Impact Factor (SJIF): 6.126 E-ISSN: 2583-1615

International Journal of Research in Academic World

Received: 05/February/2025 **IJRAW:** 2025; 4(SP3):44-50 **Accepted:** 19/March/2025

Bitcoin Ransomware Payment Analysis

[*1]G Anitha, [2]Kanimozhi P and [3]Sivavarshinika P

[*1]Assistant Professor, Department of Data Analytics (PG), PSGR Krishnammal College for Women, Coimbatore, Tamil Nadu, India.

[2, 3]PG Student, Department of Data Analytics (PG), PSGR Krishnammal College for Women, Coimbatore, Tamil Nadu, India.

Abstract

The increasing prevalence of ransomware attacks has posed a significant threat to global cybersecurity, with Bitcoin serving as the primary medium for ransom payments due to its decentralized and pseudonymous nature. This paper presents a data-driven approach to analyzing ransomware-related Bitcoin transactions. A web-based analytical dashboard is developed using Streamlit to visualize transaction patterns and detect anomalies in real time. Machine learning techniques, including Isolation Forest and Random Forest, are employed to classify transactions, identify suspicious activities, and predict high-risk payments. Furthermore, network analysis methods are utilized to uncover relationships between ransomware families and their associated Bitcoin addresses. The study also incorporates a predictive risk-scoring mechanism to assess future ransomware payment trends. The insights gained from this research provide valuable intelligence for cybersecurity experts, to enhanced detection and mitigation strategies against ransomware threats.

Keywords: Ransomware, Bitcoin transactions, anomaly detection, machine learning, risk scoring, cybersecurity.

1. Introduction

Ransomware attacks have become one of the most significant cybersecurity threats, leading to massive financial losses worldwide. Attackers often demand payments in cryptocurrencies, primarily Bitcoin, due to its pseudonymous nature. Identifying and monitoring suspicious transactions in the Bitcoin network is crucial for early detection and mitigation of potential threats. Traditional detection methods often rely on post-incident forensic analysis, which delays response time and reduces the effectiveness of countermeasures. In contrast, this paper proposes an automated system for real-time transaction monitoring and anomaly detection, significantly improving cybersecurity defenses.

Traditional methods of tracking ransomware payments rely on forensic analysis, law enforcement investigations, and blockchain monitoring tools. However, these approaches often face challenges due to the dynamic nature of Bitcoin transactions, the use of mixing services, and the emergence of privacy-enhancing technologies such as CoinJoin and tumbling services. The increasing complexity of illicit financial transactions highlights the need for data-driven methodologies capable of identifying suspicious activities and predicting potential threats.

This study introduces a comprehensive framework for analyzing ransomware-related Bitcoin transactions using machine learning and statistical techniques. An interactive web-based dashboard is designed to facilitate real-time transaction monitoring and visualization. Anomaly detection models, such as Isolation Forest, are employed to flag suspicious transactions, while classification algorithms, including Random Forest, are utilized to assess risk levels associated with ransomware payments. Furthermore, network analysis is applied to map relationships between Bitcoin addresses and ransomware families, revealing hidden connections within the blockchain ecosystem.

The proposed approach also includes a risk-scoring mechanism to classify transactions based on their likelihood of being associated with ransomware payments. Predictive modeling techniques are incorporated to forecast future ransomware payment trends, enabling proactive threat mitigation.

2. Problem Statement

Ransomware attacks have become increasingly sophisticated, leveraging the anonymity of Bitcoin transactions to evade detection. The decentralized and pseudonymous nature of blockchain technology poses significant challenges for tracking and analyzing illicit financial activities. Law enforcement agencies, financial regulators, and cybersecurity professionals face difficulties in identifying ransomware payment patterns due to the high volume of Bitcoin transactions, the use of mixing services, and obfuscation techniques employed by cybercriminals.

Existing monitoring systems struggle to differentiate legitimate Bitcoin transactions from those associated with

***Corresponding Author:** G Anitha

ransomware due to the lack of contextual information and advanced analytical capabilities. The absence of a standardized approach for risk classification further complicates efforts to proactively detect and prevent ransomware-related financial transactions. Traditional forensic techniques often fail to provide real-time insights, limiting the effectiveness of response strategies against ransomware operations.

