHIS represents an innovative fusion of Long Short-Term Memory (LSTM) and CNN for ransomware detection, contributing to the advancement of defense mechanisms in the cybersecurity landscape. Alamro et al. [14] provided Automated Android Malware Detection using the Optimal Ensemble Learning Approach for Cybersecurity (AAMD-OELAC) in their research. Ensemble learning using Least Square Support Vector Machines (LS-SVM), Kernel Extreme Learning Machine (KELM), and Regularized Random Vector Functional Link Neural network (RRVFLN) optimized parameter tweaking with hunter-prey optimization. This work solved android malware challenges by outperforming previous approaches and improving model resilience. Wei et al. [15] emphasized computer learning techniques in phishing website detection to combat worldwide cyber-crime. This research compared ML with DL approaches and showed that ensemble ML algorithms improve detection accuracy and processing efficiency. Ensemble approaches for binary phishing categorization in real-time were examined. Bertoli et al. [16] presented the Attack, Bonafide, Train, RealizAtion, and Performance (AB-TRAP) framework which is a five-step process designed to address the challenges of increasing connected devices and evolving attack techniques in network intrusion detection systems. It focused on dataset generation, model training, implementation, and performance evaluation, and was adaptable to both local and global environments. However, this work lacked an in-depth discussion on the ML algorithms used and could benefit from a more detailed analysis of performance metrics and comparison with existing frameworks.

Almarshad et al. [17] addressed android malware detection, concentrating on data scarcity for effective DL solutions. The research presented Drebin's dataset-based Siamese Shot Learning method. Compared to other methods, the suggested technique accurately identified and categorized android malware. To clarify the Siamese network design, the study may include additional helpful information discussing how the suggested approach applies to various datasets. Siewruk et al. [18] presented work to manage vulnerabilities in massive communication networks. Mixeway system automated context-based software vulnerability classification using ML and natural language processing. The ML model utilized is not specified in this research, which may impair repeatability. Discussion about its scalability and flexibility might boost its efficacy. Tran et al. [19] presented a study to address Industry 4.0 cybersecurity issues by using IoT and ML for online induction machine malfunction diagnostics. It suggested an ML-based IoT infrastructure for cyberattack detection and motor condition monitoring. Faults and cyberattacks were shown accurately in experiments. Discussion of ML methods and their limits would improve the review. Another work presented a framework for malware detection in reverse-engineered android applications, utilizing static features and ensemble learning with ML algorithms [20]. The model achieved high accuracy rates in detecting malware, contributing to the effectiveness of ML in tackling android threats. This work could have been more beneficial by including more details on specific static features and ensemble learning algorithms, as well as a discussion on the model's generalizability and robustness in real-world scenarios. In another work [21], RANSOMNET+, a hybrid model combining CNNs and pre-trained transformers, effectively classified ransomware attacks on cloud-encrypted data, outperforming ResNet 50 and VGG 16. Its decision-making process was revealed through interpretability analysis and graphics, and its usage for investigating malware in encrypted communication channels and integrating proactive mitigation strategies with real-time threat intelligence is crucial. Table 1 discusses some relevant studies conducted on RaaS attack detection.

**Table 1:** Relevant studies conducted on RaaS attack detection

| Ref. | Techniques | Dataset | Key findings |
|---|---|---|---|
| [14] | Optimal ensemble learning for android malware detection | Android data | AAMD-OELAC outperforms existing approaches in android malware detection using ensemble learning and optimal parameter tuning. |
| [15] | Ensemble ML for phishing website detection | Website data | Ensemble methods excel in both accuracy and efficiency for phishing website classification, particularly with reduced feature sets. |

(Continued)

**Table 1 (continued)**

| Ref. | Techniques | Dataset | Key findings |
|---|---|---|---|
| [16] | End-to-end framework for network intrusion detection | LAN, Internet (dataset not specified) | AB-TRAP framework achieves high detection scores for TCP port scanning attacks in both LAN and internet scenarios with minimal resource usage. |
| [17] | Siamese shot learning for android malware detection | Drebin dataset (9476 good ware and 5560 malware applications) | Siamese one-shot model outperforms standard methods with 98.9% accuracy in android malware detection. |
| [18] | Context-aware software vulnerability classification | Real-life dataset from a mobile network operator | Mixeway automates software vulnerability classification showing effectiveness in managing security scanning reports. |
| [19] | IoT-based cyber secure fault diagnosis with ML | Real-life dataset from a network operator | The proposed IoT architecture using ML effectively detects cyber-attacks and faults in induction motors with high accuracy. |
| [20] | Ensemble learning and ML-based android malware detection | UNSW-NB15 | The proposed model achieves 96.24% accuracy in detecting malware from reverse-engineered android applications. |
| [21] | RANSOMNET+: A hybrid of CNNs and transformers | Ransomware Attacks dataset of cloud-encrypted data | Enhancing the model's utility by integrating feature importance analysis, outlier detection, and feature distributions. |

The literature review highlighted the need for sophisticated detection methods and multi-layered security against ransomware. While several effective approaches were introduced, limitations included reliance on specific features or behaviors, resource-intensive requirements, and potential evasion by ransomware variants. Integrating diverse detection methods and focusing on emerging platforms are critical for effective ransomware defense.

## 3 Materials and Methods

The research strategy and methods used to accomplish the study goals are outlined in the methodology section. The study details the preparation of the dataset, the building and training of the machine learning models, and the subsequent assessment of their efficacy. The methods used in this research include an ensemble strategy based on MLP models, to accurately identify and analyze cyber threats. This section tries to provide openness and clarity into the technique used to carry out the research by detailing the procedure in depth. Fig. 1 depicts the recommended research approach.

