Bitcoin Heist Ransomware Attack Prediction Using Machine Learning

Maanaswini K[1], Akila G[2], Sneka S[3], Tejavii D[4]
[1, 2, 3, 4] Meenakshi Sundararajan Engineering College

Abstract- *Bitcoin is a cryptocurrency, or digital asset, that operates like real money and can be used to make payments without being controlled by any one person, organisation, or other entity. As a result, it eliminates the need for third parties to get involved in financial transactions. It runs on a decentralised network, which means that a centralised entity like a government or bank does not have control over it. In recent years, ransomware attacks have become a significant source of malware intrusion. The idea of the work is to present a ransomware attack prediction techniques that uses machine learning algorithms such as Logistic regression, Random forest classifier, XGBoost classifier and Voting classifier. The accuracy of these machine learning algorithms is compared to the accuracy of the pre-processed data to determine which algorithm performed better. Other performance metrics, such as precision, recall, and f1-score are also taken into account when evaluating the model. The outcome of the ransomware attack is predicted using a machine learning model.*

Keywords- Logistic regression, Random forest classifier, XGBoost classifier, Voting classifier

I. INTRODUCTION

Bitcoin is the most popular cryptocurrency followed by ethereum, binancecoin, cardano. It emerged as the first digital coin to be launched in the crypto currency market. Bitcoin also referred as crypto currency can be used for buying or selling goods or services with vendors those who accept bitcoin as payment. Crypto currency is operated in a decentralised network where there is no central authority like banks or government to monitor the transactions [6]. It uses cryptography to secure and verify the transactions. That is it uses encryption and decryption to perform verification. During encryption the message or the information is converted to a changing combination of zeros and ones and one needs a decryption key to retrieve or to view those information. The value of bitcoin is increasing day by day and it mainly depends on the number of users.

Bitcoin operates in the blockchain technology. Blockchain technology operates in a decentralised network and the transaction is viewed by all users present in the network. It is a distributed ledger system in which the transaction that is carried out from one user to the other user is noted down on pages and these pages are known as blocks. Each transaction is given a hash value.

Ransomware attack is a type of attack in which the personal and private information of the user is encrypted by the attacker and the attacker demands for a certain amount of ransom to be paid inorder to provide the decryption key. It is a malware in which the attacker can access the files of the user's system. This malware takes the entire power of the control and communication centre of the system. [4] There are totally five types of Ransomware attack:

- Crypto Attack:

This type of Ransomware attack encrypts all the parts of data in the system and releases these informations only by doing ransom payment to them. The victim's screen will only display a ransom note stating the details and instructions to be followed by the user in order to do the ransom payment.

- Cryptolocker Attack:

This type of attack is caused when the attacker sends the malware through a recognised website, by doing so the user will trust the source and eventually gets struck into the ransomware malware. The major cause for this attack is phishing emails which has malicious attachments in it.

- Cryptowall Attack:

This type of attack is more common form of Ransomware attack. It is a type of Trojan horse attack in which the Trojan viruses download the malware by downloading any form of pdf or documents. These viruses are very cheap to use and they end up by paying huge ransom payment. This attack is well known for it's strong algorithm making it difficult to recover the informations or files without making a ransom payment.

- Locky Attack:

It is a type of attack in which an email is sent to the user that contains Ms word documents attached, which are difficult for the user to understand and prompts the user to enable the macrons. Once it is deployed, the virus loads the system memory and control centre [1].

- Cerber Attack:

It is a service based attack which takes place only in areas of weak firewall. The attacker aims at finding the loopholes in the firewall and encrypts the data present in it. This attack infects computers through spam emails that target vulnerabilities in the software.

II. RELATED WORK

In [1] the authors studied that the crypto locker attack is carried out in large number than it is expected. In [2] the researchers have analysed that the absence of middle-man for monitoring the transactions in the decentralised network,has increased the complexity in finding out the attackers.

In [3] the author analysed and compared the previous papers and concluded a survey on detection of ransomware attacks in bitcoin transaction and it's classification. In [4] the author in uses context aware AI for the predictive analysis of ransomware attacks in the IoT systems.

