International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 15, No.1 (Feb-24)

http://dx.doi.org/10.12785/ijcds/150165

RFSA: A Ransomware Feature Selection Algorithm for Multivariate Analysis of Malware Behavior in Cryptocurrency

Mike Nkongolo Wa Nkongolo[1]

[1]*Department of Informatics, University of Pretoria, Gauteng, South Africa*

Received 25 Sep. 2023, Revised 24 Jan. 2024, Accepted 31 Jan. 2024, Published 5 Feb. 2024

Abstract:
This research introduces innovative features tailored to capture distinctive characteristics of ransomware activity within the cryptocurrency ecosystem. The study employs a multifaceted analysis to delve into ransomware-related data encompassing transaction metadata, ransom analysis, behavioral patterns, and financial aspects. A feature selection algorithm is explored to discern ransomware transactions in Bitcoin (BTC) and the United States Dollar (USD) using the UGRansome dataset. This comprehensive dataset of ransomware-related transactions facilitates the proposal of novel features designed to capture the unique traits of ransomware activity. The correlation matrix and temporal analysis of these features contribute to a nuanced understanding of the dynamic nature of ransomware threats. The research presents the Ransomware Feature Selection Algorithm (RFSA) based on Gini Impurity and Mutual Information (MI) to effectively select crucial ransomware features. Evaluation metrics such as precision, recall, accuracy, and F1 score highlight the effectiveness of the RFSA. The analysis reveals that approximately 68% of ransomware incidents involve BTC transactions ranging from 1.46 to 2.56, with an average of 2.01 BTC transactions per attack. Moreover, ransomware causes financial damages ranging from 4.38 to 172.36 USD, with an average damage of 88.37 USD. The RFSA identifies 17 ransomware types and their associated malware to shed light on their characteristics. The study investigates the pricing of ransomware and reveals that TowerWeb is associated with the highest fee, amounting to 135.26 BTC, while CryptoLocker has the lowest fee, recorded at 10.51 BTC. Additionally, the impact of ransomware duration on financial gains and network flow is investigated, disclosing a correlation between extended duration and higher financial gains. The research achieves outstanding performance metrics, including an MI score of 95%, accuracy of 93%, recall of 92%, and precision of 89%. These results showcase the superiority of the proposed approach over existing studies, emphasizing the dynamic and adaptable nature of ransomware demands. The findings suggest that there is no fixed amount for specific cyberattacks. This underscores the importance of adapting to the evolving landscape of ransomware threats.
Keywords: Ransomware, cryptocurrency, feature selection, UGRansome dataset, cybersecurity threats, machine learning

1. INTRODUCTION

Cryptocurrency is a type of digital currency that uses cryptographic methods for secure transactions. This technology has experienced an exponential surge in popularity and widespread adoption in recent years [1]. Prominent among cryptocurrencies is Bitcoin (BTC) [2], which operates on a decentralized ledger called the blockchain. While cryptocurrencies offer numerous advantages, including transparency and decentralization [3], they have also become a focal point for criminal activities, particularly in the context of ransomware. Ransomware attacks have emerged as a formidable threat to critical infrastructure and organizations worldwide [4]. These malicious attacks involve encrypting a victim's data or locking them out of their systems, with cybercriminals demanding a ransom, typically in cryptocurrency, for the decryption key or system access. BTC has often been the preferred currency for ransom payments [5] due to its relative anonymity and ease of use in conducting financial transactions across borders. Classifying BTC transactions as ransomware-related or benign holds paramount importance in the realm of critical infrastructure and cybersecurity [6]. Critical infrastructure encompasses the essential systems and assets, such as energy, transportation, and healthcare, that are vital for the functioning of a society and its economy. Ransomware attacks targeting critical infrastructure can lead to catastrophic consequences, including disruptions to public services, economic losses, and even threats to national security [2], [3], [6]. Therefore, the ability to swiftly identify and mitigate ransomware-related BTC transactions is critical for safeguarding critical infrastructure. In response to this imperative, this paper introduces novel features specifically tailored to capture the distinctive characteristics of ransomware activity within the cryptocurrency ecosystem. Our research aims to provide a comprehensive analysis of ransomware-related data which encompasses transaction metadata, ransom analysis, behavioral patterns, and financial aspects. The primary objectives of this study include the investigation of a feature

E-mail address: mike.wankongolo@up.ac.za

selection algorithm to discern ransomware transactions in BTC contexts. Our research contribution can be summarized as follows:

Novel Feature Set Development

We propose a set of innovative features meticulously designed to capture the unique attributes of ransomware activity within the cryptocurrency ecosystem. These features form the basis for our multifaceted analysis. Our research contributes by utilizing the UGRansome dataset [7] to derive insights into the dynamic nature of ransomware threats.

Feature Selection Algorithm

We introduce a Ransomware Feature Selection Algorithm (RFSA) based on Gini Impurity and Mutual Information (MI) to select crucial ransomware features from the UGRansome dataset. This algorithm contributes to the field by providing an effective method for selecting features that are instrumental in ransomware detection systems. Through rigorous experimentation and evaluation, we demonstrate the effectiveness of our feature set in accurately extracting BTC and USD (United States Dollar) transactions. The performance metrics, including precision, recall, accuracy, and F1 score, showcase the superiority of our approach over existing studies. The research achieves outstanding performance metrics, including an MI score of 95%, accuracy of 93%, recall of 92%, and precision of 89%. These results underscore the superiority of our approach in comparison to existing studies.

Insights into Ransomware Incidents

Our analysis reveals key insights into ransomware incidents, including transaction characteristics, financial damages, ransomware types, associated malware, and pricing dynamics. These findings contribute to a deeper understanding of the landscape and potential impact of ransomware threats. The findings emphasize the dynamic and adaptable nature of ransomware demands. This highlights the evolving landscape of ransomware threats. Insights into ransomware pricing, duration impact on financial gains, and network flow shed light on the nuanced nature of these cyber threats. The present manuscript is structured in the following manner: Section 2 provides a comprehensive overview of the existing literature relevant to this research. It discusses the strengths and weaknesses of prior works, enabling the reader to discern the advantages of the proposed RFSA and its performance enhancements compared to other techniques. Section 3 introduces the research methodology, data processing workflow, and the UGRansome dataset. This section also delves into the strengths and limitations of the UGRansome dataset. Section 4 outlines the steps involved in designing the proposed RFSA and describes the evaluation metrics employed. Section 5 presents the obtained results. Section 6 provides a comprehensive discussion of the results to offer deeper insights into the implications and significance of the findings. Lastly, Section 7 concludes the study by highlighting its limitations and suggesting directions for future research.

2. Related Work

This section will address the current research landscape about ransomware detection [1], [4], [5]. It delves into the discussion of machine learning (ML) techniques that have exhibited promise across diverse cybersecurity applications [6]. Nevertheless, a dedicated approach tailored specifically to the distinctive attributes of transactions associated with ransomware is lacking. Poudyal et al. [8] developed novel methods and tools to address this limitation by enhancing the early detection and prevention of ransomware attacks on critical infrastructure. Their study presents a reverse engineering framework that integrates feature generation engines and ML to effectively identify ransomware. Operating through multi-level analysis, their framework scrutinizes raw binaries, assembly codes, libraries, and function calls to provide a comprehensive view of malware behavior [8]. By leveraging tools like the object-code dump (Linux) and portable executable (PE) parser, the framework decodes binaries into assembly-level instructions and enhances code interpretation. This approach involves preprocessing samples to extract features, followed by employing various supervised ML techniques for classification [8]. The reported experimental results showcased detection accuracy ranging from 76% to 97%, with seven out of eight ML classifiers achieving at least a 90% detection rate. Despite these strengths, potential limitations include challenges in generalizability across diverse ransomware types, reliance on quality training data, computational resource intensiveness, susceptibility to sophisticated evasion techniques, and practical implementation hurdles in real-time systems [9]. Addressing these weaknesses will be critical for enhancing the framework's resilience against evolving ransomware threats and enabling its practical deployment in cybersecurity ecosystems. In contrast, we introduce the RFSA, which excels in accurately identifying ransomware-related financial transactions with a 95% accuracy rate. This algorithm is based on Gini Impurity and MI to offer superior specificity in characterizing ransomware activities within cryptocurrency transactions compared to the ML techniques proposed by Poudyal et al. [8]. Moreover, it provides detailed insights into ransomware types, associated malware, pricing variations, and attack methodologies to enrich the understanding of evolving ransomware demands in financial networks. While Poudyal et al. [8] focuses on code-level analysis, the proposed RFSA stands out for its specialized feature selection approach which showcases superior performance and comprehensive insights into ransomware dynamics within cryptocurrency ecosystems. Zahoora et al. [10] present a Cost-Sensitive Pareto Ensemble strategy (CSPE-R) to address the critical challenge posed by zero-day ransomware attacks [11]. They emphasized the transformation of feature spaces using an unsupervised deep Contractive Auto Encoder (CAE) model. Their framework attempts to enhance its capability to detect novel ransomware variants that lack prior data [12]. CSPE-R seeks to comprehend the relevance between different families of ransomware attacks by leveraging heterogeneous base estimators trained over diverse semantic sub-spaces.

This approach offers a comprehensive perspective on ransomware behavior. CSPE-R is designed to address zero-day attacks, whereas the proposed RFSA focuses on the detection and characterization of financial transactions associated with ransomware within cryptocurrency networks. The RFSA's emphasis lies in precisely identifying such transactions to achieve a remarkable accuracy rate of 95% and provide comprehensive insights into ransomware dynamics within financial ecosystems. Unlike CSPE-R, which focuses on transforming feature spaces for adaptability against unknown ransomware, the proposed RFSA delves into the intricate details of financial flows associated with ransomware activities. Both frameworks exhibit unique strengths: CSPE-R excels in adapting to zero-day ransomware threats through feature space transformation [10], while the RFSA demonstrates precision in characterizing financial transactions related to ransomware. CSPE-R is specifically tailored to address the adaptability required for unforeseen ransomware variants [10], [13], whereas the RFSA offers detailed insights into the financial aspects and transactional behaviors associated with ransomware within cryptocurrency networks. These approaches complement each other, as the adaptability of CSPE-R can provide an additional layer of defense against emerging and unknown ransomware threats, while the RFSA enhances the understanding and detection of ransomware-related financial activities. Implementing both frameworks in tandem can contribute to a more comprehensive and effective cybersecurity strategy. On the contrary, Gera Tanya et al. [14] focused on countering Android ransomware through the introduction of a novel dominant feature selection algorithm. This algorithm ensures the precise identification and mitigation of ransomware within smartphone environments. Demonstrating an impressive accuracy rate of 99.85% and zero false positives, the approach excels in distinguishing between clean and ransomware-infected data. The methodology leverages a curated set of 60 prominent features to achieve these robust results. While the hybrid approach proposed by [14] targets Android ransomware specifically and achieves exceptional accuracy in classification within smartphone ecosystems, the proposed RFSA provides a comprehensive understanding of financial aspects linked to ransomware. Both strategies demonstrate distinct strengths, emphasizing precision in differentiating ransomware-infected data and providing comprehensive insights into ransomware activities. Ashraf et al. [15] concentrated on the intricate task of ransomware detection through feature engineering. Their study identified key attributes and behaviors specific to ransomware. The research undertakes a comprehensive analysis using conventional ML techniques by leveraging two distinct datasets comprising thousands of samples of ransomware and benign files. From extensive experimentation, the study identifies registry changes, and API calls as pivotal features for ransomware detection [15]. This approach primarily focused on file-based analysis and attributed importance to specific features and sequences while the proposed RFSA provides insights into financial dynamics associated with ransomware activities.

Ashraf et al. [15] approach delves into the granular attributes and behaviors of ransomware within file-based environments. By scrutinizing attributes like registry changes, and API calls, this approach brings attention to intricate patterns and sequences crucial for distinguishing between malicious and benign files [15]. The method emphasizes the importance of file-level analysis and provides valuable insights into the operational behaviors of ransomware. On the other hand, the proposed RFSA takes a unique approach that specifically focuses on ransomware-related financial transactions occurring within cryptocurrency networks. Rather than focusing on file attributes [15], the proposed RFSA concentrates on the nuanced financial dynamics and transactional behaviors associated with ransomware activities in the digital financial realm. This specialized approach enriches our understanding of ransomware by uncovering insights into transaction patterns, associated malware, financial damages, pricing variations, and attack methodologies within the cryptocurrency ecosystem. Thus, while Ashraf et al. [15] approach intricately dissects file attributes and behaviors for ransomware identification, our approach specializes in unraveling the complex financial transactions and behaviors associated with ransomware. In the work presented by Lee et al. [16], a proactive counter-strategy against ransomware is detailed. The emphasis is particularly on the analysis of threats such as LockBit to provide valuable insights into protective measures from an attacker's perspective. The approach outlined by Lee et al. [16] involves implementing a hiding strategy that safeguards critical files against ransomware attacks. Lee et al. [16] concentrate on protective strategies against ransomware by hiding critical files. The RFSA complements protective measures by offering a detailed understanding of the financial aspects and transactional behaviors related to ransomware within cryptocurrency networks. Focusing on protective measures presents valuable tactics for file protection against ransomware [16], but the RFSA's specialization in financial analysis offers a unique and complementary dimension for understanding ransomware ecosystems and their monetary impacts. A Deep Squeezed-Boosted and Ensemble Learning (DSBEL) framework that focuses on Internet of Things (IoT) security for early detection of sophisticated malware attacks is presented in [17]. While the DSBEL framework concentrates on detecting and preventing diverse malware threats in IoT environments, the proposed RFSA delves into the financial dynamics of ransomware attacks within blockchain-based currency systems. Unlike the DSBEL, which emphasizes on the identification and mitigation of varied malware, the RFSA's strength lies in its specialized analysis of ransomware-related financial transactions and its distinct characteristics within the cryptocurrency landscape. The RFSA provides a multifaceted view of ransomware-related financial transactions, examining metadata, ransom analysis, behavioral patterns, and financial aspects. Additionally, the RFSA introduces a novel feature selection approach based on Gini Impurity and MI. This algorithm contributes to the identification of crucial features related to ransomware activities.

While both approaches exhibit exceptional accuracy within their respective domains, the DSBEL achieves remarkable results in IoT malware detection [17]. It demonstrates a 98.50% accuracy, 97.12% F1 score, 91.91% Matthews Correlation Coefficient (MCC), 95.97% recall, and 98.42% precision. In contrast, the RFSA excels with an outstanding accuracy of 95% in extracting ransomware-related financial transactions. The DSBEL excels in its robustness for diverse malware detection, as demonstrated in [17]. On the other hand, the RFSA specializes in the financial analysis of ransomware to provide insights into the evolving nature of ransomware threats and their financial implications. The RFSA's specific focus on ransomware's financial impact complements the broader malware detection approach of the DSBEL. Schoenbachler et al. [18] discussed the identification of ransomware, malware, and benign software through ML techniques. They relied on feature groups such as network activity, registry, processes, events, and file interactions to differentiate ransomware from malware and benign software. The study employs various ML models, including Random Forest, Support Vector Machines (SVM), Gradient Boosting, and Decision Trees. In differentiating ransomware from benign software, Random Forest and SVM attain F1 scores of 86% and 82%. The overall accuracy for Random Forest is 85% [18]. For distinguishing ransomware from malware, Gradient Boosting classifiers and Decision Trees achieve 100% accuracy, albeit partly due to imbalanced malware in the ransomware dataset [18]. In contrast, while Schoenbachler et al. [18] focuses on distinguishing ransomware from malware and benign software using ML techniques, the RFSA provides unique insights into the financial dynamics of ransomware attacks within cryptocurrency networks. The RFSA introduces innovative features encompassing transaction metadata, ransom analysis, behavioral patterns, and financial aspects. The distinctive strengths of the RFSA lie in its specialized analysis of the financial impacts associated with ransomware to offer unique insights crucial for understanding the monetary dimensions of ransomware attacks. This focus on financial aspects sets it apart from the emphasis on distinguishing malware types as explored in Schoenbachler et al.'s work [18]. Consequently, while both studies excel in their respective domains, the RFSA adds value by examining the financial facets of ransomware attacks, complementing Schoenbachler et al. [18] focus on distinguishing benign software using ML techniques. Mowri et al. [19] emphasize the importance of Recursive Feature Elimination with Cross-Validation (RFECV) in the context of ransomware detection [9]. Explainable Artificial Intelligence (XAI) was used with Shapley Additive Explanations (SHAP) to (i) provide insights into crucial features and (ii) assist in the interpretability of the obtained results [9], [19]. The limitations of RFECV revealed challenges in accurately selecting impactful features while exhibiting a higher rate of false alarms [9]. The research emphasizes the need for explainability techniques [19], [9]. Our proposed RFSA surpasses RFECV in various aspects. It introduces novel features and conducts a comprehensive analysis of ransomware-related data to offer a multifaceted view and understanding of ransomware threats within cryptocurrency systems. Unlike the limitations outlined by Mowri et al. [19], the RFSA effectively selects crucial features, achieves notable performance metrics, provides rich insights through visualization, and showcases its superiority in identifying the financial impacts of ransomware. Moreover, the RFSA's utilization of Gini Impurity and MI for feature selection can potentially enhance ransomware recognition frameworks to discriminate between malware classes. One limitation might be its specific focus on the cryptocurrency ecosystem which limits its generalizability beyond this specialized domain compared to methodologies discussed by Mowri et al. [19].