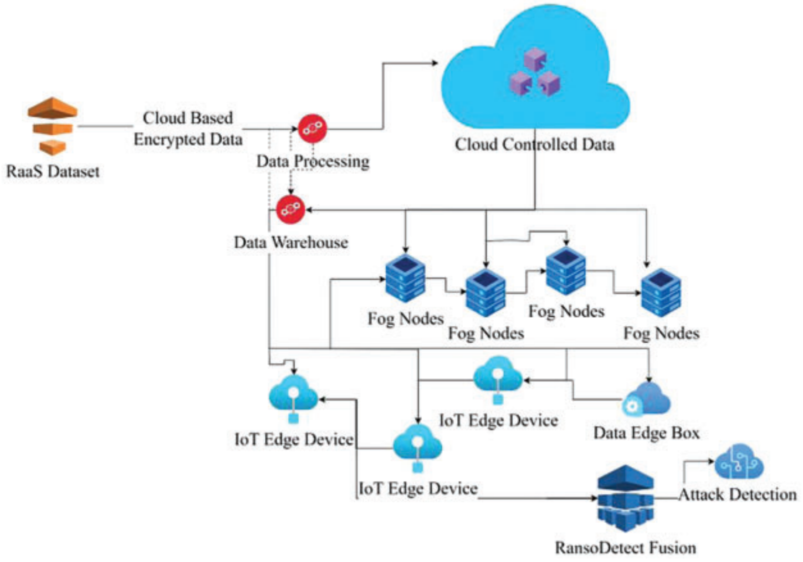


**Figure 1:** Proposed flow of the study

### *3.1 Dataset Description of Network Features*

A large number of features, captured from representative samples of network traffic, are included in the dataset. Various useful features include the duration and protocol of the connection, type of service, and type of RaaS attack, etc. These features are useful for detecting cyber threats. The class distribution for this binary class dataset is 45% for normal samples and 55% for all RaaS attacks cumulatively. Fig. 2 contains two separate charts. Fig. 2a displays a distribution plot for various protocols, detailing the variation in the frequency of occurrence for each protocol category. Fig. 2b shows a distribution plot for several types of services, illustrating how frequently they occur. These charts provide a better understanding of the widespread use of protocols and services. Fig. 3a shows the breakdown of RaaS attack categories. This visualization offers insights into the distribution of attacks across categories, helping to identify the most prevalent types of cyberattacks.

