information

Article

An Incremental Mutual Information-Selection Technique for Early Ransomware Detection

Mazen Gazzan [1,2,*] and Frederick T. Sheldon [1]

[1] Department of Computer Science, College of Engineering, University of Idaho, Moscow, ID 83844, USA; sheldon@uidaho.edu.
[2] Department of Information Systems, College of Computer Science & Information Systems, Najran University, Najran 11001, Saudi Arabia
* Correspondence: gazz6545@vandals.uidaho.edu or mzgazzan@nu.edu.sa

Abstract: Ransomware attacks have emerged as a significant threat to critical data and systems, extending beyond traditional computers to mobile and IoT/Cyber–Physical Systems. This study addresses the need to detect early ransomware behavior when only limited data are available. A major step for training such a detection model is choosing a set of relevant and non-redundant features, which is challenging when data are scarce. Therefore, this paper proposes an incremental mutual information-selection technique as a method for selecting the relevant features at the early stages of ransomware attacks. It introduces an adaptive feature-selection technique that processes data in smaller, manageable batches. This approach lessens the computational load and enhances the system's ability to quickly adapt to new data arrival, making it particularly suitable for ongoing attacks during the initial phases of the attack. The experimental results emphasize the importance of the proposed technique in estimating feature significance in limited data scenarios. Such results underscore the significance of the incremental approach as a proactive measure in addressing the escalating challenges posed by ransomware.

Keywords: ransomware; early detection; mutual information; incremental feature selection; deep learning

Citation: Gazzan, M.; Sheldon, F.T. An Incremental Mutual Information-Selection Technique for Early Ransomware Detection. *Information* **2024**, *15*, 194. https://doi.org/10.3390/info15040194

Academic Editor: Aneta Poniszewska-Maranda

Received: 7 March 2024
Revised: 26 March 2024
Accepted: 29 March 2024
Published: 31 March 2024

1. Introduction

Ransomware attacks have become a major threat to essential data and systems, as evidenced by the challenges they pose [1–3]. Their reach extends beyond traditional computers to mobile and IoT/Cyber–Physical Systems, necessitating a deep dive into ransomware behavior and the evaluation of defense strategies across different platforms [4]. The substantial impact of such attacks is evident from the global damages inflicted on various systems around the world [5–8]. Given the complexity of ransomware, showcased by variants like LockBit 2.0, it is clear that advanced preventative and remediation strategies are needed [9,10]. Research is being directed toward developing detection systems that leverage behavioral, network traffic, and machine learning techniques for real-time detection and categorization of ransomware threats [11–13]. Efforts are also increasing in the area of recovery solutions to restore data access following ransomware disruptions [14,15]. Addressing ransomware comprehensively requires an understanding of its attack vectors, patterns, and behaviors, alongside the establishment of resilient defense infrastructures [16,17]. As these threats evolve, proactive steps, such as predicting and swiftly detecting attacks, become crucial, particularly in critical infrastructure sectors like healthcare and industrial systems [18,19]. The vulnerabilities ransomware introduces are also affecting diverse sectors such as IoT and AI-dependent equipment, which underscores the extensive impact of this cyber threat [20,21]. Therefore, a thorough understanding of ransomware's evolution, taxonomy, and effective countermeasures is essential [22–25].

The present strategies used for identifying ransomware utilize a variety of methods, including those based on detecting known signatures and observing behaviors, in addition to more progressive techniques like machine learning and smart systems. These strategies employ regular pattern detection for tracking threats and gathering intelligence, utilize in-depth systems for ransomware threat tracking, and implement adaptable prevention methods for the Internet of Medical Things (IoMT) [26–28]. Detection techniques that make use of fuzzy hashing, analysis of file entropy, and machine learning classifiers have been examined in numerous studies to reduce ransomware risks [29–31]. Additionally, there has been an exploration into employing dynamic analysis, decoy-based security, and process monitoring to improve ransomware detection [32–34]. The creation of smart and adaptable detection systems, alongside the use of performance counters and detectors that focus on file-based ransomware, is indicative of the complex nature of these detection solutions [35–37]. Furthermore, the adoption of AI-driven hybrid methods and layered profiling with machine learning has been pivotal in enhancing ransomware-detection processes [38]. Altogether, these varied methods are designed to tackle the changing dynamics of ransomware threats and boost system robustness against these malicious incursions.

The emphasis on recognizing ransomware attacks before they begin the encryption process is a key focus in cybersecurity research [39,40]. The early detection of ransomware behavior is particularly challenging due to the stealthy nature of ransomware attacks, which often do not leave clear indicators or generate significant anomalies that can be easily detected by traditional security measures. Ransomware attacks are designed to encrypt files quietly without alerting users or security systems until the attack is fully deployed and a ransom demand is made. This makes it difficult for detection systems to identify and mitigate these attacks in their early stages before significant damage.

Innovative methods have been suggested to improve early detection. For instance, Ref. [26] highlighted the crucial role of analyzing system logs for early signs, which facilitates rapid response to preempt ransomware threats. Furthermore, Ref. [8] introduced strategies aimed at the pre-encryption activities of crypto-ransomware, showing the benefits of early, proactive detection. The study by [41] also underlined the effectiveness of estimating file entropy for early detection in cloud services, pointing out the importance of file analysis in these strategies. In addition, research on employing machine learning for the classification of Bitcoin transactions related to ransomware provides a significant boost to early detection methods, underscoring the importance of early interventions in the fight against ransomware [42]. Collectively, these initiatives highlight the progressive nature of early detection techniques, which aim to strengthen cybersecurity defenses by stopping ransomware before it can encrypt and compromise data, thus preventing potential harm and data loss.

The current challenges in the early detection of ransomware are primarily linked to the lack of sufficient data during the attack's pre-encryption stage. This scarcity of data hampers the ability to effectively identify and counter ransomware threats before they fully execute. The study by [43] pointed out the difficulties in gathering behavioral data in the brief window before the ransomware deploys its payload, which often results in ineffective detection, as the harmful activity has usually commenced by then. Additionally, Ref. [44] brought attention to the shortcomings of existing early detection mechanisms, noting the struggle to acquire and process the necessary data in the pivotal moments before encryption by ransomware. These identified limitations highlight the urgent necessity for more advanced and all-encompassing early detection systems capable of overcoming the data-gathering obstacles present in the initial stages of ransomware attacks.

Deep learning techniques like Deep Belief Networks (DBN), Convolutional Neural Networks (CNN), and Generative Adversarial Networks (GAN) have been used for detecting malware. The GAN, for instance, can be used for creating synthetic data to boost the effectiveness of detection systems [40]. These synthetic instances are particularly useful in countering the adaptive techniques that malware uses to evade detection. The

application of GANs in identifying malware has been validated through numerous studies, which demonstrate their capacity to refine detection processes. For example, Ref. [45] employed GANs to produce adversarial examples, thereby improving the system's ability to identify malicious network traffic. In addition, Ref. [46] showed how GANs could expand an original dataset by generating variations of malicious code, highlighting the benefits of enhancing dataset variability for better detection outcomes. Further, Ref. [47] showcased the integration of GANs with various node attributes, illustrating how GANs can outperform traditional detection models. The deployment of GANs in the realm of malware detection holds significant promise in managing the increasing complexity of malware challenges and bolstering the ability of detection models to adapt to new malware types, ultimately aiding in the development of more resilient and effective malware detection frameworks.

The process of selecting features is pivotal in simplifying the complexity of data for models that detect malware by minimizing the number of data attributes that need to be processed. This was made clear by [48], who underlined the deep importance of choosing the right features for tasks like visual recognition to ensure precise detection. Javaheri, et al. [49] showed that careful feature selection can significantly boost the rate of correctly identified threats in deep learning systems, proving its value in elevating the performance of such systems. Moreover, Ref. [50] integrated both comprehensive and detailed imagery of disguised and non-disguised malware, illustrating how selecting the right features is essential when preparing data for GAN-based models. In addition, Ref. [51] applied feature selection to sharpen the accuracy of malware detection systems, reinforcing the necessity of efficient feature-selection methods to improve the overall capabilities of these systems. Taken together, these pieces of research highlight the indispensable nature of feature selection in cutting down data dimensionality and refining the data used for GAN-based malware detection, thereby aiding in the creation of more effective and sophisticated malware detection infrastructures.