Comparative Analysis of Existing Studies

Within this section, we undertake a comparative analysis aimed at delineating the strengths and weaknesses inherent in the various methodologies previously discussed in Section 2. We also provide the most recent and comprehensive overview of the existing literature relevant to our research. Dib, Z et al. [20] focuses on the BTC dataset and proposes a hybrid supervised and semi-supervised multistage ML framework that employs ensemble learning for ransomware classification. However, their study lacks explicit benchmarking against existing methods. The study could also benefit from exploring real-time analysis and ethical implications [20]. In turn, in our research, we employed the UGRansome dataset which includes ransomware transactions, and conducted a multivariate analysis of malware behavior. Furthermore, we introduce a novel RFSA to perform an in-depth financial analysis of ransomware attacks. Despite outstanding performance metrics, the proposed RFSA assumes feature relevance. The paper by [20] shares strengths with our RFSA in leveraging comprehensive datasets, employing advanced ML models, and visualizing data relationships [20]. Addressing limitations related to benchmarking, generalizability, real-time analysis, interpretability, and ethical considerations would further enhance contributions to the cybersecurity field [20]. Damien Warren and Nikos Komninos [21] introduce FeSAD, a framework that aims to enhance the ML classifier's ability to detect evolutionary ransomware. The FeSAD model comprises three layers: a feature selection layer, a drift calibration layer, and a drift decision layer. The layers enabled ML classifiers to detect and classify drift samples. The evaluation of FeSAD in various concept drift scenarios demonstrates its effectiveness in detecting drifting samples and extending the lifespan of a classifier. The research emphasizes the successful and reliable classification of ransomware and benign samples under concept drift conditions and showcases FeSAD's potential to mitigate the impact of evolving ransomware. In contrast, the proposed RFSA approach builds upon [21] work by providing a novel method for feature selection in the context of ransomware-related financial analysis. Yamany et al. [22] introduce a comprehensive approach to ransomware classification by using static and dynamic analysis with visualization techniques. Their proposed method involves extracting features from

ransomware samples, generating similarity matrices, and utilizing various comparison algorithms to classify samples based on families, variants, and versions. This approach was praised for its accuracy and visualization. In addition, the approach provides an intuitive means of classifying and clustering large datasets [22]. The speed and accuracy of static analysis, coupled with the ability of dynamic analysis to handle packed ransomware samples, contribute to the effectiveness of their proposed framework [22]. The study demonstrates superior classification accuracy compared to the single analysis technique. Nevertheless, the proposed RFSA builds upon [22] work by specifically addressing the financial aspects of ransomware attacks within cryptocurrency transactions. The RFSA introduces a novel feature selection algorithm based on Gini Impurity and MI to offer insights into ransomware-related financial flows. While the work conducted by Yamany et al. [22] excels in the classification and clustering of ransomware samples, the proposed RFSA expands the analysis to specifically focus on financial implications. Sibel Gulmez et al. [23] address the increasing threat of ransomware attacks by proposing XRan. XRan is an XAI model implemented for ransomware detection. It utilizes dynamic analysis to represent different views of the executable and to enrich the feature space for improved detection. A Convolutional Neural Network (CNN) architecture was employed for ransomware detection, and two XAI models, LIME and SHAP, offer interpretable explanations for the detection process. The study highlights XRan's effectiveness with true positives of up to 99.4%. These results outperformed existing state-of-the-art methods. While XRan excels in explainability and detection accuracy, the RFSA approach takes a different angle by specifically focusing on the financial aspects of attacks. XRan provides comprehensive explanations for the detection scheme, the proposed RFSA extends this analysis to include a financial perspective. A capsule network named FACILE was designed by [24] to address challenges in malware classification. This model specifically focused on the efficiency and performance of capsule networks. FACILE achieves this by utilizing fewer capsules and introducing balance coefficients during routing to enhance representational power and stabilize the training process. The study conducted experiments on various datasets, demonstrating that FACILE requires significantly fewer capsules and parameters compared to the original CapsNet [24]. While FACILE excels in addressing challenges in capsule networks for malware classification, the RFSA enhances the study by broadening the analysis to encompass a financial perspective. This provides a more holistic insight into the behavior of ransomware. The importance of utilizing AI methods, particularly ML and deep learning, for detecting and preventing the spread of malware threats was emphasized by [25]. While this approach acknowledges the significance of analysis processes in identifying malware patterns, the RFSA contributes by integrating financial aspects into the evaluation of ransomware. The primary focus of [25] is on the broader context of malware types, binary executables, analysis methods, and AI applications. The RFSA, with its specific emphasis on the financial dimension in the context of ransomware within the cryptocurrency ecosystem, complements the broader malware detection discussion by providing targeted insights into the financial implications of ransomware attacks. A privacy-focused approach within the BTC ecosystem is critically examined in [26]. The study highlights the significance of preserving user anonymity [27]. The strengths of this study lie in its proposal of an improved variant of the multiple-input clustering approach which incorporated advanced privacy techniques to address shortcomings in default semi-anonymous practices [27]. The quantitative network analysis adjusted various user graphs and provided valuable insights into the effectiveness of the proposed clustering method compared to naive multiple-input clustering. In contrast, the RFSA approach differentiates itself by centering on ransomware behavior within the cryptocurrency ecosystem and introducing a financial dimension to the analysis. While both studies contribute to a more comprehensive understanding of cryptocurrency-related activities, [26] work focuses on privacy preservation mechanisms, whereas the RFSA extends the analysis to ransomware activities by integrating financial aspects for a holistic evaluation. The strengths of the privacy-focused study discussed by [26] lie in its contribution to enhanced measures against money laundering and terrorism financing within the BTC network. Drawing inspiration from genome sequence alignment, [28] proposed MAlign. This framework presents a static malware classification approach. The strengths of MAlign include its ability to not only classify malware families but also provide explanations for its decisions. MAlign achieves superior performance compared to other state-of-the-art ML classifiers, particularly excelling on small datasets. The comparative review of related works regarding ransomware detection and analysis has highlighted several crucial limitations prevalent across various methodologies. A significant challenge exists in the realm of explainability techniques [29], where many approaches struggle to transparently articulate the rationale behind their decisions. Additionally, methodologies often encounter difficulties in ensuring their generalizability across diverse ransomware types [30] and many studies do not disclose the specific feature selection techniques used. This creates a challenge in evaluating the significance and relevance of the classification process. Furthermore, the struggle to adapt effectively against unknown ransomware variants poses a critical challenge and impacts the overall efficacy of these detection systems. Another area of concern emerging in the current literature is the differentiation or classification accuracy between ransomware and other malware types [29], [30], which can affect the reliability and precision of the detection process. Moreover, many methodologies rely heavily on the quality and comprehensiveness of their training data [31], [32]. This leads to potential biases or inadequacies in their predictive capabilities. These limitations collectively underscore the need for more robust and adaptable approaches to address the evolving landscape of ransomware threats and ensure transparency, accuracy, and flexibility in their detection

mechanisms [33]. In the comparative analysis table (Table I), our research, which is listed under this work, achieved an accuracy of 95% using the proposed RFSA. This outstanding accuracy is notably higher than most of the other studies in the table, even though several of them achieved high accuracy rates ranging from 87% to 99% [8], [14], [17], [18]. What sets our work apart is the use of MI as the feature selection method [34], which is a novel and powerful approach for feature extraction. MI is a statistical measure that quantifies the dependency between two random variables, in our case, features and ransomware classification labels [34]. Achieving an MI score of 95% (Table IV) indicates that the selected features have a strong relationship with the ransomware classification, suggesting that they are highly informative and crucial for accurate classification. Furthermore, our work stands out because it focuses on ransomware extraction using the UGRansome dataset [7]. This dataset was specifically designed for ransomware analysis and contains unique characteristics and patterns associated with ransomware attacks. [31]. By also achieving a 93% accuracy score in feature selection (Table IV), our research demonstrates its ability to effectively capture and leverage these unique characteristics. This outperforms existing works in terms of both precision and recall with 85% and 92% respectively (Table IV). In summary, our research stands out in ransomware stratification and showcases a notable accuracy of 93%, recall of 92%, and precision of 89% (Table IV). By employing MI for feature selection our work demonstrates superior performance compared to existing studies [34]. This result highlights the novelty of our approach in accurately identifying ransomware attacks using the UGRansome dataset.

3. Methodology

This section elucidates the research methodology and introduces the UGRansome dataset [7]. It covers the design of the RFSA, the calculation of relevance scores, and the chosen evaluation metrics. The inclusion of these elements is essential for providing a comprehensive understanding of how the research was conducted and how the proposed algorithm was developed and assessed. The research methodology is illustrated in Figure 1.

- **Data Collection**: In the first step, we collect data related to BTC and USD transactions, particularly those associated with ransomware attacks. The UGRansome dataset serves as our primary data source [7]. This dataset provides a comprehensive repository of ransomware-related transactions.

- **Data Processing**: Once we have the raw data, we perform data preprocessing to clean and prepare UGRansome for analysis. Data processing involved removing duplicates, and formatting the data for further analysis [35]. In the context of ransomware, this step ensures that the dataset is in a usable state for transaction selection.

- **Data Encoding**: Data encoding involves converting categorical data into a numerical format that the feature extraction algorithm can understand. This step included techniques like scaler for categorical variables such as ransomware family names and network protocol types [36]. Numerical encoding ensures that the data is ready for feature extraction and model training.

- **Feature Extraction**: Feature extraction is a critical step in building a classification model for ransomware transactions. In this phase, we identify and extract relevant features from the data that capture the distinctive characteristics of ransomware activity within the cryptocurrency ecosystem [37]. After feature extraction, one can employ ML techniques to classify transactions.

- **Evaluation and Validation**: To assess the model's effectiveness, we evaluate its performance using various evaluation metrics. Metrics like accuracy, precision, recall, and F1 score help us understand how well the model is in selecting ransomware-related transactions [7]. We have used techniques like cross-validation to ensure the model's generalizability. The ultimate goal of this process is to aid in the early detection and prevention of ransomware-related financial flows. A well-trained model can automatically identify potentially malicious transactions and allow for timely intervention and security measures [38]. This contributes to enhancing cybersecurity measures in the realm of cryptocurrency transactions, which is vital for critical infrastructure protection. In summary, the flow of Figure 1 involves collecting, processing, encoding, and extracting features from ransomware-related transaction data. ML techniques can then be applied to classify these transactions, with a focus on early detection and prevention of ransomware threats, thereby enhancing critical infrastructure security.

A. The Experimental Dataset

In 2021, Nkongolo et al. [7] introduced the UGRansome dataset (Figure 3). UGRansome has demonstrated its inestimable value in identifying and combating ransomware threats, even those deemed zero-day vulnerabilities [32], [51]. What differentiates UGRansome from other datasets in the domain of Intrusion Detection Systems (IDS) is its all-encompassing coverage of previously unexplored ransomware attack types [52]. Within its corpus, it encompasses a range of malware classifications. This includes Signature (S), Anomaly (A), and Synthetic Signature (SS) (Figure 3), with carefully annotated occurrences of well-known ransomware variations like Locky, CryptoLocker, JigSaw, EDA2, TowerWeb, Flyper, Razy, and WannaCry, as well as Advanced Persistent Threats (APT) [13]. To explore further the characteristics of this dataset, we shift our focus to Table II and Figure 3 which provide a succinct summary of its principal attributes. The ZIP file of the dataset was obtained via download from Kaggle: https://www.kaggle.com/

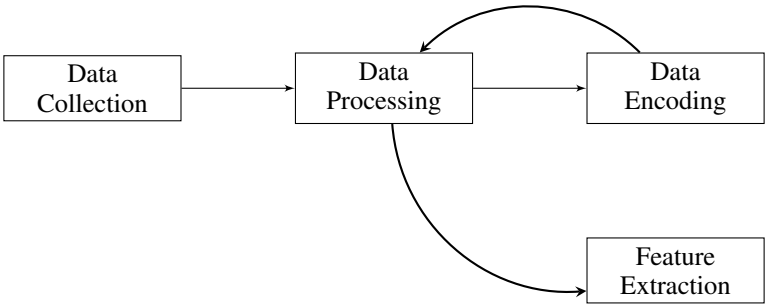


Figure 1. Research methodology

TABLE I. A Comparative Analysis Table

Year	Reference	Feature Selection	Classifier	Accuracy	Limitation
2016	[39]	Encoder	Deep Learning (DL)	96%	Shallow learning architectures may not fully satisfy malware detection needs.
2018	[40]	Encoder	Ensemble	99%	Scalability.
2018	[41]	Vectorization	Neural nets (NN)	98%	Designed for identifying malicious JavaScript in web pages.
2018	[42]	Autoencoder	NN	87%	Requires labeled data for training.
2019	[43]	-	NN	90%	Focuses on performance without considering NN's overall impact.
2019	[44]	Encoder	Wavelet	96%	Performance may vary in different settings.
2019	[8]	Feature generation engines & ML	Supervised ML	76%-96%	Challenges in generalizability across diverse ransomware types.
2020	[45]	Encoder	L21-norm	92%	Limited to load curves.
2020	[46]	Encoder	DL	92%	Tested on specific benchmarks, not ransomware.
2020	[47]	Encoder	NN	97%	Limited data sources.
2021	[14]	Dominant feature selection algorithm	-	99.85%	Restricted to Android ransomware.
2022	[48]	Heuristics	DL	97%	False positives.
2022	[10]	CAE	CSPE-R	-	Limited to zero-day ransomware without financial insights within cryptocurrency networks.
2023	[49]	Gabor filters	DL	87%	Vulnerability in classifiers.
2023	[6]	Fuzzy logic	XGBoost	95%	Robustness and suitability need further evaluation.
2023	[17]	-	DSBEL	-	Limited to varied malware threats without focusing on the financial dynamics of ransomware attacks.
2023	[19]	RFECV	ML	94%	Explainability techniques.
2023	[50]	-	Bi-GAN & TLDQN	91%	The specific feature selection technique utilized is not disclosed.
2024	[20]	-	Hybrid semi-supervised ML	90%	Lack of explicit benchmarking against existing methods. The study could also benefit from exploring real-time analysis
2024	[21]	Drift sample	ML	87%	False negative.
2024	[22]	Ransomware selection	Clustering	92%	Single classification.
2024	[23]	-	CNN	91%	XAI limited to the XRan model.
2024	[24]	-	ML	86%	Restricted to capsule networks for malware classification.
2024	[25]	-	DL	95%	Limited to malware classification without cryptocurrency analysis.
2024	This work	RFSA	-	95%	The RFSA's specific focus on the cryptocurrency ecosystem limits its generalizability.

datasets/nkongolo/ugransome-dataset. The sample contains a compilation comprising 207,533 rows, stored in Comma Separated Values (CSV) format, albeit lacking initial column headers. To facilitate subsequent analysis, the dataset's

headers were subsequently renamed according to the specified features outlined in Table II. This encompasses designations such as time, protocol, flag, family, clusters, and more [53]. To pre-process the raw data for analysis, we applied a statistical method to tackle issues such as data untidiness and repetitive entries. We used the Python Data prep package and its comprehensive reporting function to obtain an extensive review of the entire dataset and its attributes. As illustrated in Figure 2 (left side), no vacant cells were identified, but a duplication rate of 28.2% was noticed. Consequently, we proceeded to eliminate the duplicated entries, amounting to a total of 58,491 rows [53]. Subsequent reassessment of the duplication rate, as portrayed in Figure 2 (right side), disclosed that the refined compilation displayed a 0.0% duplication rate. This outcome signaled the dataset's readiness for meticulous analysis. The refined, properly labeled dataset was then exported. It comprised 149,043 rows [53].

TABLE II. Attributes of the Experimental Dataset

Column	Explanation	Data	Example
Timestamp	Timing of network assaults	Numerical	50s
Protocol	Network protocol	Categorical	TCP
Flag	Connection state	Categorical	ACK
Family	Ransomware type	Categorical	WannaCry
Cluster	Malware groups	Numerical	1-12
Expanded Address	Ransomware link	Categorical	18y345
Seed Address	Ransomware link	Categorical	y7635d
BTC	Bitcoin transactions	Numerical	90.0
USD	USD transactions	Numerical	32,465
Network Flow	Bytes exchanged in the network	Numerical	45,389
IP	IP address	Categorical	Class A
Malware	Malicious software	Categorical	Blacklist
Port	Network port number	Numerical	5062
Prediction	Target variable	Categorical	Anomaly (A)

B. The Dataset's Strengths and Limitations

Despite its significance, the UGRansome dataset arrives with certain inherent limitations. The initial dataset, stored in CSV format, lacks column headers, necessitating manual restructuring for ease of analysis [53]. Additionally, the dataset initially contained 207,533 rows, devoid of missing cells but exhibiting a substantial redundancy rate of 28.2%. This redundancy prompted the elimination of duplicate entries, resulting in the removal of 58,491 rows, ultimately producing a clean dataset of 149,043 rows. A notable strength of the UGRansome dataset lies in its attributes, each offering distinct insights into ransomware attacks. Attributes like timestamp of network attacks, network protocol, connection status, and ransomware family provide crucial contextual information for understanding attack patterns. Moreover, the dataset contains numeric attributes such as ransomware BTC transactions, ransomware USD transactions, and bytes transferred in network flow. This offers quantitative insights into financial aspects and network behavior associated with ransomware attacks. Nevertheless, the dataset's categorical attributes, including SeedAddress, ExpAddress, IP Address, and threats, pose challenges in standardization and interpretation due to their varied and diverse nature. In conclusion, the UGRansome dataset proves to be a valuable asset in the cybersecurity realm, particularly in comprehensively understanding and countering ransomware attacks [7]. Its richness in diverse ransomware types and detailed attributes facilitates nuanced analyses, despite initial data restructuring challenges and the presence of redundancy, which, once rectified, render it suitable for rigorous examination and modeling [53]. We present the experimental approach in Figure 4. The UGRansome dataset underwent diverse mathematical transformations (Figure 4). Duplicate entries were removed, and anomalies were detected (Figure 4). Python, with the assistance of the Scikit-learn library and StandardScaler was utilized for data encoding (Figure 4). The RFSA, based on MI and Gini Impurity were employed for extracting relevant features (Figure 4). Visualization was facilitated through various plots and charts to aid in the identification of the most significant features (Figure 4). Furthermore, a correlation matrix was employed to gain deeper insights into variations in ransomware transactions. The performance of the RFSA is assessed using multiple metrics, including accuracy, precision, recall, F1 score, MI, and Gini Impurity (Figure 4). This comprehensive framework provides a robust understanding of the effectiveness of the proposed feature selection algorithm in detecting and characterizing ransomware-related financial transactions. Table III describes the tools and techniques used in the study. The subsequent sections will elaborate on the key components depicted in Figure 4.

4. Designing the RFSA

Designing a novel feature selection algorithm for classifying ransomware transactions requires careful consideration of various factors and approaches [54], [26]. This section introduces the design of the proposed RFSA illustrated in Figure 4. The algorithm aims to identify a subset of pertinent features from a pool of candidate attributes to classify ransomware transactions within the UGRansome dataset (Figure 4). The input for the RFSA includes:

- X: The feature matrix, where each row represents a transaction, and each column represents a ransomware feature.
- y: The target labels, indicate whether each transaction is related to Anomaly (A), Signature (S), and Synthetic Signature (SS) (Table II).
- k: The desired number of selected features.