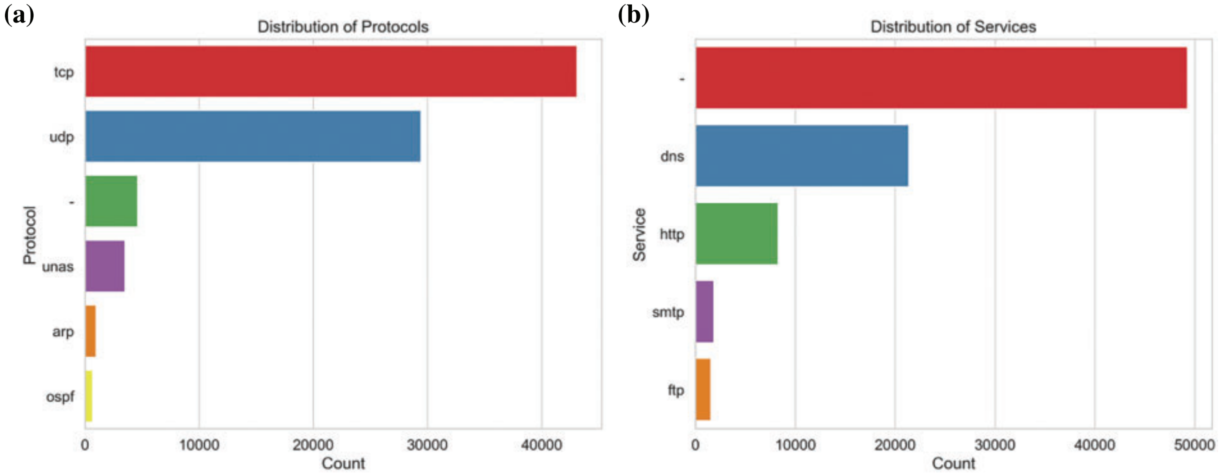


**Figure 2:** Data distribution among various: (a) connection protocols, and (b) connection services

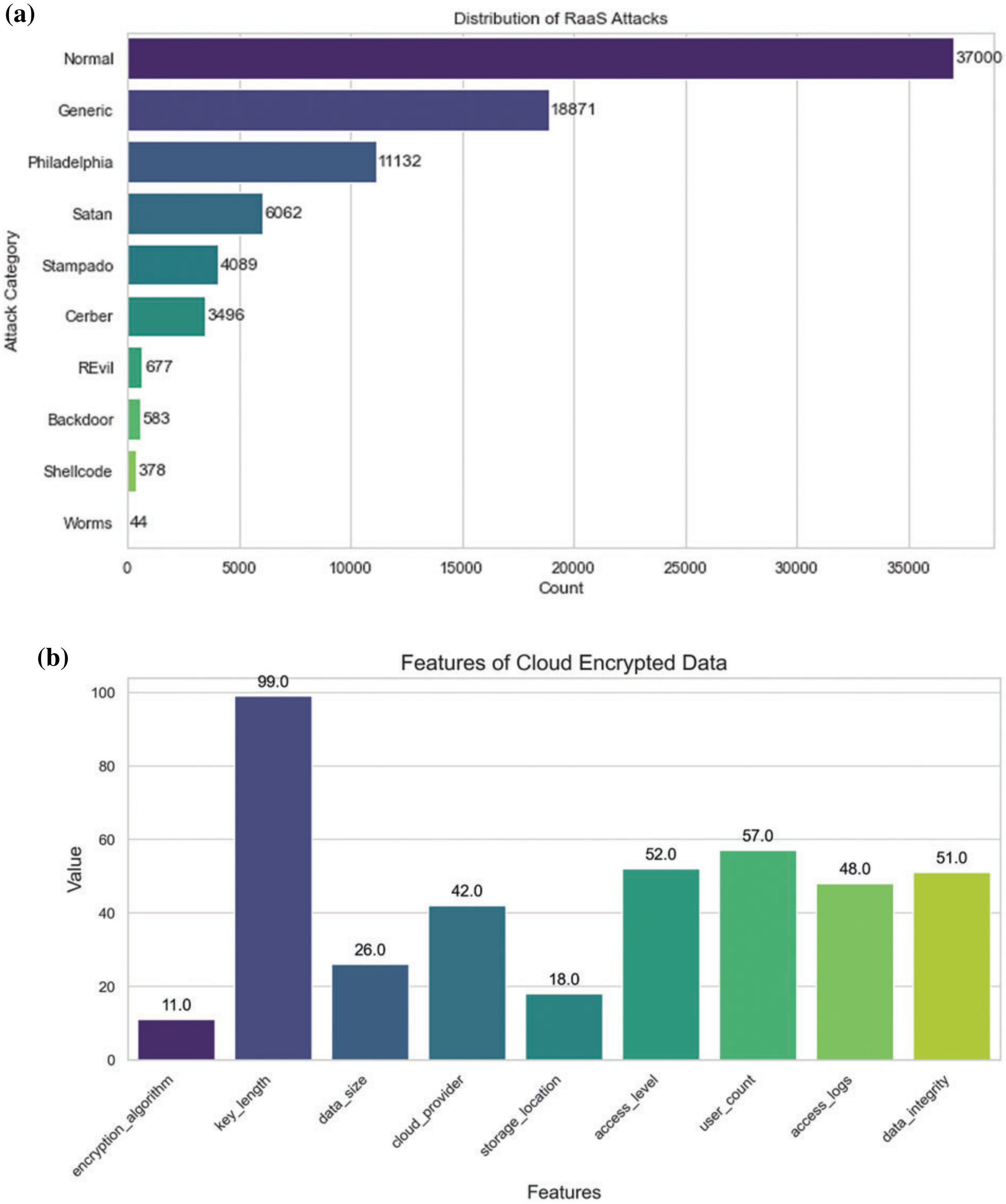


**Figure 3:** Data distribution among various: (a) RaaS attack categories, and (b) cloud encryption features

### *3.2 Dataset Description of Encrypted Cloud Features*

The ability to remotely store and analyze data, made possible by cloud computing, has made it a crucial component of today's IT architecture. The potential for unauthorized access and data breaches, however, makes the security of cloud-stored data a top priority. Protecting encrypted data stored in the cloud has become an urgent field of study because of this problem. Here, the study describes in detail the dataset and its pertinent properties and describes the methods used to keep them secure in cloud storage systems. The dataset used in this research is comprised of cloud-stored, encrypted information. This protected material is supposed to represent real-world circumstances where private information, such as medical records, financial records, or trade secrets, is saved in the cloud. Encryption algorithm, encryption key length, data size, cloud provider, storage location, data integrity, user count, access level, and access logs are prominent characteristics of the dataset that aid in the evaluation of the current level of security.

The selected features were chosen to create a comprehensive representation of the multifaceted nature of RaaS attacks. By encompassing behavioral, cryptographic, communication, and system-level aspects, our feature set aims to equip the model with a nuanced understanding of the diverse tactics employed by Ransomware-as-a-Service campaigns.

Fig. 3b shows the data distribution among various cloud-encrypted features. Fig. 4a represents the ratio of "Normal" to "Attack" cases emphasizing how many instances there are of each type in the dataset among various network protocols. Fig. 4b shows the flag distribution in typical network traffic, demonstrating how flags are distributed within the "Normal" and "Attacked" scenarios highlighting flag patterns that are unique to attacks.

