Hybrid-NN for Predicting the News Impact on Bitcoin price with Crypto Cyber-Attacks Analysis

Submitted in partial fulfillment of the requirements for the degree of

Bachelor of Technology

in

Computer Science and Engineering

by

Malla Jyotsna Sree Mahima (18BCE0912)

Chinthala Lavanya (18BCI0201)

Under the guidance of

Prof. Jayashree J

Scope

VIT, Vellore.

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

June, 2022

DECLARATION

I hereby declare that the thesis entitled "Hybrid-NN Model for Predicting the News Impact on Bitcoin price with Crypto Cyber-Attacks Analysis" submitted by me, for the award of the degree of *Bachelor of Technology in Computer Science and Engineering* to VIT is a record of bonafide work carried out by me under the supervision of Prof. Jayashree J.

I further declare that the work reported in this thesis has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Place : Vellore

Date : 03/06/2022

Signature of the Candidate

Malla Jyotsna Sree Mahima

Malla Jyotsna

Chinthala Lavanya

C. Lavanya

CERTIFICATE

This is to certify that the thesis entitled "Hybrid-NN Model for Predicting the News Impact on Bitcoin price with Crypto Cyber-Attacks Analysis" submitted by **Malla Jyotsna Sree Mahima & 18BCE0912**, **SCOPE**, VIT University and **Chinthala Lavanya & 18BCI0201**, **SCOPE**, VIT University for the award of the degree of *Bachelor of Technology in Programme*, is a record of bonafide work carried out by him under my supervision during the period, 03.01.2022 to 04.04.2022, as per the VIT code of academic and research ethics.

The contents of this report have not been submitted and will not be submitted either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university. The thesis fulfills the requirements and regulations of the University and in my opinion meets the necessary standards for submission.

Prof. Jayashree J.
SCOPE

Place : Vellore

Date : 03/06/2022

Signature of the Guide

Internal Examiner

External Examiner

Dr. S. Vairamuthu

School of Computer Science and Engineering

ACKNOWLEDGEMENT

We take this platform in expressing our gratefulness to everyone at VIT for being our pillar of strength throughout our B. Tech. To begin with, we would like to convey our gratitude to our mentor, Professor (Prof. Jayashree J), for being our guide. Her timely recommendations and guidance have steered our thesis to get escalated to the next higher level. Her incessant and practical advises, perspective and thought promoting comments were the guiding lights for us. Presence of the element of her immense knowledge and patience is vivid all through our thesis –Hybrid-NN Model for Predicting the News Impact on Bitcoin price and Crypto Cyber-Attacks Analysis. Her professional expertise and boundless knowledge scaffolded our thesis. Imagining our thesis without her relentless help isn't possible to us.

We sincerely would like to express our gratitude SCOPE School, Vellore Institute of Technology (VIT) for extending continuous support throughout the four years of B. Tech in developing the abilities in us.

Our gratefulness and humble thanks to our parents whose unfailing support has encouraged at all the stages of our studentship.

Student Name

Malla Jyotsna Sree Mahima-18BCE0912

Chinthala Lavanya-18BCI0201

Executive Summary

Media news constantly changes the sentiment of traders and investors in the cryptocurrency market and impacts their decisions. Data collected from various news aggregators aid in the early indication of the cryptocurrency market movement. The sentiment and public mood states can be uncovered using different techniques such as data mining, natural language processing, and opinion mining. Bitcoin plays the most dominant role in the global economy and it is extremely important to understand the correlation between News Sentiment and Bitcoin price volatility. News collections are assessed and interpreted to forecast the Bitcoin market movement Sentiment Analysis and deep-learning methods, namely Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), Bidirectional Long Short-Term Memory (BiLSTM), Bidirectional Gated Recurrent Units (BiGRU) were used for prediction modeling of bitcoin prices. Each model was considered on its ability to forecast the bitcoin early market movement using news sentiment in the Covid-19 era. BiLSTM and BiGRU achieved least MAPE scores of 2.48% and 2.36% respectively. The proposed Hybrid-NN model achieved a lowest MAPE score of 1.78%. The proposed hybrid-NN model showed better performance than the existing sentiment analysis based cryptocurrency price prediction models. The cryptocurrency market is highly vulnerable to cyber threats and cyber-attacks. A detailed study is presented on the various cyber-attacks on the cryptocurrency platform and its prevention mechanisms and practically implemented an attack manually on the Ethereum platform along with a prevention method and written a new attack that might take place in the future on the cryptocurrency platform.

CONTENTS

Page No.

List of Figures

List of Tables

List of Abbreviations

Hybrid-NN	Hybrid Neural Network
ANN	Artificial Neural Networks
RNN	Recurrent Neural Networks
LSTM	Long Short-Term Memory
GRU	Gated Recurrent Units
BiLSTM	Bidirectional Long Short-Term Memory
BiGRU	Bidirectional Gated Recurrent Units
RFE	Recursive Feature Elimination
API	Application Programming Interface
crypto	cryptocurrency

1. INTRODUCTION

Cryptocurrencies, like Bitcoin, Litecoin, and Ethereum, are digital assets, mostly used as a medium of payment . Bitcoin was introduced in 2009 and is the earliest cryptocurrency in the world. It is a peer-to-peer decentralized and electronic transaction system enabling assets to be transferred between parties anonymously without the need of a central authority like a bank, central government, country, etc. It has gained immense popularity and has attracted a huge consumer base owing to its ever-increasing market capitalization[1],[2],[3],[4].

The rise of cryptocurrencies has led to huge amounts of data generated online in various forums, blogs, social media sites, etc. This data can be used to generate useful patterns related to Bitcoin price fluctuations with the help of Machine Learning, Deep Learning, and Natural Language Processing. Quite a few researchers have got notable predictions about Bitcoin price patterns based on sentiment on social media platforms[5],[6],[7] .

The year 2021 recorded the highest number cyber attacks on the cryptocurrency platforms and over $12 billion was lost. The cryptocurrency market is highly vulnerable to cyber threats and cyber attacks.