In [5] the author describes about the machine learning algorithm XGBoost and the impact of the system and the importance of tree boosting of this classifier. The authors studied about the decentralised network and the need for introducing bitcoin design. Further discussion on the existing system contribution and the introduction of bitcoin protocol in eliminating centralised authority such as banks are [6].

By evaluating the authentic Bitcoin system, this work evaluates the privacy of Bitcoin. It is the first piece of study to analyse and assess Bitcoin's privacy perspective. The study's findings indicate that, because Bitcoin is a digital currency, the present safeguards put in place to protect user privacy are insufficient [7].

The ransomwares are basically categorised in [8] this paper depending on their behaviour. A total of 150 ransomware samples from ten unique ransomware families are taken into consideration.

In this work [9], the system analysis of how and when the Bitcoin flows from one transaction to another one, the Bitcoin system was evaluated by its usability study which was collected from the feedback of nine people in which two of them are detectives investigating financial crimes. This paper states that the block chain technology is decentralised, transparent, secure, and trustworthy. Blockchain technology plays the most important role in uplifting the crypto currencies [10].

In [11] this work explains that the ransomware attack is a growing threat that encrypts user's files and only by using a decryption key the files are retrieved. This decryption key is sent only when a certain amount of ransom payment is paid by the victim. The experiment tests CryptoDrop against four hundred and ninety two real world ransomware samples and find an accurate 100% detection rate.

III. PROPOSED METHODOLOGIES

This section briefly covers the dataset data preprocessing, data visualization, logistic regression, Random forest classifier, XGBoost classifier, Voting classifier and deployment.

The Source data that includes the data of previous ransomware attacks are collected together and those data are subjected for preprocessing to remove noise and the data are given to each algorithm that predicts independent of the other. Logistic regression, XGBoost and Random forest classifier predicts the type of attack individually and then the voting classifier combines the results of all the other algorithms and finally gives the highly accurate results. Voting classifier takes the majority of the algorithms which predicts the same to give the final result. By using voting classifier algorithm, the output which is predicted sustains.

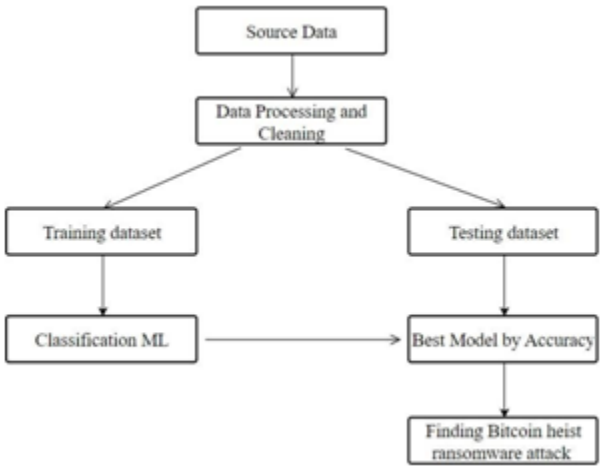

Fig. 1. Basic flow diagram

In Fig. 1 shows the workflow diagram of the methodology followed in this study.

A. Data preprocessing

The first stage is preprocessing, which includes missing value, duplicate value and description of data type whether it is float variable or integer. The Python pandas library is used to carry out the various data cleaning tasks. The analysis of one, two, or more variables is used to identify the variables.

B. Data visualization

Data visualization deals with visual representation of data. It graphically plots the data and is an effective way to communicate inferences from data. The data is presented visually, such as in charts and plots, through data visualisation and exploratory data analysis.

C. Logistic Regression

Classification tasks use logistic regression. It is a statistical technique that examines a dataset that contains one or more independent variables and forecasts a result or a binary variable depending on input variables. Dependent variable present in a logistic regression is binary, meaning there exists only two possible results, such as Yes/No or True/False. Instead of giving the exact value as 0 and 1, it gives the probabilistic values which lie between 0 & 1.

