IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

Ransomware detection system using machine learning

N. Nagoor Meeravali[1], Mogamatam Ramyasri[2], Sandhireddy Poojitha[3], Shaik Khajavali[4], Komatineni Srinikhil[5]

[1]Assistant Professor, Department of Computer Science Engineering, Chalapathi Institute of Engineering and Technology, Chalapathi Rd, Nagar, Lam, Guntur, Andhra Pradesh- 522034

[2,3,4,5] Students, Department of Computer Science Engineering, Chalapathi Institute of Engineering and Technology, Chalapathi Rd, Nagar, Lam, Guntur, Andhra Pradesh- 522034

Email id: meeravali587@gmail.com[1], ramyasrimogamatam@gmail.com[2], poojithasandireddy@gmail.com[3], khajaktm11@gmail.com[4], srinikhilkomatineni357@gmail.com[5]

Abstract:

Ransomware attacks represent a growing cybersecurity threat, affecting individuals and organizations by compromising data integrity, causing financial losses, and damaging reputations. Early and accurate detection of ransomware is essential to mitigate these risks. This study provides a comprehensive review of modern ransomware detection methods, examining various approaches and highlighting their advantages and limitations. The research covers techniques for detecting, preventing, and recovering from ransomware, based on an analysis of studies published between 2017 and 2022. The goal is to present the latest trends in automated ransomware detection and offer insights into future research challenges. Additionally, this study discusses the potential for improving ransomware detection using machine learning and other advanced techniques. The work concludes with a focus on unresolved issues in ransomware detection, encouraging further investigation.

Keywords: Ransomware detection, Cyber security, Machine learning, Automated detection, Data security, Prevention techniques, Future research challenges

1.Introduction

The rapid growth in the use of mobile devices has made Android one of the leading operating systems for smartphones and tablets. As of July 2023, Android has the highest market share of 70.8% [1]. Android is an open-source, Linux-based mobile operating system developed by Google [2]. Android 13 is the most recent version, released in 2022. It supports many technologies such as Wi-Fi, short message service (SMS), Bluetooth, accelerometers, camera, global positioning systems (GPS), voice over LTE (VoLTE), etc. Because of its open nature, Android has become immensely popular among developers and consumers. Additionally, software developers can quickly alter and upgrade it to conform to the most recent standards for mobile technology. Unfortunately, this popularity has also attracted cybercriminals who exploit users' private data and personal information without their consent [3]. One of the most prevalent and disruptive attacks targeting Android devices is ransomware. Ransomware constitutes a type of malware that encrypts files on a device and demands payment for their decryption. Typically, cybercriminals demand payment in cryptocurrencies such as Bitcoin to

evade detection. A typical scenario in ransomware attacks often begins when the user downloads a fraudulent application from either the Google Play Store or an alternative third-party marketplace [4]. With the increasing presence of Android devices and the open nature of the platform, which allows easy app downloads from unofficial sources, the severity of ransomware attacks has reached alarming levels. In such a situation, data recovery can be challenging, and the risk of further attacks and identity theft is increased, leading to a diminished trust in security solutions by users [5,6]. Ransomware attacks commonly focus on specific industries. In 2022, manufacturing companies worldwide experienced 437 such attacks, while the food and beverage sector followed closely with more than 50 ransomware incidents. When it comes to the distribution of ransomware attacks on critical infrastructure, North America took the lead among global regions, with Europe following in second place [7]. Additionally, the global number of ransomware attacks per year from 2017 to 2022 is as follows: in 2022, organizations detected a staggering 493.33 million ransomware attacks worldwide [7].