1.1. OBJECTIVE

The objective of this study is to find solutions for some of the limitations and research gaps identified in the existing state-of-art models used for prediction of bitcoin prices and the ever-rising problem of identifying and preventing the cyber attacks on cryptocurrency platforms. The limitations and research gaps are:

- ➢ Does News have an Impact on the Bitcoin Price Volatility?
- ➢ Which model should be used for Bitcoin Price Prediction with the highest possible accuracy?
- ➢ How vulnerable are the cryptocurrency trading platforms and what are the basic countermeasures of the cyber attacks?

- Can we implement such type of an attack practically in an Ethereum Platform?

This study would help to fill the gaps identified in the existing work by developing a hybrid deep learning model for Bitcoin Price Prediction using News Sentiment Analysis, a detailed study on various cyber-attacks and their prevention mechanisms on cryptocurrency platforms, Implementing a Cyber attack along with a Prevention Method and written a New Attack that could be performed in the future.

1.2. MOTIVATION

The rising popularity of Bitcoin has garnered it a lot of media attention lately. There is an evident association between the Bitcoin price volatility and Bitcoin Sentiment in the form of news but is not still quite clear. The Impact of News on Bitcoin prices is understated. News Sentiment constantly changes the perception and sentiment of traders and investors of Bitcoin and has an impact on their decisions. Researchers have contributed several works in the field of predicting the bitcoin market movement based on sentiment analysis. However, very few focus on the capability of media news to detect Bitcoin price behavior.

The cryptocurrency wallets are highly vulnerable to cyberattacks[8],[9],[10],[11],[12],[13]. There is a lack of research in the field of the identification and prevention of cyberattacks on various cryptocurrency platforms.

These findings are starting steps that motivate the work of Predicting the Impact of News on Bitcoin Price with Crypto Cyber-Attacks Analysis.

1.3. BACKGROUND

Researchers have contributed several works in the field of predicting the bitcoin market movement based on sentiment analysis[5],[6],[7],[14],[15],[16],[17],[18],[19],[20].

In [5], the authors have forecasted the cryptocurrency price fluctuations based on tweet sentiment causality, the volume of tweets along with the daily price closings and various cryptocurrencies volumes traded. It has been found that Twitter has the ability to impact the cryptocurrency market movement.

Li et al. [6] tried extending this concept by developing a model employing Extreme Gradient Boosting Regression(XGBoost) and social media sentiment to forecast the volatility of ZClassic cryptocurrency.

In [7], Authors developed KryptoOracle to predict the next-minute bitcoin prices using current Bitcoin prices and Twitter sentiments. XGBoost was used to develop KryptoOracle because of its high speed and high performance and training simplicity.

Jain et al. in [14] tried to forecast the bi-hourly prices of various cryptocurrencies such as LiteCoin and Bitcoin taking into account the social factors. A Linear Regression model based on a large volume of neutral, negative, and positive sentiments generated from tweets bi-hourly was developed for this purpose.

The authors in [15] studied the importance of various data preprocessing methods for Twitter sentiment analysis. 16 different preprocessing techniques were tested. They stated it is important to preprocess the data using techniques such as lemmatization, replacing shortened words, removing punctuations, etc.

Research work in [16] was to detect the Twitter users using contentious words while posting tweets related to Covid-19. Their model used different ml algorithms such as Logistic Regression, Multi-Layer Perception(MLP), Support Vector Machine(SVM), and Stochastic Gradient Descent for detect such users. Random Forest was found to give the highest accuracy for the input data.

Wang et.al [17], tried comparing different models like Long Short-Term Memory and Artificial Neural Networks to analyze the cost dynamics related to Bitcoin. Their findings showed that LSTM works better than ANN to predict the future price of bitcoin.

Rizwan et.al [18], tried to outperform the state-of-art models used for Bitcoin Price Prediction like ARIMA, and LSTM. Their modeling showed that their proposed Gated Recurrent Unit model is best able to forecast the cryptocurrency prices achieving an 94.7% accuracy and an error rate of 5.3%.

Jackson et.al[19], tried to develop a BiLSTM model which would help traders and investors in deciding whether to invest in Bitcoin or not by looking at the slope of the graph. The BiLSTM model generated a graph for 30 days depicting when to invest. The model achieved a MAPE score of 13%.

Gupta et.al[20], tried to show the effect of Sentiment Classification on the volatility of stock markets. Their findings showed that adding sentiment(VADER) to stock markets prediction helped increase its accuracy.
Work has been contributed by researchers in the field of detection and prevention of cyber-attacks and cyber-threats on the cryptocurrency platforms[8],[9],[11],[12],[13],[10],[21].

Salman et al. [8] examines blockchain-based security approaches for various security services like privacy, confidentiality, authentication, access control list, and Provenance and gives insights about its use in current blockchain applications and discussed on how blockchain technology can solve attacks.

The authors in [9] developed a model in which a company’s cyber threat risk is optimal. They focused on how successful cyberattacks have a detrimental effect on the stock prices. Various Android systems have a low level of security. Because of these characteristics, Android smartphones are the most commonly affected by malware.

According to a survey published in [11], two-thirds of mobile malware targets Android handsets. This study depicts how vulnerable Android is to malware. As a result, it necessitates the implementation of proper security solutions to handle the problem promptly.

Zhang et al. [12] presents an overview of privacy and security involved in a decentralized platform. They first discussed the use of blockchains in the bitcoin for making online transactions and also described the bitcoin requirements like basic security properties and applications. However, only a few blockchain attacks are discussed. They explained the security techniques used in blockchain.

In the study [13] , the authors examined the security risks and vulnerabilities that exist in cryptocurrencies, threat exposures, mainly working upon cases of privacy of users .At several levels, they explored the types of assaults performed on Blockchain Technology. Finally, they provided the possible directions on countermeasures for Blockchain security vulnerabilities.

2. PROJECT DESCRIPTION AND GOALS

2.1. PROJECT OVERVIEW

Bidirectional GRU(BiGRU) is an extension of the GRU, a recurrent neural network consisting of input and forget gates. BiGRU uses two GRUs to take input in both forward and backward directions and works extremely well with time-series data. Bidirectional LSTM(BiLSTM) is an extension of the LSTM, a recurrent neural network consisting of input and forget gates. BiLSTM uses two LSTMs to take input in both forward and backward directions and works extremely well with time-series data. This work proposes a Hybrid-NN Model composed of BiLSTM , BiGRU layers for bitcoin price forecasting using news sentiment analysis along with a study of various cyberattacks on cryptocurrency platforms. The neural network framework is composed of various steps. Sentiment analysis in the second step is done on the preprocessed news headline data. In the third step various deep learning algorithms are used to find the most efficient algorithm for prediction. The best performing algorithms are chosen to develop the Hybrid Model. This model shows that it is able to outperform the various other models in its accuracy. It can be used as a reliable Bitcoin Price Predictor to understand patterns in Bitcoin price movement.