Proposed Solution

To address these challenges, a data-driven framework is introduced for the analysis of ransomware-related Bitcoin transactions. The proposed solution integrates machine learning algorithms, anomaly detection models, and network analysis techniques to enhance the identification of suspicious transactions. A web-based analytical dashboard is developed using Streamlit, providing an interactive platform for real-time transaction monitoring and risk assessment.

3. Domain: Cryptocurrency Forensics

Cryptocurrency forensics is a specialized branch of digital forensics that focuses on analyzing blockchain transactions to identify and track illicit financial activities, including ransomware payments, fraud, and money laundering. Unlike traditional banking systems, cryptocurrencies operate on decentralized and pseudonymous networks, making it difficult to trace ownership and movement of funds. However, forensic techniques such as address clustering, transaction pattern analysis, and machine learning-based anomaly detection enable investigators to link suspicious transactions to known criminal entities. By leveraging blockchain analytics tools, forensic experts can reconstruct fund flows, identify high-risk wallets, and uncover hidden relationships between cybercriminal networks.

Additionally, forensic investigations extend to darknet marketplaces and decentralized finance (DeFi) platforms, where illicit activities often take place. As ransomware attacks continue to rise, cryptocurrency forensics remains essential in tracking ransom payments, preventing financial crimes, and enhancing global cybersecurity resilience.

4. Literature Survey

Hassan *et al.* (2023) [1] provide a comprehensive analysis of anomaly detection techniques in blockchain networks, highlighting challenges like scalability, data privacy, and real-time detection. They also explore integrating anomaly detection with federated learning and zero-trust architectures.

Pahuja and Kamal (2023) [2] propose *Enlfade*, an ensemble learning-based framework for detecting fake accounts on Ethereum, demonstrating improved accuracy over single-model approaches and analyzing the impact of feature selection and dataset imbalance on fraud detection.

Aziz *et al.* (2022) [3] introduce *LGBM*, a LightGBM-based fraud detection approach for Ethereum transactions, emphasizing efficiency, low computational costs, and model interpretability for real-world deployment.

Akcora *et al.* (2020) [4] present *BitcoinHeist*, a topological data analysis method for ransomware detection in Bitcoin transactions, showing how graph-based features enhance detection accuracy.

Dalal *et al.* (2021) [5] analyze Bitcoin ransomware actors, using clustering and machine learning to track suspicious transactions, discussing limitations in detection frameworks and proposing regulatory enhancements.

Nkongolo (2024) [6] reviews heuristic-based and deep learning techniques for ransomware detection, assessing their effectiveness while highlighting evolving cybercriminal evasion strategies.

Gupta *et al.* (2023) [7] categorize cryptocurrency fraud detection methods into supervised, unsupervised, and hybrid approaches, evaluating feature engineering and preprocessing techniques for improving model performance.

Brown and Peterson (2022) [8] explore blockchain security risks, including double-spending and Sybil attacks, emphasizing anomaly detection and behavioral analysis techniques for improved security.

Vasilomanolakis *et al.* (2022) [11] conduct an empirical analysis of ransomware activities in Bitcoin, discussing statistical trends, blockchain tracing techniques, and regulatory countermeasures.

Saad *et al.* (2021) [12] estimate total ransomware payments in Bitcoin, analyzing laundering tactics via cryptocurrency mixers and discussing emerging anti-money laundering (AML) strategies.

Gray *et al.* (2023) [13] analyze the Conti ransomware group's operational structure and financial strategies, offering insights into the ransomware-as-a-service (RaaS) model and its cybersecurity impact.

Foster and Zhang (2023) [14] explore blockchain forensic techniques for investigating illicit transactions, presenting case studies on financial crimes and law enforcement strategies.

Johnson (2022) [15] examines cybercrime and cryptocurrency, covering fraud, money laundering, and ransomware while discussing legal and technological countermeasures.

5. Data Modeling

Data modeling is a crucial process that ensures the accuracy, integrity, and timeliness of data used for analysis and prediction. It encompasses key stages such as data extraction, transformation, and loading, which collectively enhance data reliability and usability.