Moving forward to how ransomware is carried out in Android devices; firstly, it is important to know that ransomware continually grows with advanced encryption capabilities by displacing established standards, such as phishing, banking trojans, distributed denial-of-service (DDoS), and crypto-jacking. However, criminals use these models as an initial stepping-stone, then escalate the attack and eventually carry out the targeted attacks, hence forcing payment from victims. By opening an email attachment or clicking an ad, accessing a link, or even navigating to a website that has malware embedded in it, one can unknowingly download ransomware onto an electronic device. Once the code has been loaded on a device, it locks access to the device and any stored files and data. Versions that are more destructive can encrypt data on networked devices as well as local drives and attached drives. The users discover it when their data become inaccessible, or when messages pop up informing them of the attack and demanding ransom payments. Criminals threaten to publicly expose confidential data if their victims do not pay within the specified time frame or opt to recover encrypted data through backups. Some attackers even sell confidential data at auction on the dark web. It is essential to know that ransomware attacks have numerous different appearances, and they show up in all shapes and sizes. There are two main categories, namely lock-screen and crypto [8]. In the lock screen, the ransomware blocks access to the system, asserting that the system is encrypted. Lock-screen ransomware does not usually target critical files; it generally only wants to lock the user out. On the other hand, crypto ransomware encrypts data on a system, such as documents, pictures, and videos, making the content useless without the decryption key and without interfering with basic device functions. Users can see their files but cannot access them unless they pay the ransom demand, or all their files would be deleted. Some examples of Android ransomware include Android/Simplocker, Android/Lockerpin, WannaLocker, etc. [8]. Consequently, there is a dire need to develop effective methods for detecting Android ransomware to counter this escalating danger.

2.Materials and methods

This work suggests a multi-phase novel Cost-Sensitive Pareto Ensemble framework named “CSPE-R” against zero-day Ransomware detection. The workflow is decomposed into 5

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

phases: (1) core features hunting, (2) cost matrix formulation, (3) learning heterogeneous base estimators, (4) estimator selection, and (5) decision aggregation. The general context of the suggested model is displayed in Fig

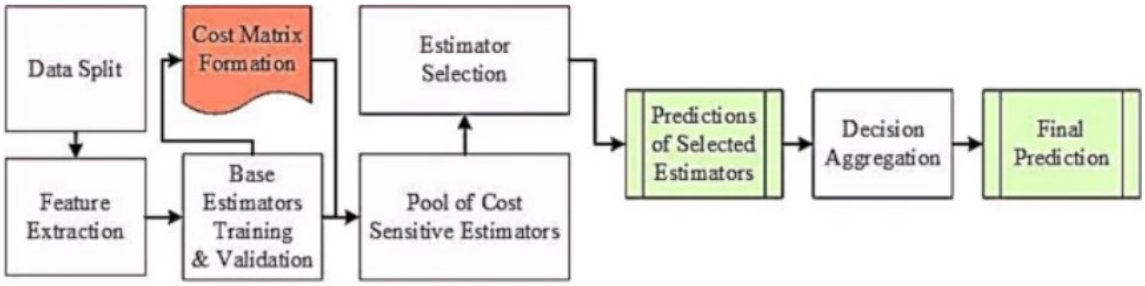

Figure: proposed CSPE-R system

This section discusses the rationale of using our design choices to detect zero-day ransomware and handle its related challenges. In the proposed approach, we exploit the heterogeneous runtime events as an alternative to static and specific events, as in the static analysis features may not always detect the attack modalities. Also, particular events are not suitable as they might not happen, or happen when the process is terminating.

Dataset

We used the dataset developed established in February 2016 as a training dataset to construct the Elde Ran prediction model. The dataset is obtained by analyzing the samples in a sandboxed environment. The dataset comprehensively includes the dynamic behaviour of running the sample in a safe environment. In the dataset, malicious samples are labelled as ransomware (one or positive class), and benign samples are labelled as good ware (zero or negative class). It contains of 582 ransomware and 942 good ware instances. Ransomware samples are further classified into 11 families