Securing our digital wallets from cyber-criminals by knowing the safety precautions and keeping our system up-to-date is mandatory to protect from vulnerabilities. In this work, through in-depth research, we analyzed the cyber threats that are performed on cryptocurrency platforms and in exchange wallets along with their prevention mechanisms and Implemented an attack practically on an Ethereum platform along with a prevention technique, and written a new attack that could be performed in the future on the cryptocurrency platform.

2.2. ARCHITECTURE DIAGRAM AND MODULES DESCRIPTION

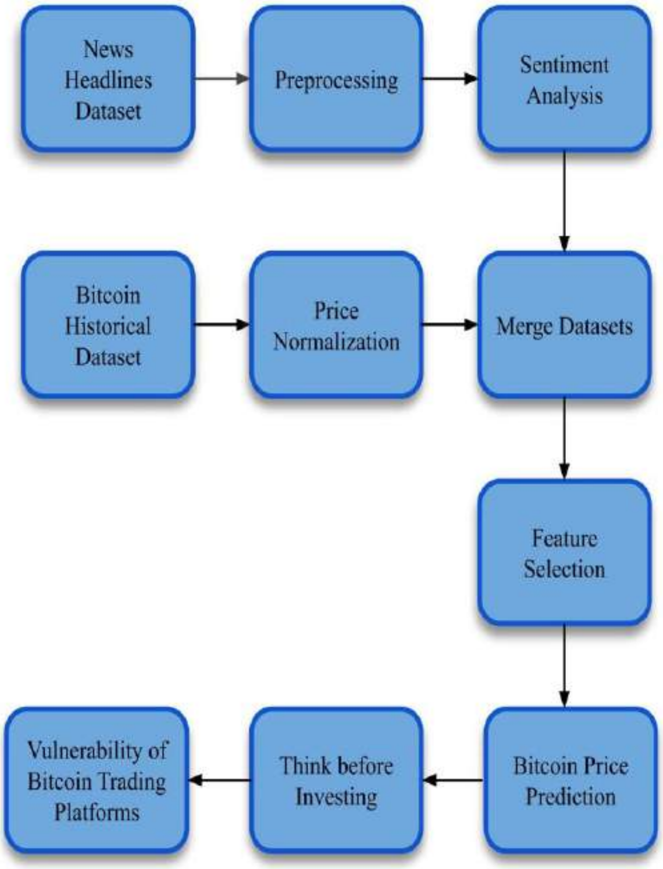


Fig 1. Architecture Diagram

2.3. HYBRID BITCOIN PRICE PREDICTION MODEL

Various steps are involved in the modelling of the Bitcoin Price Prediction Hybrid Model. In the first step, News headline articles are scraped from Newsapi.org and the Bitcoin Historical dataset is scraped from CryptocompareAPI.com.

In the second step various text preprocessing techniques are applied on the News Articles Dataset and then the News Sentiment is calculated using Sentiment Analysis scoring techniques.

Various RNN deep-learning models are compared for their accuracy in the Bitcoin Price Prediction and lastly the best performing algorithms are chosen for developing the hybrid model.

2.3.1. NEWS ARTICLES DATASET PREPROCESSING

To use a large dataset for prediction modeling such as the news headlines dataset, before modeling the data needs to be properly clean and processed to increase the overall accuracy of the model and to decrease the computational time involved in prediction. Removing the Stop words and Text Stemming are some of the techniques for preprocessing text-based data [22],[23],[24],[25].

a. Text-Lemmatization

Text-Lemmatization is a text preprocessing technique widely used in text-mining, information- retreival systems. This technique extracts the root or the stem form of the word by removing the word and grammar conjugations. This helps in faster searching of these words. It also helps to reduce the total sum of distinct words since various word forms have the same meaning. Lesser the variability in text data the lesser time it takes for processing the data and generates the output faster in Natural Language Processing systems. It removes similar meaning words from the data and all the resulting words in the data have different meanings.

b. Removing Stop Words

Stop words of text data appear quite regularly and are mostly helpful in conjugating the sentences. They do not add significant meaning to the text thereby can be safely ignored. They can be removed to decrease the quantity of text data which would otherwise hinder fast information retrieval and data processing in Natural Language Processing applications. Commonly occurring stop words in text data are ’is’, ’a’, ’are’, ’the’ etc.

2.3.2. SENTIMENT ANALYSIS USING TEXTBLOB

Sentiment Analysis helps to understand the emotions and sentiment of the data and generate hidden patterns based on the context. It helps to analyze the data and classify it depending on the needs of the work [26],[27].

TextBlob is a Natural Language Processing Python Library mainly used for sentiment analysis and performing complex tasks on text data. It returns the subjectivity and polarity of data. [-1,+1] is the range of polarity values. +1 indicated a positive sentiment and -1 indicates a negative sentiment. Subjectivity expresses the quantity of personal information and facts contained in the data. The higher the subjectivity, the higher is the amount of personal information contained in the text. Its values range between [0,1].

2.3.3. FORECASTING DEEP LEARNING MODELS

Different machine learning algorithms to analyze how the social factors can be an indicator of bitcoin and other cryptocurrency's market movements. Research depicts different RNN models are commonly used for developing the cryptocurrency market movement prediction model [28],[29].

a. Long Short-Term Memory(LSTM)

LSTM is an improved model of Vanilla RNN. It was developed to get rid of the vanishing gradient problem. The network of LSTM included 3 gates namely input, output and forget gates. It also includes a cell state which carries the data from the earlier stages to the later stages without losing any of it.

b. Gated Recurrent Units(GRU)

A newer version of RNN is GRU. The working of it is similar to LSTM but it works faster than LSTM because it does not contain the cell state. It contains 2 gates namely the reset and update gates. It works faster for smaller datasets since the information is directly stored in the memory.

c. Bidirectional Long-Short Term Memory(BiLSTM)

It contains two LSTM units. This helps to increase the total information in the network as one LSTM unit processes the input data in forward direction and the second unit processing it in backward direction.

d. Bidirectional Gated Recurrent Units(BiGRU)

BiGRU is an improved variation of GRU. It contains two GRU units. This helps to increase the total information in the network as one GRU unit processes the input data in forward direction and the second unit processing it in backward direction.