Process Flow

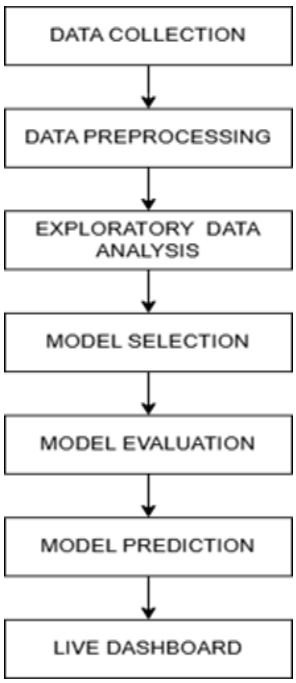

Fig 1: This Figure shows the process flow diagram

i). Data Collection

This step involves gathering real-time and historical Bitcoin transaction data from multiple sources:

- **Blockchain APIs:** Fetches live Bitcoin transactions, including sender-receiver addresses, timestamps, and transaction amounts Historical Datasets: Loads previously identified ransomware-related Bitcoin transactions to train detection models.
- **External Financial Data:** Includes BTC-to-USD conversion rates to assess the financial impact of transactions.

Proper data collection ensures the completeness, authenticity, and relevance of transaction data for ransomware payment detection.

ii). Data Pre-processing

In this stage, the acquired transaction data is cleaned and structured for analysis:

- **Handling Missing Values:** Removes incomplete or irrelevant transactions.
- **Anomaly Detection Features:** Creates risk scoring parameters such as transaction frequency, amount fluctuations, and clustering analysis.
- **Normalization & Transformation:** Standardizes numerical values and converts categorical attributes for model training.

This step ensures that data is consistent, accurate, and ready for machine learning-based risk classification.

iii). Machine Learning-Based Risk Analysis

- **Anomaly Detection Model:** Implements Isolation Forest and Random Forest Classification to detect suspicious transactions.
- **Risk Scoring System:** Assigns risk labelssuch as High-Risk, Medium-Risk, and Low-Risk based on behavioral patterns.
- **Transaction Clustering:** Groups similar Bitcoin transactions to uncover potential ransomware-linked addresses.

  By applying data-driven modeling, this step classifies and highlights transactions that require further security analysis.

iv). Visualization and Dashboard Implementation

Once the risk analysis is completed, the data is visualized in an interactive format:

- **Streamlit Dashboard:** Displays live transaction tracking, anomaly trends, and risk scores.
- **BTC-to-USD Impact Analysis:** Converts Bitcoin payments to fiat currency to measure the financial impact of ransomware payments.

This step ensures that security analysts and financial regulators can easily interpret risk patterns in cryptocurrency transactions.

6. Analysis and Interpretation

The Bitcoin Ransomware Payment Analysis Dashboard provides insights into ransomware-related Bitcoin transactions, as shown in the Figure 2. The Dataset Preview displays key details like datetime, address, amount_BTC, and amount_USD. Transactions vary in BTC amounts, with some being small and others significantly larger. The left-side Navigation Panel allows users to explore Overview, Analysis, Risk Scoring, and Live Data, while the Year Filter helps analyze trends over time.

Fig 2: Bitcoin Transaction Overview

The distribution of ransomware payments across different ransomware families is represented in Figure 3. The chart shows that the "Unlabeled" category accounts for the highest total ransom payments, exceeding $700 million, indicating a large number of transactions without an identified ransomware group. Among labeled families, Conti received the highest payments, around $100 million, followed by Cuba with a significant but lower amount. Other ransomware groups, such as BlackCat, BlackSuit, DarkSide, Locky, Netwalker, REvil/Sodinokibi, and RagnaLocker, received considerably smaller payments.