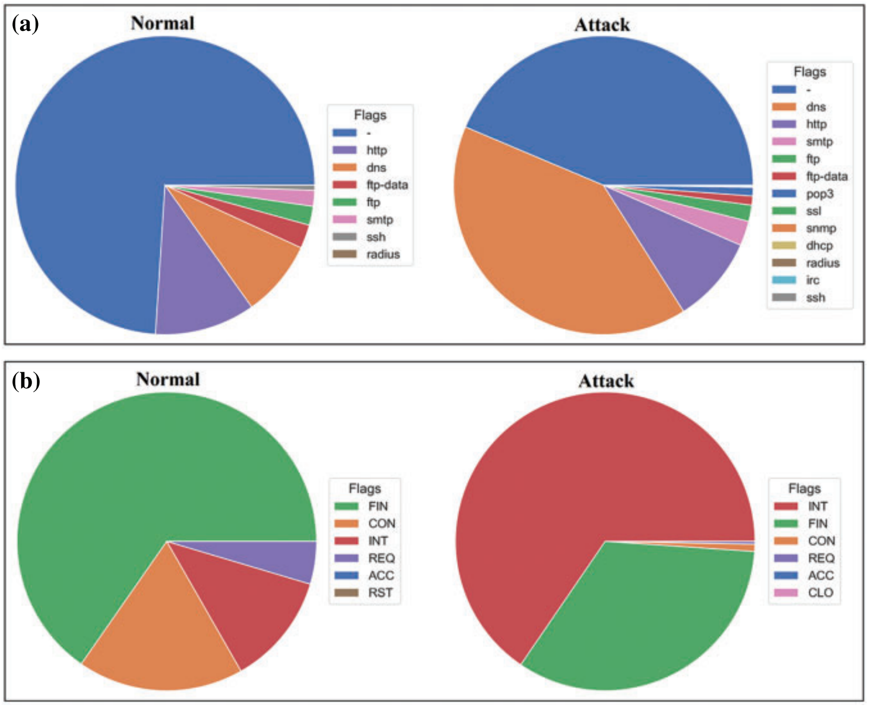


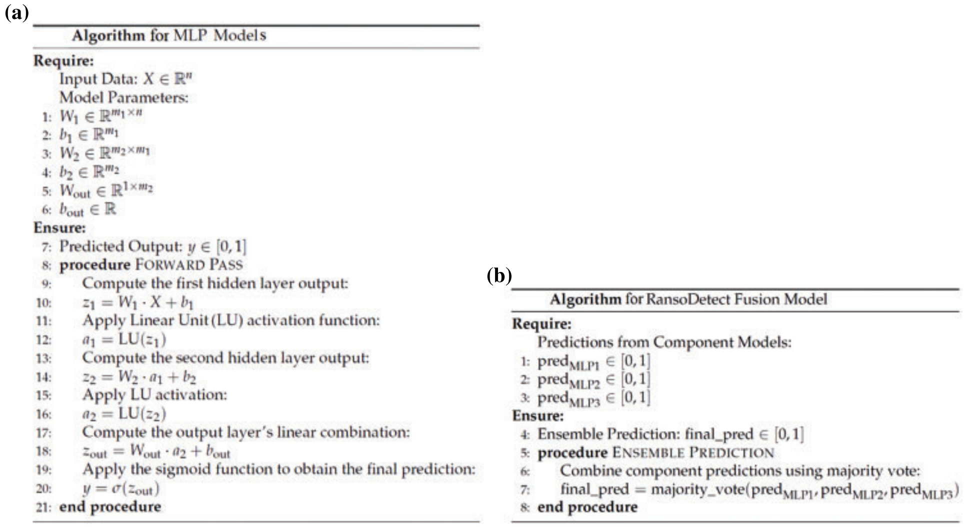
**Figure 4:** Class-wise flag distribution among various: (a) network protocols, and (b) connection states

### 3.3 *Proposed Model*

The purpose of this research is to evaluate the efficacy of different security measures in preventing unauthorized access to and violations of data integrity for cloud-encrypted data by examining these features. In this approach, machine learning models are used to foresee security breaches in light of the encrypted data features. In this section, the study presents the proposed model, which integrates multiple MLPs to enhance RaaS attack detection. The proposed model aggregates the results of several MLP models to improve RaaS assault identification by leveraging their strengths. The study provides detailed descriptions of MLP1, MLP2, MLP3, and the ensemble model named "RansoDetect Fusion," along with model parameters.

#### *3.3.1 Multilayer Perceptron Model*

The MLP model is a standalone neural network architecture designed for RaaS attack identification. It consists of an input layer, two hidden layers, and an output layer. Three MLPs with varying hyperparameters are designed, trained, and tested in this study to enhance RaaS attack detection. These MLP models consist of input and output layers of size 50 and two, respectively, and three hidden layers having two fully connected dense layers and one activation layer. Three MLP models differ in activation functions used in their activation layers. The rectified linear unit (ReLU), scaled exponential linear unit (SeLU), and exponential linear unit (ELU) activation functions are employed in MLP 1, MLP 2, and MLP 3 models, respectively. The generalized structure of MLPs is detailed in Fig. 5a.



**(a)**

```
Algorithm for MLP Models
Require:
    Input Data: $X \in \mathbb{R}^n$
    Model Parameters:
$W_1 \in \mathbb{R}^{m_1 \times n}$
$b_1 \in \mathbb{R}^{m_1}$
$W_2 \in \mathbb{R}^{m_2 \times m_1}$
$b_2 \in \mathbb{R}^{m_2}$
$W_{out} \in \mathbb{R}^{1 \times m_2}$
$b_{out} \in \mathbb{R}$
Ensure:
Predicted Output: $y \in [0, 1]$
procedure FORWARD PASS
    Compute the first hidden layer output:
    $z_1 = W_1 \cdot X + b_1$
    Apply Linear Unit (LU) activation function:
    $a_1 = LU(z_1)$
    Compute the second hidden layer output:
    $z_2 = W_2 \cdot a_1 + b_2$
    Apply LU activation:
    $a_2 = LU(z_2)$
    Compute the output layer's linear combination:
    $z_{out} = W_{out} \cdot a_2 + b_{out}$
    Apply the sigmoid function to obtain the final prediction:
    $y = \sigma(z_{out})$
end procedure
```

**(b)**

```
Algorithm for RansoDetect Fusion Model
Require:
    Predictions from Component Models:
$pred_{MLP1} \in [0, 1]$
$pred_{MLP2} \in [0, 1]$
$pred_{MLP3} \in [0, 1]$
Ensure:
Ensemble Prediction: final_pred $\in [0, 1]$
procedure ENSEMBLE PREDICTION
    Combine component predictions using majority vote:
    final_pred = majority_vote($pred_{MLP1}, pred_{MLP2}, pred_{MLP3}$)
end procedure
```

**Figure 5:** Algorithms for (a) MLP models, and (b) RansoDetect fusion model

#### *3.3.2 RansoDetect Fusion Model*

The RansoDetect fusion ensemble model is designed to enhance detection accuracy by integrating three individual MLP models, namely MLP 1, MLP 2, and MLP 3. This ensemble approach combines the predictive outputs of these models to form a unified final prediction. The fusion process is mathematically expressed by the following relation:

$$Final_{Pred} = MV(P_{MLP1}, P_{MLP2}, P_{MLP3}) \tag{1}$$

where MV represents the fusion function that combines the predictions of the component MLP models.

The RansoDetect Fusion model aims to improve overall performance in detecting RaaS assaults. By integrating insights from multiple MLP models, it leverages the unique strengths of each component model to address the limitations inherent in relying on a single model for detection. For a detailed explanation of the proposed model, refer to the algorithm presented in Fig. 5b. Furthermore, the detailed neural network architecture of the RansoDetect fusion model is shown in Fig. 6.

