Analyzing Ransomware Incidents in Healthcare: Patterns and Risk Assessment

Dominik Degele and Muhammad Abusaqer

Department of Math, Data, & Technology

Minot State University

Minot, North Dakota 58703

dominik.degele@minotstateu.edu and
muhammad.abusaqer@minotstateu.edu

Abstract

Ransomware attacks pose a grave threat to healthcare organizations, compromising patient safety, financial stability, and data integrity. This study analyzes a synthetic ransomware dataset of 5,000 records (publicly sourced from Kaggle and supplemented with scenario-based simulations) to identify common attack vectors, quantify the severity of disruptions, and examine factors influencing the decision to pay a ransom. Three core experiments were conducted: (1) descriptive statistical analysis of primary targets and entry methods, (2) a predictive modeling approach using random forests to assess ransom payment likelihood, and (3) clustering to categorize incidents based on severity and recovery metrics. Results indicate that hospitals and clinics are the most frequently targeted, with "Compromised Credentials" being the leading point of intrusion. Ransom-payment predictions yielded an accuracy of only 49%, suggesting that external, non-quantifiable factors influence the decision to pay. Clustering revealed four incident profiles, ranging from low-impact to severe-impact events. These findings underscore the need for robust cybersecurity practices, proactive incident response plans, and a deeper understanding of non-technical factors impacting organizational decision-making.

1. Introduction

Ransomware involves malicious software that encrypts or otherwise blocks access to critical data, demanding payment for restoration. Healthcare organizations are particularly vulnerable due to their reliance on continuous patient data availability and the industry's often-outdated infrastructure. Despite the urgency to resolve disruptions promptly, the outcomes of paying a ransom are not guaranteed, and the long-term financial and reputational effects can be substantial.

The research uses descriptive analysis, predictive modeling, and cluster analysis to examine ransomware attacks targeting hospitals, offering insights into how various organizational factors correlate with ransom payment decisions. Descriptive analysis highlights overarching themes in the dataset, while predictive modeling—implemented via a Random Forest machine learning algorithm—aims to estimate whether an institution is more likely to pay the demanded ransom. Lastly, cluster analysis facilitates identifying statistical patterns that may reveal common factors among healthcare organizations experiencing ransomware incidents. Together, these three approaches provide a more comprehensive understanding of how ransomware disrupts healthcare systems and what measures may mitigate future attacks.

The Kaggle dataset central to this research is the "Healthcare Ransomware Dataset," which captures various aspects of ransomware incidents in healthcare institutions. Its features include how often each organization performs system monitoring, the frequency and reliability of backups, the ransomware infection rate, whether data were encrypted or stolen, the system's recovery time, the method of intrusion, and whether the institution ultimately paid the ransom [8]. By inputting these features into our models, we aim to identify predictive factors and help healthcare organizations avoid repeating past security lapses.

Although the information gathered in this paper may not be groundbreaking in isolation, it contributes additional evidence and contextual analysis for understanding ransomware trends in healthcare. Building on prior research, this work offers expanded predictive and descriptive insights, guiding stakeholders toward more informed decisions about ransom payment, backup strategies, and preventative measures.

2. Background

A clear understanding of key terminology is essential for comprehending the impact of ransomware on healthcare organizations. This section provides definitions and explanations of concepts fundamental to our study.

2.1 Ransomware

Ransomware is a type of malware that encrypts or disables a system, holding it hostage until a payment, often made in cryptocurrencies, is received. However, paying the ransom

does not guarantee the restoration or integrity of the data. Conversely, refusing to pay may force organizations to rely on outdated or unreliable backups, potentially resulting in significant data loss [4].

2.2 Descriptive Statistical Analysis

Descriptive statistical analysis involves extracting immediate insights from a dataset. By computing measures such as the mean, mode, and distribution trends, researchers can identify overarching patterns that guide subsequent modeling efforts.

2.3 Machine Learning

Machine learning encompasses a range of algorithmic techniques used to predict outcomes based on historical (or training) data [11].

2.4 Supervised Machine Learning

Supervised machine learning algorithms are trained on labeled data, where the correct output is already known, allowing the model to learn the relationships between input features and the target variable [1].

2.5 Random Forest Algorithm

The Random Forest algorithm is a supervised learning method that constructs a multitude of independent decision trees. Its final prediction is derived either by majority voting (in classification tasks) or by averaging the outputs (in regression tasks). This ensemble approach enhances generalizability and helps mitigate overfitting [7].