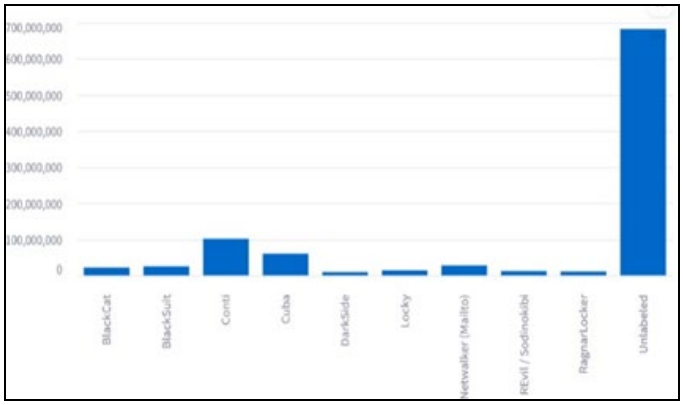

Fig 3: Distribution of Ransomware Families by USD Payments

The Bitcoin Ransomware Payment Analysis Dashboard, as shown in Figure 4, provides an interactive interface for analyzing ransomware-related Bitcoin transactions. The dashboard includes filtering options such as year selection, ransomware family selection, and transaction amount range (BTC) to refine the displayed data. The data table presents key transaction details, including Bitcoin addresses, transaction count, total transaction value in USD, transaction frequency, and risk scores. Addresses with a higher transaction count and total USD value suggest greater involvement in ransomware payments. A noticeable trend in the dataset is that a few addresses handle significantly large transaction volumes, implying their crucial role in ransomware-related Bitcoin payments. The risk score metric is particularly useful for identifying suspicious addresses that require further scrutiny. This dashboard enables users to track ransomware payments, detect high-risk transactions, and conduct deeper investigation into Bitcoin-based ransom activities.

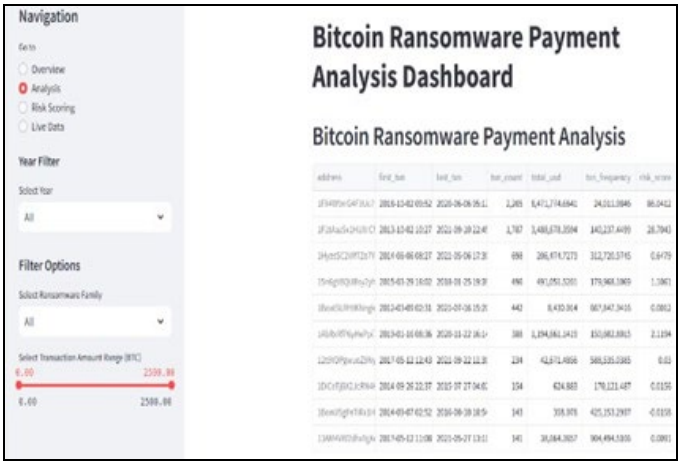

Fig 4: Bitcoin Ransomware Payment Analysis Dashboard

The Risk Label Distribution, as shown in Table 1, categorizes transactions into two groups: Low-Risk and High-Risk. The dataset contains 20,757 low-risk transactions and 1,045 high-risk transactions, indicating that the majority of transactions are considered low risk. The high-risk category remains crucial for further analysis and investigation, as these transactions could involve significant ransom payments, laundering activities, or other illicit financial movements.

Table 1: Risk Label Distribution

	Risk Label	Count
0	Low Risk	20,757
1	High Rsik	1,045

The Ransomware Transaction Network Analysis, as shown in Figure 5, visualizes Bitcoin transactions linked to ransomware payments. Each node represents a Bitcoin address, while edges show fund transfers, helping identify key addresses in the ransom payment chain. The left panel allows navigation through different sections like "Analysis" and "Risk Scoring," with filters for year, ransomware family (e.g.,Qlocker), and transaction amount range. This analysis helps investigators track ransom payments, uncover hidden connections, and support law enforcement in disrupting cybercriminal financial operations.