Data dimensionality plays a vital role in the precision of early ransomware detection, and its management is key to crafting accurate detection models. The reduction in features has led to higher accuracy in various studies, showcasing the influence of data dimensionality on the accuracy of these models [52]. Yet, Al-Rimy and colleagues cautioned against the negative impact that a lack of data in the pre-encryption stage can have on the effectiveness of feature selection, which in turn can reduce the accuracy of detection [12]. These insights reveal a complex interplay between data dimensionality and the accuracy of early ransomware-detection systems. They suggest that while reducing dimensionality can make models more efficient, the availability and integrity of data during the critical pre-encryption phase remain essential to ensure the selection of high-quality features.

The integration of feature selection with malware-detection models has faced scrutiny due to the inflexibility of these selection methods, which often overlook the dynamic progression of malware traits. Lall, et al. [53] pointed out the difficulties in managing data that is both high-dimensional and limited in sample size, a scenario that complicates the process of classification. Similarly, Ref. [54] employed feature extraction and selection on time-series data to streamline the training of monitors, which revealed the shortcomings of conventional feature-selection methods in keeping pace with the changing attributes of malware. Furthermore, Ref. [55] discussed the interpretability issues of GAN models, stressing the necessity for feature-selection techniques that are capable of adapting to the fluidity of malware features. Collectively, these studies draw attention to the limitations of standard feature-selection approaches when combined with GAN frameworks, accentuating the demand for more flexible and evolving feature-selection methods in the realm of malware detection.

To address the rigidity issue that existing feature selection suffers from when applied to malware attack detection, this paper proposes an adaptive feature-selection technique based on mutual information. It leverages a batch-based approach to process data in smaller, manageable segments. This strategy not only reduces the computational burden

but also allows the system to adapt to new data trends and anomalies more efficiently. The methodology is underpinned by the principle of processing data incrementally and updating feature relevance dynamically, making it highly suited for resource-constrained environments where real-time data processing is critical. The primary focus of this study is on the early detection of ransomware attacks, specifically addressing the challenge of selecting relevant and non-redundant features for detection models when only limited data are available. This study proposes an incremental mutual information-selection technique aimed at selecting the most relevant features at the early stages of ransomware attacks. This technique is designed to process data in smaller batches, which reduces computational load and enhances the system's adaptability to new data, making it suitable for early detection of ongoing attacks. To this end, the contribution of the paper is three-fold.

- An incremental mutual information-selection (IMIS) technique was developed to adaptively reassess the relevancy of selected features dynamically when new data arrives.
- The IMIS was integrated into a DBN-based ransomware-detection model for better detection accuracy.
- An extensive experimental evaluation of the IMIS was conducted and compared with the existing methods to measure the improvement achieved.

The rest of this paper is organized as follows. Section 2 details the related works. Section 3 describes the methodology adopted to implement the model. Section 4 presents and discusses the results obtained. The paper ends with the conclusion section that summarizes the contribution.

2. Related Works

Ransomware represents a serious challenge to cybersecurity, demanding advanced detection strategies. The process of selecting pertinent features is key to refining the precision and operational efficiency of these models. Bijitha, et al. [56] provided a thorough review of the various techniques used for detecting ransomware, shedding light on different feature-selection methods. Scalas, et al. [39] examined the use of system API data for detecting Android ransomware, pointing out the crucial impact of feature selection on enhancing detection capabilities. Additionally, Ref. [57] discussed the advantages and the constraints of using automated dynamic analysis in ransomware detection, indicating the importance of feature selection in such active detection frameworks. Lee, et al. [30] looked into the use of machine learning to analyze file entropy for detecting ransomware in backup systems, stressing the necessity of careful feature selection for effective detection across various settings. Moreover, Ref. [26] stressed the urgency for innovative approaches in the prevention, detection, and elimination of ransomware, highlighting the vital role of feature selection in crafting strong detection systems. Within the scope of ransomware detection, the implementation of feature-selection methods has proven to be effective in increasing the accuracy and efficiency of the detection models, as demonstrated by Almashhadani, et al. [11], who proposed a multi-classifier system for detecting crypto ransomware on networks, underlining the enhancement of ransomware activity classification through the use of feature selection.

Maimó, et al. [35] concentrated on the detection of ransomware spread in integrated clinical environments, underscoring the importance of selecting the right features for identifying ransomware activities in these complex systems. Similarly, Song, et al. [34] investigated effective ransomware-prevention methods on the Android platform through process monitoring, emphasizing the significance of feature selection in proactive detection. Additionally, Ref. [44] provided a comprehensive review of ransomware attack-detection methods, offering insights into the challenges and limitations inherent in current feature-selection approaches used in ransomware detection. The crucial role of feature selection in ransomware detection was further highlighted by [25], who introduced a weighted minimum redundancy maximum relevance technique for the early detection of

ransomware in industrial environments, focusing on the need to reduce data complexity and extract succinct representations of attack patterns. Furthermore, Ref. [58] developed an intrusion detection system using the Social Leopard algorithm to identify ransomware attacks, pointing out the intricacies and shortcomings of existing security models in the context of ransomware detection. Collectively, these studies underline the vital contribution of feature-selection methods in improving the precision, efficiency, and adaptability of ransomware-detection models across various sectors and settings.

Abbasi [59] introduced a wrapper feature-selection approach to tackle the challenge of high data complexity in ransomware behavior analysis, employing evolutionary algorithms and deep neural networks for this purpose. Alqahtani and Sheldon [44] emphasized the crucial role of effective feature extraction and selection in the early stages of ransomware-detection models. Additionally, Ref. [60] created a system for ransomware detection that monitors API calls, underlining the value of feature selection in addressing the shortcomings of traditional signature-based and static detection approaches. Chen, et al. [61] showcased the utility of TF-IDF in pinpointing distinctive features for automated analysis of ransomware behavior. Al-Rimy, et al. [12] devised a Dynamic Pre-encryption Boundary Delineation and Feature Extraction (DPBD-FE) strategy for precise feature extraction and selection during the critical pre-encryption phase. Furthermore, Ref. [26] applied Sequential Pattern Mining to detect maximal frequent patterns in ransomware activities, using these as key features for classification. Taken together, these studies highlight the indispensable role of feature selection in boosting the precision and efficiency of models designed to detect ransomware.

3. Methodology

The idea behind Incremental Mutual Information (IMI) lies in its ability to dynamically update the relevance of features as new data are acquired. In traditional MI, feature relevance is typically evaluated once against the entire dataset, which can become quickly outdated in the rapidly evolving ransomware landscape. IMI addresses this limitation by iteratively reassessing the mutual information of features as new batches of data are processed. This continual update ensures that the feature selection remains current with respect to data characteristics. Furthermore, IMI incorporates a weighting mechanism to balance the contribution of historical data against new data when estimating the feature significance. Therefore, a more nuanced feature selection can be guaranteed. The weighting coefficient is adjusted based on the correlation between historical and new data, ensuring that the most relevant and current features are prioritized for ransomware detection. Implementing IMI in the ransomware-detection model involves several key steps. Using a small set of data, the initial mutual information score is calculated for all features concerning the class variable. Subsequent batches are then incrementally added, and the MI scores are recalculated and updated. This incremental approach ensures a quick adaptation to new attack patterns.

3.1. Incremental Mutual Information Selection (IMIS)

The Incremental Mutual Information (IMI) technique dynamically updates feature relevance by processing new batches of data and recalculating the mutual information between features and the target class. As new data arrive, the IMI technique evaluates the relevance of each feature in the context of the newly arrived data, allowing for the detection model to adapt to new patterns or behaviors associated with ransomware attacks. This dynamic update mechanism ensures that the feature-selection process remains relevant and effective over time, enhancing the model's ability to detect ransomware attacks at their early stages.