2.6 Unsupervised Machine Learning and Clustering

Unsupervised machine learning algorithms work with unlabeled data, inferring the underlying structure solely from input features. Clustering, a common unsupervised technique, groups data points based on similarity. Although correlation among variables does not imply causation, effective cluster analysis can reveal meaningful groupings that inform more focused investigations [1].

By clarifying these concepts, this study establishes a foundation for interpreting the results obtained from descriptive, predictive, and clustering analyses. In particular, examining how healthcare organizations respond to ransomware—whether by paying the ransom or relying on backups—provides valuable insights into effective deterrence strategies and risk mitigation measures.

3. Related Work

Several prior studies have addressed ransomware detection and mitigation using machine learning. For instance, [2] surveyed privacy-preserving approaches for malware detection and highlighted the value of clustering methods for behavioral analysis, a technique this paper also employs.

Similarly, [5] evaluated the accuracy of different machine learning models in network-based malware detection, underscoring the importance of selecting appropriate algorithms for reliable predictions.

In the healthcare domain, [6] demonstrated that simple models can achieve high accuracy when trained with well-structured datasets, which aligns with our decision to use Random Forest for its interpretability and efficiency.

A study titled "Cyber risk quantification and mitigation framework for healthcare using Machine Learning [9]" introduced a machine learning framework tailored to healthcare-specific cyber risk quantification, reinforcing the need for domain-specific model tuning. This ties back to [2] in deciding on the best structural growth for our algorithm, which supports that any given model must be trained correctly to be accurate. An inaccurate machine that aids in the protection against malicious entities can only lead to disaster.

Although [3] focused on IoT in healthcare, its risk mitigation strategies provide context for broader cybersecurity planning. The devices connected to any network and the users that operate those devices are the frontline for preventing any attack. Proper training is needed to mitigate front-layer threats.

Finally, the study of "A Multi-level Ransomware Detection Framework using Natural Language Processing and Machine Learning" advocated for hybrid analysis tools, showing that combining techniques like NLP and machine learning can enhance detection capabilities —an idea echoed in our multi-method approach [10]. This gives our algorithm the framework to be built upon, as it will make its training data more accurate, and thus its predictions will be accurate in and of itself when faced against a live ransomware attack.

4. Methodology

4.1 Dataset Description

The study utilizes a dataset sourced from Kaggle[1]. The dataset (5,000 records) was generated to reflect real-world ransomware trends in healthcare. Each record includes:

[1] https://www.kaggle.com/datasets/rivalytics/healthcare-ransomware-dataset

- **Incident context**: Organization type (hospital, clinic, research lab, etc.), organization size (small, medium, or large), and timestamp of attack.
- **Security measures**: Monitoring frequency (daily, weekly, or monthly), number of cyber threats tracked, and presence of compromised backups.
- **Attack characteristics**: Attack entry method (e.g., compromised credentials, exploited vulnerabilities, phishing), percentage of systems infected, and whether data were encrypted or stolen.
- **Impact and response**: Number of facilities affected, recovery time, data restored percentage, and whether a ransom was paid.

All columns are non-null, and no duplicated rows were detected in the dataset. The dataset provides additional insights into how these variables were synthesized using real-world industry benchmarks.

4.2 Experiment 1: Descriptive Statistical Analysis

4.2.1 Identifying Frequently Targeted Organizations

Organization types were tallied to determine their prevalence among ransomware incidents. A bar chart, Figure 1, shows that hospitals have the highest incidence rate, followed by clinics, while insurance companies, pharmacies, and research labs appear somewhat less frequently.