2.3.4. PROPOSED SYSTEM MODEL

In this chapter we discuss about Hybrid-NN Model for Bitcoin Price Prediction System and system flow of execution of the actors and operations with help of UML diagrams.

USE CASE DIAGRAM

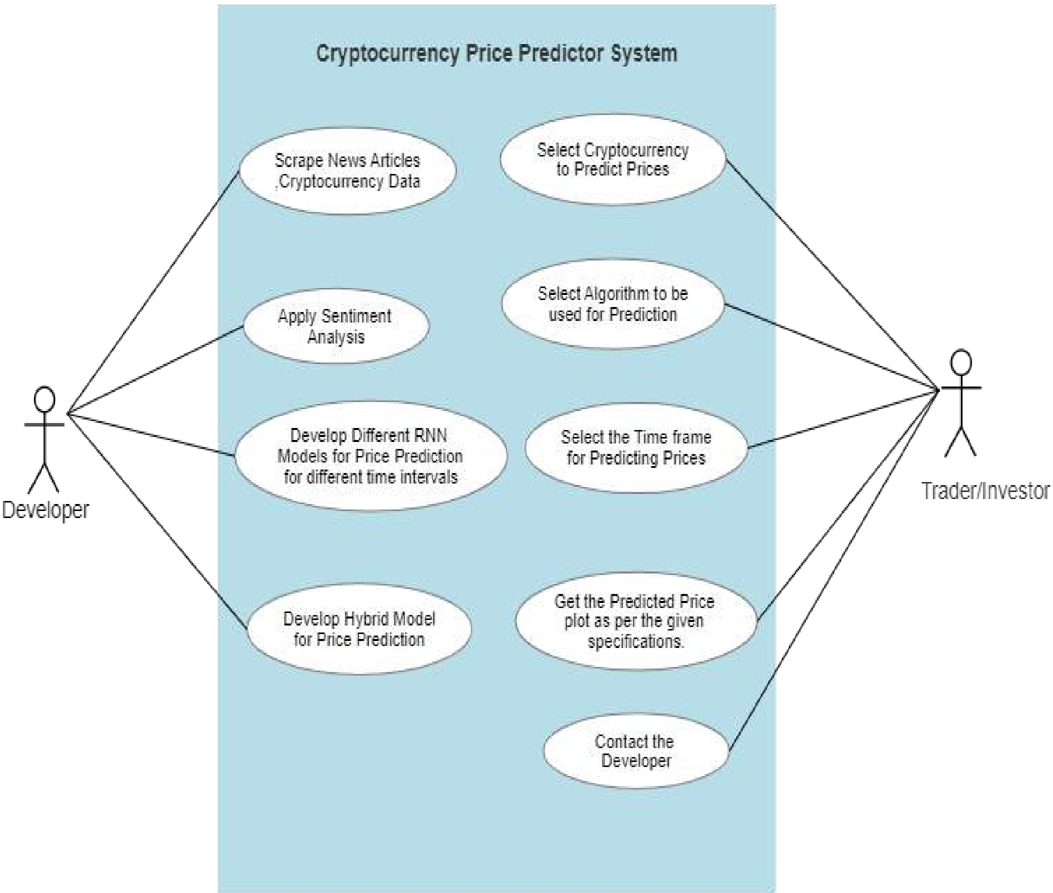

Cryptocurrency Price Predictor System
Scrape News Articles ,Cryptocurrency Data
Select Cryptocurrency to Predict Prices
Apply Sentiment Analysis
Select Algorithm to be used for Prediction
Develop Different RNN Models for Price Prediction for different time intervals
Select the Time frame for Predicting Prices
Develop Hybrid Model for Price Prediction
Get the Predicted Price plot as per the given specifications.
Contact the Developer
Developer
Trader/Investor

Fig 2. Use-Case Diagram for Bitcoin Price Prediction System

Actors

There are two main actors in the Cryptocurrency Price Predictor System namely the Developer and the Trader/Investor.

Actor : Developer

Table 1. Description of Actor Developer

Name	**End User**
Actor	Developer
Description	Here, the developer’s main tasks are to scrape News Articles dataset and Bitcoin Historical Dataset. Then pre-processing techniques are to be applied on the dataset. Sentiment Analysis is to be done to get the News Sentiment. Various RNN models are to be compared and the best performing algorithms are to be choosen to develop the hybrid model.

Actor : Trader/ Investor

Table 2. Description of Actor Trader/Investor

Name	End User
Actor	Trader/Investor
Description	Here, the trader’s main role is to analyse the Cryptocurrency Price Trends to make strategic trading decisions. He can choose the cryptocurrency he wants the prediction for and then choose the algorithm to be used and the time frame for which he requires the price prediction for. According to the specifications given a Price Prediction plot is shown for the chosen cryptocurrency, choosen algorithm and choosen time frame.