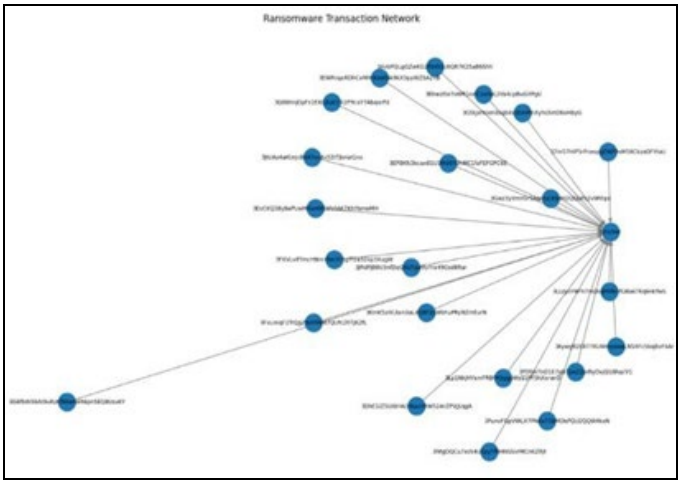

Fig 5: Ransomware Transaction Network Analysis

The Monthly Ransomware Activity Trend, as shown in Figure 6, visualizes the total ransom paid in USD across different months. The box plot represents the distribution of ransomware payments, where each box shows the interquartile range (IQR), and the whiskers extend to 1.5 times the IQR. Outliers, represented as individual points, highlight exceptionally high ransom payments. This visualization helps analysts identify seasonal trends in ransomware payments, uncover peak ransom payment months, and detect anomalies. Such insights can assist cybersecurity professionals and law enforcement in anticipating ransomware activity and allocating resources effectively to combat cyber threats.

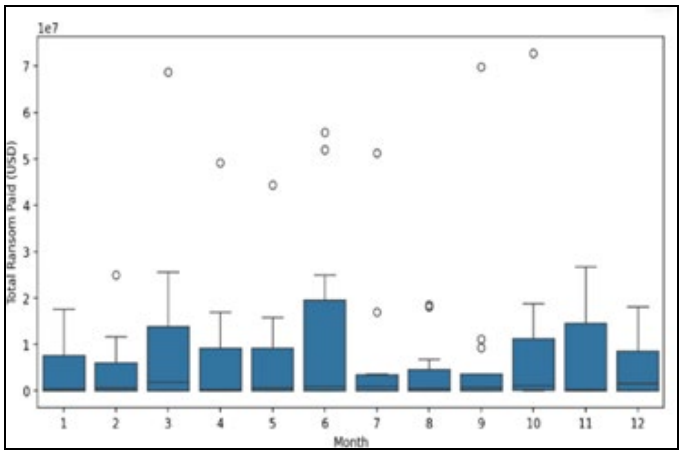

Fig 6: Monthly Ransomware Activity Trend

7. Algorithm Specification

i). Model Selection

The model selection and evaluation process is a crucial step in ensuring the accuracy and reliability of ransomware transaction classification and anomaly detection. This study employs both supervised and unsupervised learning techniques to assess and predict ransomware-related risks effectively.

a) **Risk Prediction Model:** For ransomware risk prediction, Random Forest Classifier is choosen as the final model due to its superior performance in handling structured time-series data. One of the key reasons for selecting this model is its high accuracy and stability, as it combines multiple decision trees to reduce overfitting while improving predictive performance. Since ransomware attack trends are often non-linear and complex, Random Forest effectively captures these patterns by leveraging multiple decision paths. Additionally, this model is well-suited for both small and large datasets, ensuring robust performance even when limited ransomware transaction data is available for certain time periods.

Another major advantage of using Random Forest is its feature importance analysis, which helps identify key factors that influence ransomware payments, leading to more informed decision-making. Furthermore, compared to single decision trees, Random Forest generalizes better to unseen data, making it highly reliable for predicting high-risk.

b) **Anomaly Detection Model:** For anomaly detection in Bitcoin transactions, the Isolation Forest algorithm is selected due to its effectiveness in identifying outliers based on transaction behavior. This unsupervised learning technique isolates anomalies by recursively partitioning the dataset, making it well-suited for detecting irregular patterns in financial transactions.

One of the primary advantages of Isolation Forest is its efficiency in handling large transaction datasets while

maintaining a low computational cost. Unlike traditional clustering-based methods, Isolation Forest does not require prior knowledge of normal transaction distributions, making it highly adaptable to evolving ransomware tactics.

i). Model Evaluation

Evaluation Metrics Performance

Performance evaluation metrics for Ransomware Risk Prediction involve assessing the effectiveness of our machine learning model on a validation set or test dataset using various metrics.