D. Random forest classifier

Random Forest Classifier is an ensemble learning technique that combines multiple decision trees to create a strong predictive model. The Random Forest Classifier makes a final prediction by building multiple decision trees and combining their results. A random subset of the training data and a random subset of the features are used to construct each decision tree. This enhances the generalisation of the model and lessens overfitting [2].

E. XGBoost classifier

Extreme gradient boosting, or XGBoost, is a well-liked and potent gradient boosting algorithm used in machine learning for classification, regression, and ranking issues. It is an ensemble-based algorithm that combines a number of weak predictive models to produce a strong one. The XGBoost algorithm builds weak decision trees onto a combined model iteratively, each new tree enhancing the model's overall prediction [5].

F. Voting classifier

Voting Classifier that combines the results of various separate classifiers to produce a single final prediction. It is an ensemble learning technique that relies on the idea of majority voting to reach a conclusion. Different types of classifiers, including Random Forests, Logistic Regression, and XGBoost classifier, can be used as individual classifiers. Combining multiple classifiers is intended to increase the model's overall performance by lowering the possibility of individual errors.

G. Deployment

A software application or service is deployed when it is made available for use. It involves transferring the application from a testing environment to a live environment where users can access it.

IV. EXPERIMENTAL EVALUATION

A. Dataset

The dataset is collected from kaggle which contains 14,514 data and we have also added a duplicate row in our Data preprocessing dataset to check the flow of our project is correct. Dataset is divided into two sets- Training and Testing

- Training dataset:

The training data is fed to the ML algorithms, which lets them learn how to make predictions for the given task. Here out of the given dataset we take 10,159 data as training data.

- Testing dataset:

An independent evaluation of the final model verification for the given training data set is made using the testing dataset. Out of the 14,514 we have taken 4355 data as testing data.

B. Dataset description

- Address: String that represents the transaction address.
- Year: An integer describing the transaction's year.
- Day: An integer describing the transaction's day.
- Length: It i s the number of unsuccessful transactions in the transaction's longest chain.
- Neighbours: The transactions that comes up with this address as output.
- Count: The no. of transaction initiators that is linked to this address.
- Weight: The total amount of Bitcoin coins from a starter to start transaction that arrive at this address.

- Looped: It represents number of successful transactions that have large number of direct path leading to this address.
- Income: Integer containing the Satoshi value (one Bitcoin is equal to 100,000,000 Satoshi). The smallest unit of Bitcoin is called a Satoshi.

C. Performance measure

Finally, our proposed model's performance was measured in terms of accuracy, precision, recall, and f1_score performance metrics.

True Positive (TP)**:**True positive model correctly predicts a positive outcome when the actual outcome is positive.

False Positive (FP)**:** False positive is a term used in binary classification, where the model incorrectly predicts a positive outcome when the actual outcome is negative.

True Negative (TN): True negative is a model correctly predicts a negative outcome when the actual outcome is negative.

False Negative (FN)**:** False negative is a model that incorrectly predicts a negative outcome when the actual outcome is positive

- Accuracy: Accuracy is the ratio of the total number of correct predictions (true positives and true negatives) to the total number of predictions made by the model. It is given in (1).

$$\text{Accuracy} = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (1)$$

- Precision: It is the estimation analysis of true positive to the aggregate value of true positive and false positive rate. It is given in (2).

$$\text{Precision} = \frac{TP}{(TP + FP)} \quad (2)$$

- Recall: It is the estimation analysis of true positive rate to the aggregate value of the true positive and false negative rate. It is given in (3).

$$\text{Recall} = \frac{TP}{(TP + FN)} \quad (3)$$

- F-Score: F-Measure is the harmonic mean of recall and precision. Precision and recall are given equal weight in the standard F- measure (F1). It is given in (4).

$$\text{F1 Score} = \frac{2*(\text{Recall} * \text{Precision})}{(\text{Recall} + \text{Precision})} \quad (4)$$

V. RESULTS

The Bitcoin heist ransomware attack is predicted by the following modules:

A. Data preprocessing

In this stage, null value or duplicate value present in the input dataset is removed.

```
data.isnull().sum()
```

```
address      0
year         0
day          0
length       0
weight       0
count        0
looped       1
neighbors    0
income       0
label        0
dtype: int64
```