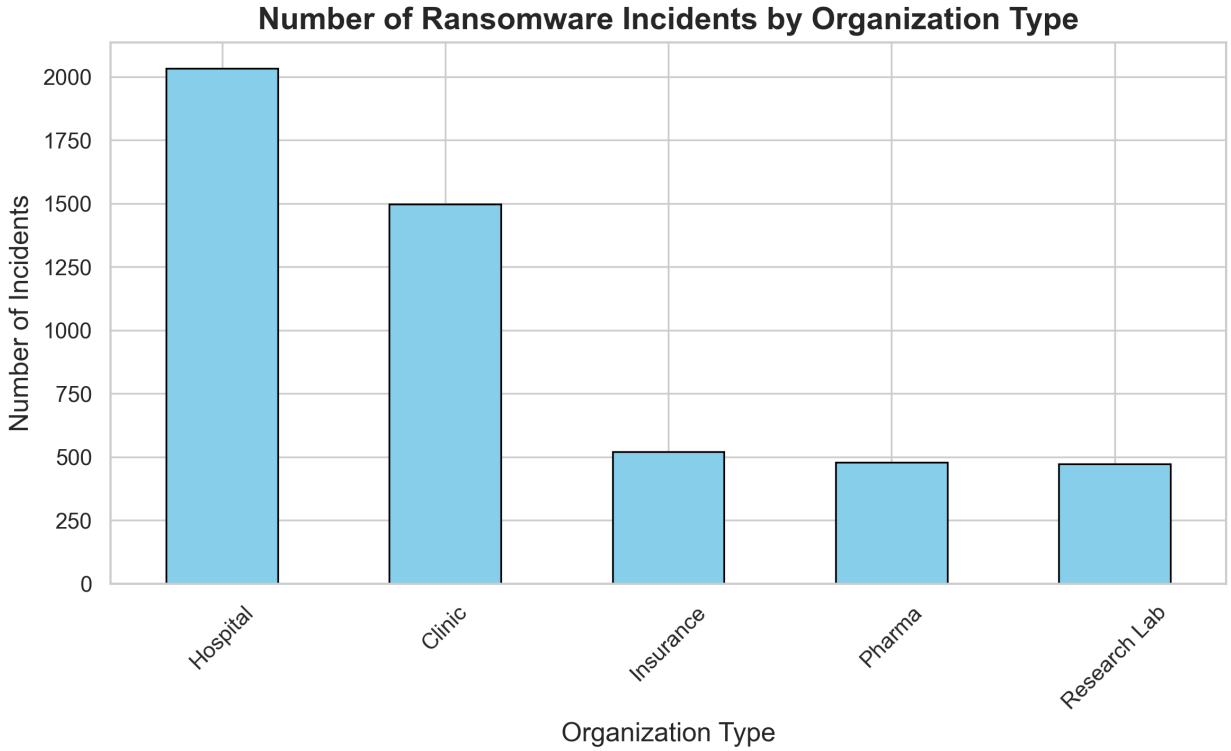

Figure 1. Number of Ransomware Incidents by Organization Type

4.2.2 Primary Attack Entry Methods

Attack methods such as "Compromised Credentials," "Exploited Vulnerabilities," and "Phishing Emails" were compared. A second bar chart, Figure 2, revealed "Compromised Credentials" as the most frequent attack vector, closely followed by "Exploited Vulnerabilities." "Phishing Emails" ranked third.