Key Metrics:

- **Accuracy:** The ratio of correctly predicted instances to the total instances, providing an overall measure of model performance.
- **Precision:** The ratio of correctly predicted high-risk ransomware months to the total predicted high-risk months, indicating how precise our model is in identifying ransomware risk.
- **Recall (Sensitivity):** The ratio of correctly predicted high-risk ransomware months to all actual high-risk months, measuring how well the model identifies risky periods.
- **F1-Score:** The balance between precision and recall, showing how well the model identifies high-risk ransomware months. It is useful when data is imbalanced, ensuring both accuracy and completeness.

Table 2: Evaluation metrics comparison between the algorithms.

Algorithm	Accuracy	Precision	Recall	F1-Score
Random forest classifier	85	0.88	0.70	0.78
Logistic Regression	81	0.73	0.80	0.76

The figure 7, illustrates the anomaly score distribution generated by the Isolation Forest model, with the x-axis representing anomaly scores and the y-axis showing transaction frequency. The histogram reveals that most transactions are clustered around higher anomaly scores, while fewer transactions have lower scores. The overlaid density curve provides a smooth representation of this distribution, indicating how the model differentiates between normal and anomalous transactions. The clear separation between normal and high-anomaly transactions suggests that the model effectively captures transaction patterns. A strong ROC-AUC score further supports the model's ability to rank anomalies correctly. This visualization helps in fine-tuning anomaly detection thresholds and ensures that the model is making reliable predictions.

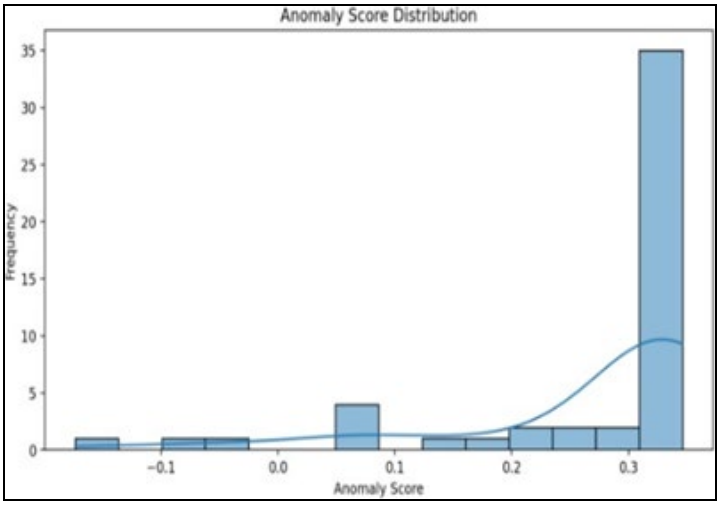

Fig 7: Anomaly Score Distribution

9. Result

Risk Prediction

The ransomware risk prediction model employs a Random Forest Classifier, known for handling complex attack patterns and delivering stable results. With an accuracy of 85%, the model effectively forecasts high-risk months based on historical ransomware data. The dataset is preprocessed to ensure consistency, including data cleaning, feature engineering, and normalization. Key features such as attack frequency, transaction values, and attack types are used to train the model. By constructing multiple decision trees, the classifier determines high-risk periods through an ensemble approach, enhancing predictive reliability.

As shown in Table 3, the model predicts elevated ransomware activity in March, May, June, and July 2026. This insight allows organizations to proactively enhance cybersecurity defenses, allocate resources effectively, and mitigate potential threats. By leveraging machine learning, security teams can implement preventive measures in advance, reducing the impact of ransomware incidents during these critical periods.

Table 3: Predicted High-Risk Months for Ransomware Attacks

Year	Month	Risk Prediction
2025	3	1
2025	5	1
2025	6	1
2025	7	1

Live Dashboard

The system monitors live Bitcoin transactions to detect potential ransomware-related payments using real-time blockchain data retrieval and anomaly detection. It fetches unconfirmed Bitcoin transactions via the Blockchain.info API, extracts key details, and converts BTC to USD using the CoinGecko API for accurate valuation.