Use Cases

Use Case 1:

Table 3. Use-Case table of UC_01

Use Case ID:	UC_ 01_ Scrape News Articles ,Cryptocurrency Data
Use Case Name:	Scrape News Articles ,Cryptocurrency Data
Summary	This use case describe that the Developer needs to scrape Cryptocurrency data and News Articles data.
Actors	Developer

Use Case 2:

Table 4. Use-Case table of UC_02

Use Case ID:	UC_ 02_ Apply Sentiment Analysis
Use Case Name:	Apply Sentiment Analysis
Summary	This use case describe that the Developer needs to apply Sentiment Analysis on the News Articles Dataset.
Actors	Developer

Use Case 3:

Table 5. Use-Case table of UC_03

Use Case ID:	UC_ 03_ Develop Different RNN Models for Price Prediction for different time intervals
Use Case Name:	Develop Different RNN Models for Price Prediction for different time intervals
Summary	This use case describe that the Developer needs to develop Prediction models for different RNN algorithms.
Actors	Developer

Use Case 4:

Table 6. Use-Case table of UC_04

Use Case ID:	UC_ 04_ Develop Hybrid Model for Price Prediction
Use Case Name:	Develop Hybrid Model for Price Prediction
Summary	This use case describe that the Developer needs to develop the Hybrid Model for Cryptocurrency Price Prediction.
Actors	Developer

Use Case 5:

Table 7. Use-Case table of UC_05

Use Case ID:	UC_ 05_ Select Cryptocurrency to Predict Prices
Use Case Name:	Select Cryptocurrency to Predict Prices
Summary	This use case describe that the Trader need to select the required Cryptocurrency for Price Prediction.
Actors	Trader

Use Case 6:

Table 8. Use-Case table of UC_06

Use Case ID:	UC_ 06_ Select Algorithm to be used for Prediction
Use Case Name:	Select Algorithm to be used for Prediction
Summary	This use case describe that the Trader need to select the required RNN algorithm for Cryptocurrency for Price Prediction.
Actors	Trader

Use Case 7:

Table 9. Use-Case table of UC_07

Use Case ID:	UC_ 07_ Select the Time frame for Predicting Prices
Use Case Name:	Select the Time frame for Predicting Prices
Summary	This use case describe that the Trader need to select the required time frame for Cryptocurrency for Price Prediction.
Actors	Trader

Use Case 8:

Table 10. Use-Case table of UC_08

Use Case ID:	UC_ 08_Get the Predicted Price plot as per the given specifications.
Use Case Name:	Get the Predicted Price plot as per the given specifications.
Summary	This use case describe that the Trader will get the Prediction Price plot of his choosen cryptocurrency according to the choosen algorithm for the choosen time frame.
Actors	Trader

2.4. VULNERABILITY ANALYSIS ON CRYPTOCURRENCY PLATFORMS

There is a strong requirement to be careful about the ever-rising cyber-crimes in the cryptocurrency trading platforms. A detailed study is presented on the latest cyber-attacks and their respective counter-measures. A case-study is presented on the most recent and biggest cyber-attacks on the cryptocurrency trading platforms.

2.4.1. TYPES OF CYBER ATTACKS ON CRYPTOCURRENCY PLATFORMS

A detailed case-study is presented on the types of cyber attacks along with their prevention mechanisms, and the recent cases of cyber attacks on the cryptocurrency platforms.

a. Crypto-clipping attack

Crypto-clipping is stealing cryptocurrency by a hacker when a victim makes a transaction. By the use of malware, which automatically replaces the recipient's wallet address with the attacker's wallet address. Figure 1 , shows the architecture of this attack. The malware can be downloaded by an innocent third- party apps/ PDF reader on the victim's device and monitor's victim's device clipboard where the wallet address is copied. Just like how we enter the intended recipient account number to make the payment in banks, in blockchain organizations we enter the recipient's public address by copying it to make a transaction, When the victim pastes the recipient's wallet address, he unknowingly pastes the attacker's wallet address and makes the transaction. The basic first prevention would be double checking the wallet address to whom we need to send and before sending a large cryptocurrency amount, it's safe to send a small amount to ensure that the amount has reached the right person to whom we need to send, the second one would be to update OS, firewall up to date and not downloading anything from unofficial platforms.

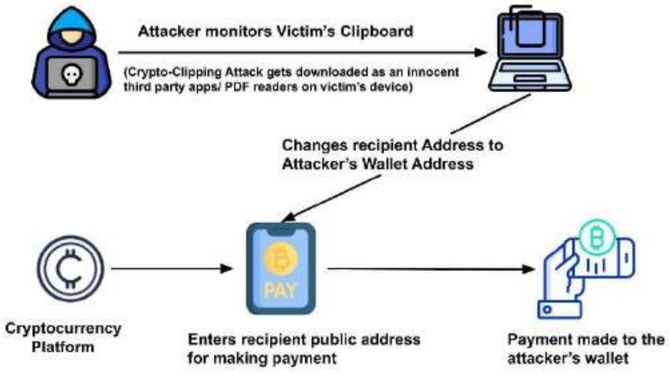

Attacker monitors Victim's Clipboard
(Crypto-Clipping Attack gets downloaded as an innocent third party apps/ PDF readers on victim's device)
Changes recipient Address to Attacker's Wallet Address
PAY
Cryptocurrency Platform
Enters recipient public address for making payment
Payment made to the attacker's wallet

Fig 3. Crypto-clipping attack

Fig 3. shows the architecture of Crypto-Clipping Attack. The malware can be downloaded by an innocent third-party apps/ PDF reader on the victim's device and monitor's victim's device clipboard where the wallet address is copied.

b. Crypto-jacking attack

In this type of attack the cyber criminal hacks into our devices by installing crypto-jacking software. This software mainly works in the background by stealing our cryptocurrency exchange wallets. Cybercriminals follow mainly two ways to get into a victim's device either by making the victim click on a link sent through email which loads crypto mining script on the victim's computer or by infecting an ad or website which instinctively gets loaded in victim's browser when the victim clicks on it. As shown in attackers begin crypto mining using the resources of the targeted devices. Hackers begin by breaking the difficult algorithms and by adding the data block to the blockchain, attackers earn the cryptocurrency rewards. It is very difficult to detect crypto- jacking attacks on our devices. But we can notice that when our system works ultraslow, overheat. Basic prevention would be disabling JavaScript while visiting a suspicious website, Blocking ads from untrusted or unofficial sources.