To mathematically formulate how feature relevance in IMI is updated, we start with defining features as an input matrix X and the class label as an output vector Y as follows. Let $X = \{x_1, x_2, \ldots, x_n\}$ be the set of n features in the dataset, and Y be the target

variable. The mutual information between a feature x_i and the target Y is denoted as $I(x_i; Y)$.

The dynamic updating process can be outlined as follows:

Initially, the mutual information is calculated for each feature x_i with respect to the target Y using the following equation:

$I(x_i; Y)$ for $i = 1,2,\ldots,n$.

When new data arrive, mutual information for each feature is recalculated and updated as follows.

Let X_{new} represent the new data. The updated mutual information is

$$I_{new}(x_i; Y) = \alpha \cdot I_{prev}(x_i; Y) + (1 - \alpha) \cdot I(x_i; Y \mid X_{new})$$

where $I_{prev}(x_i; Y)$ is the previous mutual information value, and α is a weighting factor $(0 \leq \alpha \leq 1)$ that balances the impact of new data versus historical data. If new features $x_n + 1, x_n + 2, \ldots, x_n + m$ are added, calculate $I(x_n + j; Y)$ for $j = 1,2,\ldots,m$.

Periodically reassess the relevance of each feature based on the updated mutual information. Features with significantly lower updated mutual information are deprioritized and removed (based on number of desired features).

The Feedback Loop for Model Adjustment relies on the performance metric ($Perf$) of the model (e.g., accuracy and precision). If $Perf$ decreases below a threshold, the reevaluation of the feature set is triggered. Calculating the weighting factor (α), in the context of dynamic updating in feature selection, involves balancing the influence of historical data against new data. This factor determines how much weight is given to previous MI values compared to the MI calculated from the new data. The value of α is adjusted using correlation analysis, which involves assessing the relationship between historical and new data. The idea is to adjust α based on the correlation between new data and historical data. The mathematical formulation is as follows.

3.1.1. Correlation Coefficient Calculation

Let X_{hist} represent the historical data and X_{new} represent the new data for a certain feature. Calculate the Pearson correlation coefficient, denoted as r, between X_{hist} and X_{new}. The formula for Pearson correlation coefficient is

$$r = \frac{\sum(X_{hist} - \bar{X}_{hist})(X_{new} - \bar{X}_{new})}{\sqrt{\sum(X_{hist} - \bar{X}_{hist})^2 (X_{new} - \bar{X}_{new})^2}}$$

Here, $\bar{X}_{hist}$ and $\bar{X}_{new}$ are the means of the historical and new data, respectively.

3.1.2. Adjusting the Weighting Factor

The correlation coefficient r ranges from −1 to 1, where 1 indicates a perfect positive linear relationship, −1 indicates a perfect negative linear relationship, and 0 indicates no linear relationship.

The value of r can be used to adjust α. For example:

If |r| is high (close to 1), it implies that the new data are highly correlated with the historical data. In this case, a higher α may be appropriate, as it suggests that historical data are still very relevant.

If |r| is low (close to 0), it indicates that the new data are not well-correlated with the historical data. A lower α might be more suitable in this scenario to give more weight to the new data.

3.1.3. Formulating the Adjustment Function

To avoid drastic changes in α due to minor fluctuations in r, a threshold value can be set. If the change in r is below this threshold, α remains unchanged. This approach allows the weighting factor α to adapt dynamically based on the changing relationship between historical and new data. It ensures that the feature-selection process remains relevant and

responsive to the most current data trends, which is particularly important in ransomware attacks.

3.2. Integration of Incremental Mutual Information Selection (IMIS) into a DBN-Based Ransomware-Detection Model

The integration of Incremental Mutual Information Selection (IMIS) into a Deep Belief Network (DBN)-based ransomware-detection model improves accuracy. Deep Belief Networks, with their robust feature learning capabilities, are well-suited for the complex and high-dimensional data characteristic of ransomware behavior. However, the effectiveness of a DBN in detecting ransomware relies on the quality and relevance of the input features. The proposed IMIS can select the important features based on the attack patterns, hence ensuring that the DBN is trained with a compact set of relevant features. Such an integration enhances the detection accuracy and ensures that the computational overhead remains within the feasible limits of the user device.

The integration of IMIS within a DBN-based ransomware-detection model involves two steps. In the first step, IMIS is used to continually assess and update the feature set as new data arrive. This process begins with the initial selection of features based on their MI score given the target class. As the system receives new data, IMIS dynamically updates this feature set, which allows the DBN to work with the most current and relevant information. The incremental nature of IMIS makes this process efficient and scalable, which is crucial for resource-constrained systems.

In the second step, the selected features are fed into the DBN for deep learning-based ransomware detection. Here, the DBN utilizes its layered structure to extract high-level representations and patterns from the input data, which are essential for identifying complex and sophisticated cyber threats. The adaptability of IMIS ensures that the DBN is not overwhelmed by the volume of data or misled by outdated or irrelevant features. This is particularly important in evasive attacks, where the nature of data and patterns of malicious activities can change rapidly. By providing a continually optimized set of features, IMIS improves the DBN's ability to learn and adapt, resulting in a more accurate and robust ransomware-detection model.

The dynamic feature-selection capability of IMIS enables the system to not only detect known types of attacks but also to identify new, previously unseen attacks. This proactive detection is crucial for fighting malware with an evolving nature.

Figure 1 shows the pseudocode for the IMIS. It presents a methodical approach for selecting and updating ransomware features necessary for malware detection. It begins by initializing an empty set for selected features and a list to store previous mutual information values. As it processes each batch of data, the algorithm calculates the current mutual information for each feature with respect to the target class. If historical data exist, it updates this information using a weighting factor to balance the influence of both new and historical data. Features are then selected based on their relevance score, which is calculated based on a predefined threshold. The selected features are continuously updated with each new batch of data. This process makes IMIS particularly effective for dynamic ransomware behavior, as it efficiently adapts to new data patterns while maintaining computational efficiency. Algorithm 1 shows the Psudocode of the proposed IMIS.

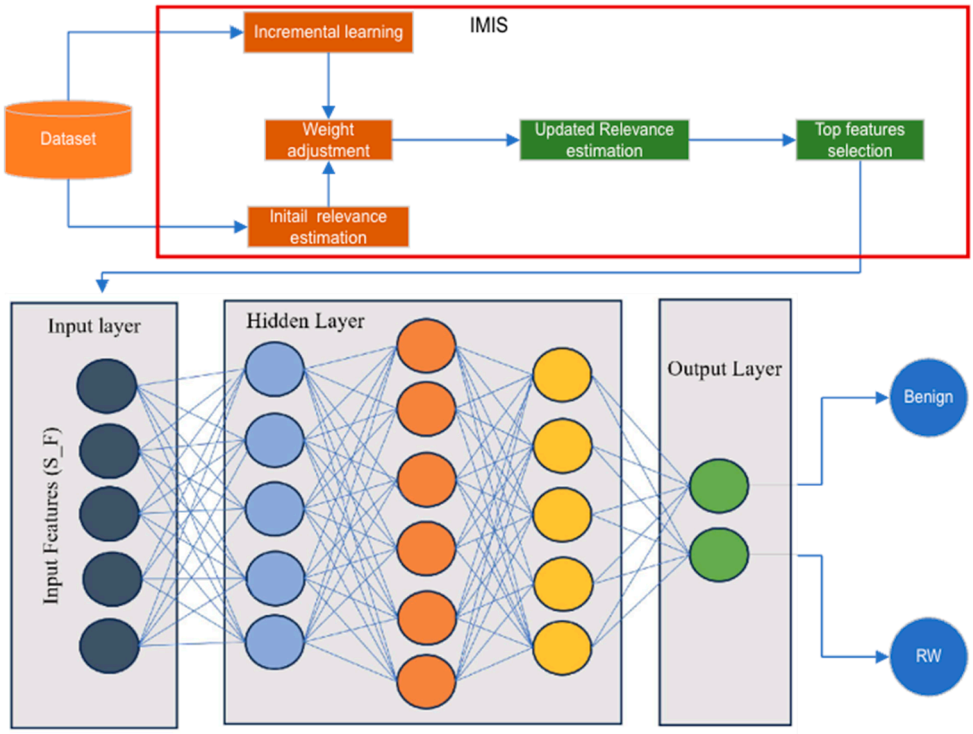

Figure 1. IMIS-DBN design.