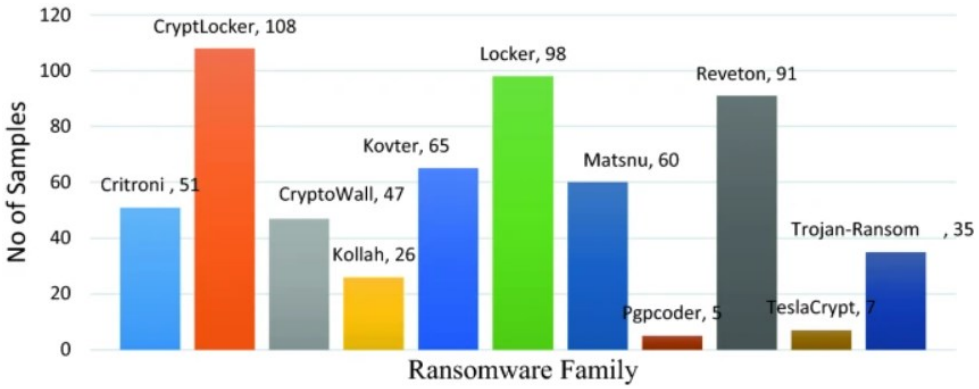

Figure: Ransomware family vs. no of samples

Ransomware sensitive heterogeneous base estimators

In case of data scarcity, it is challenging to hybridize the ensemble of deep learning models. Therefore, the proposed CSPE-R method exploited both structural and empirical minimization benefits by training multiple classifiers such as SVM, *Random Forest (RF),* and *Logistic*

Regression Classifier (LRC) on derived deep features. As, classifiers with similar training performances may have different generalization results. The set of classifiers, when worked together, can explore a more exhaustive solution space. Therefore, the proposed technique ensemble the heterogeneous base estimators, e.g. cost sensitive SVM, weighted LR, and cost sensitive RF, to overcome the cost indifference and class imbalance problem. These ransomware sensitive base estimators are trained on the derived semantic core features of sizes 100 and 500. The parameter configuration of these classifiers is carried out using five cross-validations. Parameter values obtained after optimization are: SVM (C = 100, kernel = , gamma = 0.1.), RF (max_ features = 'auto', n_estimators = 700, max_depth = 9, criterion = 'gini') and LR(C = 0.1, penalty = 'l1', tol = 0.01). These models are optimized on precision and recall due to highly imbalance data. To resolve the issue of imbalance and high priority minority class derived the cost matric for different class.

Cost matrix formation

The optimal cost matrix of different base estimators is made by using the five cross-validation method. The ransomware dataset was separated into seen classes and unseen classes, where the training classes (seen classes) and test classes (unseen classes) are disjoint to ensure zero-day attack in the test phase. All the base estimators were trained with the seen class dataset, class weights, and additional hyperparameters alignments were designated based on estimator average performance on the five-fold validation dataset.

Table: Cost matrix of errors

Models	FN	FP
SVM	2	8
RF	6	12
LR	2	16

Proposed Pareto optimality-based estimator selection strategy

The ensemble selection process is inherently a multi-objective problem that possess two or more objectives simultaneously e.g. maximizing the classifiers diversity, maximizing the classifier's accuracy, minimizing error and minimizing the number of base classifiers so on39. All these goals are conflicting, as insufficient number of base estimators lead to decline in accuracy and gain in error. In order to achieve these objectives simultaneously, previous ensemble selection approaches can only deal with a single cost function. But more recently, it has been revealed that, explicit formulation of each goal is more effective this is due to the effective application of multi-objective genetic algorithms in the field of machine learning such as features optimization, Pareto-optimization, clustering etc. The proposed ensemble selection technique simultaneously optimizes false negative and net-error.

$$arg\,mins\ (fN(H),\ \mathrm{Net}-error(H)) \quad \text{..... (1)}$$

Decision aggregation

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

A decision aggregation scheme combines the output of multiple base estimators into a single result. The proposed decision scheme bifurcates between ransomware and good ware. This methodology aggregates the decision of selected heterogeneous estimators by OR logic. It is flagged as ransomware positive if any of the estimators mark it. Otherwise, it is good ware.