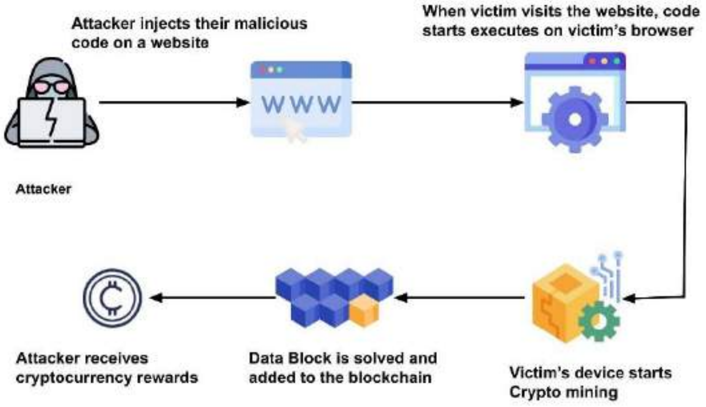

Attacker injects their malicious code on a website
When victim visits the website, code starts executes on victim's browser
Attacker
WWW
Attacker receives cryptocurrency rewards
Data Block is solved and added to the blockchain
Victim's device starts Crypto mining

Fig 4. Crypto-jacking attack

Figure 4 shows how attackers begin crypto mining using the resources of the targeted devices.

c. Investment Scams

This scam involves where one attacker party promising great returns by just sending them cryptocurrency. By letting us know we would see immediate gains once we invest a small amount. Some fake websites may also make it look like our investment is growing which is a kind of trap where few investors fall for it. It’s important that investors know which one is legitimate and not.

d. Race attack

This attack occurs when a hacker does two conflicting transactions. Attackers can send the same coin to two different vendors in following one another at short intervals by using different machines. Usually, a transaction in blockchain gets confirmed after undergoing 6 different steps which take around 10 mins. This attack worked because the merchants accepted unconfirmed transactions instead of waiting for confirmation.

e. Email-phishing attack

There are many ways in which phishing attack can be performed. Attackers implement phishing attacks aiming to steal users' credentials and funds from victims' cryptocurrency exchange wallets. As shown in Fig. 5 , Attacker sends a spam email to the victim saying to reset our cryptocurrency login password by using the given link or any other tactics. If we click on the link it redirects to the specially created phishing website that asks us to enter personal information that is required to get access into the victim's cryptocurrency platform. Once these are provided attacker steals all the funds from the victim's wallets. The basic preventions would be not to disclose any sensitive information to strangers, not to open attachments in any suspicious or strange emails, avoid clicking links from the malicious or suspicious senders, and purchase anti-virus software.

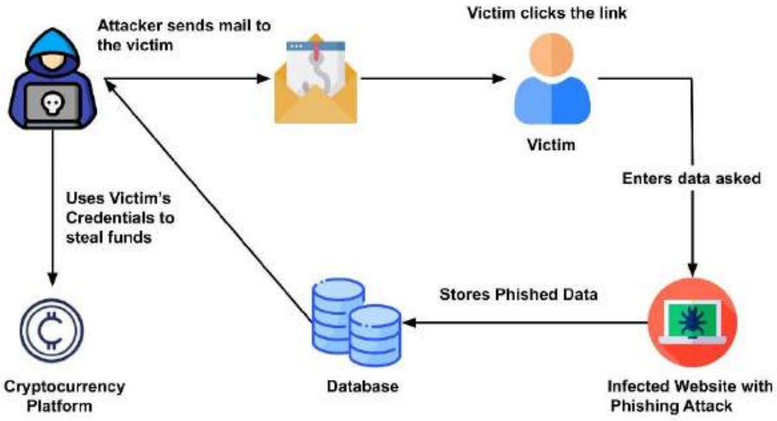

Attacker sends mail to the victim
Victim clicks the link
Victim
Enters data asked
Uses Victim's Credentials to steal funds
Stores Phished Data
Cryptocurrency Platform
Database
Infected Website with Phishing Attack

Fig 5. Email-phishing attack

Figure 5 shows the architecture of the Email-phishing attack. The attacker sends a spam email to the victim saying to reset our cryptocurrency login password by using the given link or any other tactics.

f. Crypto-ransomware attack

This is one of the most common cyber-attacks. This attack is increasing widely in number. Crypto-ransomware is an attack that encrypts files stored in a computer to get ransom money in return. In Fig. 6 ,Type 1 represents the crypto-ransomware attack where the victim's files get encrypted and when the victim opens the file a ransomware message gets displayed demanding money in digital currency. Once the payment is done victim receives a key to unlock the data. Basic prevention requires a combination of anti-malware software on our devices, frequent file backups, good monitoring applications.

g. Locker ransomware attack

This attack locks the user interface and demands a ransom. In Fig 6 ,Type 2 represents a locker-ransomware attack that locks or shuts down the entire computer or victim's device. A locked system only allows for limited access. Where only the victim can view ransomware cyber-criminal messages or allow the victim to respond only to ransomware demands. Once the payment is done victim receives a key to unlock the data. The basic preventions cannot completely reduce risk but we can greatly limit the chances.

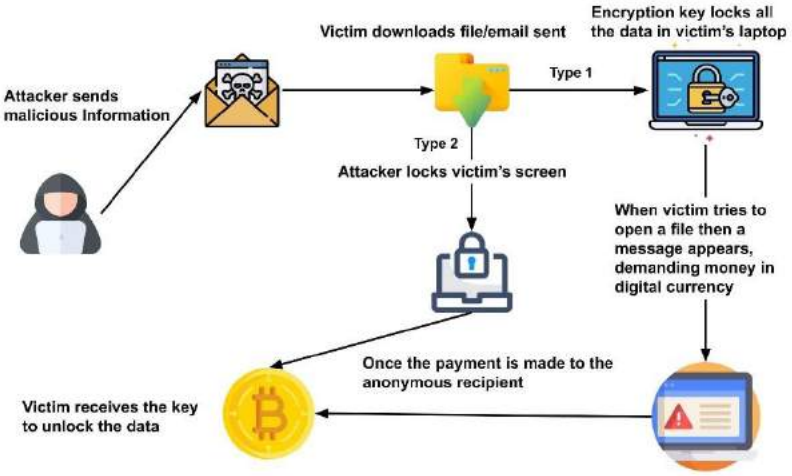

Victim downloads file/email sent
Encryption key locks all the data in victim's laptop
Attacker sends malicious Information
Type 1
Type 2
Attacker locks victim's screen
When victim tries to open a file then a message appears, demanding money in digital currency
Once the payment is made to the anonymous recipient
Victim receives the key to unlock the data

Fig 6. Ransomware attack

In Fig. 6. Type 1 represents the crypto-ransomware attack where the victim's files get encrypted and Type 2 represents a locker-ransomware attack that locks or shuts down the entire computer or victim's device.