Algorithm 1: Incremental Mutual Information Selection (IMIS)

Input:
Data_Batches: Stream of data batches from devices
Target_Class: The class variable for intrusion detection (e.g., normal or attack)
Alpha: Weighting factor for balancing historical and new data (initially set)
Threshold: Threshold for significant change in mutual information
Output:
Selected_Features: Set of features selected for intrusion detection
Procedure IMIS(Data_Batches, Target_Class, Alpha, Threshold):
Initialize Historical_MI as an empty dictionary
Initialize Selected_Features as an empty set
for each Batch in Data_Batches:
Current_MI = CalculateMutualInformation(Batch, Target_Class)
Historical_MI = UpdateFeatureRelevance(Historical_MI, Current_MI, Alpha)
Selected_Features = SelectAndUpdateFeatures(Historical_MI, Selected_Features, Threshold)
Yield Selected_Features
Procedure CalculateMutualInformation(Batch, Target_Class):
return {Feature: ComputeMutualInformation(Feature, Target_Class) for Feature in Batch}
Procedure UpdateFeatureRelevance(Historical_MI, Current_MI, Alpha):
return {Feature: Alpha × Historical_MI.get(Feature, 0) + (1 - Alpha) × MI for Feature, MI in Current_MI.items()}
Procedure SelectAndUpdateFeatures(Historical_MI, Selected_Features, Threshold):
return {Feature for Feature, MI in Historical_MI.items() if MI > Threshold or Feature in Selected_Features}

3.3. Training the IMIS-DBN Ransomware-Detection Model

Here, we detail the model's design, layer structure, and the training/testing process. As pointed out above, the proposed IMIS-DBN model is designed to provide effective ransomware detection. It combines the dynamic feature-selection capabilities of IMIS with the deep learning strength of DBNs to detect both known and novel attack patterns. The IMIS component serves as the initial layer of the model and is responsible for selecting and updating the feature set from the ransomware data streams. The DBN parameters were set as follows. The number of epochs was 100, the batch size was 64, the L2 regulation was 0.0002, the Momentum was 0.7, and the learning rate was 0.05. Those parameters were selected following the standard setup. It starts with an initial selection of features based on their MI score. This selection is aimed at reducing dimensionality while retaining

critical information. As new data batches arrive, IMIS updates the feature set by recalculating MI values and adjusting the feature relevance. Figure 1 shows the diagram representing the IMIS-DBN design. The model comprises two main components: feature selection and detection. The dataset is used as input to the feature selection (IMIS), in which several procedures like initial relevance estimation, weight adjustment, update relevance score, and top n features selection take place. Then, the selected features are used as input to train a DBN classifier for the detection model.

The DBN is structured as a stack of Restricted Boltzmann Machines (RBMs), each comprising a layer of visible and hidden units. The number of layers and the number of units in each layer are normally determined based on the complexity of the task and the computational constraints of the environment. In this study, we used five hidden layers with several units reduced by 30% from the previous layer. The first layer receives the processed input from the IMIS feature selection, and each subsequent layer receives input from the hidden units of the preceding layer, which enables the extraction of abstract representations of the data.

Each RBM in the DBN is trained in an unsupervised manner, starting from the bottom layer and moving upwards. During this phase, the RBMs learn to reconstruct their inputs and capture the underlying distributions and correlations within the data. This pre-training helps in initializing the weights of the network, which is crucial for the subsequent supervised fine-tuning. After pre-training, the entire DBN undergoes supervised fine-tuning using labeled data to adjust the weights of the entire network. This helps to minimize classification error, which consequently improves the model's ability to distinguish between normal and malicious activities. The trained IMIS-DBN model is evaluated using a test dataset that contains samples that have not been used for training. The accuracy, precision, recall, and F1 score were used as performance metrics to assess the model's performance.

4. Results and Discussion

In this section, the experimental evaluation of the proposed Incremental Mutual Information Select (IMIS) technique against existing feature-selection methods, namely, RCGU [15], EMRMR [62], MIFS [63], and JMI [64], is performed within the context of ransomware detection. These related works were implemented based on the available repository on the SKFeature Python library and the details of implementation provided by the respective papers. The Python version that was used was 3.11.7. We also used several Python-based packages, such as Sklearn (1.3.1), Pandas (2.1.0), Numpy (1.25.0), SkFeature (1.0.0), and TensorFlow (2.3). The effectiveness of each technique is quantitatively assessed through a series of metrics, including accuracy, false positive rate, detection rate, and the F1 score across varying sizes of feature sets. The incremental nature of the IMIS approach, which dynamically updates feature relevance in response to new data, is posited as a significant advancement over traditional methods that often become outdated against the rapidly evolving ransomware threats. This section delves into the empirical data gathered from our experiments, highlighting the impact of IMIS's iterative reassessment and weighting mechanisms on maintaining the currency and precision of feature selection and, ultimately, on enhancing the performance of ransomware-detection systems. The model was trained in an Intel Core i5 machine with a 4.3 GHz CPU, 8 GB of RAM, and Windows 10 Professional.

Figure 2 compares the accuracy of the proposed Incremental Mutual Information Select (IMIS) technique with RCGU, EMRMR, and MIFS across a range of features between 5 and 50. It shows that IMIS consistently outperforms the existing techniques. The accuracy of the proposed IMIS is 0.949 with 5 features and maintains its lead throughout. It can also be noticed that IMIS peaks at 25 features with 0.979 accuracy. While there are slight decreases in its performance at higher feature counts, IMIS remains competitive, particularly against RCGU, its closest rival in most cases. This consistent performance

across different feature numbers shows IMIS's robustness and effectiveness in comparison to the related techniques.

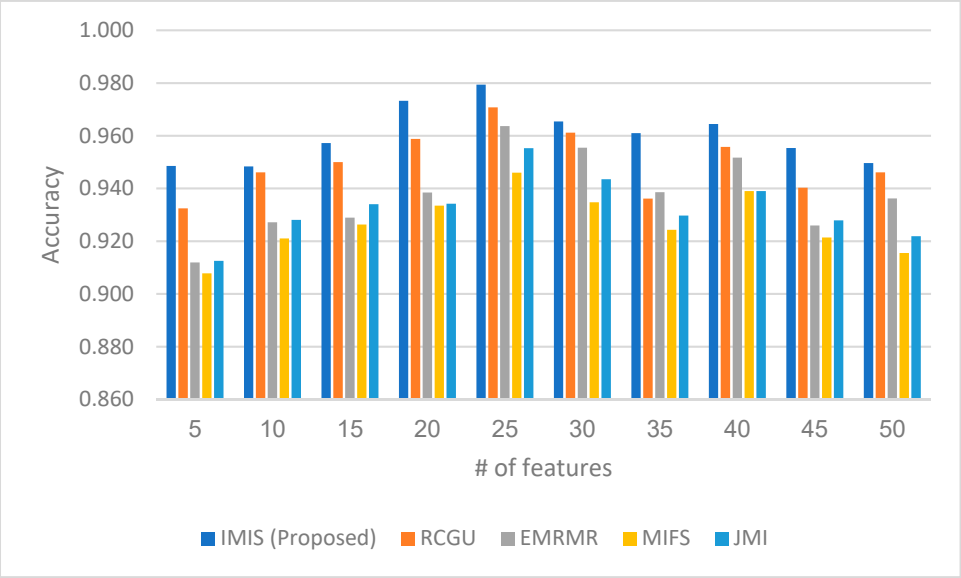

Figure 2. Comparison of the accuracy of the proposed IMIS technique with RCGU, EMRMR, MIFS, and JMI across a range of features between 5 and 50.