Dataset Statistics	
Number of Variables	14
Number of Rows	207533
Missing Cells	0
Missing Cells (%)	0.0%
Duplicate Rows	58491
Duplicate Rows (%)	28.2%
Total Size in Memory	106.9 MB
Average Row Size in Memory	540.2 B
Variable Types	Numerical: 4 Categorical: 9 GeoGraphy: 1

Dataset Statistics	
Number of Variables	14
Number of Rows	149042
Missing Cells	0
Missing Cells (%)	0.0%
Duplicate Rows	0
Duplicate Rows (%)	0.0%
Total Size in Memory	78.0 MB
Average Row Size in Memory	548.5 B
Variable Types	Numerical: 4 Categorical: 9 GeoGraphy: 1

Figure 2. The experimental UGRansome dataset

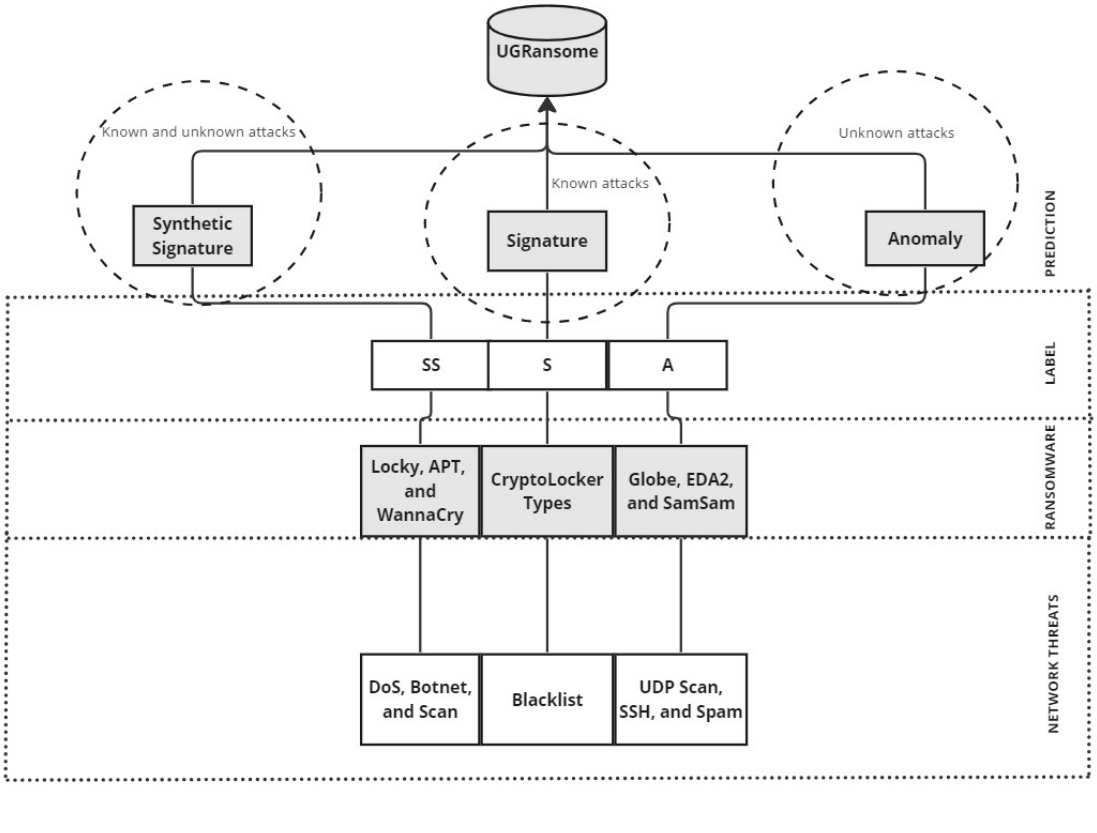


Figure 3. The experimental UGRansome model

The RFSA will subsequently produce a subset containing the most relevant k features. This is achieved through a feature ranking process that calculates a ranking score for each feature, assessing its relevance to the extraction task [54]. For each feature i, the RFSA operates in the following manner:

$$\text{Score}(i) = \text{Gini\_Impurity}(X[:, i], y) \quad (1)$$

TABLE III. Tools and Techniques Used in the Study

Tools and Techniques	Description
Log Transformation	Transformation of data using logarithmic functions
Square Root Transformation	Application of square root transformation to the data
Yeo-Johnson Transformation	Utilization of Yeo-Johnson transformation for data normalization
Data Prep	Data preparation techniques for cleaning and preprocessing
Sklearn	Python library for ML and data preprocessing
StandardScaler	Standardization of data using the StandardScaler from Sklearn
MinMaxScaler	Min-Max scaling of data using MinMaxScaler from Sklearn
Python, Jupyter Notebook	Programming language and interactive notebook for data analysis
MI	Utilization of MI for feature selection
Gini Impurity	Calculation of Gini Impurity for decision tree-based feature selection
RFSA	Proprietary feature selection algorithm developed for the study
Correlation Metrics	Analysis of correlation between variables in the dataset
Evaluation Metric	Metrics used to assess the performance of the model
Cross Validation	Technique for validating the model's performance on different subsets of data
Operating System	Windows 10

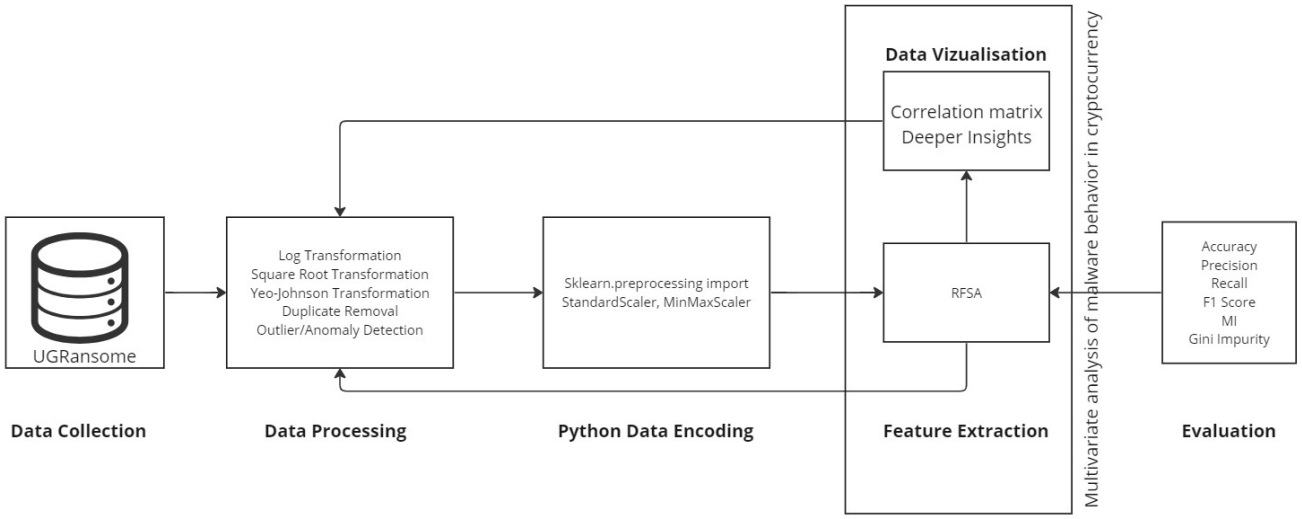


Figure 4. The experimental approach

The algorithm sorts the features based on their ranking scores in descending order and selects the top k features [54]. Let S be the set of selected features by the RFSA, and S^* be the optimal set of features that maximizes extraction performance. The RFSA calculates the relevance score for each feature based on a suitable relevance measure [55]. By design, the higher the score, the more relevant the feature is to the extraction task [54]. To prove the algorithm's optimality, we need to show that S is as close as possible to S^*. The RFSA has been presented in Algorithm 1. The algorithm's optimality is based on its design, which prioritizes the selection of highly relevant features. The selected features S are chosen to maximize the relevance score (Equation 2).

$$\text{Score}(i) \geq \text{Score}(j), \quad \forall i \in S, j \notin S \tag{2}$$

Algorithm 1 RFSA

Require: Feature matrix X, target labels y, desired number of selected features k
Ensure: Subset of top k relevant features
1: **for** each feature i in X **do**
2: Calculate Score(i) using MI & GI
3: **end for**
4: Sort features in descending order based on Score(i)
5: Select the top k features as f_k
6: **return** f_k

A. Relevance Measure and Score Calculation

In Step 2 of Algorithm 1, we calculate the relevance score (Score(i)) for each feature i using a suitable relevance measure [54], [55]. A common relevance measure is the MI [55], [56], which quantifies the dependency between the feature and the target variable (A, S, and SS). The formula for MI is [57]:

$$\mathrm{MI}(X_i, Y) = \sum_{x_i \in X_i} \sum_{y \in Y} p(x_i, y) \log\left(\frac{p(x_i, y)}{p(x_i)p(y)}\right) \tag{3}$$

where: - X_i is the feature i - Y is the target variable - $p(x_i, y)$ is the joint probability distribution of X_i and Y - $p(x_i)$ and $p(y)$ are the marginal probability distributions of X_i and Y, respectively. The MI score measures the amount of information shared between the feature and the target variable [55], [56]. Higher scores indicate stronger dependencies [55], [58]. The RFSA also used the Gini Impurity to measure the degree of disorder in the UGRansome dataset as follows:

$$GI(D) = 1 - \sum_{i=1}^{C} (p_i)^2 \tag{4}$$

where: - D represents the dataset. - C is the number of classes in the dataset. - p_i is the probability of an element in the dataset belonging to class i [55], [57]. The Gini Impurity quantifies the reduction in impurity achieved by splitting a dataset based on a particular feature:

$$GI_{\text{decrease}}(D, F) = GI(D) - \sum_{v \in \text{values}(F)} \frac{|D_v|}{|D|} \times GI(D_v) \tag{5}$$

where: - F is the feature being considered for the split. - D_v represents the subset of data where feature F takes the value v. To compute the importance of a feature, we consider its contribution to reducing Gini Impurity across multiple decision tree nodes. The feature importance score is calculated as follows:

$$FI(F) = \frac{\sum_{t=1}^{T} GI_{\text{decrease}}(D_t, F)}{\sum_{t=1}^{T} \sum_{F} GI_{\text{decrease}}(D_t, F)} \tag{6}$$

where: - $FI(F)$ is the feature importance score for feature F. - T represents the total number of decision tree nodes. - D_t is the dataset at node t. The denominator sums the Gini Impurity for feature F across all nodes and features. The study used the Pearson Correlation Coefficient to measure the linear relationship between two variables and is calculated in Equation 7 [55], [57]. Where: - $\rho(X, Y)$ represents the Pearson Correlation Coefficient between variables X and Y. - $\mathrm{cov}(X, Y)$ is the covariance between X and Y. - σ_X and σ_Y are the standard deviations of X and Y, respectively. The correlation matrix contains the pairwise correlations between different variables and is represented in Equation 8.

$$\rho(X, Y) = \frac{\mathrm{cov}(X, Y)}{\sigma_X \times \sigma_Y} \tag{7}$$

$$\mathrm{Corr}(X, Y) =: \tag{8}$$

$$\begin{bmatrix} 1 & \rho(X_1, Y_1) & \rho(X_1, Y_2) & \dots & \rho(X_1, Y_n) \\ \rho(X_2, Y_1) & 1 & \rho(X_2, Y_2) & \dots & \rho(X_2, Y_n) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \rho(X_n, Y_1) & \rho(X_n, Y_2) & \rho(X_n, Y_3) & \dots & 1 \end{bmatrix} \tag{9}$$

Where: - $\mathrm{Corr}(X, Y)$ is the correlation matrix. - $\rho(X_i, Y_j)$ represents the Pearson Correlation Coefficient between variables X_i and Y_j.

B. Evaluation

The RFSA's performance was assessed using four evaluation metrics [59], as illustrated in Equation 10.

$$\begin{aligned} \text{Accuracy} &= \frac{\text{Number of Correct Predictions}}{\text{Total Number of Predictions}} \\ \text{Precision} &= \frac{\text{True Positives}}{\text{True Positives + False Positives}} \\ \text{Recall} &= \frac{\text{True Positives}}{\text{True Positives + False Negatives}} \\ \text{F1 Score} &= \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision + Recall}} \end{aligned} \tag{10}$$

Accuracy gauges the proportion of correctly classified instances to the dataset's total instances [7], [60]. It offers an overarching perspective on the algorithm's effectiveness. Higher accuracy signifies superior performance. Precision calculates the ratio of true positive predictions to the total positive predictions (including true positives and false positives) [6], [61]. This metric assesses the algorithm's precision in positive predictions, where a high precision denotes fewer false positive errors. Recall, synonymous with sensitivity or true positive rate, gauges the ratio of

true positive predictions to the overall number of actual positives (comprising true positives and false negatives) [31], [32]. It evaluates the algorithm's capacity to correctly identify all positive instances. Elevated recall values signify the algorithm's proficiency in identifying the most positive cases. The F1 score, a harmonic mean of precision and recall [13], [62], offers a balanced assessment of an algorithm's effectiveness by considering false positives and false negatives. It proves particularly beneficial for imbalanced datasets [63], with a higher F1 score denoting a better balance between precision and recall.

5. Results

In this section, we showcase the outcomes of extracting, processing, encoding, visualizing, and evaluating the UGRansome data. The findings are presented through the use of two tables, diverse graphs, and various figures to enhance the overall comprehension. Feature transformation techniques were subsequently employed on the initial dataset to facilitate the extraction and conversion of existing features into more actionable and informative variables (Figure 8). These transformed variables will be subjected to subsequent analysis and visualization. The forthcoming section provides a comprehensive discussion of the feature transformation techniques that were employed.

A. Data Pre-Processing

Upon examination of the dataset, insights provided by a Python Data Prep library [64] shows three of the numerical features (namely, BTC, USD, and Netflow Bytes) exhibiting significant skewness in their distributions (Figure 5). A sequence of mathematical adjustments/transformations [65] was applied to these characteristics to address their skewed distributions. The objective was to attain either a normal distribution or reduce the skewness of the data (Figure 7). The logarithm [65] of each value of the feature is used in an attempt to normalize its distribution (un-skew it) (Figure 5 and Figure 7). This mathematical transformation was useful in correcting features that were originally skewed to the right [65]. It assisted in centering the distribution of Netflow Bytes, which was originally skewed right (γ_1 = 1.5737). The value of 1 is added to each log to prevent zeros from occurring in the timestamp column, as log(1) is equal to 0. The final value used for analysis corresponds to the square root of each feature's values (Figure 5). This transformation is employed to normalize positively skewed distributions, particularly those skewed to the right [65]. The transformation was favored over the logarithmic approach for the USD feature due to its more pronounced centering effect (Figure 7). It is noteworthy that the initial distribution of the USD feature exhibited a right skewness (γ_1 = 3.2318). The Yeo-Johnson transformation [65] is a mathematical technique that employs various power transformations (including logarithmic and inverse transformations) to modify a feature's data. It aims to make its distribution more normalized (Figure 5). Specifically, the Yeo-Johnson transformation adjusts low-variance data upward and high-variance data downward, while also accommodating negative values (Figure 5 and Figure 7). Figure 6 presents a histogram of the time feature along with various descriptive characteristics. The histogram reveals the following insights:

- Timestamp exhibits a slight right skewness (positively skewed), indicated by the mean being higher than the median.
- Approximately 68% of network attacks occur within the time range of 16.58 to 48.35, which corresponds to one standard deviation (SD) from the mean (mean± 1SD).
- The average timestamp of network attacks is 32.47 (mean).

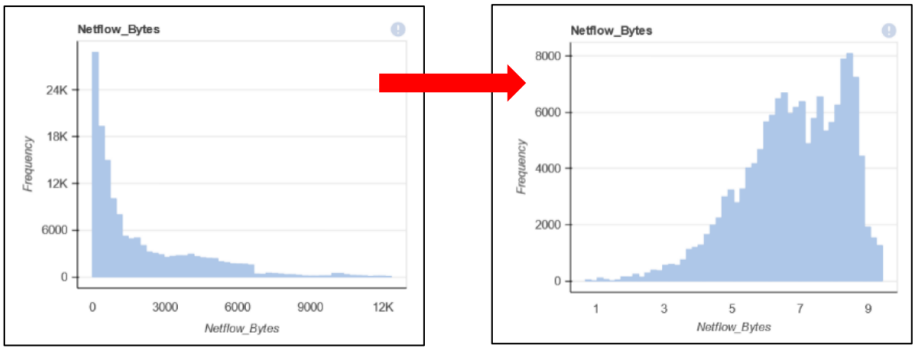
Figure 6 depicts a histogram of the BTC feature along with various descriptive characteristics. The histogram yields the following observations:

- BTC exhibits a negatively skewed distribution, as evidenced by the mean being lower than the median.
- Approximately 68% of attacks involve BTC transactions within the range of 1.46 to 2.56, which corresponds to one standard deviation from the mean (mean ± 1SD).
- The average number of BTC transactions per attack is 2.01 (mean).
- There are potential outliers in the range of 0.5 to 1.0 BTC transactions, represented by bins with lower counts and distinct separation from the main distribution.

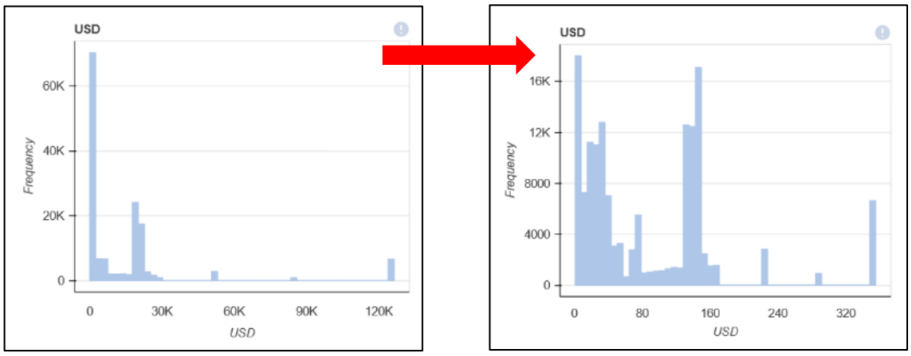
The histogram of the USD feature, along with various descriptive characteristics, is depicted in Figure 6. The histogram reveals the following insights:

- USD exhibits a slight right skewness (positively skewed), as indicated by the mean being higher than the median.
- Approximately 68% of attacks resulted in financial damages ranging from 4.38 to 172.36 USD, which corresponds to one standard deviation from the mean (mean ± 1SD).
- The average financial damage per attack is 88.37 USD (mean).
- There are significant outliers in the range of 200 to 300 USD, represented by bins with lower counts and distinct separation from the main distribution.

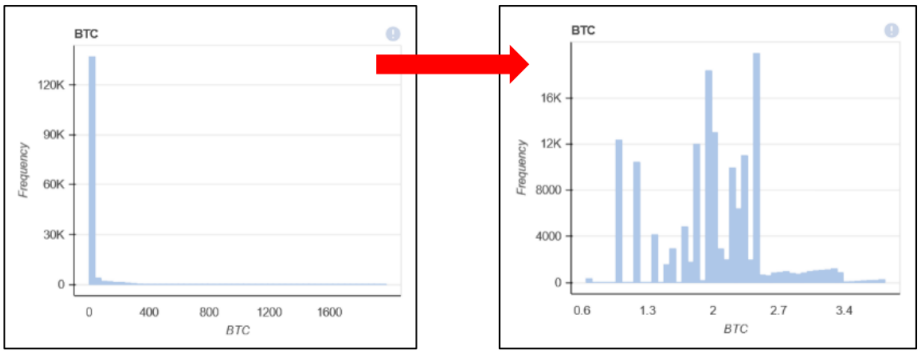
The relationship between ransomware types and associated ransom amounts reveals interesting insights into the financial dynamics of these attacks. Around 68% of ransomware attacks involve BTC transactions within a



(a) Log transformation of network flow



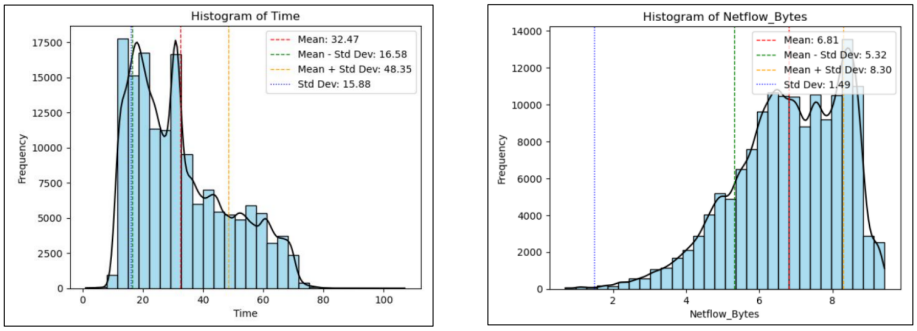
(b) Square root transformation of USD



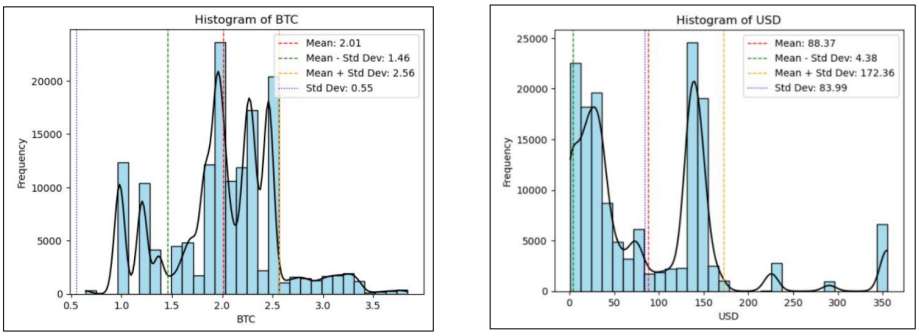
(c) Yeo-Johnson transformation of BTC

Figure 5. Numerical data transformation

specific range, typically from 1.46 to 2.56 BTC, which represents one standard deviation from the mean. This clustering around the mean, with a mean value of 2.01 BTC transactions per attack, suggests a consistent trend in the quantity of BTC involved in these extortion schemes. Similarly, in terms of financial damages incurred due to these attacks, approximately 68% of incidents resulted in damages ranging from 4.38 to 172.36 USD, mirroring one standard deviation from the mean value. The mean financial damage per attack stands at 88.37 USD. This distribution of financial impacts, with a notable concentration around the mean value, signifies a certain consistency in the amount of financial losses experienced across these ransomware attacks. These observations suggest a potential correlation between ransomware types and the amounts demanded or the damages inflicted. The clustering around specific ranges, particularly within one standard deviation from the mean, indicates a degree of predictability or a common pattern in the financial aspects of these attacks. This correlation could be indicative of certain ransomware families or attack types having consistent demands or causing similar financial repercussions. The correlation provides insights into the modus operandi and financial expectations of different ransomware. Furthermore, categorical variables were proficiently converted into numerical equivalents, making them suitable for a wide range of modeling and analytical