2.4.2. RECENT CASES OF CYBER ATTACKS ON CRYPTOCURRENCY PLATFORMS

The following is a list of the biggest and the most recent cyber attacks and cyber hacks on the cryptocurrency platforms in the year 2021.

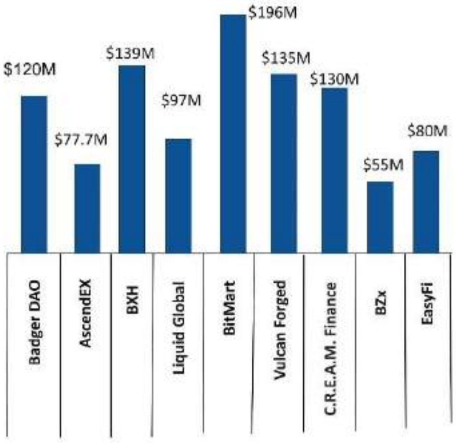


Fig 7. Recent cyber attacks on crypto platforms

Fig 7. , shows the biggest cyber attacks on cryptocurrency platforms in the year 2021.

a. Badger DAO

Badger DAO, a decentralized finance platform reported a loss of about $120 million due to cyber attacks in December 2021.Hackers injected malicious code into the platform website well before the attack in advance and stole cryptocurrency assets from customer wallets. A blockchain security firm, PeckShield reported the single largest loss of 896 Bitcoins amounting to $44 million from a cryptocurrency wallet.

b. AscendEX

A cryptocurrency exchange stated a loss of about $77.7 million owing to a cryptocurrency hack that occurred on December 11, 2021.Tokens were stolen from hot wallets. Peck Shield reported that the majority of the loss was from the Ethereum blockchain.

c. Boy X Highspeed(BXH)

BXH, a decentralized cryptocurrency exchange platform reported a loss of about $139 million in November 2021 owing to an exposed administrator key. PeckShield reported that the exploit was a result of an insider.

d. Liquid Global

Liquid Global, the Japanese fintech company reported a loss of $97 million in August 2021.Hackers looted all the major cryptocurrencies from the hot wallets. The loot was directed to various other decentralized platforms. Ethereum cryptocurrency accounted for the major part of the loss.

e. BitMart

BitMart, a real-time cryptocurrency trading platform reported a loss of $196 million in December 2021. This resulted from an exposed private key linked to two hot wallets. BitMart stated that the majority of the loss was accounted for the Ethereum blockchain.

f. Vulcan Forged

Vulcan Forged, a play-to-earn game studio stated a loss of $135 million in December 2021. Private keys of almost 100 crypto wallets were stolen leading to cryptocurrency asset loss. this resulted in lowering the market cap of Vulcan Forged by about 35%.

g. C.R.E.A.M Finance

C.R.E.A.M Finance, a decentralized exchange platform reported a total loss of $215 million over three consecutive cyber attacks in October 2021. Liquid assets on the Ethereum blockchain were stolen which lead to the loss.

h. BZX

BZX, a margin cryptocurrency trading company stated a loss of about $55 million in November 2021 owing to a phishing attack.

i. EasyFi

EasyFi, a decentralized lending platform stated a loss of about $80 million in April 2021 owing to a cyber attack. The private key of the Meta Mask administrator account was exploited to steal its tokens worth $75 million.

2.5. GOALS

The goals of the proposed work are as follows

- To analyze the impact of News Sentiment on Bitcoin prices.
- To develop a hybrid deep learning neural network model to forecast the bitcoin prices accurately and efficiently.
- To analyze the vulnerability of cyber-attacks on the cryptocurrency exchange platforms.
- To Implement an attack manually on the Solidity platform along with a prevention method.

3. TECHNICAL SPECIFICATIONS

3.1. HARDWARE SPECIFICATIONS

- Processor:Intel® Core(TM) i5-5200U CPU @ 2.20GHz 2.20GHz
- Cache:256kb
- RAM: Minimum – 256 MB
- Hard Disk: 5GB minimum disk capacity

3.2. SOFTWARE SPECIFICATIONS

- Operating System: Windows 7/8/10
- Machine Learning Editors: Jupyter Notebook, Google Colab
- Min 4 GB Ram
- Min 100 GB Hard Disk
- Jupyter Notepad
- Google collab
- Remix - Ethereum IDE
- EthFiddle - Solidity IDE
- Windows Operating System
- Advanced Browser
- JavaScript Object Notation(JSON)
- Request module
- Keras
- Sequential
- Matplotlib
- Numpy
- Seaborn
- Pandas
- Scikit-learn

3.3. MODULE DESCRIPTION

Libraries used in this project are discussed.

a. JavaScript Object Notation(JSON)

The JSON module in Python can assist in the conversion of data structures to JSON strings. JSON can store dictionaries, tuples, and Lists. It must, however, be converted to strings in order to be stored in a file.

b. Request module

The requests module in Python makes it simple to process HTTP requests.

c. Keras

Keras is an open-source library for artificial neural networks which provides a Python interface. It is utilized to build machine learning models.

d. Sequential

In the sequential model the data transmits through layers till the data is transferred to the output layer.

e. Matplotlib

Matplotlib is a two-dimensional plotting library that helps in the visualization of data. Matplotlib is a library that simulates Matlab graphs and visualizations.

f. Numpy

Numpy is a Python module that allows us to work with matrices and large multi-dimensional arrays.

g. Pandas

Pandas is an open-source tool in ML and data manipulation library written in python.

h. Seaborn

Seaborn is a data visualisation library in Python that is used to plot statistical graphs.