The accuracy comparison in Figure 2 illustrates the effectiveness of the incremental mechanism employed by IMIS, which substantially impacts maintaining feature relevance. The core advantage of IMI lies in its capability for a dynamic update that allows for a continual reassessment of feature relevance when new data arrive. This is important due to the changing nature of ransomware behavior. The accuracy improvement achieved by IMIS is evident in the incremental improvements in accuracy from 5 to 25 features, where IMIS not only starts strong but also exhibits a growing advantage as the number of features increases. This is attributed to the ability of IMI to weigh the historical against new data effectively, allowing for a more adaptive and nuanced feature-selection process. Such adaptability explains the superior performance of IMIS, as it consistently adapts to the latest data trends and maintains high accuracy across all feature set sizes.

For the False Positive Rate (FPR), Figure 3 shows a comparison between the proposed IMIS and related techniques, i.e., RCGU, EMRMR, and MIFS, across various feature set sizes. In general, it can be observed that IMIS consistently demonstrates a lower FPR compared to the other techniques. With five features, IMIS shows a lower FPR of 0.175, marginally better than RCGU (0.180), EMRMR (0.178), and MIFS (0.176). This trend continues for 10, 15, and 20 features, showing a gradual decrease in FPR, reaching its lowest at 25 features with a rate of 0.104, which is also better than the other techniques. At 30 features, IMIS and RCGU achieved the same FPR (0.123), which is still outperforming EMRMR and MIFS. Beyond 30 features, although the FPR for IMIS slightly increases, it remains competitive, particularly at 40 and 45 features, where it is lower than those of other techniques. At 50 features, IMIS maintains an FPR of 0.150, which is lower than RCGU and MIFS and slightly lower than EMRMR.

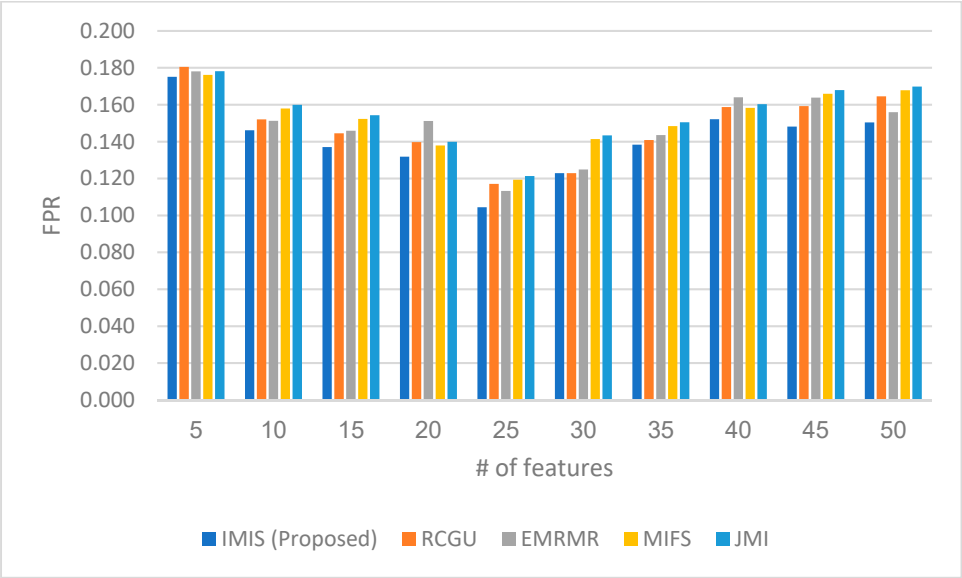

Figure 3. Comparison of the false positive rate (FPR) of the proposed IMIS technique with RCGU, EMRMR, MIFS, and JMI across a range of features between 5 and 50.

The false positive rate (FPR) comparison in Figure 3 shows the efficacy of the proposed IMIS compared to RCGU, EMRMR, and MIFS. The IMIS consistently records lower FPRs, which can be attributed to the incremental MI calculation approach of IMI. Unlike traditional MI, which evaluates feature relevance statically, the proposed IMIS dynamically updates the relevance of features as new data arrive. Such continuous reassessment allows IMIS to adapt to the changing patterns in ransomware, which consequently reduces the likelihood of falsely identifying benign activities as ransomware. The weighting mechanism within IMI balances the old and new data, which allows the model to re-evaluate the feature to ensure that the selected features remain relevant to the new behavior of ransomware. This results in a more accurate and current model that shows consistent FPR improvements across all feature sets for IMIS compared to the other techniques, underlining the impact of the iterative update strategy in maintaining relevancy and reducing false positives in ransomware detection.

Figure 4 compares the detection rates of the proposed IMIS against RCGU, EMRMR, and MIFS across various numbers of features ranging between 5 and 50. It can be seen that IMIS consistently achieves a high detection rate, beginning at 0.913 for 5 features and showing an improvement as the number of features increases, peaking at 0.942 for 25 features. This trend outperforms all other techniques, with RCGU being the closest at 0.934 when using 25 features. In most instances, IMIS's detection rates maintained the highest score, especially at 15, 25, 35, and 40 feature counts where it outperforms other methods by a significant margin. Even at 50 features, where many techniques show a reduced detection rate, IMIS maintains a good detection rate at 0.927. These data suggest that IMIS not only starts strongly but also scales effectively with increasing feature set sizes, often maintaining a lead over the other techniques in detection performance.

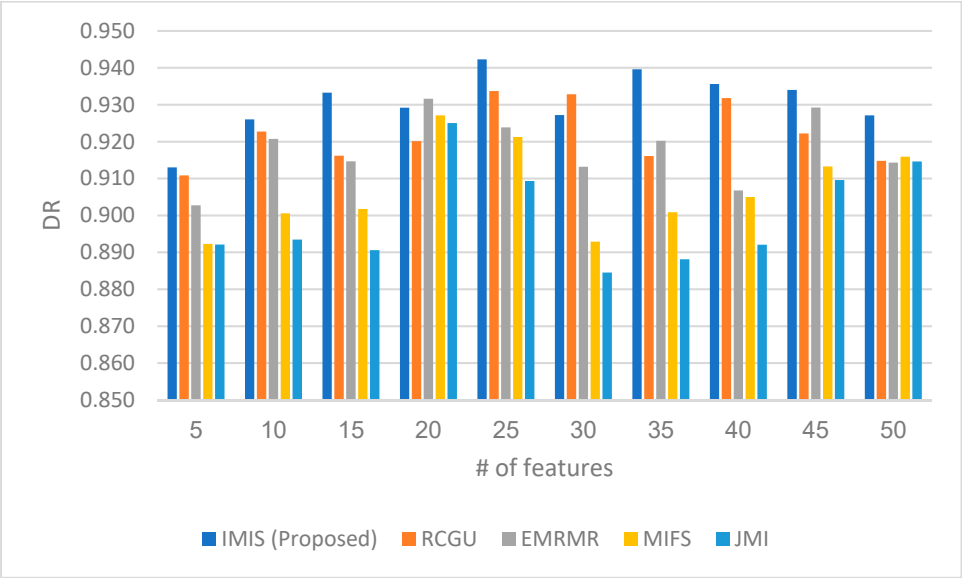

Figure 4. Comparison of the detection rates (DR) of the proposed IMIS technique with RCGU, EMRMR, MIFS, and JMI across a range of features between 5 and 50.

The detection rate comparison shown in Figure 4 indicates that the proposed IMIS achieves higher detection rates across various feature set sizes compared to RCGU, EMRMR, and MIFS. This is attributed to the incremental nature of the MI calculation in the proposed technique, which, unlike traditional MI-based methods, employs a dynamic update mechanism that iteratively reassesses feature relevance as new data arrive. This ensures that the detection model remains current and more responsive to emerging ransomware behavior. The weighting mechanism in IMIS further refines this process by balancing historical data against new data, leading to select features that are more relevant to ransomware, thereby improving detection rates.