3. Result and discussions

to develop a framework that can efficiently acquire the robust representation from the raw data for ransomware detection. In this study Citroni, Crypt Locker, Cryp to wall, Kollah, Kovter, Locker, and Matsnu families of ransomware were used for training and validation, and Pgp coder, Reveton, Tesla Crypt and Trojan Ransomware were used for testing. Ransomware detection is tedious task due to varying underlying distribution and data scarcity. Hence, we offered a multi-phase framework, "CSPER," for ransomware detection. The phases of proposed framework can be divided as: deep features extraction and ransomware detection. Ransomware detection phase is subdivided into: (1) base estimators training, (2) estimators' selection and, (3) estimators aggregation strategy. The generalization aptitude is evaluated by weighing the proposed method on zero-day ransomware. Overall, the performance of the proposed method is evaluated on error measures and recall. Evaluation with former related approaches is also accompanied and discussed.

Effectiveness of different feature spaces

In this section, we will show the effectiveness of using CAE based feature spaces. Figure 8 shows the effectiveness of reduced representation achieved using CAE based transformation on three base learners SVM, RF, and LR. The feature size of the reduced representation shown is 100. It can be observed that all base estimators trained on reduced latent features are showing improved recall performance (CFH-RF (0.85), CFH-LR (0.90), CFH-SVM (0.90)) compared to the recall performance (RF (0.79), LR (0.81), SVM (0.79)) on original features. Consequently, the CAE can bring core discriminative representation by which all base estimators can perform better.

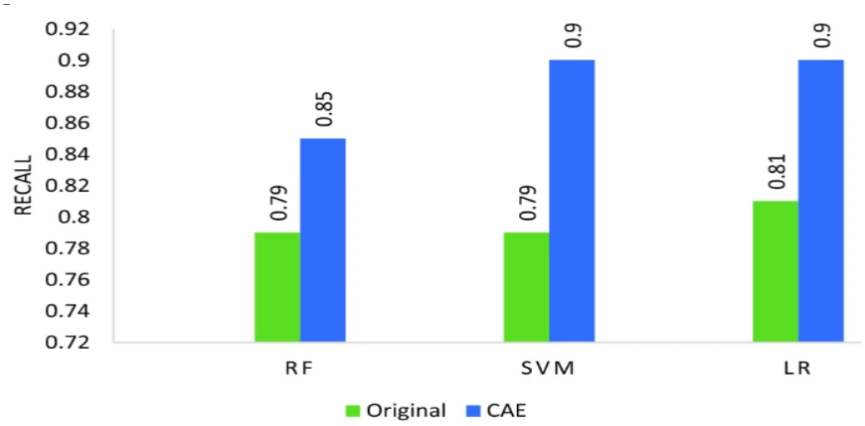

Figure: Comparison of original features vs. CAE reduced transformation on zero-day test data

The results for the selection of different feature sizes are visualized in Fig. It shows the effect of zero-day attacks on two reduced set of features (100 and 500) and a complete set of original

features (16,382) trained on RF. A feature reduction is carried out by training CAE by varying the number of hidden neurons and careful selection of penalty parameters in the validation phase.