Fig. 2. Input data with Null value

```
df.info()
```

```
<class 'pandas.core.frame.DataFrame'>
Int64Index: 14514 entries, 0 to 14513
Data columns (total 10 columns):
 #   Column     Non-Null Count  Dtype
---  ------     --------------  -----
 0   address    14514 non-null  object
 1   year       14514 non-null  int64
 2   day        14514 non-null  int64
 3   length     14514 non-null  int64
 4   weight     14514 non-null  float64
 5   count      14514 non-null  int64
 6   looped     14514 non-null  float64
 7   neighbors  14514 non-null  int64
 8   income     14514 non-null  float64
 9   label      14514 non-null  object
dtypes: float64(3), int64(5), object(2)
memory usage: 1.2+ MB
```

Fig. 3. Input data after preprocessing

Fig 2. shows a null value is added in the looped column of the dataset and Fig 3. Shows after data preprocessing, the null value is removed.

B. Data preprocessing

The data visualisation is the pictorial representation of the dataset and gives a clear cut view of how the data in the dataset and makes it easy to understand the data.

```
Text(0.5, 1.0, 'Yearwise Count')
```

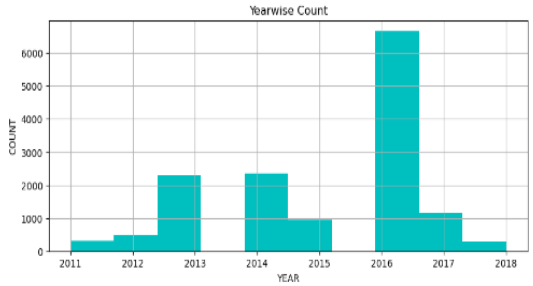

Fig. 4. Bar chart of input data

Fig. 5. Pie chart of input data

Fig 4. shows bar graph depicts the plotting of count with respect to the year of transaction and Fig 5. shows the percentage of ransomware attack that has occurred. Major attacks were carried out in the year 2016.

C. Logistic regression

```
Getting Accuracy

accuracy = accuracy_score(y_test,predicted_lr)
print('Accuracy of Logistic Regression is: ',accuracy*100)

Accuracy of Logistic Regression is:  16.670493685419057

Finding Loss

loss = hamming_loss(y_test,predicted_lr)
print('Loss of Logistic Regression is: ',loss*100)

Loss of Logistic Regression is:  83.32950631458094
```

Fig. 6. Accuracy prediction of Logistic Regression

In Fig. 6 the logistic regression predicts an accuracy of approximately 16% and comes out with a loss of 83%.

D. Random forest classifier

```
Getting Accuracy

accuracy = accuracy_score(y_test,predicted_rfc)
print('Accuracy of Random Forest Classifier is: ',accuracy*100)

Accuracy of Random Forest Classifier is:  90.42479908151549

Finding Loss

loss = hamming_loss(y_test,predicted_rfc)
print('Loss of Random Forest Classifier is: ',loss*100)

Loss of Random Forest Classifier is:  9.5752009184845
```

Fig. 7. Accuracy prediction of Random forest classifier

In Fig. 7 the accuracy prediction of random forest classifier is displayed above. This machine learning classifier predicts an accuracy of 90% and comes out with a loss of approximately 9.5%. The accuracy predicted by this classifier is higher than the previous classifier that is the logistic regression.

E. XGBoost classifier

```
Getting Accuracy

accuracy = accuracy_score(y_test,predicted_xg)
print('Accuracy of XGBoost Classifier is: ',accuracy*100)

Accuracy of XGBoost Classifier is:  91.34328358208955

Finding Loss

loss = hamming_loss(y_test,predicted_xg)
print('Loss of XGBoost Classifier is: ',loss*100)

Loss of XGBoost Classifier is:  8.656716417910449
```

Fig. 8. Accuracy prediction of Xgboost classifier

In Fig. 8 the accuracy predicted by the XGBoost classifier is displayed above. This machine learning classifier predicts an accuracy of approximately 91% and comes out with a loss of approximately 8.6%. The accuracy predicted by this classifier is higher than the previous mentioned classifiers that is the logistic regression and random forest classifier.