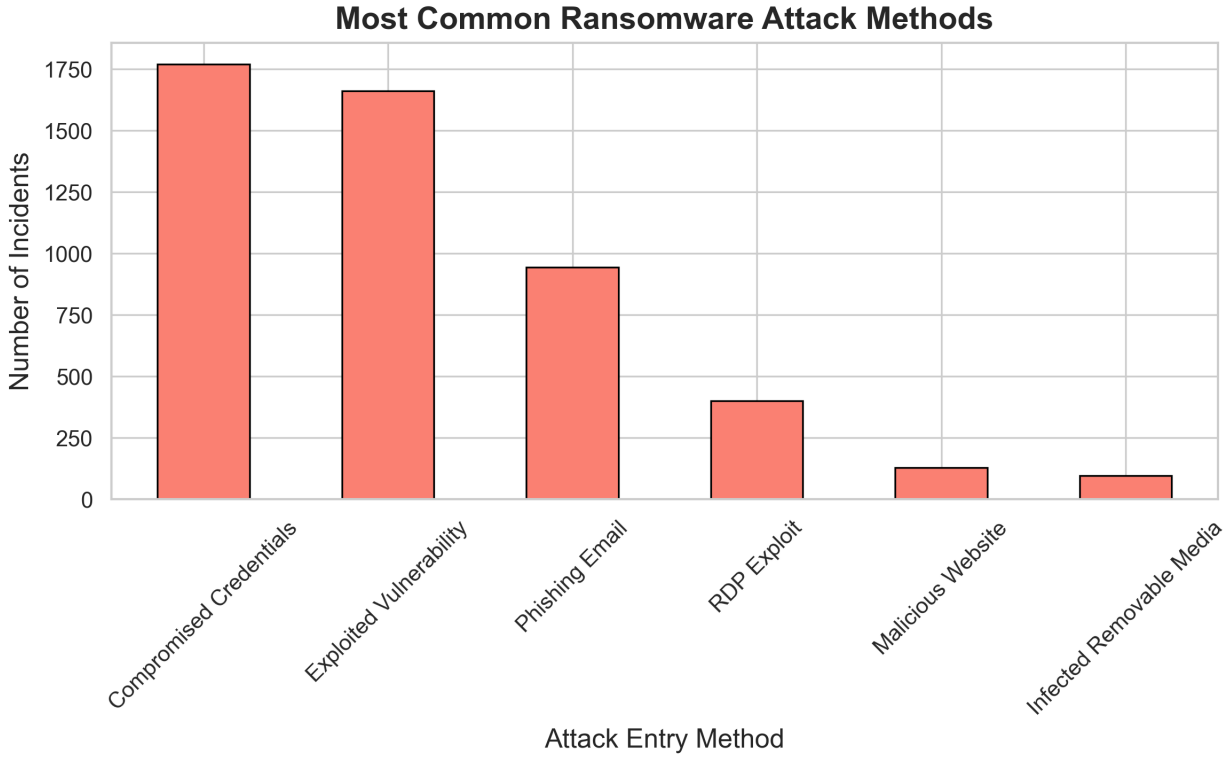

Figure 2. Most Common Ransomware Attack Methods

4.2.3 Ransom Payment Distribution

The proportion of organizations that paid a ransom was plotted in a third bar chart in Figure 3. The data showed an almost even split between organizations that decided to pay and those that did not.

Figure 3. Percentage of Organizations Paying Ransom

4.2.4 Correlation Analysis

A heatmap of key numerical variables shown in Figure 4 indicated:

- A positive correlation between ransomware infection rate and recovery time.
- A relationship between compromised backups and lower percentages of data restored.
- Minimal correlation between paying ransom and data restored, suggesting that payment alone may not guarantee successful data recovery.