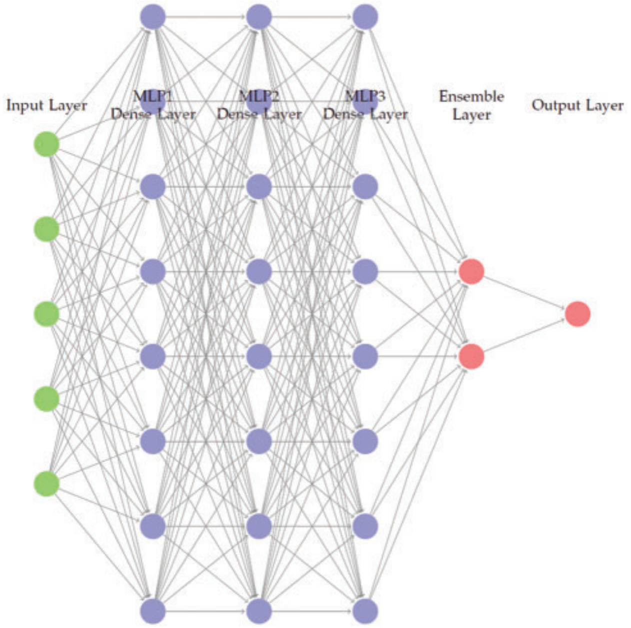


**Figure 6:** Hybrid architecture combining MLP1, MLP2, MLP3, ensemble, and output layers

### *3.4 Performance Evaluation Metrics*

Several metrics are used to compare the proposed RansoDetect Fusion model to the three standalone MLP models (MLP1, MLP2, and MLP3). These settings provide valuable context for understanding how well and reliably the models can identify RaaS intrusions. The evaluation parameters and corresponding equations are described as follows.

The accuracy of a classification system is evaluated by the percentage of training data that is properly labeled. It gives a comprehensive picture of the model's efficiency as per the following relation:

$$Accuracy = \frac{TP + TN}{FP + FN + TP + TN} \tag{2}$$

Recall or sensitivity is determined by the ratio of correct attack classifications to the total number of positive cases.

$$Recall, Sensitivity = \frac{TP}{FN + TP} \tag{3}$$

The precision of a model is measured by how many occurrences it correctly labels as positive, relative to the total number of examples. This proves that optimistic forecasts are reliable.

$$Precision = \frac{TP}{FP + TP} \tag{4}$$

F1-score is the optimal compromise between accuracy and recall. It takes into account both false positives and false negatives, striking a compromise between accuracy and memory.

$$F_1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{5}$$

## 4 Results

The focus of this section is the detection of RaaS attacks, presenting the findings of the proposed RansoDetect Fusion model and the individual MLP models (MLP1, MLP2, and MLP3). All the models have shown better classification performance with their class separation boundaries for discriminating the test data in respective classes as shown in Fig. 7. The models' strengths and weaknesses are analyzed based on various evaluation metrics, shedding light on their performance in addressing evolving cyber threats. The reported results contribute to understanding the models' capabilities and limitations in the context of cybersecurity. The model exhibited an adaptive learning behavior, showcasing improved detection accuracy over time. As it encountered novel instances of RaaS patterns during the evaluation phase, it demonstrated an ability to incorporate this new knowledge, resulting in enhanced detection performance. This dynamic learning aspect is crucial for addressing the evolving landscape of cyber threats.

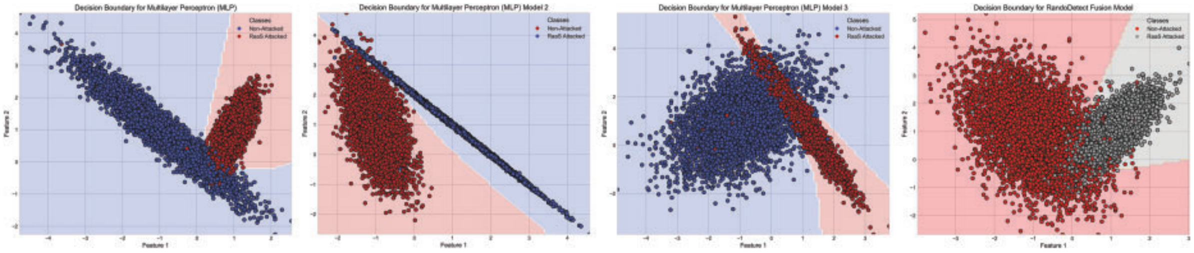


**Figure 7:** Decision boundaries generated with all MLP and RansoDetect fusion models

### *4.1 Multilayer Perceptron Models Performance*

The detection performance of MLP1, MLP2, and MLP3 alone is comparable to that of the combined models. MLP3 consistently captures RaaS and non-RaaS traffic occurrences, as seen by its 96.80 percent accuracy, recall, and F1-score in Fig. 8. Similar to MLP1, MLP2 displays a 96.97 percent accuracy, a 96.99 percent precision, and an F1-score of 96.97 percent. With an F1-score of 96.40 percent, 96.39 accuracy, 96.39 percent recall, and 96.39 percent precision, MLP1 performs somewhat worse.

### *4.2 RansoDetect Fusion Model Performance*

RaaS attacks can be detected with remarkable precision using the RansoDetect Fusion model, an ensemble of the separate MLP models (MLP1, MLP2, and MLP3). The model has a 98.79 percent success rate in correctly labeling data as shown in Fig. 8. The model can accurately identify instances of RaaS assaults while minimizing false positives, as evidenced by the recall and precision values of 98.79 percent and 98.85 percent, respectively. Fig. 8 demonstrates the efficacy of the RansoDetect Fusion model in identifying genuine positive and negative results, with an F1-score of 98.80 percent reflecting the balance between precision and recall. Fig. 9 represents the simulated cloud-encrypted data in which the RaaS attack is successfully detected with higher precision and accuracy using the RansoDetect fusion model.