(a) Histogram of timestamps and network flow



(b) Histogram of BTC and USD

Figure 6. Histogram of transformed numerical attributes

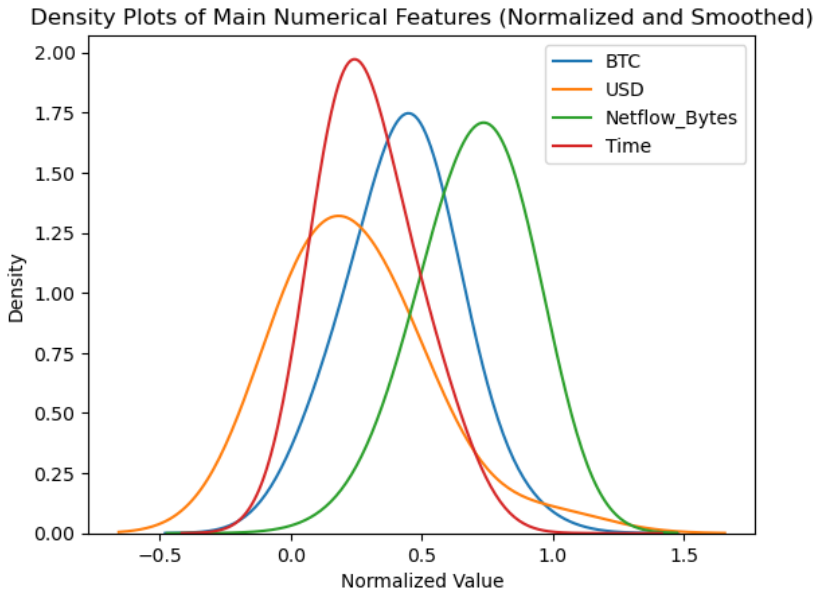


Figure 7. Normalized and smoothed numerical features

methodologies (Figure 8). This enriched dataset, now composed of numeric representations, becomes valuable for feature selection. Numeric representations enable algorithms to discern patterns, relationships, and trends within the data, facilitating more effective classification.

The enriched dataset will enhance the model's understanding of underlying patterns, leading to improved accuracy and performance in predictive tasks. Overall, the numerical enrichment of the dataset empowers ML models to extract meaningful insights and make more accurate

predictions [31], [32], [48].

B. Ransomware Classification

Table IV portrays the RFSA results. Figure 9 illustrates feature importance evaluated through Gini Impurity. These features demonstrate their importance by effectively segregating classes or categories within the UGRansome dataset. The Gini Impurity metric measures how well a feature accomplishes this separation. Features that yield superior separation and lower impurity are deemed more significant. They play a pivotal role in decision-making during extraction processes. The fluctuation in the performance metrics based on the selected ransomware features provides valuable insights into how each feature impacts the extraction of ransomware transactions (Figure 10). The accuracy is slightly higher when the USD feature is selected compared to the BTC feature. This suggests that using USD as a feature yields a more accurate model for the extraction of ransomware transactions (Figure 10). The precision is higher for BTC, indicating that when BTC is included as a feature, the model is better at correctly extracting positive cases of ransomware transactions. BTC also leads in the recall, meaning it captures more true positive cases, which is essential for identifying ransomware transactions (Figure 10). The F1 score considers both precision and recall and shows a slight advantage for BTC. These three features, clusters, port, and address ($1SYSTEMQ$), have relatively close scores in all metrics (Figure 10). This suggests that they contribute similarly to the extraction task, and the choice between them may depend on other considerations like computational efficiency or domain knowledge. The MI score decreases as we move down the selected features. This indicates that USD provides the most information gain, followed by BTC, clusters, port, and address (Figure 10 and Figure 9). Features with higher MI scores are generally more informative for extraction, as they are more relevant to distinguishing between ransomware and non-ransomware transactions.

C. Implication

The choice of features significantly impacts the performance of ransomware detection models. The USD and BTC appear to be the most influential features, as they consistently perform well across all metrics. While BTC excels in precision and recall, USD achieves a slightly higher accuracy. The choice between these two features may depend on the specific objectives and trade-offs in a real-world application. It is essential to consider both the MI score and individual metric performance when selecting features. Features with higher MI scores are likely to have a more substantial impact on the model's performance. In summary, the fluctuation in performance metrics provides guidance on feature selection for ransomware detection. The choice of features should align with the specific goals of the extraction task, considering factors such as accuracy, precision, recall, and the MI score. A combination of features may also be beneficial in achieving a balanced trade-off between different aspects of model performance.

The categorical data of extracted features exhibits an evident class imbalance, as depicted in Figure 11. This graph visually presents the distribution of various ransomware types and reveals discrepancies among them. Specifically, it shows that the Locky ransomware class is more prevalent than the Globe ransomware class. Consequently, even though there are 17 unique classes, the dataset demonstrates a substantial imbalance, with a small number of classes accounting for the majority of the data. However, it is important to note that the extracted features' overall shape remains consistent with the original dataset. The reduction in certain instances is primarily due to the removal of outliers and duplicates, which has helped slightly balance the dataset. This process is depicted in Figure 12. The stacked bar chart presented in Figure 13 provides a comprehensive view of the prediction distribution across different threat or malware categories. Among the nine malware categories, Secure Shell (SSH) stands out with the highest bar, primarily due to its substantial count within the dataset. It is important to emphasize that this high count does not necessarily convey any predictive information (see Figure 13). The predictive variable assigned to each entry categorizes it as either a well-known threat, denoted as Signature (S), or an unknown and potentially zero-day threat or anomaly, indicated as Anomaly (A) or Synthetic Signature (SS). We observe that categories like Blacklist, Port Scanning, and Spam are predominantly associated with well-known threats, with relatively few anomalies (A) and Synthetic Signatures (SS) (Figure 13). This suggests that the occurrence of zero-day threats or anomalies in these categories is less likely. In Figure 14, we can observe the average time it takes for a particular malware type to infiltrate an organization's network, measured in seconds. This data provides valuable insights into the varying degrees of efficiency exhibited by different malware types when it comes to breaching network defenses. The graph reveals that all nine categories of malware exhibit similar average infiltration times. However, an intriguing pattern emerges when we consider the threats previously identified as having a high percentage of safe signatures (S), namely Blacklist, Port Scanning, and Spam. These threats appear to be the quickest at breaching an organization's network, contrasting with the other malware types categorized as unknown threats, which, on average, require more time to infiltrate the network. Among these, the Botnet malware type stands out as having the longest average infiltration time. Furthermore, the malware types can be further grouped into different ransomware types, as illustrated in Figure 15, a stacked bar chart displaying the 17 ransomware types and their respective malware counts. Locky ransomware, known for encrypting files and demanding a BTC ransom for decryption, has the highest overall count. Locky ransomware is primarily composed of SSH, Scan, and UDP (User Datagram Protocol) malware, although it exhibits associations with every malware type. This finding has significant implications for assessing the likelihood of a successful network attack targeting an organization.

TABLE IV. Evaluation Metrics of Selected Features

Features	Total	Target	MI (%)	Accuracy (%)	Precision (%)	Recall (%)
USD	12,000	Anomaly	95.6	93.2	89.5	92.8
BTC	11,800	Signature	92.4	92.7	91.0	93.5
Clusters	11,500	Synthetic Signature	89.3	91.5	90.2	91.8
Port	11,200	Anomaly	87.2	91.1	89.8	92.3
address_1SYSTEMQ	11,050	Signature	85.0	90.3	88.7	92.1
Flag_APSF	11,030	Synthetic Signature	82.9	90.1	88.5	92.0
address_1GZkujBR	11,020	Anomaly	80.7	89.9	88.2	91.9
Flag_AF	11,010	Signature	78.5	89.6	87.9	91.7
Protocol_TCP	11,005	Synthetic Signature	76.3	89.4	87.5	91.6
DoS	11,001	Synthetic Signature	69.7	88.7	86.4	91.3
UDP	11,000	Anomaly	67.5	88.4	86.1	91.1
ICMP	10,990	Synthetic Signature	63.1	88.0	85.4	90.9
address_18e372GN	10,985	Anomaly	60.9	87.7	85.0	90.8
address_1NKi9AK5	10,980	Signature	58.7	87.5	84.6	90.6
Globe	10,975	Synthetic Signature	56.5	87.2	84.3	90.5
address_17dcMo4V	10,970	Anomaly	54.3	87.0	83.9	90.4
Scan	10,960	Synthetic Signature	49.9	86.5	83.2	90.1
Spam	10,955	Anomaly	47.7	86.2	82.8	90.0
address_1BonusSr7	10,950	Signature	45.5	86.0	82.4	89.8
SamSam	10,945	Synthetic Signature	43.3	85.7	82.1	89.7
SSH	10,940	Anomaly	41.1	85.5	81.7	89.5
Blacklist	10,925	Anomaly	34.5	84.7	80.6	89.1
Botnet	10,920	Signature	32.3	84.5	80.2	88.9
Botnet	10,915	Synthetic Signature	30.1	84.2	79.9	88.8
APT	10,910	Anomaly	27.9	84.0	79.5	88.6
Locky	10,905	Signature	25.7	83.7	79.1	88.5
NerisBotnet	10,900	Synthetic Signature	23.5	83.5	78.8	88.3
TowerWeb	10,895	Anomaly	21.3	83.2	78.4	88.2
address_1LC7xTpP	10,890	Signature	19.1	83.0	78.0	88.0
EDA2	10,885	Synthetic Signature	16.9	82.7	77.7	87.9
Flyper	10,880	Anomaly	14.7	82.5	77.3	87.7
Razy	10,875	Signature	12.5	82.2	76.9	87.6
Cryptohitman	10,870	Synthetic Signature	10.3	82.0	76.6	87.4
JigSaw	10,865	Anomaly	8.1	81.7	76.2	87.3
address_1AEoiHYZ	10,860	Signature	5.9	81.5	75.8	87.1
WannaCry	10,855	Synthetic Signature	3.7	81.2	75.5	87.0
CryptXXX	10,850	Anomaly	1.5	81.0	75.1	86.8
DMALocker	10,845	Signature	0.3	80.7	74.7	86.7
NoobCrypt	10,840	Synthetic Signature	0.1	80.5	74.4	86.5
address_1KZkcvx4	10,835	Anomaly	0.0	80.2	74.0	86.4
CryptoLocker	10,830	Signature	0.0	80.0	73.6	86.2
Globev3	10,825	Synthetic Signature	0.0	79.7	73.3	86.1

	Time	Protocol	Flag	Family	Clusters	SeedAddress	ExpAddress	BTC	USD	Netflow_Bytes	IPaddress	Threats	Port	Prediction
0	50	TCP	A	WannaCry	1	1DA11mPS	1BonuSr7	1	500	5	A	Botnet	5061	SS
1	40	TCP	A	WannaCry	1	1DA11mPS	1BonuSr7	1	504	8	A	Botnet	5061	SS
2	30	TCP	A	WannaCry	1	1DA11mPS	1BonuSr7	1	508	7	A	Botnet	5061	SS
3	20	TCP	A	WannaCry	1	1DA11mPS	1BonuSr7	1	512	15	A	Botnet	5061	SS
4	57	TCP	A	WannaCry	1	1DA11mPS	1BonuSr7	1	516	9	A	Botnet	5061	SS
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
149038	33	UDP	AP	TowerWeb	3	1AEoiHYZ	1SYSTEMQ	1010	1590	3340	A	Scan	5062	A
149039	33	UDP	AP	TowerWeb	3	1AEoiHYZ	1SYSTEMQ	1014	1596	3351	A	Scan	5062	A
149040	33	UDP	AP	TowerWeb	3	1AEoiHYZ	1SYSTEMQ	1018	1602	3362	A	Scan	5062	A
149041	33	UDP	AP	TowerWeb	3	1AEoiHYZ	1SYSTEMQ	1022	1608	3373	A	Scan	5062	A
149042	33	UDP	AP	TowerWeb	3	1AEoiHYZ	1SYSTEMQ	1026	1614	3384	A	Scan	5062	A

149043 rows × 14 columns

(a) Original dataset: categorical vs. numerical features

	Time	Protocol	Flag	Ransomware	Clusters	SeedAddress	ExpAddress	BTC	USD	Netflow_Bytes	IPaddress	Malware	Port	Prediction
0	40	1	0	16	1	2	2	1	504	8	0	1	5061	2
1	30	1	0	16	1	2	2	1	508	7	0	1	5061	2
2	20	1	0	16	1	2	2	1	512	15	0	1	5061	2
3	57	1	0	16	1	2	2	1	516	9	0	1	5061	2
4	41	1	0	16	1	2	2	1	520	17	0	1	5061	2
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
149037	33	2	2	15	3	1	6	1010	1590	3340	0	6	5062	0
149038	33	2	2	15	3	1	6	1014	1596	3351	0	6	5062	0
149039	33	2	2	15	3	1	6	1018	1602	3362	0	6	5062	0
149040	33	2	2	15	3	1	6	1022	1608	3373	0	6	5062	0
149041	33	2	2	15	3	1	6	1026	1614	3384	0	6	5062	0

149042 rows × 14 columns

(b) Encoded dataset: numerical features

Figure 8. The original and encoded dataset

Lastly, it is worth highlighting that not all malware types are intricately linked to specific ransomware categories. For instance, CryptoLocker is exclusively associated with one type of Blacklist malware. In the experiments, Blacklist attacks have been often predicted to be recognized as a signature attack (S). Another intriguing aspect of the dataset involves examining the average ransom prices associated with each ransomware type. TowerWeb emerges as the ransomware demanding the highest fee in terms of BTC, amounting to 135.26, in stark contrast to CryptoLocker, which commands the lowest fee at 10.51 (figures 15 and 16). This insight sheds light on the considerable variation in ransom demands across different ransomware types. The visual representation of the correlation matrix, depicted in Figure 17, illustrates a noteworthy correlation coefficient of 0.26 between the ransomware cluster and the anticipated BTC transactions. This discovery emphasizes a strong link between particular ransomware attack categories and unique trends within cryptocurrency transactions. For instance, if we consider a scenario in which the Locky ransomware cluster consistently demands BTC payments as ransom. The pronounced correlation observed suggests that analyzing BTC transaction patterns can serve as a practical approach to identifying and forecasting Locky ransomware attacks. Security systems and ML models can harness this correlation to bolster their detection and response mechanisms to ultimately enhance their capacity to thwart ransomware incidents and fortify defenses against cyber threats effectively. Moreover, Figure 18 provides valuable insights into the intricate relationship between ransomware timestamp and the variables USD, BTC, and Netflow Bytes. Essentially, it addresses the question of how the duration of a ransomware attack impacts financial gains and the volume of Netflow Bytes. The visualizations clarify that, generally, a more extended duration corresponds to higher financial gains, but this correlation does not guarantee substantial gains, with the trend typically commencing around a time value of 2.5, except for a few outliers. The same pattern emerges concerning Netflow Bytes, emphasizing not only the connection between timestamp and USD, BTC, and Netflow Bytes but also the pivotal role of increased Netflow Bytes in achieving financial gains. The graphs reveal that the significant gains in currency and Netflow Bytes predominantly occur within the time interval of 2.5 to 4.5. This observation leads us to predict that during a ransomware attack, these time intervals are critical junctures for assessing potential financial gains and gauging the flow of Netflow Bytes (Figure 19). Figure 20 provides a comprehensive analysis of the financial gains in USD associated with ransomware attacks based on the originating port or utilized protocol. It also offers insights into the financial gains influenced by the specific ransomware family