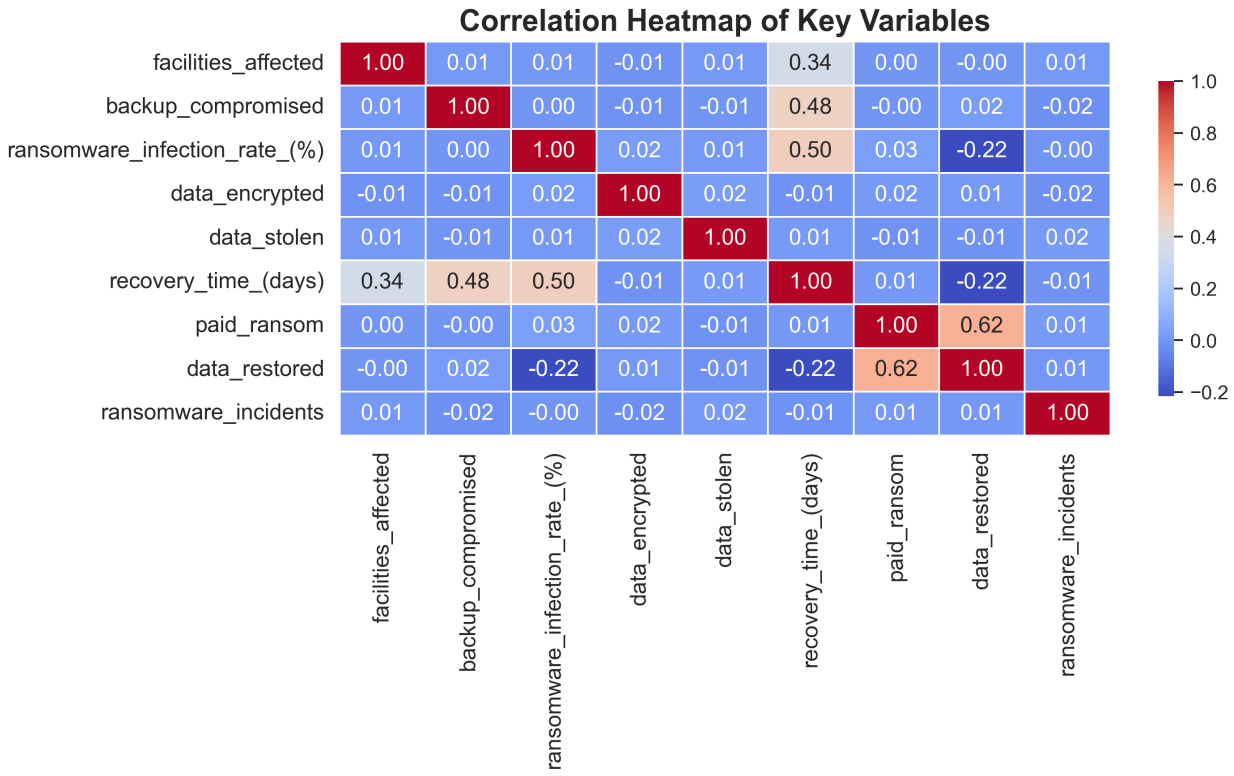

Figure 4. Correlation Heatmap of Key Variables

4.3 Experiment 2: Predictive Modeling (Ransom Payment)

A random forest classifier was used to predict whether an organization would pay a ransom. Ten predictor features were selected, including organizational size, number of facilities affected, backup compromise status, and entry method. After encoding categorical variables (label encoding), the dataset was split 80:20 into training and test sets.

4.3.1 Model Performance

The classifier achieved an overall accuracy of **49%**, with nearly identical precision and recall values around 50% for both "Pay" and "Not Pay" classes. This result suggests that ransom payment decisions are not sufficiently captured by the dataset's internal factors (e.g., infection rate, facilities affected). Instead, external considerations—such as insurance coverage, executive decisions, or negotiation tactics—may play a substantial role.

4.3.2 Feature Importance

The top five factors associated with ransom payment predictions were:

1. Ransomware Infection Rate

2. Recovery Time
3. Facilities Affected
4. Entry Method
5. Monitoring Frequency

Though these factors do influence payment decisions, *the model's poor predictive power underscores the significance of external or unobserved variables*.

4.4 Experiment 3: Clustering Analysis

To categorize the severity of the impact, a K-Means model (k=4) was applied to four scaled numeric features: facilities affected, ransomware infection rate, recovery time, and percentage of data restored.

Cluster Profiles (see Table 1 for summarized means):

Cluster	Facilities Affected	Infection Rate (%)	Recovery Time (Days)	Data Restored (%)	Interpretation
0	~18.68	~48.52	~37.31	~49.39	Moderate infection & recovery, decent restoration
1	~6.63	~43.63	~24.28	~56.67	Lower impact, faster recovery, highest restoration
2	~7.10	~62.22	~39.72	~32.56	High infection, moderate recovery, low restoration
3	~17.73	~67.52	~70.23	~36.74	Severe infection, longest recovery, poor restoration

Table 1. Cluster Means for Facilities Affected, Infection Rate, Recovery Time, and Data Restored

The clusters reveal notably different outcomes in terms of severity. Cluster 3, for instance, experiences the highest infection rate alongside an extended recovery period, suggesting a need for improved backup procedures and faster response strategies.

5. Results

5.1 Descriptive Highlights

- **Organization Types**: Hospitals exhibited the highest rate of ransomware incidents, potentially because of their large user base and legacy systems.
- **Entry Methods**: Compromised credentials topped the list, exposing weaknesses in authentication and password policies.
- **Payment Decisions**: Approximately half of the organizations paid ransoms, indicating frequent resort to financial settlements despite inherent risks.

5.2 Predictive Modeling Outcomes

The random forest model confirmed that internal dataset features have limited predictive power regarding ransom payment. The classification report (precision, recall, F1-score) hovered around 50%, effectively mirroring random guessing.

5.3 Clustering Findings

Four clusters based on severity and recovery patterns suggest that healthcare organizations face diverse ransomware outcomes. Some organizations restore a large portion of data quickly, while others endure protracted recovery times and widespread infections.

6. Discussion

The findings indicate that commonly measured variables (e.g., infection rate, monitoring frequency) do not sufficiently explain an organization's decision to pay ransom. External factors, such as legal advice, insurance coverage, financial constraints, or executive directives, might likely influence payment behavior. Further research in this side needs to explore which actually might play the significant influence in driving decision process. Moreover, *organizations should note that paying a ransom offers no guarantee of full data restoration*, as demonstrated by the weak correlation between "paid ransom" and "data restored."