Figure 5 shows the F1 score comparison of the proposed IMIS with RCGU, EMRMR, and MIFS across different feature set sizes ranging between 5 and 50 features. It can be observed that IMIS consistently exhibits higher F1 values, starting at 0.935 for five features, and outperforms the related techniques. The IMIS maintains its lead with a peak value of 0.950 at 20 features, outperforming all other methods. Although there is a slight convergence of scores among the techniques as the number of features increases, IMIS continues to demonstrate competitive or superior performance. At 40 features, IMIS almost reaches its peak again with a value of 0.949, showing its robustness. The trend indicates that IMIS is quite effective, maintaining F1 values higher than RCGU, EMRMR, and MIFS across all feature set sizes.

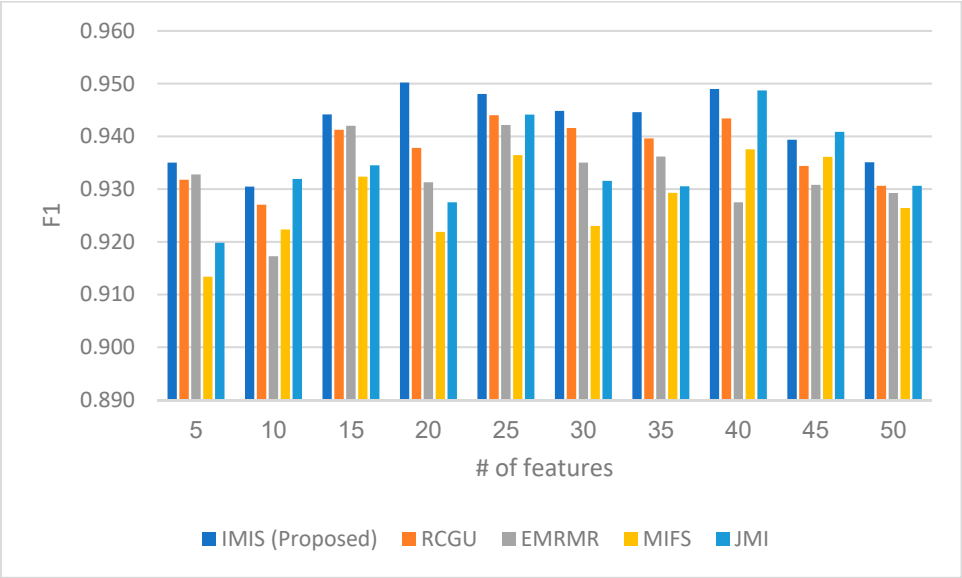

Figure 5. F1 score comparison of the proposed IMIS with RCGU, EMRMR, and MIFS across different feature set sizes ranging between 5 and 50 features.

The F1 score comparison shown in Figure 5 across various feature set sizes ranging between 5 and 50 reveals that the proposed IMIS consistently achieves high F1 scores, which outperforms the related techniques, i.e., RCGU, EMRMR, and MIFS. This performance indicates that the proposed IMIS achieved a good balance between precision and recall in its detection capability. These results can be attributed to the underlying incremental MI calculation mechanism employed in IMIS. Unlike traditional MI approaches that assess feature relevance in a static context, IMIS dynamically updates this relevance with the arrival of new data. This mechanism ensures that the feature selection is continuously optimized to reflect the latest attack behavior manifested by ransomware. The weighting mechanism used in IMIS re-assesses the influence of historical data while considering new attack patterns, thereby maintaining a relevant feature set for ransomware detection. The consistently superior F1 scores of IMIS compared to its counterparts underscore the advantage of this incremental approach, providing a more relevant and current feature set that helps in improving the detection performance.

In Table 1, The performance evaluation using Python profiler demonstrates the proposed IMI technique's computational efficiency compared to related techniques (RCGU, EMRMR, MIFS, and JMI). IMIS shows the lowest per-call execution time (0.01 s) and total time (Tottime) (3.5 min), significantly outperforming others in training time as well (19 min). This improvement can be attributed to the incremental nature of IMIS, which selectively updates feature relevance with incoming data, reducing unnecessary computations and enhancing adaptability.

Table 1. The performance evaluation between the proposed IMIS and related techniques.

	Proposed	**RCGU**	**EMRMR**	**MIFS**	**JMI**
Percall (s)	0.01	0.054	0.063	0.03	0.07
Tottime (min)	3.5	10.8	12.6	6	14
Training time (min)	19	33	37	28	24

Table 2 shows the top 10 API call features identified by IMIS. It can be observed that these features are directly linked to the actions ransomware typically performs, which makes them crucial to understanding ransomware behavior. Crypto APIs like CryptEncrypt and CryptGenKey are vital for encrypting files, a hallmark of ransomware attacks. File access APIs, including CreateFile and DeleteFile, are used for accessing and

potentially altering or deleting files, indicating unauthorized file manipulation. Network APIs such as WinHttpConnect and WinHttpOpenRequest are essential for establishing network connections, possibly for data exfiltration or command-and-control communication. The high relevance and ranking of these APIs underscore the ability of the proposed IMIS technique to identify the crucial features necessary for detecting ransomware activities.

Table 2. The top 10 features (API calls) commonly used by ransomware.

Type	Features	Rank
Crypto APIs	CryptEncrypt	1
	CryptGenKey	3
	CryptDestroyKey	6
	BCryptGenRandom	9
File access APIs	CreateFile	2
	FindFirstFileEXA	5
	FindNextFileA	8
	DeleteFile	10
Network APIs	WinHttpConnect	4
	WinHttpOpenRequest	7

The limitations of this research are represented by the reliance on the incremental mutual information technique, which may not fully capture the diversity of ransomware behaviors, potentially limiting its adaptability to new threats. Additionally, the effectiveness of the feature-selection and early detection capabilities could be challenged by the variability and volume of incoming data. Scaling the solution for large-scale deployments and integrating it into existing frameworks might also present performance challenges. A broader validation across various environments and ransomware types is suggested to enhance the robustness and generalizability of the findings. During the incremental feature selection, the incoming data needs to be processed and prepared to be used as input for the feature-selection technique. While this processing step can be easily performed during offline training, it adds extra overhead when switching to incremental (online) feature processing.

5. Conclusions

This study developed incremental mutual information and integrated it into feature selection for ransomware detection. This incremental approach helps to estimate feature significance in limited data scenarios during the initial phase of the attack. It gives the model the ability to select the best features even if data are scarce, which improves the detection accuracy. This research highlights the significance of early detection in combating ransomware attacks and emphasizes the need for proactive defense strategies. By leveraging this technique, this study underscores the importance of early detection capabilities to strengthen defense strategies against ransomware. The findings of this study emphasize the effectiveness of the incremental approach integrated into the mutual information for early detection, thereby contributing to improved defense mechanisms against ransomware. Overall, this study sheds light on the importance of incremental learning for estimating feature significance in addressing the issue of data insufficiency during the initial stages of ransomware attacks.

Author Contributions: Conceptualization, M.G. and F.T.S.; methodology, M.G.; software, M.G.; validation, M.G. and F.T.S.; formal analysis, M.G. and F.T.S.; investigation, M.G.; resources, M.G. and F.T.S.; data curation, M.G. and F.T.S.; writing—original draft preparation, M.G.; writing—review