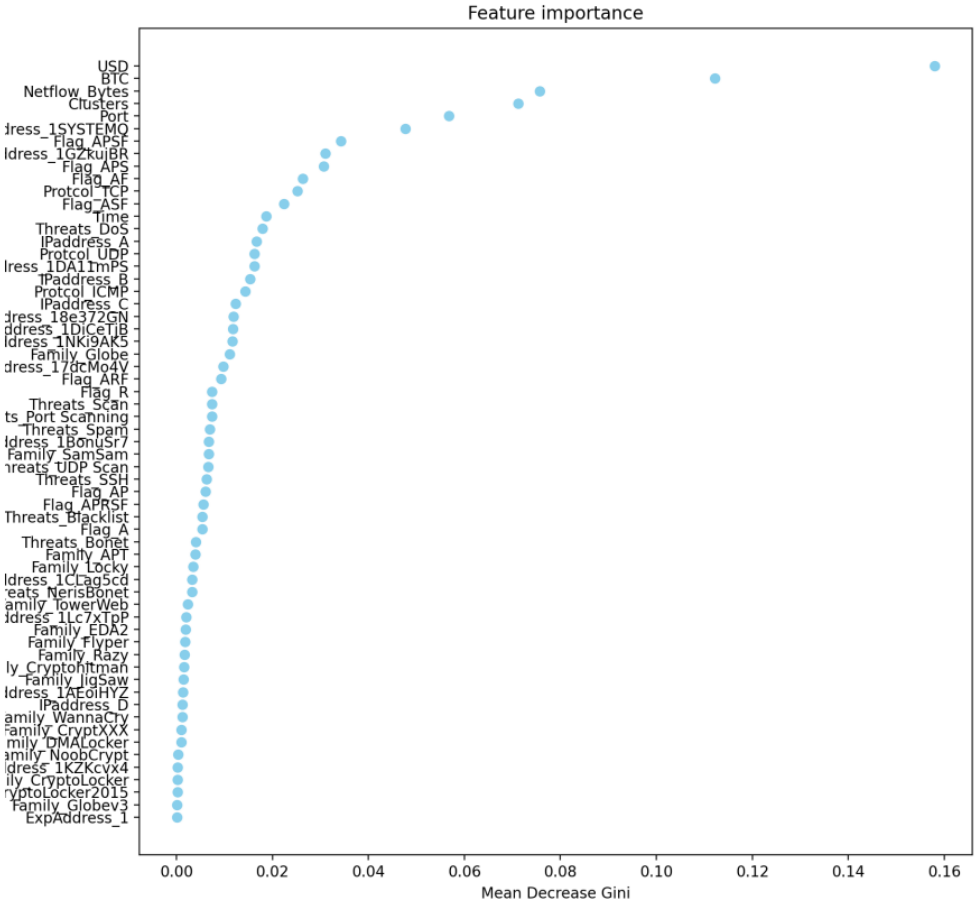


Figure 9. Feature importance

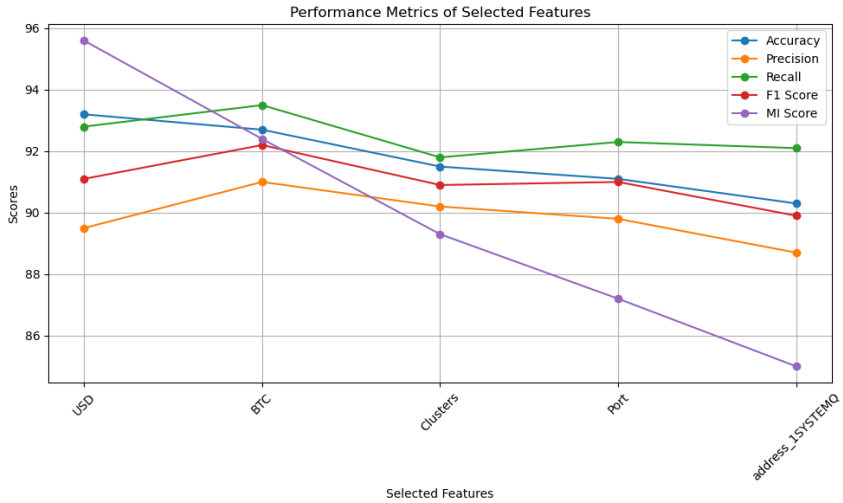


Figure 10. Performance metrics of selected features

or malware threat in conjunction with the port or protocol. These visualizations offer the means to predict the potential success of an attack by considering factors such as the ransomware family or threat type alongside the port or protocol used. For instance, it is notable that port 5066 yields the highest financial gains in USD at an earlier time

point, whereas port 5068 leads to the highest gains at a later time point. Among the pairings of protocol and threat, the TCP protocol paired with the NerisBotnet threat stands out as the most successful, while the combination of Port 5068 and the Spam threat emerges as highly effective. In terms of ransomware and protocol pairings, the TCP protocol combined with the NoobCrypt family is successful, as is the combination of port 5068 with the NoobCrypt family. Consequently, these findings suggest that the most successful attacks tend to originate from port 5068 or employ the TCP protocol, with the NoobCrypt family exhibiting proficiency in both scenarios. Another correlation matrix generated in Figure 21 reveals valuable insights into the relationships between various features in ransomware transaction recognition within digital ecosystems. The moderate positive correlation between network flow and IP address (0.4) suggests a certain level of association between the volume of traffic flow and specific IP addresses involved in ransomware transactions (Figure 21). This indicates that certain IP addresses might be consistently engaged in higher traffic during these transactions. The positive correlations between ExpAddress and network flow (0.34), ExpAddress and USD (0.38), as well as SeddAddress and network flow (0.31) indicate potential connections between specific transaction links (ExpAddress and SeddAddress) and the volume of network flow or the financial impact (USD) of ransomware activities (Figure 21). This implies that certain transaction links might coincide with higher network activity or financial consequences. Additionally, the moderate positive correlation between the network flag and network flow (0.34) suggests that specific flags within the network might be associated with increased traffic flow during ransomware transactions. Understanding these correlations aids in identifying potential patterns or relationships among features, thereby contributing to the development of more effective models for recognizing ransomware transactions in digital ecosystems. For instance, the interplay between network flow and transaction links (ExpAddress and SeddAddress) could imply specific transaction behaviors or traffic patterns associated with ransomware activities.

6. Discussion

The financial aspects of ransomware attacks revealed a lack of a clear-cut relationship between ransomware types and the associated ransom amounts. This observation underscores the variability in the ransom demands across different ransomware families and suggests that there is no fixed or predetermined amount for a particular type of cyber attack [66]. The ransomware landscape remains dynamic and adaptable, with threat actors continuously adjusting their ransom demands. Furthermore, upon scrutinizing the correlation matrix of the extracted features, a significant correlation of 0.26 emerged between the ransomware clusters and the anticipated BTC transactions. This correlation signifies a robust association between specific ransomware attack types and distinctive patterns in cryptocurrency transactions. For instance, the high correlation suggests that monitoring BTC transaction patterns can serve as a practical means of identifying and predicting ransomware attacks, such as the Locky ransomware. Leveraging this correlation can enhance the effectiveness of security systems and ML models. This will lead to improved detection and response mechanisms against ransomware threats. The examination of temporal aspects, particularly the relationship between attack duration and gains in currency (USD and BTC), shed light on critical time intervals during ransomware attacks. The analysis indicated that the most significant gains in currency typically occurred between specific time points. This highlights the importance of monitoring and responding to threats during these critical phases. The comprehensive analysis of ransomware-related data provides valuable insights into the dynamic and evolving nature of cyber threats. It emphasizes the need for adaptable cybersecurity strategies and proactive measures that leverage data-driven approaches to mitigate the risks posed by ransomware attacks. Figure 22 offers crucial insights into the financial impact of various ransomware attacks within the cryptocurrency ecosystem. Each ransomware variant, represented along the x-axis, showcases distinct financial implications in terms of both BTC and USD transactions. TowerWeb emerges as the ransomware demanding the highest fee in BTC, reaching 2.56, while displaying a substantial financial impact of 172.36 USD. Locky, although having a relatively lower average BTC transaction count of 2.01, inflicts an average financial damage of 88.37 USD. In contrast, Globe, despite having fewer BTC transactions between 1.46 to 2.56, showcases the lowest financial impact, ranging from 4.38 to 172.36 USD. This disparity in financial impact emphasizes the varied ransomware demands and the potential financial risks associated with each attack type. Understanding these fluctuations is crucial for effective ransomware classification in the crypto ecosystem to enable better predictive models and proactive measures. Figure 23 illustrates the relationship between Gini Impurity and MI scores for various ransomware classes categorized into Signature (S), Synthetic Signature (SS), and Anomaly (A). Each ransomware class exhibits distinct patterns, with TowerWeb displaying higher MI scores. This result indicates more predictable web-based transaction behaviors. Conversely, NoobCrypt demonstrates greater variability in both criteria. These dynamics underscore the need for adaptive detection methods to account for evolving web and cryptographic ransomware behaviors. Insights gleaned from this graph suggest that feature selection based on Gini Impurity and MI can effectively discriminate between ransomware classes, which has significant implications for improving ransomware detection and classification systems. Understanding these dynamics can contribute to the development of more accurate and adaptive ML models to enhance cybersecurity efforts against web-based cryptographic threats. Figure 24 illustrates the performance metrics associated with different target variables (A, SS, and S) used in the evaluation of the proposed RFSA. The performance metrics include the MI score, accuracy, recall, and precision. These metrics are vital in assessing the algorithm's effectiveness in correctly identifying and classifying ransomware instances within the cryptocurrency

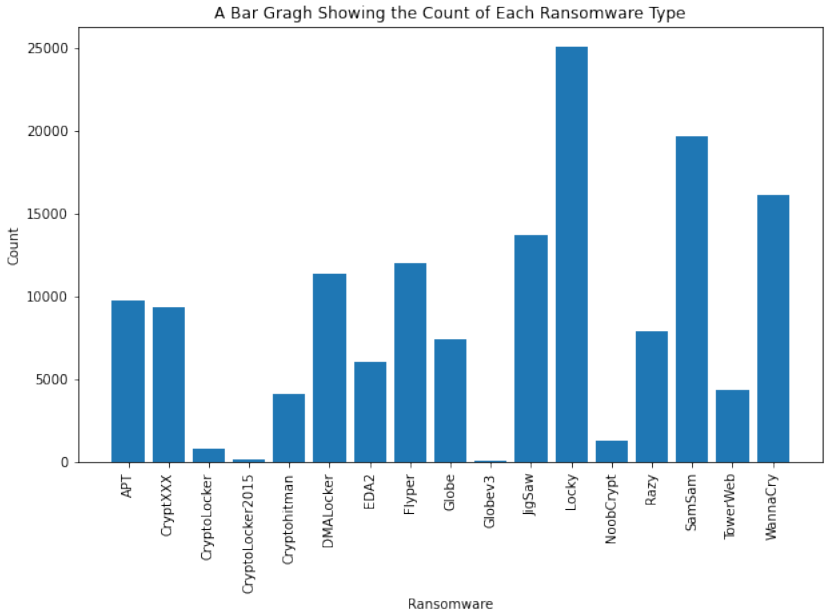


Figure 11. Extracted ransomware families

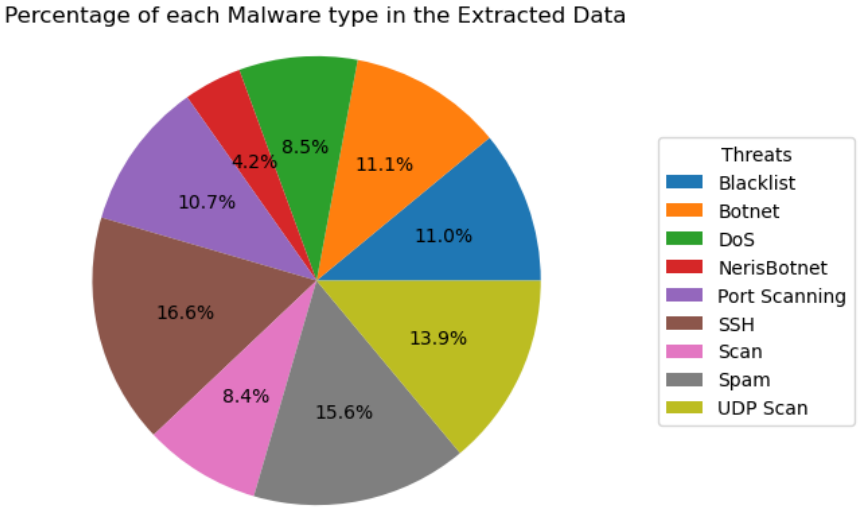


Figure 12. Extracted malware

ecosystem. Figure 24 indicates that the anomalous (A) category consistently outperforms the SS and S categories across all metrics. For the MI, the A category achieves the highest score of 95%, followed by SS at 90% and S at 85%. Similarly, in terms of accuracy, the A category leads with 93%, followed by SS at 88% and S at 82%. Moreover, the A category maintains higher recall (92%) and precision (89%) compared to SS (recall: 85%, precision: 80%) and S (recall: 78%, precision: 75%). These findings suggest that targeting the A category yields the most robust and accurate results in identifying zero-day ransomware instances in the cryptocurrency domain.

It demonstrates the algorithm's enhanced capability in effectively selecting features specific to the zero-day (A) category, resulting in superior performance across the evaluated metrics. The SS and S categories, although performing less effectively than the A, still show reasonably good performance, implying that the algorithm remains fairly capable across different target variables, albeit with varying degrees of success (Table V). The findings of this study present significant implications for understanding and combating ransomware attacks within the cryptocurrency ecosystem. The key observations highlight the dynamic and adaptable nature of ransomware which emphasizes the

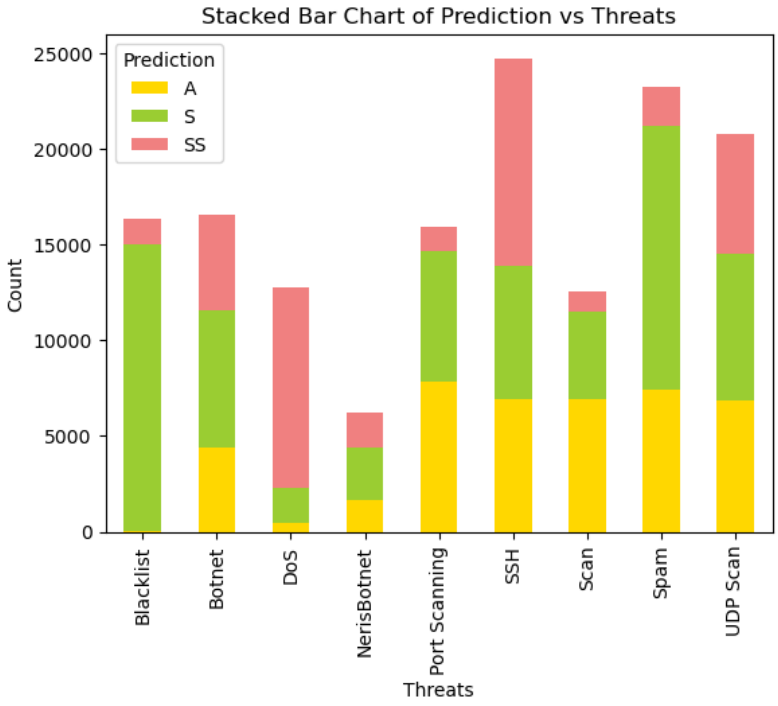


Figure 13. Threat prediction

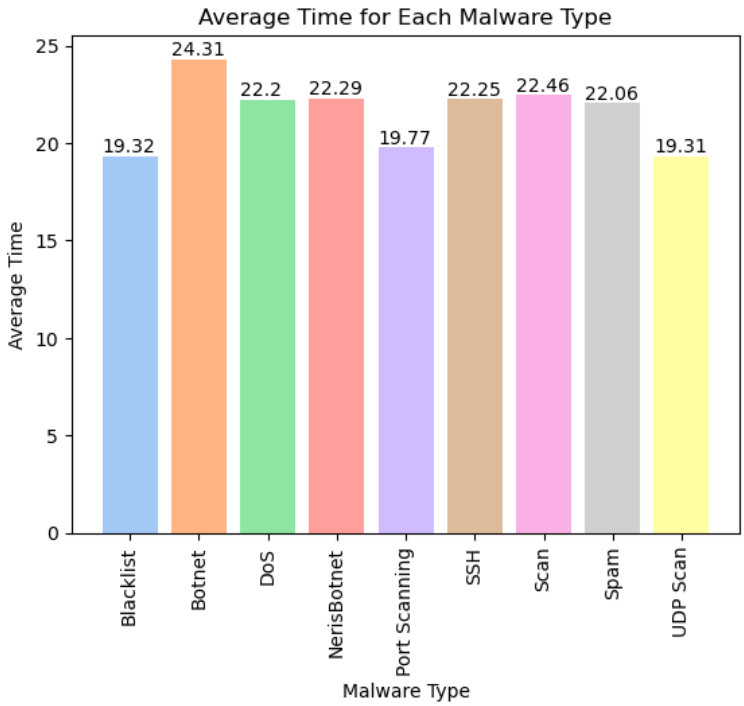


Figure 14. Average timestamp of each ransomware

lack of a fixed relationship between ransomware types and associated ransom amounts. This variability underscores the challenge of predicting or determining a specific ransom amount based solely on the type of cyberattack. The study also reveals a noteworthy correlation (0.26) between ransomware clusters and BTC transactions.

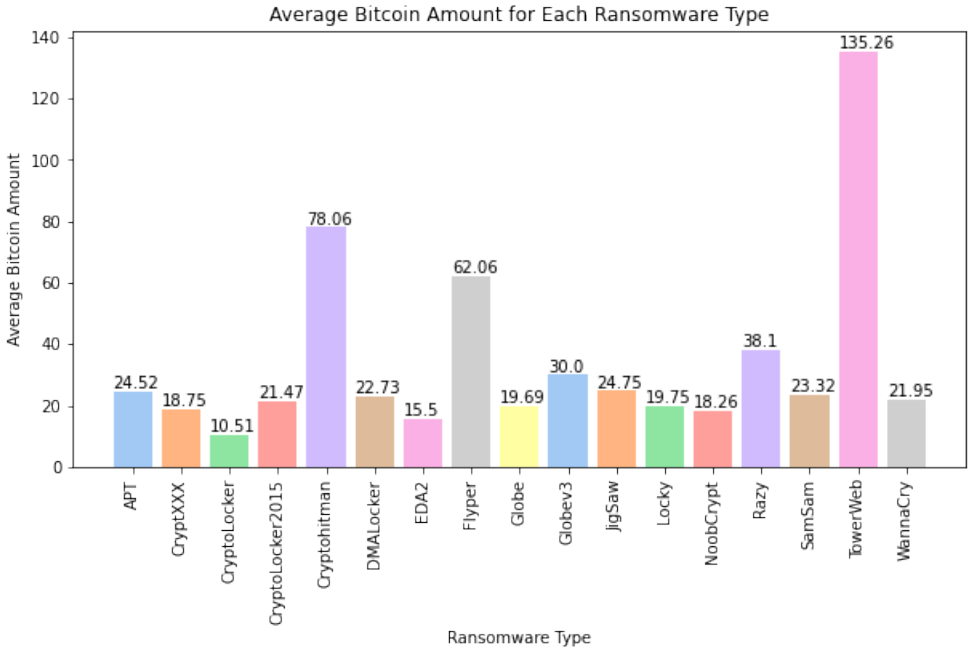


Figure 15. Financial impact of malware

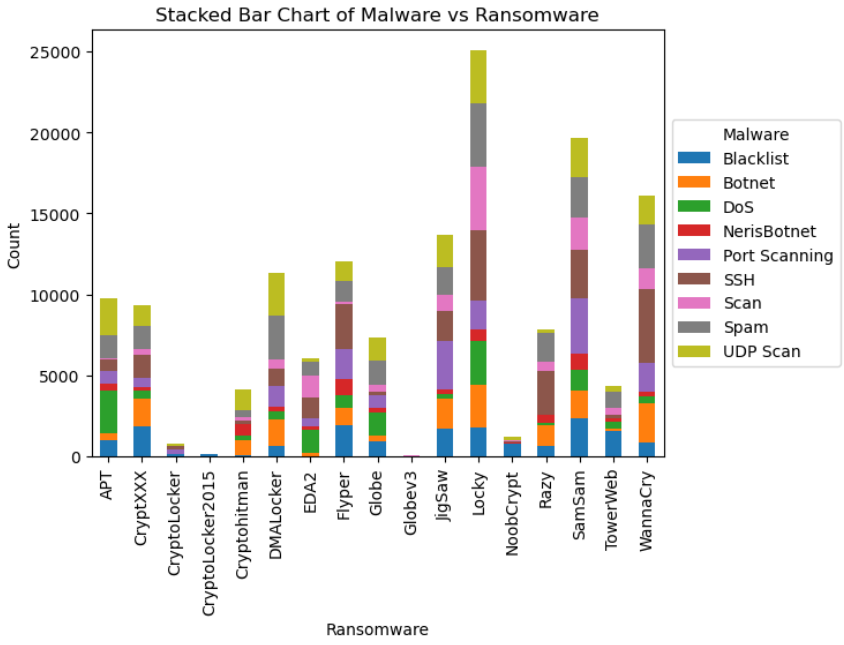


Figure 16. Selected malware and ransomware

This correlation suggests a robust association between specific ransomware attack types and distinctive patterns in cryptocurrency transactions. Monitoring BTC transaction patterns emerges as a practical means of identifying and predicting ransomware attacks. The analysis of temporal aspects, particularly the relationship between attack duration and gains in currency (USD and BTC), provides insights into critical time intervals during ransomware attacks. Identifying specific time points associated with significant gains in currency highlights the importance of monitoring and responding to threats during these phases to enhance the effectiveness of cybersecurity defenses. The comprehensive analysis of ransomware-related data underscores the need for adaptable cybersecurity strategies and proactive mea-

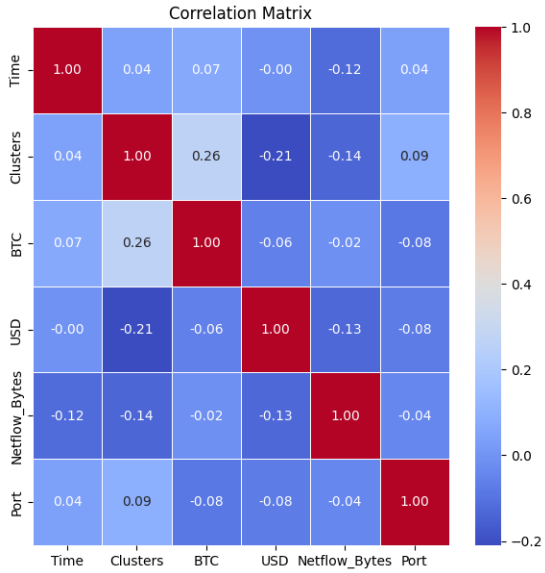


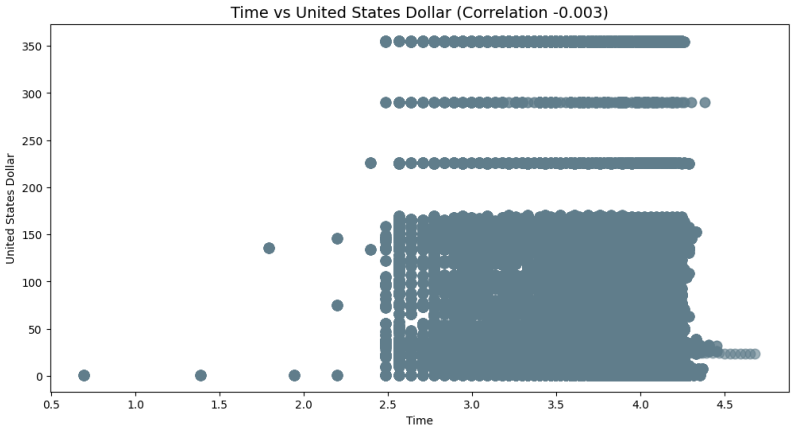
Figure 17. Correlation matrix of extracted features

sures based on data-driven approaches. The study emphasizes the importance of understanding the evolving nature of cyber threats and tailoring defense mechanisms accordingly.