Anomaly detection is performed using the Isolation Forest algorithm, which flags suspicious transactions based on deviation from normal patterns. Sensitivity is adjustable with contamination rates of 5%, 10%, and 15%. The dashboard visualizes anomalies through histograms and box plots, highlights the top five ransomware wallets based on total

BTC transacted, and dynamically computes the total ransom paid in USD. Streamlit presents this data in an interactive format, enabling real-time risk assessment and transaction monitoring.

The output fig 8, displays a real-time dashboard for tracking Bitcoin transactions. It features a live transaction table showing the hash, timestamp, and BTC amount of recent unconfirmed transactions. At the bottom, the live Bitcoin-to-USD conversion rate (e.g., 84,636 USD per BTC) is displayed for estimating the USD value of transactions. This dashboard provides a dynamic view of Bitcoin transactions, aiding in financial analysis and monitoring.

Fig 8: Live Bitcoin Transaction Table

The output fig 9, displays a real-time dashboard for tracking ransomware payments. It highlights the Top 5 Most Active Ransomware Wallets, showing wallet hashes and the amount of Bitcoin (BTC) associated with each. Below, the Total Ransom Paid in USD is dynamically updated based on the live BTC-to-USD conversion rate. In this instance, the total ransom paid is
$1,394,112.02 USD. This dashboard provides a critical view of ransomware activity, aiding in financial crime investigations and cybersecurity monitoring.

Fig 9: Top 5 Most Active Ransomware Wallet

The output fig 10, displays a real-time dashboard detecting Flagged Anomalous Bitcoin Transactions at 5.0% and 10.0% contamination rates. The first table lists flagged transactions at 5.0%, while the second expands detection to 10.0%, capturing more anomalies. This dashboard aids in identifying suspicious activities, supporting fraud detection, cybersecurity, and financial crime investigations.

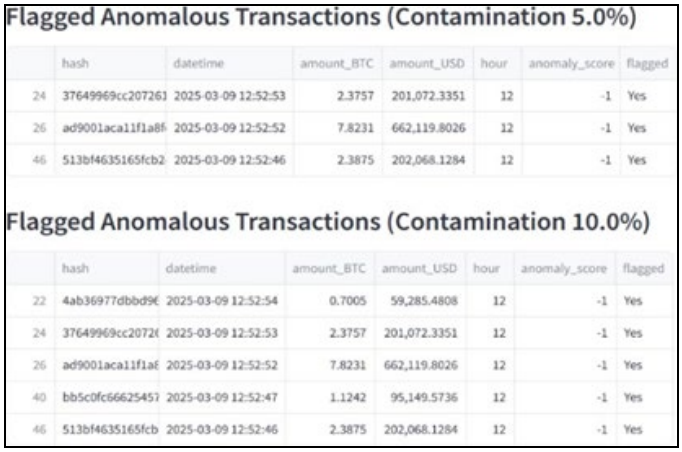

Fig 10: Flagged Anomalous Transaction Table at 5.0% and 10.0%.

The output fig 11, displays a histogram showing the distribution of normal vs. anomalous Bitcoin transactions at different contamination rates (5%, 10%, and 15%). The x-axis represents the transaction amount in BTC (log scale), while the y-axis represents the frequency of transactions. Different colors distinguish between normal and anomalous transactions at each contamination rate. This visualization helps in identifying patterns and outliers in Bitcoin transactions, aiding in fraud detection and anomaly analysis.