and editing, F.T.S.; visualization, M.G.; supervision, F.T.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Neprash, H.T.; McGlave, C.C.; Cross, D.A.; Virnig, B.A.; Puskarich, M.A.; Huling, J.D.; Rozenshtein, A.Z.; Nikpay, S.S. Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016–2021. *JAMA Health Forum* **2022**, *3*, e224873. https://doi.org/10.1001/jamahealthforum.2022.4873.
2. Wang, Z.; Liu, C.; Qiu, J.; Tian, Z.; Cui, X.; Su, S. Automatically Traceback RDP-Based Targeted Ransomware Attacks. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 7943586 https://doi.org/10.1155/2018/7943586.
3. Aboaoja, F.A.; Zainal, A.; Ghaleb, F.A.; Al-rimy, B.A.S. Toward an ensemble behavioral-based early evasive malware detection framework. In Proceeding of the 2021 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 6–7 October 2021; IEEE: New York, NY, USA, 2021; pp. 181–186.
4. Oz, H.; Aris, A.; Levi, A.; Uluagac, A.S. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. *ACM Comput. Surv.* **2022**, *54*, 1–37. https://doi.org/10.1145/3514229.
5. Razaulla, S.; Fachkha, C.; Markarian, C.; Gawanmeh, A.; Mansoor, W.; Fung, B.C.M.; Assi, C. The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. *IEEE Access* **2023**, *11*, 40698–40723. https://doi.org/10.1109/access.2023.3268535.
6. Gazzan, M.; Alqahtani, A.; Sheldon, F.T. Key Factors Influencing the Rise of Current Ransomware Attacks on Industrial Control Systems. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 27–30 January 2021; IEEE: New York, NY, USA 2021; pp. 1417–1422.
7. Benmalek, M. Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet Things Cyber-Phys. Syst.* **2024**, *4*, 186–202.
8. Urooj, U.; Maarof, M.A.B.; Al-rimy, B.A.S. A proposed Adaptive Pre-Encryption Crypto-Ransomware Early Detection Model. In Proceedings of the 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29–31 January 2021; IEEE: New York, NY, USA, 2021; pp. 1–6.
9. Eliando, E.; Purnomo, Y. LockBit 2.0 Ransomware: Analysis of infection, persistence, prevention mechanism. *CogITo Smart J.* **2022**, *8*, 232–243. https://doi.org/10.31154/cogito.v8i1.356.232-243.
10. Gazzan, M.; Sheldon, F.T. An enhanced minimax loss function technique in generative adversarial network for ransomware behavior prediction. *Futur. Internet* **2023**, *15*, 318.
11. Almashhadani, A.O.; Kaiiali, M.; Sezer, S.; O'Kane, P. A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware. *IEEE Access* **2019**, *7*, 47053–47067. https://doi.org/10.1109/access.2019.2907485.
12. Al-Rimy, B.A.S.; Maarof, M.A.; Alazab, M.; Alsolami, F.; Shaid, S.Z.M.; Ghaleb, F.A.; Al-Hadhrami, T.; Ali, A.M. A Pseudo Feedback-Based Annotated TF-IDF Technique for Dynamic Crypto-Ransomware Pre-Encryption Boundary Delineation and Features Extraction. *IEEE Access* **2020**, *8*, 140586–140598.
13. Dini, P.; Elhanashi, A.; Begni, A.; Saponara, S.; Zheng, Q.; Gasmi, K. Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity. *Appl. Sci.* **2023**, *13*, 7507.
14. Zimba, A.; Wang, Z.; Simukonda, L. Towards Data Resilience: The Analytical Case of Crypto Ransomware Data Recovery Techniques. *Int. J. Inf. Technol. Comput. Sci.* **2018**, *10*, 40–51. https://doi.org/10.5815/ijitcs.2018.01.05.
15. Al-Rimy, B.A.S.; Maarof, M.A.; Alazab, M.; Shaid, S.Z.M.; Ghaleb, F.A.; Almalawi, A.; Ali, A.M.; Al-Hadhrami, T. Redundancy coefficient gradual up-weighting-based mutual information feature selection technique for crypto-ransomware early detection. *Futur. Gener. Comput. Syst.* **2021**, *115*, 641–658.
16. Kumar, P.; Ramlie, H.R.E.B.H. Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques. In Proceedings of the International Conference on Computational Intelligence in Information System, Bandar Seri Begawan, Brunei Darussalam, 25-–27 January 2021. https://doi.org/10.1007/978-3-030-68133-3_20.
17. Al-Dwairi, M.; Shatnawi, A.S.; Al-Khaleel, O.; Al-Duwairi, B. Ransomware-Resilient Self-Healing XML Documents. *Futur. Internet* **2022**, *14*, 115. https://doi.org/10.3390/fi14040115.
18. Gazzan, M.; Sheldon, F.T. Opportunities for Early Detection and Prediction of Ransomware Attacks against Industrial Control Systems. *Futur. Internet* **2023**, *15*, 144. https://doi.org/10.3390/fi15040144.
19. Garmehi, M. Risks, Limitations and the Need for Additional Measures Against Ransomware in the Health Information Technology Infrastructure. *J. North Khorasan Univ. Med. Sci.* **2022**, *14*, 79–85. https://doi.org/10.52547/nkums.14.1.79.
20. Tzachor, A.; Devare, M.; King, B.; Avin, S.; Héigeartaigh, S. Responsible artificial intelligence in agriculture requires systemic understanding of risks and externalities. *Nat. Mach. Intell.* **2022**, *4*, 104–109. https://doi.org/10.1038/s42256-022-00440-4.

21. Ali, A.; Al-Rimy, B.A.S.; Almazroi, A.A.; Alsubaei, F.S.; Almazroi, A.A.; Saeed, F. Securing secrets in cyber-physical systems: A cutting-edge privacy approach with consortium blockchain. *Sensors* **2023**, *23*, 7162.
22. Beaman, C.; Barkworth, A.; Akande, T.D.; Hakak, S.; Khan, M.K. Ransomware: Recent advances, analysis, challenges and future research directions. *Comput. Secur.* **2021**, *111*, 102490. https://doi.org/10.1016/j.cose.2021.102490.
23. Dargahi, T.; Dehghantanha, A.; Bahrami, P.N.; Conti, M.; Bianchi, G.; Benedetto, L. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *J. Comput. Virol. Hacking Tech.* **2019**, *15*, 277–305. https://doi.org/10.1007/s11416-019-00338-7.
24. Szücs, V.; Arányi, G.; Dávid, Á. Introduction of the ARDS—Anti-Ransomware Defense System Model—Based on the Systematic Review of Worldwide Ransomware Attacks. *Appl. Sci.* **2021**, *11*, 6070. https://doi.org/10.3390/app11136070.
25. Ahmed, Y.A.; Huda, S.; Al-Rimy, B.A.S.; Alharbi, N.; Saeed, F.; Ghaleb, F.A.; Ali, I.M. A Weighted Minimum Redundancy Maximum Relevance Technique for Ransomware Early Detection in Industrial IoT. *Sustainability* **2022**, *14*, 1231.
26. Homayoun, S.; Dehghantanha, A.; Ahmadzadeh, M.; Hashemi, S.; Khayami, R. Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence. *IEEE Trans. Emerg. Top. Comput.* **2017**, *8*, 341–351. https://doi.org/10.1109/tetc.2017.2756908.
27. Homayoun, S.; Dehghantanha, A.; Ahmadzadeh, M.; Hashemi, S.; Khayami, R.; Choo, K.-K.R.; Newton, D.E. DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. *Futur. Gener. Comput. Syst.* **2018**, *90*, 94–104. https://doi.org/10.1016/j.future.2018.07.045.
28. Tariq, U.; Ullah, I.; Uddin, M.Y.; Kwon, S.J. An Effective Self-Configurable Ransomware Prevention Technique for IoMT. *Sensors* **2022**, *22*, 8516. https://doi.org/10.3390/s22218516.
29. Naik, N.; Jenkins, P.; Gillett, J.; Mouratidis, H.; Naik, K.; Song, J. Lockout-Tagout Ransomware: A Detection Method for Ransomware Using Fuzzy Hashing and Clustering. In Proceedings of the IEEE Symposium Series on Computational Intelligence (SSCI), Xiamen, China, 6–9 December 2019. https://doi.org/10.1109/ssci44817.2019.9003148.
30. Lee, K.; Lee, S.-Y.; Yim, K. Machine Learning Based File Entropy Analysis for Ransomware Detection in Backup Systems. *IEEE Access* **2019**, *7*, 110205. https://doi.org/10.1109/access.2019.2931136.
31. Bae, S.I.; Bin Lee, G.; Im, E.G. Ransomware detection using machine learning algorithms. *Concurr. Comput. Pract. Exp.* **2019**, *32*, e5422. https://doi.org/10.1002/cpe.5422.
32. Jaya, M.I.; Razak, M.F.A. Dynamic Ransomware Detection for Windows Platform Using Machine Learning Classifiers. *JOIV Int. J. Informatics Vis.* **2022**, *6*, 469–474. https://doi.org/10.30630/joiv.6.2-2.1093.
33. Genç, Z.A.; Lenzini, G.; Sgandurra, D. On Deception-Based Protection against Cryptographic Ransomware. In Proceedings of the DIMVA 2019: Detection of Intrusions and Malware, and Vulnerability Assessment, Gothenburg, Sweden, 19–20 June 2019. https://doi.org/10.1007/978-3-030-22038-9_11.
34. Song, S.; Kim, B.; Lee, S. The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform. *Mob. Inf. Syst.* **2016**, *2016*, 2946735. https://doi.org/10.1155/2016/2946735.
35. Fernández Maimó, L.; Huertas Celdrán, A.; Perales Gómez, Á.L.; García Clemente, F.J.; Weimer, J.; Lee, I. Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments. *Sensors* **2019**, *19*, 1114. https://doi.org/10.3390/s19051114.
36. Alam, M.; Sinha, S.; Bhattacharya, S.; Dutta, S.; Mukhopadhyay, D.; Chattopadhyay, A. RAPPER: Ransomware Prevention via Performance Counters. *arXiv* **2020**, arXiv:2004.01712.
37. Hitaj, D.; Pagnotta, G.; Gaspari, F.D.; Carli, L.D.; Mancini, L.V. Minerva: A File-Based Ransomware Detector. *arXiv* **2023**, arXiv:2301.11050.
38. Poudyal, S.; Dasgupta, D. Analysis of Crypto-Ransomware Using ML-Based Multi-Level Profiling. *IEEE Access* **2021**, *9*, 122532–122547. https://doi.org/10.1109/access.2021.3109260.
39. Scalas, M.; Maiorca, D.; Mercaldo, F.; Visaggio, C.A.; Martinelli, F.; Giacinto, G. On the effectiveness of system API-related information for Android ransomware detection. *Comput. Secur.* **2019**, *86*, 168–182. https://doi.org/10.1016/j.cose.2019.06.004.
40. Urooj, U.; Al-Rimy, B.A.S.; Zainal, A.B.; Saeed, F.; Abdelmaboud, A.; Nagmeldin, W. Addressing Behavioral Drift in Ransomware Early Detection Through Weighted Generative Adversarial Networks. *IEEE Access* **2024**, *12*, 3910–3925. https://doi.org/10.1109/ACCESS.2023.3348451.
41. Lee, K.; Lee, J.; Lee, S.-Y.; Yim, K. Effective Ransomware Detection Using Entropy Estimation of Files for Cloud Services. *Sensors* **2023**, *23*, 3023.
42. Alsaif, S.A. Machine Learning-Based Ransomware Classification of Bitcoin Transactions. *Appl. Comput. Intell. Soft Comput.* **2023**, *2023*, 6274260.
43. Rhode, M.; Burnap, P.; Jones, K. Early-stage malware prediction using recurrent neural networks. *Comput. Secur.* **2018**, *77*, 578–594, https://doi.org/10.1016/j.cose.2018.05.010.
44. Alqahtani, A.; Sheldon, F.T. A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook. *Sensors* **2022**, *22*, 1837. https://doi.org/10.3390/s22051837.
45. Liu, Y.; Li, J.; Liu, B.; Gao, X.; Liu, X. Malware detection method based on image analysis and generative adversarial networks. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e7170. https://doi.org/10.1002/cpe.7170.
46. Wang, Z.; Wang, W.; Yang, Y.; Han, Z.; Xu, D.; Su, C. CNN- and GAN-based classification of malicious code families: A code visualization approach. *Int. J. Intell. Syst.* **2022**, *37*, 12472–12489. https://doi.org/10.1002/int.23094.