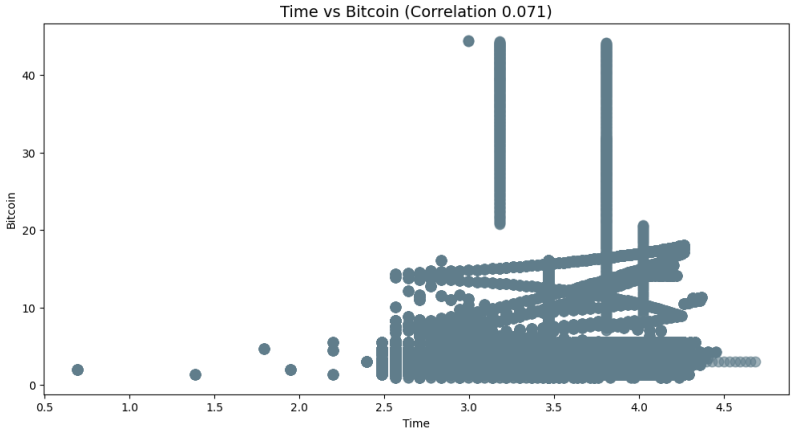
A. Limitations and Future Research Directions

Despite the valuable insights gained from this study, some limitations should be considered. The lack of a comprehensive dataset covering all ransomware attacks and variations may limit the generalizability of findings. Additionally, the study focuses on cryptocurrency transactions, and other aspects of ransomware attacks, such as social engineering tactics, are not fully explored. Future research directions could involve expanding the dataset to include a broader range of ransomware attacks and incorporating additional features for a more comprehensive analysis. Exploring the socio-technical aspects of ransomware attacks, such as user behaviors and organizational responses, could provide a more holistic understanding. Moreover, research efforts could focus on developing adaptive models that can dynamically adjust to emerging ransomware behaviors and enhance predictive capabilities. In conclusion, this study opens avenues for further research to address existing limitations and adapt to the ever-changing cybersecurity landscape. Future research in the field of ransomware attacks and cybersecurity can explore several promising directions to address existing gaps and contribute to the evolving landscape. We provide the following potential avenues for future research:

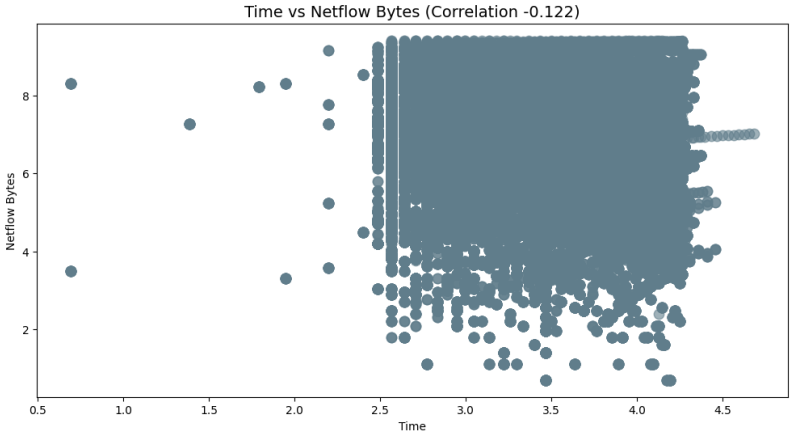
- Behavioral Analysis and Social Engineering. To investigate the role of social engineering tactics in ransomware attacks and understand how threat actors exploit human behavior [67].
- Dynamic Threat Intelligence. To develop dynamic threat intelligence models that continuously update based on emerging ransomware behaviors. This can involve real-time monitoring and analysis to stay ahead of evolving threats [9].
- Multi-Modal Data Fusion. To combine diverse data sources beyond cryptocurrency transactions, such as network traffic, user behavior, and system logs, to create a more comprehensive understanding of ransomware attacks [31]. Investigate the synergy of various data modalities to improve the accuracy and robustness of ransomware detection and classification models.
- XAI for Ransomware Detection. Develop XAI models to enhance the interpretability of ransomware detection systems. Understanding how models make decisions is crucial for building trust in cybersecurity applications. Explore methods to balance model interpretability with the complexity required for accurate detection in dynamic environments.
- Adversarial ML. Investigate adversarial ML techniques to assess the vulnerability of ransomware detection models [68]. This can lead to the development of more robust and resilient cybersecurity systems.
- Human-Centric Security Measures. Study the human factors in cybersecurity incidents, considering the psychological and cognitive aspects of both attackers and defenders [69]. Develop interventions and training programs that empower users and organizational stakeholders to recognize and respond effectively to ransomware threats.
- Legal and Policy Implications. Examine the legal



(a) Timestamp and USD correlation



(b) Timestamp and BTC correlation



(c) Timestamp and Network Flow correlation

Figure 18. Numerical feature correlation

and policy frameworks surrounding ransomware attacks, including international cooperation, jurisdictional challenges [70], and legal consequences for cybercriminals [67]. Propose and evaluate policy recommendations to enhance international collaboration in combating ransomware.

- Blockchain and Decentralized Security. Explore the potential of blockchain technology and decentralized security measures in preventing, detecting, and responding to ransomware attacks.

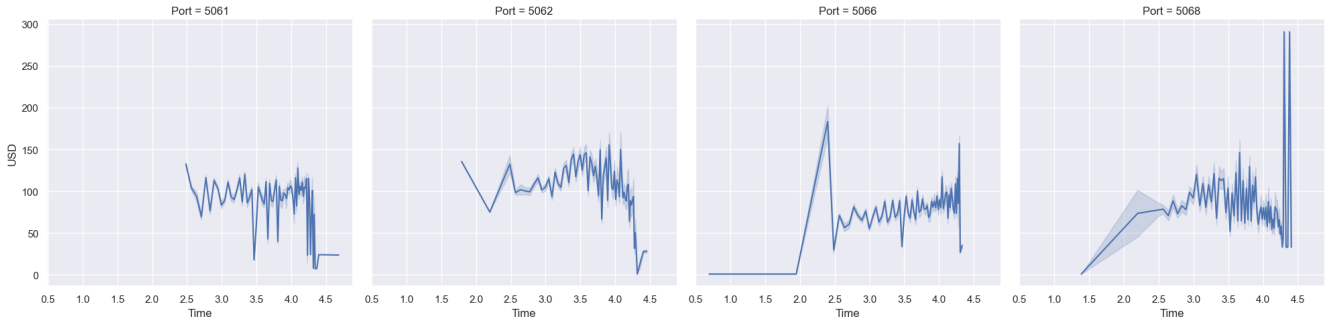
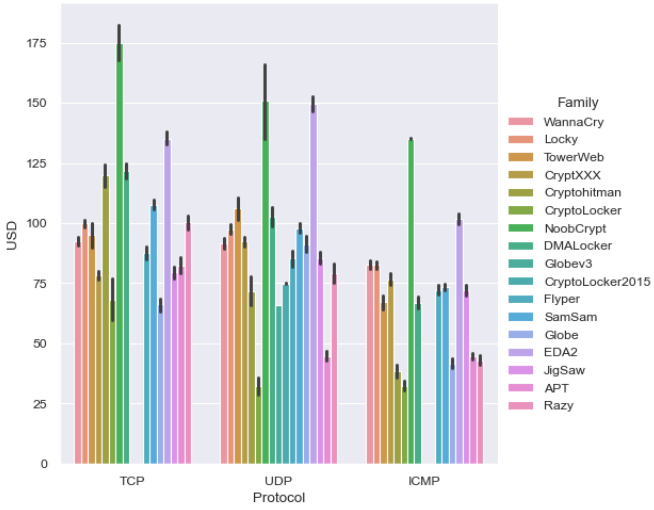
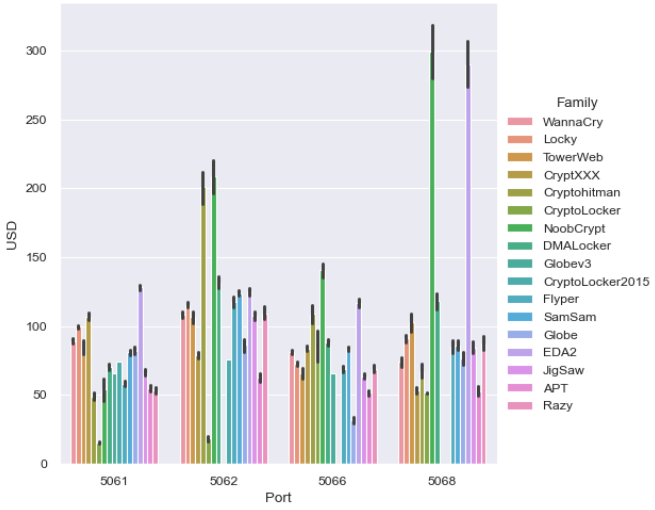


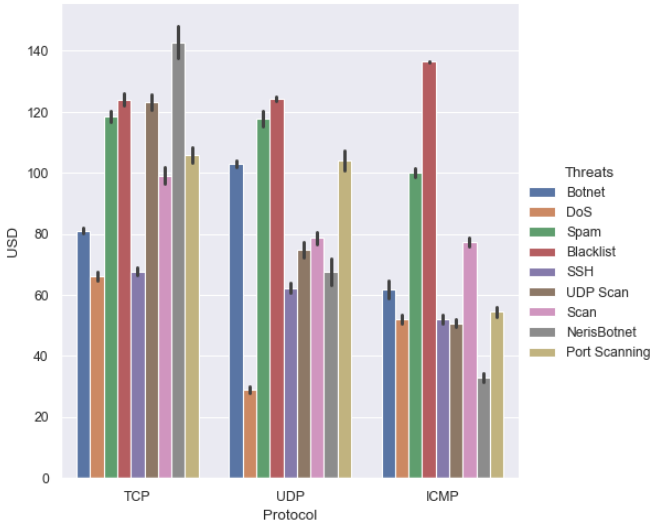
Figure 19. Attack timestamp prediction



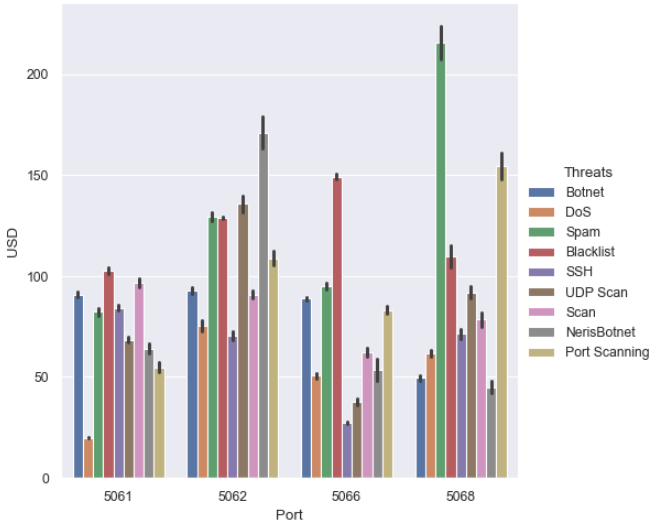
(a) USD and ransomware protocol



(b) USD and ransomware ports



(c) USD and malware protocols



(d) USD and malware ports

Figure 20. Malware extracted

Investigate the use of decentralized ledgers for secure and tamper-proof storage of critical data to mitigate the impact of ransomware. These future research directions aim to advance the understanding of ran-

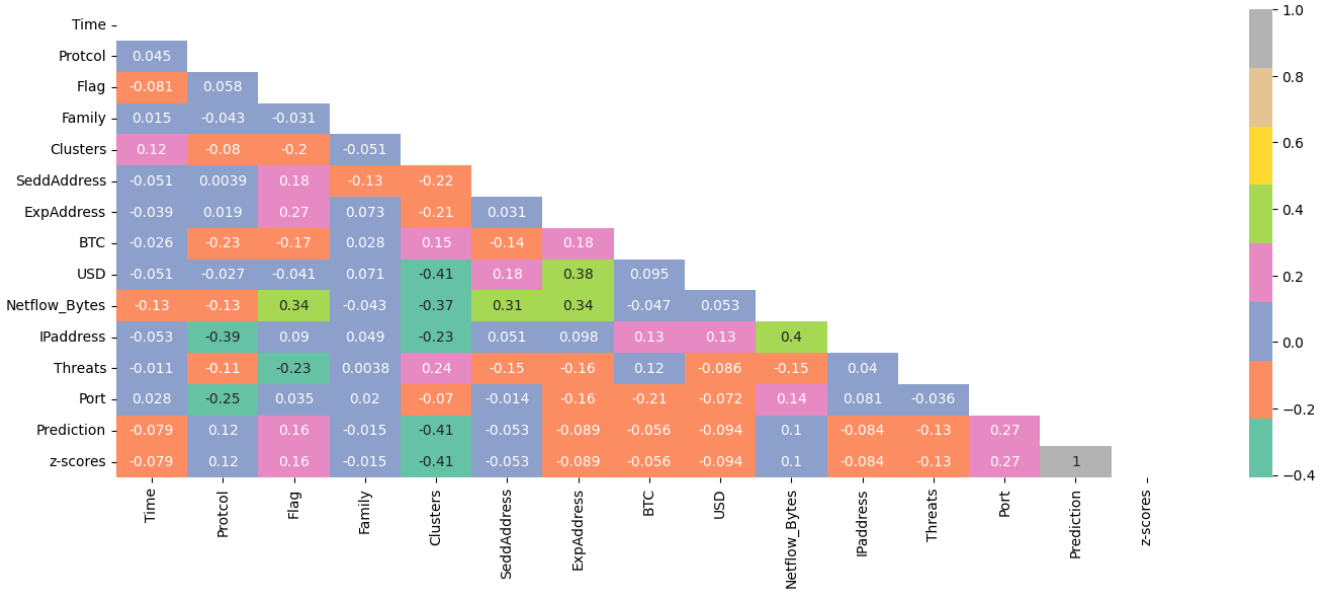


Figure 21. Additional feature correlation

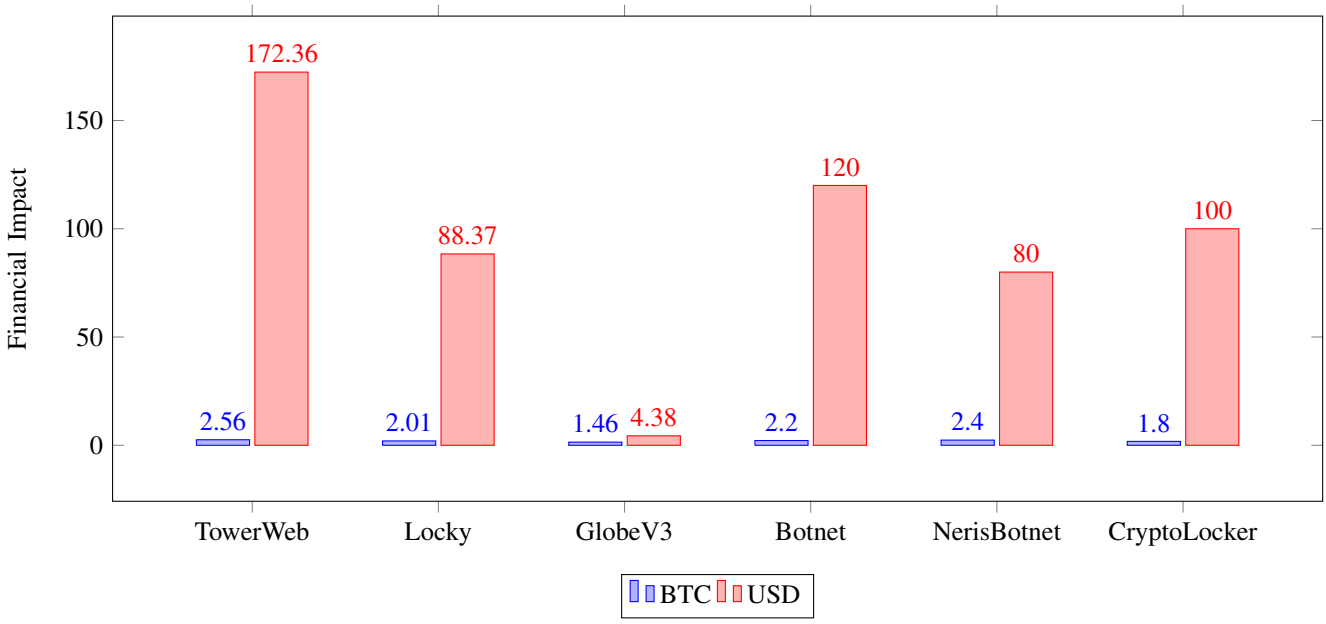


Figure 22. Financial impact of ransomware attacks

somware attacks and contribute to the development of resilient cybersecurity strategies. The RFSA can find applications in blockchain and decentralized security research by aiding in the identification and characterization of ransomware activities within these domains. Specifically, the RFSA can be utilized to analyze and extract relevant features from datasets related to blockchain transactions and decentralized systems. By identifying distinctive characteristics of ransomware within the context of blockchain and decentralized security, the RFSA contributes to enhancing threat detection, classification, and overall security measures in these environments. This algorithm can provide valuable insights into the dynamics of ransomware attacks in decentralized networks, facilitating the development of more effective security strategies and preventive measures within the blockchain and decentralized technology landscape.