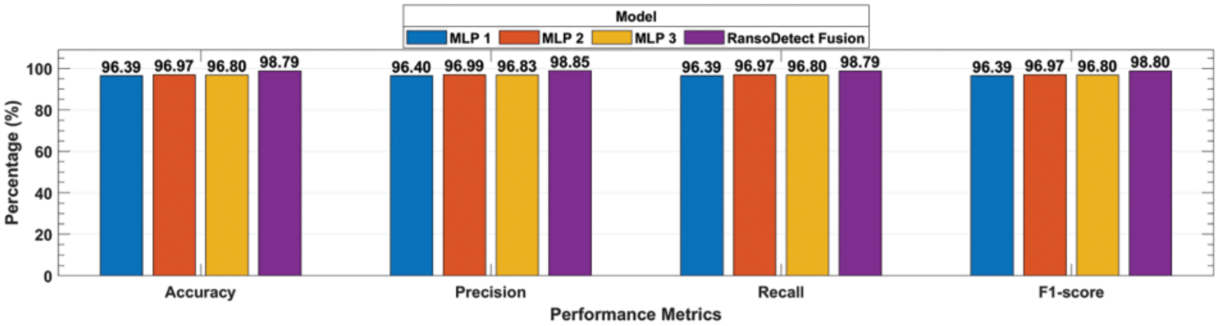


**Figure 8:** Performance assessment metrics results for proposed individual and ensemble models

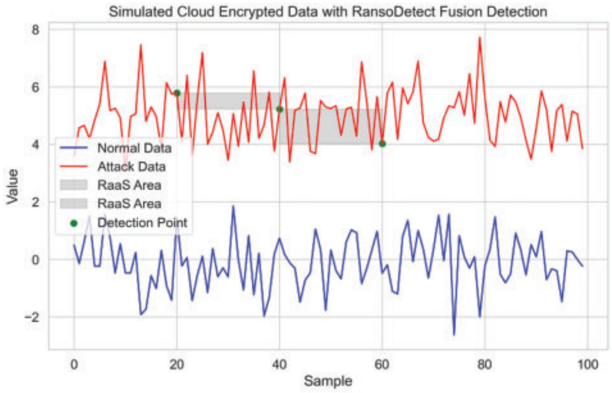


**Figure 9:** Simulated cloud-encrypted data with RansoDetect fusion detection

### *4.3 Performance Comparison*

By merging the strengths of various models, the RansoDetect Fusion model achieves better results than the separate MLP models. The Fusion model's capacity to capture exact patterns in the data and produce more informed predictions is evidenced by a 2%–3% increase in accuracy. To achieve high accuracy in cyberattack detection, the results show that feature selection, hyperparameters tunning, and model design are crucial. Different model configurations have a noticeable effect on performance, as evidenced by the somewhat differing outcomes among the individual MLP models.

Confusion matrices for all of the models are displayed in Fig. 10. Notably, even though the combined MLP model of RansoDetect performs better, the standalone MLP models do an excellent job at detecting RaaS attacks. This suggests that these models, in particular, may be subject to additional optimization and fine-tuning in further investigations, yielding even better results. In Table 2, the study has compared the proposed work with the previous studies along with detection results.

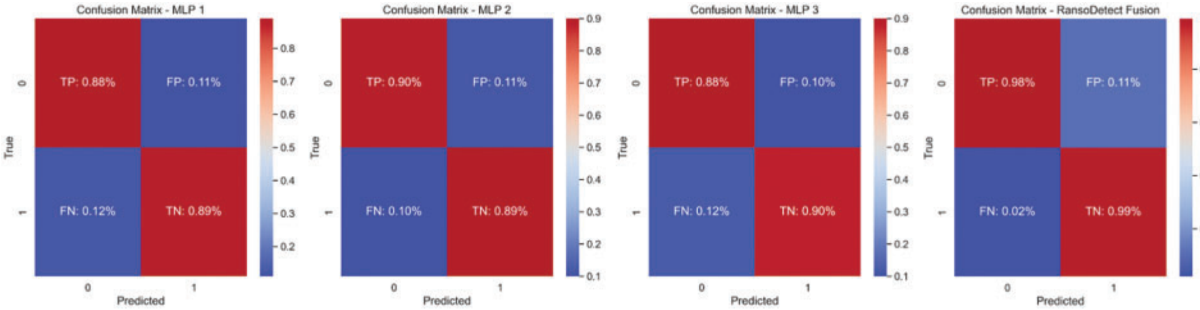


**Figure 10:** Confusion matrices for all the MLP models and RansoDetect fusion model

**Table 2:** Comparative analysis of the proposed model with previous studies

| Reference | Techniques | Dataset | Accuracy |
|---|---|---|---|
| Proposed model | RansoDetect fusion | Ransomware dataset | 98.79% |
| [22] | Autoencoder-based Unsupervised DL | Ransomware dataset | 90.00% |
| [23] | XAI-AMD-DL | Ransomware dataset | 97.98% |
| [24] | Deep Ensemble | Ransomware dataset | 98.76% |
| [25] | LSTM-CNN Hybrid | Ransomware dataset | 93.53% |

## 5 Discussion

One key factor contributing to the success of the proposed model is its robustness. The ensemble model, RansoDetect Fusion, effectively combines the individual strengths of MLP1, MLP2, and MLP3. This ensemble approach allows the model to capture nuanced patterns and behaviors of RaaS attacks. By pooling the predictive power of these individual models, the ensemble model is less susceptible to overfitting and can make more informed predictions.

Another critical aspect of the proposed model's success is feature engineering and data quality. Before training, the study carefully selected and engineered features that are highly relevant to RaaS detection. These features allow the model to differentiate between normal and attack traffic effectively. Additionally, the study ensured the quality of the proposed dataset, which is essential for the model's performance. Clean, well-labeled data plays a pivotal role in training a reliable machine learning model.

The study conducted thorough hyperparameter tuning for each MLP model. Fine-tuning the hyperparameters, such as learning rates, batch sizes, and regularization methods, ensures that the models are optimized for their respective tasks. This approach maximizes the overall performance of the ensemble model. The ensemble model, RansoDetect Fusion, leverages the strengths of all three MLP models. By combining the results of MLP1, MLP2, and MLP3, the ensemble model achieves a more comprehensive view of the data and improves its overall predictive power. The ensemble approach effectively reduces the variance and bias, making the proposed model more reliable.