F. Voting classifier

```
Getting Accuracy

accuracy = accuracy_score(y_test,pred_vc)
print('Accuracy of Voting Classifier is: ',accuracy*100)

Accuracy of Voting Classifier is:  91.3203214695752

Finding Loss

loss = hamming_loss(y_test,pred_vc)
print('Loss of Voting Classifier is: ',loss*100)

Loss of Voting Classifier is:  8.679678530424798
```

Fig. 9. Accuracy prediction of Voting classifier

In Fig. 9 the final prediction of this classifier is made by taking the majority vote. Thus the voting classifier predicts

an accuracy of 91% and this is the final accuracy that is used for predicting the type of ransomware attack.

G. Deployment

The deployment is done and the output is displayed in the form of label.

Fig. 10. Prediction of CryptoWall attack

Fig. 11. Prediction of Locky attack

Fig. 12. Prediction of CryptoLocker attack

In Fig. 10, Fig. 11 and Fig. 12 shows the types of ransomware attack .

VI. CONCLUSION AND FUTURE SCOPE

This work demonstrates that significant of machine learning technology made it simple to identify relationships and patterns among the different types of data. In order to predict the ransomware attack, machine learning techniques are used to train the computer to identify particular transactions and track them back to malicious transactions. In this work, we used all 4 algorithms such as XGBoost Classifier, Random Forest Classifier, Logistic Regression, and Voting Classifier and we also considered other performance metrics, such as precision, recall, and f1-score, for assessing the model's performance. By combining the remaining three algorithms accuracy, the voting classifier performs and generates a final accuracy of 91%. The predicted ransomware attack is displayed in the form of label. In the future, it can be combined with other machine learning algorithms to build a system that is extremely reliable and potent. The effectiveness of the overall system can be improved by implementing a variety of other machine learning ideas.

REFERENCES

[1] Cuneyt G. Akcora, Yitao Li, Yulia R. Gel and Murat Kantarcioglu, "BitcoinHeist:Topological Data Analysis for Ransomware Prediction on the Bitcoin Blockchain" in proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-20)

[2] Micheline Al Harrack, "THE BITCOINHEIST: CLASSIFICATIONS OF RANSOMWARE CRIME FAMILIES" International Journal of Computer Science & Information Technology (IJCSIT) Vol 13, No 5, October 2021

[3] Sabira Karim Shemitha PA "A Survey on Detection and Classification of Ransomware Bitcoin Transactions", International Journal Of Advance Research And Innovative Ideas In Education (IJARIIE)

[4] Vytarani Mathane , P.V. Lakshmi, "Predictive Analysis of Ransomware Attacks using Context-aware AI in IoT Systems", (IJACSA) International Journal of Advanced Computer Science and Applications,

[5] Chen T and C. Guestrin, "Xgboost: a scalable tree boosting system," in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), pp. 785–794, New York, NY, USA, August 2016.

[6] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: a technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084–2123, 03 2016.

[7] Androulaki E, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in

Proceedings of the Financial Cryptography and Data Security, pp. 34–51, Okinawa, Japan, April 2013.

[8] Abraham J. A and S. M. George, "A survey on preventing crypto ransomware using machine learning," in Proceedings of the 2nd International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), vol. 1, pp. 259–263, Kannur, India, July 2019.

[9] Di Battista G, V. Di Donato, M. Patrignani, M. Pizzonia, V. Roselli, and R. Tamassia, "Bitconeview: visualization of flows in the bitcoin transaction graph," in Proccedings of the IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1–8, Chicago, IL, USA, October 2015.

[10] Yazdinejad A, H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, G. Srivastava, and M. Y. Chen, "Cryptocurrency malware hunting: a deep recurrent neural network approach," Applied Soft Computing, vol. 96, Article ID 106630, 2020.

[11] Scaife N, H. Carter, P. Traynor, and K. R.B. Butler. Cryptolock (and drop it): stopping ransomware attacks on user data. In IEEE 36th ICDCS, pages 303–312, 2016.