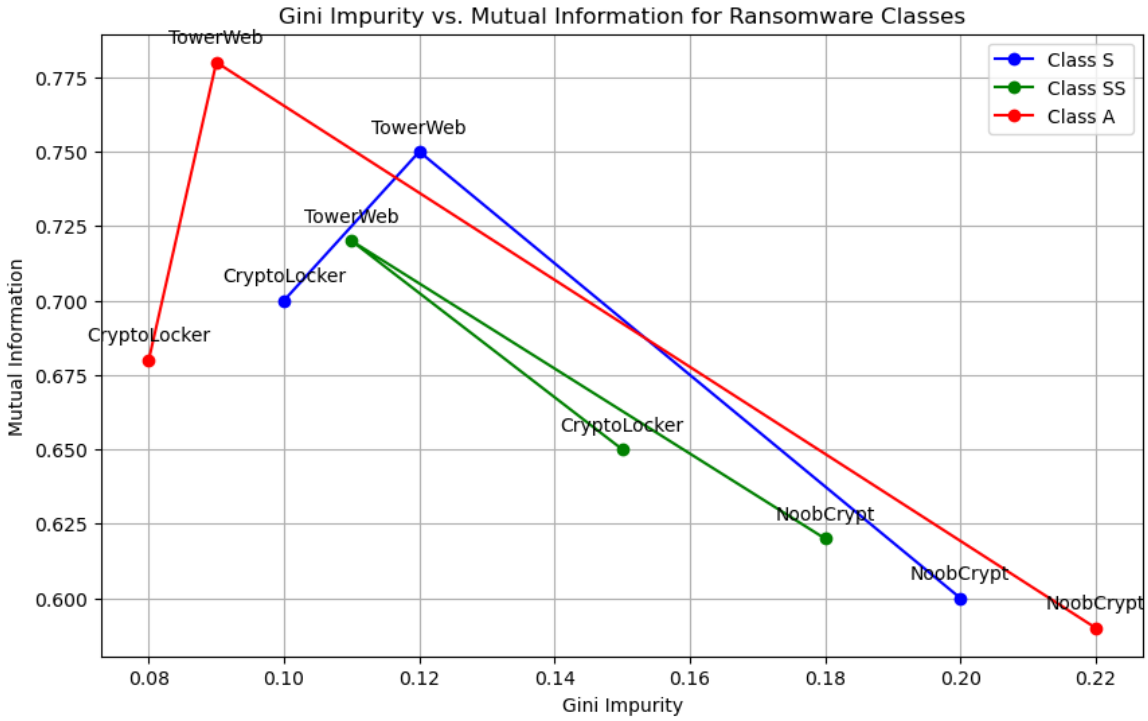


Figure 23. Gini Impurity and MI scores

B. *Deeper Insights Into the Implications and Significance of the Findings*

The comprehensive analysis conducted on ransomware transactions within cryptocurrency ecosystems has unveiled the following crucial insights that fundamentally altered our understanding of these cyber threats:

1) **Monitoring BTC transaction patterns can serve as a practical means of identifying and predicting ransomware attacks**. This proactive strategy holds profound significance and implications in the classification and detection of ransomware transactions. BTC transactions, given their decentralized and pseudonymous nature, offer a unique digital footprint that encapsulates the essence of ransomware activities within the crypto ecosystem [63]. The significance lies in the fact that ransomware attackers typically demand payments in cryptocurrencies like BTC due to their anonymity, which makes BTC transactions an invaluable source of insight into potential ransomware-related activities [63]. By meticulously monitoring BTC transaction patterns, cybersecurity experts and systems can discern anomalous behavior that aligns with characteristics often associated with ransomware incidents. This surveillance involves analyzing transactional metadata, behavioral patterns, and financial aspects inherent in BTC transactions. Anomalous patterns might include sudden spikes in transactions involving small amounts or repetitive transactions within specific time frames. These patterns might correlate with the dynamics observed during ransomware attacks, such as a surge in transactions related to extortion demands or payments to ransomware operators. Moreover, BTC transaction monitoring can aid in the early detection of potential ransomware activities by leveraging ML algorithms and anomaly detection techniques. These methods scrutinize historical transaction data to identify deviations from regular transactional behavior to enable the proactive flagging of suspicious activities indicative of ransomware activities [14], [63]. The practicality of monitoring BTC transactions lies in its real-time nature and provides an opportunity for swift action and mitigation measures in response to identified anomalies [60]. This real-time monitoring capability is pivotal in the constantly evolving landscape of ransomware threats and allows rapid responses and containment strategies to prevent or mitigate potential damages associated with ransomware.
2) **There is no fixed or predetermined amount for a particular type of ransomware**. The absence of a fixed or predetermined amount for a particular type of ransomware holds pivotal implications within the domain of ransomware analysis and response strategies within the crypto ecosystem. Ransomware, as a cyber threat, often operates with a degree of adaptability and variability in its demands [71].

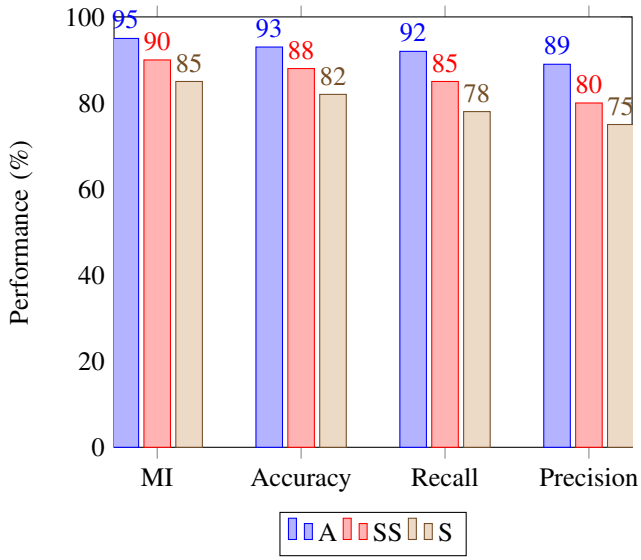


Figure 24. Performance metrics for different target variables

TABLE V. Feature Selection and Evaluation Metrics

Features	Total	Target	MI (%)	Accuracy (%)	Precision (%)	Recall (%)
Globe	11,425	Synthetic Signature	61.8	88.5	85.8	91.1
address_17dcMo4V	11,420	Anomaly	59.6	88.3	85.5	91.0
Scan	11,410	Synthetic Signature	55.2	87.8	84.8	90.7
Spam	11,405	Anomaly	53.0	87.5	84.4	90.6
address_1BonusSr7	11,400	Signature	50.8	87.3	84.0	90.4
SamSam	11,395	Synthetic Signature	48.6	87.0	83.7	90.3
SSH	11,390	Anomaly	46.4	86.8	83.3	90.1
Blacklist	11,375	Anomaly	40.8	86.0	82.2	89.7
Botnet	11,370	Signature	38.6	85.8	81.8	89.5
Botnet	11,365	Synthetic Signature	36.4	85.5	81.5	89.4
APT	11,360	Anomaly	34.2	85.3	81.1	89.2
Locky	11,355	Signature	32.0	85.0	80.7	89.1
NerisBotnet	11,350	Synthetic Signature	29.8	84.8	80.4	88.9
TowerWeb	11,345	Anomaly	27.6	84.5	80.0	88.8
address_1LC7xTpP	11,340	Signature	25.4	84.3	79.6	88.6
EDA2	11,335	Synthetic Signature	23.2	84.0	79.3	88.5
Flyper	11,330	Anomaly	21.0	83.8	78.9	88.3
Razy	11,325	Signature	18.8	83.5	78.5	88.2
Cryptohitman	11,320	Synthetic Signature	16.6	83.3	78.2	88.0
JigSaw	11,315	Anomaly	14.4	83.0	77.8	87.9

Unlike traditional fixed-value demands, ransomware attackers exhibit flexibility in their extortion demands based on various factors. This variability in the demanded ransom amount, whether in BTC or other cryptocurrencies, complicates the response strategies and risk assessments for cybersecurity professionals. This aspect challenges the notion of a standardized response protocol. It suggests that ransomware attackers might tailor their demands to the perceived vulnerability or value of the target, making it harder to predict the potential financial impact of the attack. Consequently, this unpredictability necessitates a more dynamic and adaptive approach to ransomware defense and response. For cybersecurity practitioners and organizations, this implies a need for comprehensive risk assessments and scenario planning rather than relying on fixed protocols [71], [72]. Understanding that ransomware attackers might adjust their demands according to the perceived value or potential damages underscores the need for robust backup and recovery mechanisms, cybersecurity hygiene practices, and proactive security measures. Moreover, the absence of a fixed amount underscores the importance of strategic decision-making during and after a ransomware incident [71]. Organizations need to evaluate the potential costs and benefits of different response strategies, considering factors beyond just the demanded ransom amount. Factors such as reputation damage, operational downtime, legal implications, and the effectiveness of available recovery options become critical in decision-making. It also emphasizes the significance of investing in proactive cybersecurity measures to mitigate the risk of ransomware attacks. Rather than merely preparing for a fixed ransom amount, organizations should focus on preventing potential attacks to reduce their dependency on extortion demands.

3) **A more extended ransomware duration corresponds to higher financial gains**. The correlation between extended ransomware duration and increased financial gains presents a critical insight into the economics and dynamics of ransomware attacks. This correlation indicates that the longer ransomware remains active within an infected system, the higher the potential financial impact on the victim. Extending the duration of a ransomware attack provides the threat actor with more time to extract the ransom. As the victim's urgency to regain control or access to their systems increases over time, the likelihood of them meeting the attacker's demands also rises, resulting in potentially higher payouts. From a cybersecurity standpoint, this correlation underscores the urgency of rapid detection, containment, and mitigation of ransomware attacks [72]. The objective becomes not only restoring systems but also minimizing the time during which the ransomware remains active. Timely response and effective containment measures can reduce the window of opportunity for the attacker to escalate their demands and limit the financial losses incurred by the victim. Furthermore, this insight emphasizes the critical role of robust backup and recovery strategies in mitigating the impact of ransomware attacks [72], [73]. Rapid restoration of systems and data from backups can significantly reduce the leverage of attackers who seek to prolong the attack to extort higher payments. Organizations equipped with resilient backup systems and recovery protocols can potentially negate the financial incentives for attackers to prolong the attack duration. Additionally, this correlation highlights the economic motivations behind ransomware attacks [72]. Attackers aim to maximize their financial gains by prolonging the disruption, leading to increased pressure on victims to comply with their demands. Understanding this correlation prompts organizations to adopt proactive security measures, including regular backups, network segmentation, and employee training, to reduce the susceptibility and impact of such attacks.

4) **TowerWeb emerges as the ransomware demanding the highest fee in terms of BTC in stark contrast to CryptoLocker**. The distinction between TowerWeb and CryptoLocker ransomware, particularly in their fee demands within the BTC framework, offers crucial insights into the varying economic strategies employed by ransomware actors. TowerWeb's emergence as a ransomware strain demanding the highest BTC fee signifies a deliberate and aggressive financial approach by threat actors [9], [73]. The substantial fee demanded might indicate a higher perceived value of the encrypted data or a strategic decision to target larger and potentially more lucrative organizations or entities. Conversely, the significantly lower fee demanded by CryptoLocker highlights a different approach. This ransomware strain might prioritize a higher volume of attacks over individual high-value payouts. The lower ransom demand could suggest a strategy focused on targeting a broader range of victims, possibly including smaller businesses or individual users who may be more likely to pay lower ransoms. From a cybersecurity perspective, understanding these fee discrepancies provides valuable insights for both threat mitigation and incident response [9]. It allows security professionals to anticipate potential ransomware variants based on their economic models. For instance, organizations that might be lucrative targets for high-value ransom demands could implement more stringent security measures and robust backup systems to mitigate such attacks. On the other hand, those attracting ransomware with lower demands could focus on preventive measures and education to minimize the likelihood of successful attacks.

This information also underscores the importance of threat intelligence within the cybersecurity community [9]. By disseminating knowledge about ransomware variants and their typical behavior, including their fee structures, organizations can better prepare and fortify their defenses against potential attacks. Furthermore, this insight highlights the evolving tactics of ransomware actors. The varying fee structures of TowerWeb and CryptoLocker underscore the diversity in strategies employed by threat actors to optimize their financial gains.

5) **CryptoLocker is exclusively associated with the Blacklist malware**. The exclusive association between CryptoLocker and the Blacklist malware introduces an intriguing dimension to the relationship between ransomware strains and their associated malware. This specific correlation suggests a symbiotic relationship where the operation or execution of CryptoLocker is intricately linked with the functionalities or behaviors of the Blacklist malware. Such a strong association implies that the successful deployment or functioning of CryptoLocker might heavily rely on the presence, support, or capabilities offered by the Blacklist malware. From a cybersecurity standpoint, this association emphasizes the collaborative or interdependent nature of various malware families in ransomware campaigns [73], [74]. Understanding these connections between ransomware strains and their associated malware allows cybersecurity professionals to decipher the intricate workings of these threats. It can lead to more targeted and effective mitigation strategies by focusing on disrupting or neutralizing the supporting malware components to hinder the successful execution of ransomware like CryptoLocker [73]. Additionally, this insight underscores the need for comprehensive threat analysis and incident response planning. Organizations and security researchers need to delve deeper into understanding the specific relationships between ransomware strains and associated malware to craft robust defense strategies. This understanding can aid in the identification of potential attack vectors, the development of more accurate threat models, and the creation of tailored defense mechanisms to counteract such ransomware-malware collaborations [73]. Furthermore, the exclusive association between CryptoLocker and the Blacklist malware suggests a level of specialization or customization in ransomware operations, where specific strains are tailored to function optimally in tandem with particular malware variants. This complexity in the modus operandi of ransomware underscores the continual need for advancements in cybersecurity measures and threat intelligence to combat these intricately woven threats effectively.

6) **Categories like Blacklist, Port Scanning, and Spam are predominantly associated with well-known threats, with relatively few anomalies**. Anomalies suggest the occurrence of zero-day threats in the classification scheme of the RFSA. The predominance of categories such as Blacklist, Port Scanning, and Spam being predominantly linked with well-known threats hints at the presence of more established patterns within the classification [75] (Figure 25). The prevalence of these categories in association with known threats implies certain predictability and familiarity in their occurrence [9]. However, the observation of relatively few anomalies and SS within these categories signifies a potential emergence of zero-day threats [9], [75]. This discrepancy between the abundance of established threats and the scarcity of anomalies implies the possibility of previously unseen or novel threats, often termed zero-day. These emerging anomalies might represent new attack methodologies or variations that deviate from the known patterns, potentially indicating the evolution of sophisticated threats that traditional security measures may not readily detect or mitigate [38]. Therefore, the necessity of proactive threat monitoring and adaptive ML defense mechanisms to identify and counteract evolving zero-day ransomware is recommended (Figure 25).

7) **Approximately 68% of ransomware attacks occur within the time range of 16.58 to 48.35 seconds**. This specific time frame might denote periods of heightened vulnerability or increased susceptibility to ransomware intrusions. Understanding this temporal concentration is crucial as it could signify patterns related to network activity, user behavior, or systemic vulnerabilities. Identifying and dissecting this temporal pattern might offer insights into the timing preferences of cybercriminals, enabling the implementation of more targeted and effective defensive strategies. Moreover, this concentration might also hint at specific windows of opportunity for potential attackers, emphasizing the necessity for continuous monitoring and bolstering security measures during these critical time intervals to mitigate the risk of ransomware infiltration.

8) **The average timestamp of ransomware attacks is 32.47 seconds**. The revelation that the average timestamp of ransomware attacks is 32.47 seconds is intriguing within the context of cyberattacks. This timestamp signifies the speed and immediacy with which ransomware can infiltrate systems once they become vulnerable or exposed. Such rapid intrusion could be indicative of automated or scripted attacks seeking vulnerabilities within networks or systems [76]. Understanding this swift initiation is vital for cybersecurity professionals to fortify defenses and create proactive measures that can effectively thwart or delay ransomware attacks. It underscores the importance of real-time monitoring and immediate response mechanisms within cybersecurity protocols. This finding urges the development of rapid response strategies and automated threat detection systems

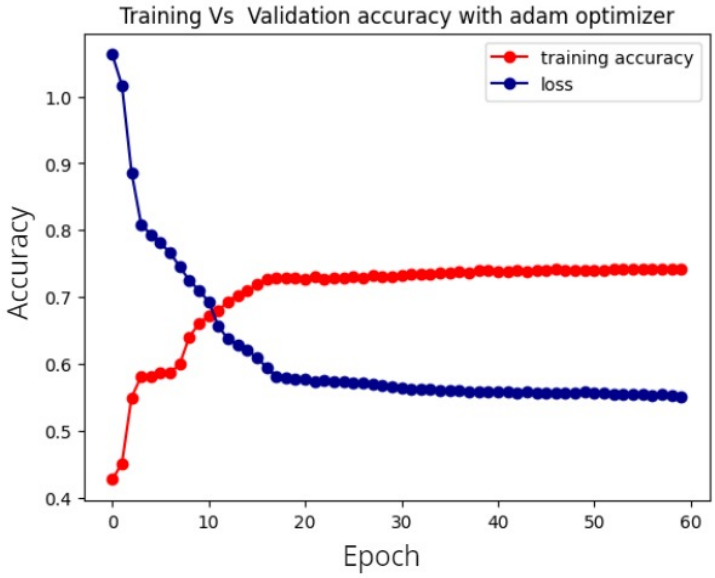


Figure 25. UGRansome classification using ML

capable of identifying and neutralizing ransomware almost instantaneously upon detection.

9) **USD provides the most information gain, followed by BTC, clusters, port, and ransomware addresses**. The indication that USD provides the highest information gain among the studied features, followed by BTC, clusters, ports, and specific ransomware addresses, underscores the significance of financial data in identifying and characterizing ransomware within the cryptocurrency landscape. USD transactions contain more discernible patterns or distinctive markers associated with ransomware activities which significantly contribute to the accuracy and information gained from the detection model. Meanwhile, BTC, clusters, ports, and ransomware addresses, although valuable, might contain less explicit or slightly more nuanced indicators of ransomware behavior. This hierarchy of information gain highlights the prominence of financial transactional data, especially in USD, suggesting its pivotal role in enhancing the effectiveness of ransomware detection and classification systems in the cryptocurrency domain.

10) **The prevalence of the Locky ransomware class exceeds that of the Globe malware, indicating data imbalance**. The observed prevalence of the Locky ransomware class over the Globe malware emphasizes the existence of data imbalance within the UGRansome dataset [7], [38]. This imbalance raises concerns about the potential biases in the model's learning process, where the abundance of Locky instances might lead to an over-representation in the training set. Consequently, this could affect the model's ability to accurately detect and classify less represented ransomware types (Figure 25). Addressing this data imbalance is critical as it ensures a more comprehensive and balanced ML process (Figure 25). The model may become biased towards the dominant class, resulting in sub-optimal performance when dealing with under-represented classes. By addressing the bias introduced by imbalanced data, the model gains increased robustness, enabling it to accurately identify different ransomware types. This improvement enhances the model's overall effectiveness in detecting and classifying threats, a crucial factor in upholding a secure and resilient cybersecurity environment. It also ensures compliance with regulatory requirements and fosters trust and confidence among stakeholders. Mitigating imbalanced data bias is essential for optimizing the model's performance, aligning with industry standards, and reinforcing the cybersecurity posture of the system.

7. Conclusion

This study provides a multifaceted analysis of ransomware-related data and offers insights that underscore the complexity and evolving nature of cybersecurity threats. Our exploration of financial aspects revealed the absence of a fixed ransom amount associated with specific ransomware types. Moreover, the correlation analysis unveiled a strong link between ransomware clusters and cryptocurrency transaction patterns to potentially enhance predictive or preventive cybersecurity models. The temporal analysis emphasized critical time intervals during ransomware attacks to guide the development of timely response strategies.