The evaluation metrics the study employed, such as Accuracy, Recall, Precision, and F1-score, are interpretable and insightful. By assessing these metrics comprehensively, the study gains a holistic view of the proposed model's performance. The high scores across these metrics demonstrate that the proposed model effectively minimizes false positives and false negatives, enhancing its overall effectiveness. While the proposed model demonstrates robust performance in detecting RaaS attacks, there is still room for improvement. Future directions for research may include exploring more advanced DL architectures and adapting to evolving RaaS tactics. Additionally, addressing real-time detection and scalability challenges presents exciting avenues for future study and development.

## 6 Conclusions

The proposed RansoDetect Fusion model, an ensemble of three individual Multilayer Perceptron (MLP) models (MLP1, MLP2, and MLP3), demonstrates remarkable performance in the detection of Ransomware-as-a-Service (RaaS) attacks. Through a combination of robustness, feature engineering, data quality, and hyperparameter tuning, the proposed model excels in distinguishing between normal and attack traffic. The ensemble approach effectively mitigates overfitting and bias, enhancing the model's reliability. Interpretability-driven metrics, such as Accuracy, Recall, Precision, and F1-score, validate the model's ability to minimize false positives and false negatives. However, it is important to acknowledge some limitations of the proposed work. The performance of the RansoDetect Fusion model, while impressive, still faces challenges in handling zero-day attacks and evolving RaaS tactics. The model's accuracy may vary depending on the data distribution and quality. Additionally, the computational resources required for training and deploying this ensemble model can be substantial. These limitations offer valuable insights for future research and development. For future work, there are several promising avenues to explore. Firstly, enhancing the adaptability of the proposed model to emerging RaaS threats is crucial. Continuous monitoring and training with real-time data can improve the model's responsiveness. Additionally, exploring advanced deep learning architectures, such as recurrent neural networks (RNN) and convolutional neural networks (CNN), could yield more robust and efficient results. Integration with threat intelligence feeds and external data sources could further strengthen the model's capabilities. Lastly, extending this research to other cybersecurity domains, such as intrusion detection and malware analysis, holds the potential for broader applications and impact. The field of cybersecurity is dynamic, with adversaries continually evolving their tactics. The proposed work represents a significant step towards proactive RaaS detection, but there remains much to be explored and developed. As the study addresses the limitations and delves into future research directions, the study aims to contribute to the ongoing battle against cyber threats and enhance the security of digital ecosystems. While our RansoDetect Fusion model demonstrates promising results in controlled environments, the aforementioned real-world challenges emphasize the need for a comprehensive approach to model deployment. Future research should focus on refining the model's scalability, addressing interpretability concerns, and developing mechanisms to counter adversarial threats. Moreover, collaboration with industry stakeholders and cybersecurity professionals is pivotal for translating research outcomes into effective, real-world cybersecurity solutions. The dynamic nature of cyber threats necessitates an ongoing commitment to innovation and adaptability in the field of RaaS detection.

**Acknowledgement:** The authors acknowledge the support from the Deanship of Scientific Research, Najran University, Kingdom of Saudi Arabia, for funding this research work.

**Funding Statement:** The authors acknowledge the support from the Deanship of Scientific Research, Najran University, Kingdom of Saudi Arabia, for funding this work under the Research Groups Funding Program Grant Code Number (NU/RG/SERC/12/43).

**Author Contributions:** The authors confirm their contribution to the paper as follows: conceptualization, methodology, A. Singh, Z. Mushtaq and S. Arif; validation, formal analysis, investigation, A. Singh, S. Arif, Z. Mushtaq, G. Abbas and A. Ali; writing—original draft preparation, A. Singh, S. Arif, Z. Mushtaq and G. Abbas; writing—review and editing, H. A. Abosaq, M. Irfan, A. Ali and A. A. Mazroa; supervision, resources, funding acquisition, H. A. Abosaq, M. Irfan, A. Ali, A. A. Mazroa. All authors reviewed the results and approved the final version of the manuscript.

**Availability of Data and Materials:** Publicly available datasets were analyzed in this study. This data can be found here: https://research.unsw.edu.au/projects/unsw-nb15-dataset.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] N. Islam *et al.*, "Towards machine learning based intrusion detection in IoT networks," *Comput. Mater. Contin.*, vol. 69, no. 2, pp. 1801–1821, Jul. 2021. doi: 10.32604/cmc.2021.018466.

[2] N. W. Khan *et al.*, "A hybrid deep learning-based intrusion detection system for IoT networks," *Math. Biosci. Eng.*, vol. 20, no. 8, pp. 13491–13520, Jun. 2023. doi: 10.3934/mbe.2023602.

[3] S. S. Chakravarthi, R. J. Kannan, V. A. Natarajan, and X. Z. Gao, "Deep learning based intrusion detection in cloud services for resilience management," *Comput. Mater. Contin.*, vol. 71, no. 3, pp. 5117–5133, Jan. 2022. doi: 10.32604/cmc.2022.022351.

[4] U. Divakarla, K. H. K. Reddy, and K. Chandrasekaran, "A novel approach towards windows malware detection system using deep neural networks," *Procedia Comput. Sci.*, vol. 215, no. 1, pp. 148–157, Dec. 2022. doi: 10.1016/j.procs.2022.12.017.

[5] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali and J. Ahmad, "Enhancing IoT network security through deep learning-powered intrusion detection system," *Int. Things*, vol. 24, no. 1, pp. 100936, Sep. 2023. doi: 10.1016/j.iot.2023.100936.

[6] S. Latif, W. Boulila, A. Koubaa, Z. Zou, and J. Ahmad, "DTL-IDS: An optimized intrusion detection framework using deep transfer learning and genetic algorithm," *J. Netw Comput. Appl.*, vol. 221, no. 1, pp. 103784, Jan. 2024. doi: 10.1016/j.jnca.2023.103784.