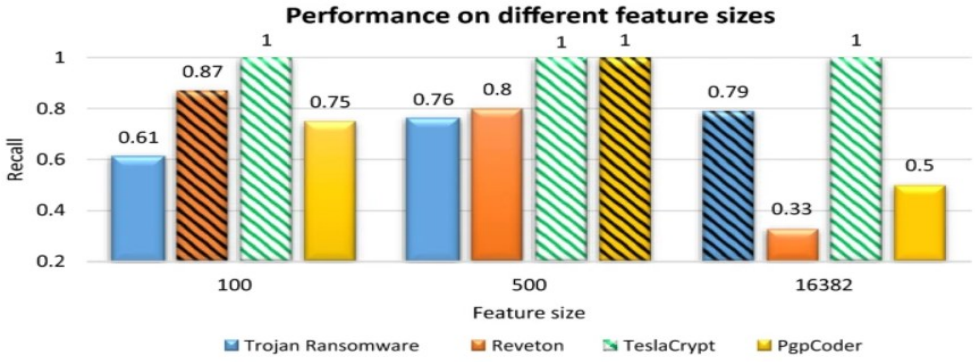

Figure: Comparison of different feature subspaces against zero-day test data

The bars filled with patterns are showing the best performer feature size for a particular variant of ransomware. It can be observed that Reveton is showing an improved detection rate on the 500-feature set. Whereas, Pgpcoder detection is showing the better result on 100 feature set. However, Trojan Ransomware is better detected by a complete set of original features. Therefore, it is proven that one single reduced feature set is not enough to detect all zero-day attacks.

Discussions:

In this work, we have developed a deep feature based multi-phase ransomware detection framework "CSPER". The uniform robust features representation can facilitate the cyber-security experts to generate the dynamic features of any unknown attacks in an unsupervised manner.

In this study, we exploited the contractive autoencoder to suppress the little changes around different families of ransomware and goodware to find core embeddings. The proposed contractive pressure based deep feature extraction overcomes the limitations of existing feature reduction and extraction techniques used by different researchers, which resulted in high false-positive and ignored true positives. Principal Component Analysis PCA, is unable to find principal component if there exist no relation between features. Similarly, CorrAUC43,44 is a correlation-based wrapper feature selection method developed to detect the malicious traffic. Simple autoencoder based feature reduction techniques presented in literature are highly sensitive to noisy data.

Conclusion:

Ransomware is one of the highly threatening malwares and is difficult to detect because of continuous increase in its new variants. Thus, IDS trained for specific ransomware events often results in suboptimal performance for new adaptations of ransomware (zero-day) attacks. In this work, a new ensemble learning strategy, "CSPE-R" is developed to address the challenge of heterogeneous behaviour of ransomware attacks by aggregating the discrimination ability of

multiple-experts and considering varied events. In this regard, we explored diverse semantic spaces, exploited cost-sensitive optimization, and developed a new Pareto-optimality based base-estimator selection strategy to improve the zero-day ransomware detection performance. The proposed ensemble selection strategy effectively improves the generalization performance against zero-day ransomware attack by gaining improvement in recall (9%) and F1-score (1%), when compared to the best performing base estimator and other ensemble learning strategies. The proposed idea of learning dissimilarities between the different families of the attacks and subsequent development of a cost sensitive based ensemble for the detection of zero-day ransomware attacks has the potential to be applied for other types of zero-day attacks as well.

References:

1. Yunus, Y.K.B.M.; Ngah, S.B. Review of Hybrid Analysis Technique for Malware Detection. *IOP Conf. Ser. Mater. Sci. Eng.* **2020**, *769*, 012075
2. Singh, R. An Overview of Android Operating System and Its Security Features. *Int. J. Eng. Res. Appl.* 2014, *4*, 519–521.
3. Aljabri, M. Machine Learning-Based Detection for Unauthorized Access to IoT Devices. J. Sens. Actuator Netw. 2023, 12, 27
4. Alsoghyer, S.; Almomani, I. Ransomware Detection System for Android Applications. *Electronics* 2019, *8*, 868.
5. Song, S.; Kim, B.; Lee, S. The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform. *Mobile Inf. Syst.* 2016, *2016*, 2946735.
6. Ekta; Bansal, U. A Review on Ransomware Attack. In Proceedings of the 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India, 21–23 May 2021.
7. Sharma, S.; Kumar, R.; Krishna, C.R. A survey on analysis and detection of Android ransomware. *Concurr. Comput. Pract. Exp.* 2021, *33*, e6272.
8. Kapratwar, A.; Di Troia, F.; Stamp, M. Static and Dynamic Analysis of Android Malware. In Proceedings of the 3rd International Conference on Information Systems Security and Privacy, Porto, Portugal, 19–21 February 2017.