These findings highlight the necessity of data-driven and adaptive cybersecurity approaches to effectively address the ever-changing landscape of ransomware threats to safeguard organizations and individuals against potential cyberattacks. Nevertheless, the research relies on the UGRansome dataset, and while it is comprehensive, it might have limitations in representing the entire landscape of ransomware-related transactions. This study's limitation lies in its exclusive focus on the cryptocurrency ecosystem, which could restrict its broader applicability and the deployment of ML classifiers. Moreover, the research is confined to the RFSA without incorporating ML classification. An additional constraint pertains to the real-time applicability of the proposed RFSA which represents a potential area for advancement within the field. In future studies, the application of ML and deep learning could be explored using the selected features for a more refined ransomware recognition framework. One promising research direction lies in the development and enhancement of real-time ML models tailored specifically for early detection and mitigation of zero-day ransomware attacks. Improving the robustness and adaptability of these models to swiftly identify and respond to evolving ransomware threats remains a crucial area of investigation. Moreover, delving deeper into the behavioral analysis of ransomware across varied technological landscapes, including IoT devices and cloud environments, could offer comprehensive insights into the diverse attack surfaces and aid in devising more effective defense mechanisms. Similarly, investigating novel cryptographic techniques and decentralized systems, particularly in the context of blockchain technology, to bolster data security and resilience against ransomware attacks represents an intriguing frontier. Collaborative research efforts between academia, industry, and government bodies could focus on creating standardized datasets and benchmarks to facilitate comparative evaluations of ransomware detection methodologies. Furthermore, considering the human factor in ransomware defenses, such as user awareness training programs, and behavioral interventions to mitigate ransomware risks could significantly contribute to holistic cybersecurity strategies. These potential research avenues hold promise in fortifying defenses against ransomware threats and shaping the future landscape of cybersecurity practices.

References

[1] C. Leuprecht, C. Jenkins, and R. Hamilton, "Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency," *Journal of Financial Crime*, vol. 30, no. 4, pp. 1036–1054, 2023.

[2] D. Chaudhari, R. Agarwal, and S. K. Shukla, "Towards malicious address identification in bitcoin," in *2021 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2021, pp. 425–432.

[3] A. Alqahtani and F. T. Sheldon, "A survey of crypto ransomware attack detection methodologies: an evolving outlook," *Sensors*, vol. 22, no. 5, p. 1837, 2022.

[4] A. Zimba, Z. Wang, and H. Chen, "Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems," *Ict Express*, vol. 4, no. 1, pp. 14–18, 2018.

[5] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the bitcoin ecosystem," *Journal of Cybersecurity*, vol. 5, no. 1, p. tyz003, 2019.

[6] M. Nkongolo and M. Tokmak, "Zero-day threats detection for critical infrastructures," in *South African Institute of Computer Scientists and Information Technologists*, A. Gerber and M. Coetzee, Eds. Cham: Springer Nature Switzerland, 2023, pp. 32–47.

[7] M. Nkongolo, J. P. Van Deventer, and S. M. Kasongo, "Ugransome1819: A novel dataset for anomaly detection and zero-day threats," *Information*, vol. 12, no. 10, p. 405, 2021.

[8] S. Poudyal, K. P. Subedi, and D. Dasgupta, "A framework for analyzing ransomware using machine learning," in *2018 IEEE symposium series on computational intelligence (SSCI)*. IEEE, 2018, pp. 1692–1699.

[9] M. N. W. Nkongolo, "Zero-day vulnerability prevention with recursive feature elimination and ensemble learning," Cryptology ePrint Archive, Paper 2023/1843, 2023. [Online]. Available: https://eprint.iacr.org/2023/1843

[10] U. Zahoora, A. Khan, M. Rajarajan, S. H. Khan, M. Asam, and T. Jamal, "Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto ensemble classifier," *Scientific Reports*, vol. 12, no. 1, p. 15647, 2022.

[11] M. Nkongolo, J. P. van Deventer, and S. M. Kasongo, "The application of cyclostationary malware detection using Boruta and PCA," in *Computer Networks and Inventive Communication Technologies*, S. Smys, P. Lafata, R. Palanisamy, and K. A. Kamel, Eds. Singapore: Springer Nature Singapore, 2023, pp. 547–562.

[12] M. Nkongolo, J. P. van Deventer, S. M. Kasongo, and W. van der Walt, "Classifying social media using deep packet inspection data," in *Inventive Communication and Computational Technologies*, G. Ranganathan, X. Fernando, and Á. Rocha, Eds. Singapore: Springer Nature Singapore, 2023, pp. 543–557.

[13] A. Rege and R. Bleiman, "A free and community-driven critical infrastructure ransomware dataset," in *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*, C. Onwubiko, P. Rosati, A. Rege, A. Erola, X. Bellekens, H. Hindy, and M. G. Jaatun, Eds. Singapore: Springer Nature Singapore, 2023, pp. 25–37.

[14] T. Gera, J. Singh, A. Mehbodniya, J. L. Webber, M. Shabaz, and D. Thakur, "Dominant feature selection and machine learning-based hybrid approach to analyze android ransomware," *Security and Communication Networks*, vol. 2021, pp. 1–22, 2021.

[15] A. Ashraf, A. Aziz, U. Zahoora, M. Rajarajan, and A. Khan, "Ransomware analysis using feature engineering and deep neural networks," *arXiv preprint arXiv:1910.00286*, 2019.

[16] S. Lee, S. Lee, J. Park, K. Kim, and K. Lee, "Hiding in the crowd: Ransomware protection by adopting camouflage and hiding strategy with the link file," *IEEE Access*, 2023.

[17] S. H. Khan, T. J. Alahmadi, W. Ullah, J. Iqbal, A. Rahim, H. K. Alkahtani, W. Alghamdi, and A. O. Almagrabi, "A new deep

boosted CNN and ensemble learning based IoT malware detection," *Computers & Security*, vol. 133, p. 103385, 2023.

[18] J. Schoenbachler, V. Krishnan, G. Agarwal, and F. Li, "Sorting ransomware from malware utilizing machine learning methods with dynamic analysis," in *Proceedings of the Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, 2023, pp. 516–521.

[19] R. A. Mowri, M. Siddula, and K. Roy, "Is iterative feature selection technique efficient enough? A comparative performance analysis of RFECV feature selection technique in ransomware classification using SHAP," *Discover Internet of Things*, vol. 3, no. 1, p. 21, 2023.

[20] O. Dib, Z. Nan, and J. Liu, "Machine learning-based ransomware classification of bitcoin transactions," *Journal of King Saud University-Computer and Information Sciences*, p. 101925, 2024.

[21] D. W. Fernando and N. Komninos, "FeSAD ransomware detection framework with machine learning using adaption to concept drift," *Computers & Security*, vol. 137, p. 103629, 2024.

[22] B. Yamany, M. S. Elsayed, A. D. Jurcut, N. Abdelbaki, and M. A. Azer, "A holistic approach to ransomware classification: Leveraging static and dynamic analysis with visualization," *Information*, vol. 15, no. 1, p. 46, 2024.

[23] S. Gulmez, A. G. Kakisim, and I. Sogukpinar, "XRan: Explainable deep learning-based ransomware detection using dynamic analysis," *Computers & Security*, p. 103703, 2024.

[24] B. Zou, C. Cao, L. Wang, S. Fu, T. Qiao, and J. Sun, "Facile: A capsule network with fewer capsules and richer hierarchical information for malware image classification," *Computers & Security*, vol. 137, p. 103606, 2024.

[25] A. Moawad, A. I. Ebada, A. El-Harby, and A. M. Al-Zoghby, "An automatic artificial intelligence system for malware detection," *Automated Secure Computing for Next-Generation Systems*, pp. 115–138, 2024.

[26] A. Wahrstätter, A. Taudes, and D. Svetinovic, "Reducing privacy of coinjoin transactions: Quantitative bitcoin network analysis," *IEEE Transactions on Dependable and Secure Computing*, 2024.

[27] Z. Pan and P. Mishra, *Explainable AI for Cybersecurity*. Springer Nature, 2024.

[28] S. Saha, S. Afroz, and A. H. Rahman, "MAlign: Explainable static raw-byte based malware family classification using sequence alignment," *Computers & Security*, p. 103714, 2024.

[29] L. Almutairi, "Explainable Artificial Intelligence-enabled android malware detection model for cybersecurity," in *International Conference On Innovative Computing And Communication*. Springer, 2023, pp. 637–655.

[30] B. Biswas, A. Mukhopadhyay, A. Kumar, and D. Delen, "A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks," *Decision Support Systems*, p. 114102, 2023.

[31] M. Komisarek, M. Pawlicki, T. Simic, D. Kavcnik, R. Kozik, and M. Choraś, "Modern netflow network dataset with labeled attacks and detection methods," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023, pp. 1–8.

[32] D. Shankar, G. V. S. George, J. N. J. N. S. S, and P. S. Madhuri, "Deep analysis of risks and recent trends towards network intrusion detection system," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 1, 2023.

[33] R. Naidoo and C. Jacobs, "Cyber warfare and cyber terrorism threats targeting critical infrastructure: A HCPS-based threat modelling intelligence framework," in *ECCWS 2023 22nd European Conference on Cyber Warfare and Security*, no. 1. Academic Conferences and publishing limited, 2023.

[34] X. Lei, Y. Xia, A. Wang, X. Jian, H. Zhong, and L. Sun, "Mutual information based anomaly detection of monitoring data with attention mechanism and residual learning," *Mechanical Systems and Signal Processing*, vol. 182, p. 109607, 2023.

[35] N. Ganesh, R. Shankar, R. Čep, S. Chakraborty, and K. Kalita, "Efficient feature selection using weighted superposition attraction optimization algorithm," *Applied Sciences*, vol. 13, no. 5, p. 3223, 2023.

[36] M. Lichtenstein and Z. Rucks-Ahidiana, "Contextual text coding: A mixed-methods approach for large-scale textual data," *Sociological Methods & Research*, vol. 52, no. 2, pp. 606–641, 2023.

[37] J. Han, J. Pei, and H. Tong, *Data mining: concepts and techniques*. Morgan kaufmann, 2022.

[38] M. Nkongolo, J. P. Van Deventer, S. M. Kasongo, S. R. Zahra, and J. Kipongo, "A cloud based optimization method for zero-day threats detection using genetic algorithm and ensemble learning," *Electronics*, vol. 11, no. 11, p. 1749, 2022.

[39] W. Hardy, L. Chen, S. Hou, Y. Ye, and X. Li, "DL4MD: A deep learning framework for intelligent malware detection," in *Proceedings of the International Conference on Data Science (ICDATA)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2016, p. 61.

[40] P. Panda, O. K. CU, S. Marappan, S. Ma, and D. Veesani Nandi, "Transfer learning for image-based malware detection for IoT," *Sensors*, vol. 23, no. 6, p. 3253, 2023.

[41] Y. Fang, C. Huang, L. Liu, and M. Xue, "Research on malicious Javascript detection technology based on LSTM," *IEEE Access*, vol. 6, pp. 59 118–59 125, 2018.

[42] C. Roberts and M. Nair, "Arbitrary Discrete Sequence Anomaly Detection with Zero Boundary LSTM," *arXiv e-prints*, p. arXiv:1803.02395, Mar. 2018.

[43] T. Wang, W. W. Y. Ng, W. Li, S. Kwong, and J. Li, "Broad autoencoder features learning for pattern classification problems," in *2019 IEEE 18th International Conference on Cognitive Informatics Cognitive Computing (ICCI*CC)*, 2019, pp. 130–135.

[44] S. Chatterjee, D. Dey, and S. Munshi, "Morphological, texture and auto-encoder based feature extraction techniques for skin disease classification," in *2019 IEEE 16th India Council International Conference (INDICON)*, 2019, pp. 1–4.

[45] X. Kong, R. Lin, and H. Zou, "Feature extraction of load curve based on autoencoder network," in *2020 IEEE 20th International Conference on Communication Technology (ICCT)*, 2020, pp. 1452–1456.

[46] Y. Wang, H. Yang, X. Yuan, Y. A. Shardt, C. Yang, and W. Gui, "Deep learning for fault-relevant feature extraction and fault classification with stacked supervised auto-encoder," *Journal of Process Control*, vol. 92, pp. 79–89, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0959152420302225

[47] J. Kim, H. Lee, J. W. Jeon, J. M. Kim, H. U. Lee, and S. Kim, "Stacked auto-encoder based CNC tool diagnosis using discrete wavelet transform feature extraction," *Processes*, vol. 8, no. 4, 2020. [Online]. Available: https://www.mdpi.com/2227-9717/8/4/456

[48] M. Tokmak, "Deep forest approach for zero-day attacks detection," *Innovations and Technologies in Engineering.*, no. ISBN: 978-625-6382-83-1, pp. 45–56, 2022.

[49] A. Jyothish, A. Mathew, and P. Vinod, "Effectiveness of machine learning based android malware detectors against adversarial attacks," *Cluster Computing*, pp. 1–21, 2023.

[50] J. Kipongo, T. G. Swart, and E. Esenogho, "Artificial intelligence-based intrusion detection and prevention in edge-assisted SDWSN with modified Honeycomb structure," *IEEE Access*, 2023.

[51] F. Suthar, N. Patel, and S. Khanna, "A signature-based botnet (emotet) detection mechanism," *Int. J. Eng. Trends Technol*, vol. 70, no. 5, pp. 185–193, 2022.

[52] 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," *Electronics*, vol. 12, no. 18, p. 3899, 2023.

[53] M. Nkongolo, "Ugransome dataset," 2023. [Online]. Available: https://www.kaggle.com/dsv/7172543

[54] A. Thakkar and R. Lohiya, "Fusion of statistical importance for feature selection in deep neural network-based intrusion detection system," *Information Fusion*, vol. 90, pp. 353–363, 2023.

[55] J. Liu, Y. Lin, J. Du, H. Zhang, Z. Chen, and J. Zhang, "ASFS: A novel streaming feature selection for multi-label data based on neighborhood rough set," *Applied Intelligence*, vol. 53, no. 2, pp. 1707–1724, 2023.

[56] P. Teisseyre and J. Lee, "Multilabel all-relevant feature selection using lower bounds of conditional mutual information," *Expert Systems with Applications*, vol. 216, p. 119436, 2023.

[57] Y. Yuan, L. Wu, and X. Zhang, "Gini-impurity index analysis," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3154–3169, 2021.

[58] M. Zhou, K. Yan, J. Huang, Z. Yang, X. Fu, and F. Zhao, "Mutual information-driven pan-sharpening," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2022, pp. 1798–1808.

[59] M. Nkongolo Wa Nkongolo *et al.*, "News classification and categorization with smart function sentiment analysis," *International Journal of Intelligent Systems*, vol. 2023, 2023.

[60] M. Nkongolo, J. P. Van Deventer, S. M. Kasongo, W. Van Der Walt, R. Kalonji, and M. Pungwe, "Network policy enforcement: An intrusion prevention approach for critical infrastructures," in *2022 6th International Conference on Electronics, Communication and Aerospace Technology*, 2022, pp. 686–692.

[61] M. Nkongolo, "Using arima to predict the growth in the subscriber data usage," *Eng*, vol. 4, no. 1, pp. 92–120, 2023.

[62] M. Nkongolo, J. P. van Deventer, and S. M. Kasongob, "Using deep packet inspection data to examine subscribers on the network," *Procedia Computer Science*, vol. 215, pp. 182–191, 2022.

[63] S. A. Alsaif *et al.*, "Machine learning-based ransomware classification of bitcoin transactions," *Applied Computational Intelligence and Soft Computing*, vol. 2023, 2023.

[64] J. Peng, W. Wu, B. Lockhart, S. Bian, J. N. Yan, L. Xu, Z. Chi, J. M. Rzeszotarski, and J. Wang, "Dataprep. eda: Task-centric exploratory data analysis for statistical modeling in python," in *Proceedings of the 2021 International Conference on Management of Data*, 2021, pp. 2271–2280.

[65] J. Osborne, "Notes on the use of data transformations," *Practical assessment, research, and evaluation*, vol. 8, no. 1, p. 6, 2002.

[66] M. Benmalek, "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges," *Internet of Things and Cyber-Physical Systems*, 2024.

[67] M. Nkongolo, "Navigating the complex nexus: cybersecurity in political landscapes," 2023.

[68] M. Nkongolo, N. Mennega, and I. van Zyl, "Requirements for a career in information security: A comprehensive review," in *Data Intelligence and Cognitive Informatics*, I. J. Jacob, S. Piramuthu, and P. Falkowski-Gilski, Eds. Singapore: Springer Nature Singapore, 2024, pp. 85–98.

[69] T. O. Abrahams, S. K. Ewuga, S. O. Dawodu, A. O. Adegbite, and A. O. Hassan, "A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection," *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 1–25, 2024.

[70] G. Widjaja, "Enhancing legal literacy: Understanding the significance of law no. 9/2019 on electronic transactions in the social media era," *Journal of Community Dedication*, vol. 3, no. 4, pp. 278–293, 2023.

[71] A. Alraizza and A. Algarni, "Ransomware detection using machine learning: A survey," *Big Data and Cognitive Computing*, vol. 7, no. 3, p. 143, 2023.

[72] L. Bekkers, S. van't Hoff-de Goede, E. Misana-ter Huurne, Y. van Houten, R. Spithoven, and E. R. Leukfeldt, "Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model," *Computers & Security*, vol. 127, p. 103099, 2023.

[73] A. Arakkal, S. Pazheri Sharafudheen, and A. Vasudevan, "Crypto-ransomware detection: A honey-file based approach using Chi-Square test," in *International Conference on Information Systems Security*. Springer, 2023, pp. 449–458.

[74] H. Yasui, T. Inoue, T. Sasaki, R. Tanabe, K. Yoshioka, and T. Matsumoto, "SPOT: In-depth analysis of IoT ransomware attacks using bare metal NAS devices," *Journal of Information Processing*, vol. 32, pp. 23–34, 2024.

[75] Y. Kumar and V. Kumar, "A systematic review on intrusion detection

system in wireless networks: Variants, attacks, and applications," *Wireless Personal Communications*, pp. 1–58, 2023.

[76] K. Ahmed, S. K. Khurshid, and S. Hina, "Cyberentrel: Joint extraction of cyber entities and relations using deep learning," *Computers & Security*, vol. 136, p. 103579, 2024.

Dr. Mike Nkongolo Wa Nkongolo was born in the Democratic Republic of the Congo (DRC) and earned his BSc in Informatics from the Université Protestante de Lubumbashi (UPL, DRC) between 2010 and 2013. He furthered his studies in computer science at the University of the Witwatersrand, earning his HDip, BSc Honours, and MSc from the School of Computer Science and Applied Mathematics (2015-2019). In 2021, he enrolled in the Ph.D. program in Information Technology at the University of Pretoria, completing the degree in 2023. Dr. Nkongolo currently holds the position of Lecturer in the Department of Informatics at the University of Pretoria. His research interests encompass cybersecurity, information retrieval, data science, machine learning, and natural language processing. He reviews for various journals, including Automatika, the International Journal of Computing and Digital Systems, the South African Computer Journal, and IEEE Transactions on Education. Dr. Wa Nkongolo Mike is a member of the South African Institute of Computer Scientists & Information Technologists (SAICSIT) and the Institute of Information Technology Professionals South Africa (IITPSA).