[7] S. Newaz, H. M. Imran, and X. Liu, "Detection of malware using deep learning," presented at the IEEE 4th Int. Conf. Comp. Pow. Comm. Tech., Kuala Lumpur, Malaysia, Sep. 24–26, 2021. doi: 10.1109/GUCON50781.2021.9573991.

[8] J. Gao and Z. Fang, "Utilizing benign files to obfuscate malware via deep reinforcement learning," presented at the 2022 4th Int. Conf. Intel. Info. Proc., Guangzhou, China, Oct. 14–16, 2022. doi: 10.1109/IIP57348.2022.00067.

[9] L. Alsharafi, M. Asiri, S. Azzony, and A. Alqahtani, "Malware detection based on deep learning," presented at the 2023 3rd Int. Conf. Comp. Info. Tech., Tabuk, Saudi Arabia, Sep. 13–14, 2023. doi: 10.1109/ICCIT58132.2023.10273961.

[10] S. Rahman, S. N. F. Mursal, M. A. Latif, Z. Mushtaq, M. Irfan and A. Waqar, "Enhancing network intrusion detection using effective stacking of ensemble classifiers with multi-pronged feature selection technique," presented at the 2023 2nd Int. Conf. Emer. Tre. Elec. Con. Tele. Eng., Lahore, Pakistan, Nov. 27–29, 2023. doi: 10.1109/ETECTE59617.2023.10396717.

[11] A. A. Darem, F. A. Ghaleb, A. A. Al-Hashmi, J. H. Abawajy, S. M. Alanazi and A. Y. Al-Rezami, "An adaptive behavioral-based incremental batch learning malware variants detection model using concept drift detection and sequential deep learning," *IEEE Access*, vol. 9, pp. 97180–97196, Jun. 2021. doi: 10.1109/ACCESS.2021.3093366.

[12] Ö. Aslan and A. A. Yilmaz, "A new malware classification framework based on deep learning algorithms," *IEEE Access*, vol. 9, pp. 87936–87951, Jun. 2021. doi: 10.1109/ACCESS.2021.3089586.

[13] S. Homayoun *et al.*, "DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer," *Future Gener. Comput. Syst.*, vol. 90, no. 1, pp. 94–104, Jan. 2019. doi: 10.1016/j.future.2018.07.045.

[14] H. Alamro, W. Mtouaa, S. Aljameel, A. S. Salama, M. A. Hamza and A. Y. Othman, "Automated android malware detection using optimal ensemble learning approach for cybersecurity," *IEEE Access*, vol. 11, pp. 72509–72517, Jul. 2023. doi: 10.1109/ACCESS.2023.3294263.

[15] Y. Wei and Y. Sekiya, "Sufficiency of ensemble machine learning methods for phishing websites detection," *IEEE Access*, vol. 10, pp. 124103–124113, Nov. 2022. doi: 10.1109/ACCESS.2022.3224781.

[16] G. D. C. Bertoli *et al.*, "An end-to-end framework for machine learning-based network intrusion detection system," *IEEE Access*, vol. 9, pp. 106790–106805, Jul. 2021. doi: 10.1109/ACCESS.2021.3101188.

[17] F. A. Almarshad, M. Zakariah, G. A. Gashgari, E. A. Aldakheel, and A. I. A. Alzahrani, "Detection of android malware using machine learning and siamese shot learning technique for security," *IEEE Access*, vol. 11, pp. 127697–127714, Nov. 2023. doi: 10.1109/ACCESS.2023.3331739.

[18] G. Siewruk and W. Mazurczyk, "Context-aware software vulnerability classification using machine learning," *IEEE Access*, vol. 9, pp. 88852–88867, Apr. 2021. doi: 10.1109/ACCESS.2021.3075385.

[19] M. Q. Tran, M. Elsisi, K. Mahmoud, M. K. Liu, M. Lehtonen and M. M. F. Darwish, "Experimental setup for online fault diagnosis of induction machines via promising iot and machine learning: Towards Industry 4.0 empowerment," *IEEE Access*, vol. 9, pp. 115429–115441, Aug. 2021. doi: 10.1109/ACCESS.2021.3105297.

[20] B. Urooj, M. A. Shah, C. Maple, M. K. Abbasi, and S. Riasat, "Malware detection: A framework for reverse engineered android applications through machine learning algorithms," *IEEE Access*, vol. 10, pp. 89031–89050, Feb. 2022. doi: 10.1109/ACCESS.2022.3149053.

[21] A. Singh, Z. Mushtaq, H. A. Abosaq, S. N. F. Mursal, M. Irfan and G. Nowakowski, "Enhancing ransomware attack detection using transfer learning and deep learning ensemble models on cloud-encrypted data," *Elect.*, vol. 12, no. 18, pp. 3899, Sep. 2023. doi: 10.3390/electronics12183899.

[22] M. Mousa, A. M. Bahaa-Eldin, M. Sobh, and A. Taha, "Zero-day malware detection through unsupervised deep learning," presented at the 2023 Int. Mob. Intel. Ubi. Comp. Conf., Cairo, Egypt, Sep. 27–28, 2023. doi: 10.1109/MIUCC58832.2023.10278325.

[23] S. K. Smmarwar, G. P. Gupta, and S. Kumar, "XAI-AMD-DL: An explainable AI approach for android malware detection system using deep learning," presented at the 2023 IEEE Wo. Conf. App. Intel. Comp., Sonbhadra, India, Jul. 29–30, 2023. doi: 10.1109/AIC57670.2023.10263974.

[24] A. A. Al-Hashmi *et al.*, "Deep-ensemble and multifaceted behavioral malware variant detection model," *IEEE Access*, vol. 10, pp. 42762–42777, Apr. 2022. doi: 10.1109/ACCESS.2022.3168794.

[25] M. Asaduzzaman and M. M. Rahman, "An adversarial approach for intrusion detection using hybrid deep learning model," presented at the 2022 Int. Conf. Info. Tech. Res. Inn., Jakarta, Indonesia, Nov. 10, 2022. doi: 10.1109/ICITRI56423.2022.9970221.