47. Catal, C.; Gunduz, H.; Ozcan, A. Malware Detection Based on Graph Attention Networks for Intelligent Transportation Systems. *Electronics* **2021**, *10*, 2534. https://doi.org/10.3390/electronics10202534.
48. He, K.; Zhang, X.; Ren, S.; Sun, J. Deep residual learning for image recognition. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR) , Las Vegas, NV, USA, 27–30 June 2016. https://doi.org/10.1109/cvpr.2016.90.
49. Javaheri, D.; Lalbakhsh, P.; Hosseinzadeh, M. A Novel Method for Detecting Future Generations of Targeted and Metamorphic Malware Based on Genetic Algorithm. *IEEE Access* **2021**, *9*, 69951–69970. https://doi.org/10.1109/access.2021.3077295.
50. Jang, S.; Li, S.; Sung, Y. Generative Adversarial Network for Global Image-Based Local Image to Improve Malware Classification Using Convolutional Neural Network. *Appl. Sci.* **2020**, *10*, 7585. https://doi.org/10.3390/app10217585.
51. Smith, D.; Khorsandroo, S.; Roy, K. Leveraging Feature Selection to Improve the Accuracy for Malware Detection. *Preprint* **2023**. https://doi.org/10.21203/rs.3.rs-3045391/v1.
52. Alsoghyer, S.; Almomani, I. Ransomware Detection System for Android Applications. *Electronics* **2019**, *8*, 868. https://doi.org/10.3390/electronics8080868.
53. Lall, S.; Ray, S.; Bandyopadhyay, S. Generating Realistic Cell Samples for Gene Selection in scRNA-seq Data: A Novel Generative Framework. *bioRxiv* **2021**. https://doi.org/10.1101/2021.04.29.441920.
54. Liu, Q.; Liang, T.; Dinavahi, V. Deep Learning for Hardware-Based Real-Time Fault Detection and Localization of All Electric Ship MVDC Power System. *IEEE Open J. Ind. Appl.* **2020**, *1*, 194–204. https://doi.org/10.1109/ojia.2020.3034608.
55. Wang, S.; Zhao, C.; Huang, L.; Li, Y.; Li, R. Current status, application, and challenges of the interpretability of generative adversarial network models. *Comput. Intell.* **2022**, *39*, 283–314. https://doi.org/10.1111/coin.12564.
56. Bijitha, C.V.; Sukumaran, R.; Nath, H.V. A Survey on Ransomware Detection Techniques. In Proceedings of the SKM 2019: Secure Knowledge Management in Artificial Intelligence Era, Goa, India, 21–22 December 2020. https://doi.org/10.1007/978-981-15-3817-9_4.
57. Sgandurra, D.; Muñoz-González, L.; Mohsen, R.; Lupu, E. Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection. *arXiv* **2016**. arXiv:1609.03020.
58. Chakkaravarthy, S.S.; Sangeetha, D.; Cruz, M.V.; Vaidehi, V.; Raman, B. Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks. *IEEE Access* **2020**, *8*, 169944–169956. https://doi.org/10.1109/access.2020.3023764.
59. Abbasi, M.S. Automating Behavior-Based Ransomware Analysis, Detection, and Classification Using Machine Learning. PhD Thesis, Victoria University of Wellington, Wellington, New Zealand, 2023. https://doi.org/10.26686/wgtn.22180858.
60. Kim, G.; Kim, S.; Kang, S.; Kim, J. A method for decrypting data infected with Hive ransomware. *J. Inf. Secur. Appl.* **2022**, *71*, 103387. https://doi.org/10.48550/arxiv.2202.08477.
61. Chen, Q.; Islam, S.R.; Haswell, H.; Bridges, R.A. Automated Ransomware Behavior Analysis: Pattern Extraction and Early Detection. In Proceedings of the SciSec 2019: Science of Cyber Security, Nanjing, China, 9–11 August 2019. https://doi.org/10.1007/978-3-030-34637-9_15.
62. Ahmed, Y.A.; Koçer, B.; Huda, S.; Al-Rimy, B.A.S.; Hassan, M.M. A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection. *J. Netw. Comput. Appl.* **2020**, *167*, 102753.
63. Gavel, S.; Raghuvanshi, A.S.; Tiwari, S. Maximum correlation based mutual information scheme for intrusion detection in the data networks. *Expert Syst. Appl.* **2021**, *189*, 116089. https://doi.org/10.1016/j.eswa.2021.116089.
64. Yuan, G.; Lu, L.; Zhou, X. Feature selection using a sinusoidal sequence combined with mutual information. *Eng. Appl. Artif. Intell.* **2023**, *126*, 107168.