Clustering analysis points to different risk profiles: some healthcare entities exhibit shorter downtime and minimal data loss, whereas others face significant disruptions. This underscores the importance of tailoring security measures and incident response strategies to an institution's specific threat profile.

The correlation heatmap suggests that routine security practices, such as more frequent threat monitoring or more robust backups, can reduce infection severity and recovery durations. Therefore, healthcare providers seeking to mitigate risk should prioritize timely

patching of vulnerabilities, robust credential management, and regular data backup verifications.

7. Future Work

Several avenues exist for strengthening future analyses:

1. **Integration of External Organizational Factors**

   Incorporate data on insurance policies, budgetary constraints, and institutional policies regarding ransom negotiations to improve predictive models of payment behavior.

2. **Temporal Analysis**

   Investigate how ransomware incidence evolves over time, measuring the impact of organizational learning, policy changes, and technology updates.

3. **Advanced Modeling Techniques**

   Employ deep learning or ensemble methods to capture non-linear relationships between technical and organizational factors. Additionally, consider domain adaptation for different healthcare segments.

8. Conclusion

This study analyzes 5,000 simulated ransomware events in the healthcare sector, detailing patterns of attack and organizational responses across three principal experiments. The descriptive statistics highlight the prevalence of compromised credentials and the vulnerability of major healthcare entities (hospitals and clinics). Predictive models reveal that current dataset features do not reliably anticipate ransom payment decisions, reinforcing the role of external, possibly unquantifiable factors. Clustering analysis exposes distinct severity profiles, ranging from quick, relatively painless recoveries to severe, protracted disruptions. These findings underscore the importance of a multi-faceted approach to ransomware preparedness, combining sound technical defenses with informed organizational policies.

References

[1] “Difference between Supervised and Unsupervised Learning,” GeeksforGeeks, Jan. 28, 2025, [Online]. Available: https://www.geeksforgeeks.org/difference-between-supervised-and-unsupervised-learning/#. [Accessed: March. 30, 2025].

[2] F. Nawshin, R. Gad, D. Unal, A. K. Al-Ali, and P. N. Suganthan, “Malware detection for mobile computing using secure and privacy-preserving machine learning

approaches: A comprehensive survey," Computers and Electrical Engineering, vol. 117, p. 109233, Jul. 2024. doi:10.1016/j.compeleceng.2024.109233

[3] M. A. Khatun, S. F. Memon, C. Eising, L. L. Dhirani, "Machine Learning for Healthcare-IOT Security: A Review and Risk Mitigation", date of publication 22 December 2023, date of current version 29 December 2023. Doi: 10.1109/ACCESS.2023.3346320

[4] M. Kosinski, "What Is Ransomware?," IBM, Jun. 4, 2024, [Online]. Available: https://www.ibm.com/think/topics/ransomware

[5] M. Stevanovic, "Machine Learning for Network-Based Malware Detection," Aalborg University, 2016, doi: 10.5278/vbn.phd.engsci.00088, [Online]. Available: https://doi.org/10.5278/vbn.phd.engsci.00088

[6] R. Buvaneshwari, K. Lavanya, R. Vanitha, "Healthcare Information Using Machine Learning Approach," International Journal of Scientific and Research Publications, Volume 2, Issue 2, February 2012, ISSN 22503153.

[7] "Random Forest Algorithm in Machine Learning", GeeksforGeeks, January 16, 2025, [Online]. Available: https://www.geeksforgeeks.org/random-forest-algorithm-in-machine-learning/

[8] Rivalytics," Healthcare Ransomware Dataset," Kaggle, [Online]. Available: https://www.kaggle.com/datasets/rivalytics/healthcare-ransomware-dataset

[9] S. Pal, A. Mukhopadhyay, "Cyber Risk Quantification and Mitigation Framework for Healthcare Using Machine Learning," in Proceedings Twenty-fourth Americas Conference on Information Systems, New Orleans, 2018.

[10] S. Poudyal, D. Dasgupta, Z. Akhtar, K. D. Gupta, "A Multi-level Ransomware Detection Framework Using Natural Language Processing and Machine Learning," in Proceedings International Conference on Malicious and Unwanted Software (MALCON 2019), October 2019.

[11] "What is Machine Learning?", GeeksforGeeks, January 13, 2025, [Online] Available: https://www.geeksforgeeks.org/ml-machine-learning/