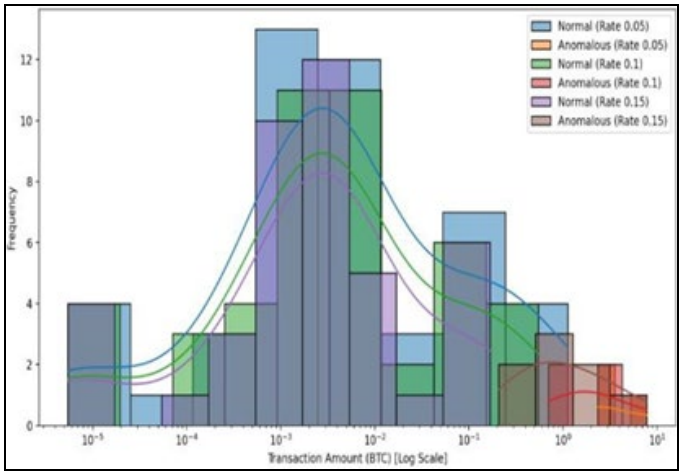

Fig 11: Normal Vs Anomalous Transactions

10. Conclusion

The Bitcoin Ransomware Payment Analysis and Risk Detection System provides a crucial solution for detecting and analyzing suspicious Bitcoin transactions linked to ransomware activities. By leveraging real-time blockchain data and machine learning-driven anomaly detection, the system enhances financial security and equips cybersecurity professionals with actionable insights to combat digital extortion. Unlike traditional manual tracking methods, this system continuously retrieves live transaction data, flags anomalies dynamically, and visualizes risks through an interactive Streamlit dashboard. The integration of risk scoring further improves threat assessment by analyzing historical transaction patterns. Additionally, the ability to adjust contamination thresholds ensures adaptability to evolving ransomware tactics. The system's intuitive reporting and visualization features streamline transaction monitoring, facilitating faster and more effective responses. Ultimately, this project offers a scalable and automated approach to mitigating ransomware threats, reinforcing the need for

advanced cybersecurity frameworks in financial crime prevention.

References

1. M. Ul Hassan, Rehmani MH and Chen J. "Anomaly detection in blockchain networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.* 2023; 25(1):289-318.
2. Pahuja L and Kamal A. "Enlfade: Ensemble learning-based fake account detection on Ethereum blockchain," *SSRN Electron. J.* 2022; 54(6)1-37.
3. Aziz RM, Baluch MF, Patel S, and Ganie AH. "LGBM: A machine learning approach for Ethereum fraud detection," *Int. J. Inf. Technol*. 2022; 14(7):3321-3331.
4. Akcora CG, Li Y, Gel YR, and Kantarcioglu M. "BitcoinHeist: Topological data analysis for ransomware detection on the Bitcoin blockchain," *IEEE Trans. Inf. Forensics Secur.* 2020; 15:2220-2235.
5. Dalal S, Wang Z. and Sabharwal S. "Identifying ransomware actors in the Bitcoin network," *arXiv preprint arXiv:2108.13807*, 2021.
6. Nkongolo M. "Ransomware detection dynamics: Insights and implications," *arXiv preprint arXiv:2402.04594*, 2025.
7. Gupta A, Wang H and Lee T. "Machine learning-based cryptocurrency fraud detection: A systematic review," *ACM Comput. Surv.* 2023; 55(8):1-29.
8. Brown J and Peterson L. "Blockchain security risks and detection methodologies," *J. Cybersecurity Res.* 2022; 12(3):77-98.
9. Sharma KR and Verma P. "Ransomware attack detection using deep learning techniques," *IEEE Access*. 2023; 11:78245-78260.
10. Chen Y, Sun X and Liu J. "Uncovering illicit financial transactions in the Bitcoin network," *J. Finance & Cybercrime*. 2022; 10(2):233-256.
11. Vasilomanolakis E, Anderson R and Meisner P. "A large-scale empirical analysis of ransomware activities in Bitcoin," *ACM Trans. Priv. Secur.* 2022; 25(4):1-30.
12. Saad M, Wahsheh LA and Mohaisen A. "Estimation of ransomware payments in the Bitcoin ecosystem," *SSRN Electron. J.* 2021; 56(2):1-22.
13. Gray IW, Cable J, Brown B, Cuiujuclu V and McCoy D. "Money over morals: A business analysis of Conti ransomware," *arXiv preprint arXiv: 2305.11681*, 2023.
14. Foster K and Zhang D. *Blockchain Forensics and Financial Crime Prevention*, 1st ed., Springer, 2023.
15. Johnson RN. *Cybercrime and Cryptocurrency: Investigating Illicit Financial Activities*, Oxford University Press, 2022.