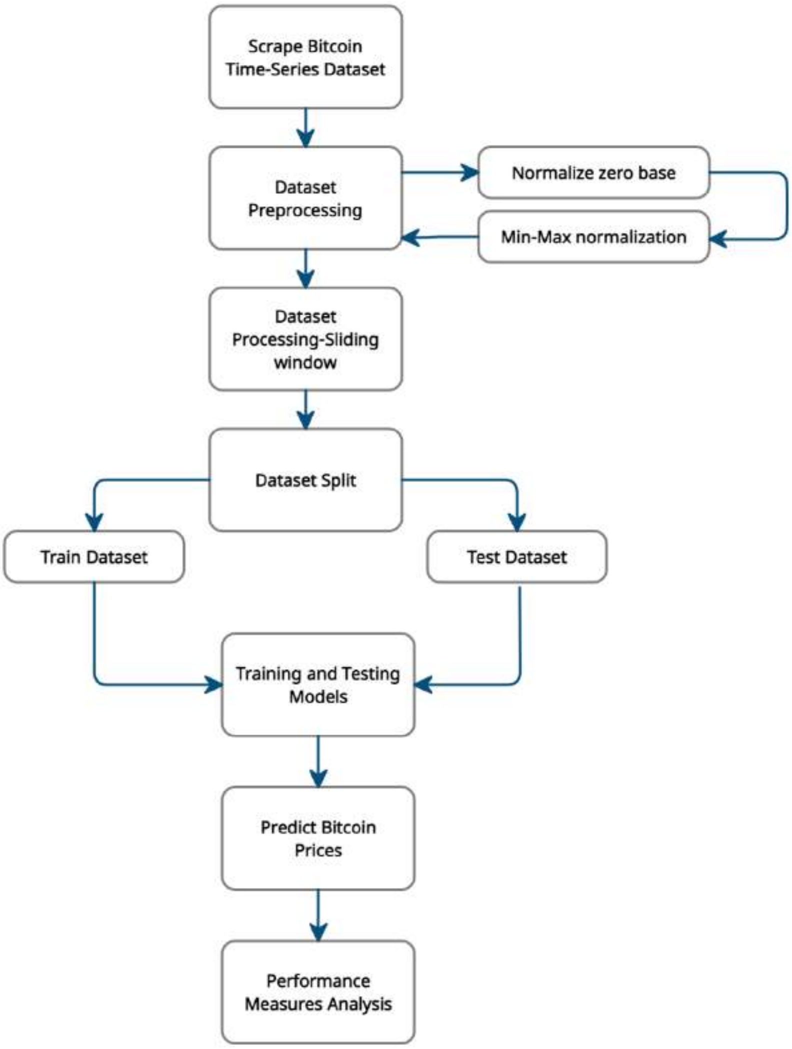
i. Scikit-learn

   For conventional ML methods, Scikit-learn is one of the most used ML libraries. Most supervised and unsupervised learning methods are supported by scikit-learn.

4. DESIGN APPROACHES AND DETAILS

4.1. MATERIALS AND METHODS

4.1.1. HYBRID BITCOIN PRICE PREDICTION MODELLING



Scrape Bitcoin Time-Series Dataset
Dataset Preprocessing
Normalize zero base
Min-Max normalization
Dataset Processing-Sliding window
Dataset Split
Train Dataset
Test Dataset
Training and Testing Models
Predict Bitcoin Prices
Performance Measures Analysis

Fig 8. Architecture model of the deep-learning prediction model

a. Experimental Datasets Used

Bitcoin Historical Dataset was downloaded from coinmarketcap.com for the period ’01-01-2021’ to ’31-12-2021’. The significant reason for using this time frame is that bitcoin cryptocurrency experienced massive fluctuations owing to various social factors during this time. The dataset contains parameters namely ’open’, ’high’, ’low’, ’close’, ’adjusted volume’, ’volume’. The news headlines related to bitcoin were collected using API and a little bit of web scraping for the above time period from cryptocurrency news aggregators online such as coindesk.com. cointelegraph.com, cryptopanic.com, etc. The datasets and their parameters description is discussed in the tables shown below. Table 11. Shows the parameters and their datatype with the descriptions of the bitcoin historical dataset. Table 12. Shows the parameters and their datatype with the descriptions of the news articles dataset.

Table 11. Parameter description of the Bitcoin Historical Dataset

FEATURE	**DATATYPE**	**MEANING**
time	Epoch timestamp	The unix timestamp for the start of the datapoint.
high	float	The highest price of Bitcoin(USD) for this period of time.
low	float	The lowest price of Bitcoin(USD) for this period of time.
open	float	The price of Bitcoin(USD) at the start of this period of time.
volumefrom	float	The total amount of Bitcoin currency traded into USD during this period of time.
volumeto	float	The total amount of USD currency traded into Bitcoin currency during this period of time.
close	float	The price(USD) of Bitcoin at the end of this period of time.

Table 12. Parameter description of the News Articles Dataset

FEATURE	**DATATYPE**	**MEANING**
time	Epoch timestamp	The unix timestamp for the start of the datapoint.
high	float	The highest price of Bitcoin(USD) for this period of time.
low	float	The lowest price of Bitcoin(USD) for this period of time.
open	float	The price of Bitcoin(USD) at the start of this period of time.
volumefrom	float	The total amount of Bitcoin currency traded into USD during this period of time.
volumeto	float	The total amount of USD currency traded into Bitcoin currency during this period of time.
close	float	The price(USD) of Bitcoin at the end of this period of time.

b. Hybrid Neural Network Architecture

We built a Hybrid based Prediction Mode which is a combination of BiGRU and BiLSTM based on Sentiment Analysis of news headlines data related to Bitcoin. This model is used to achieve higher accuracy than the other existing base models used for Bitcoin price prediction based on Twitter Sentiment Analysis. The BiGRU and BiLSTM model has the advancements of Bidirectional LSTM and RNN and has much newer modifications. A neuron in the GRU is selected to substitute RNN neuron of the Recurrent Neural Network model . A neuron in the GRU, LSTM is selected to substitute RNN neuron of the Recurrent Neural Network model .

The Hybrid prediction model with sentiment analysis is composed of 5 stages, 1)news headlines preprocessing 2)Bitcoin historical dataset preprocessing 3) Sentiment scoring using TextBlob 4)Feature Selection 5)training BiGRU prediction model 6)model validation. In stage 1, the news headlines data is preprocessed using stop word removal and textstemming. Then in stage 2, the bitcoin historical dataset is preprocessed using min-max normalization. The third stage involves converting the news headlines into sentiment scores using Sentiment Analysis. Textblob is a Natural Language Processing Python Library used for sentiment analysis. The subjectivity and polarity scores from the sentiment analysis are merged with the bitcoin historical dataset. Feature Selection is performed on the merged dataset using the Recursive Feature Elimination(RFE) technique. The selected features are used for prediction modeling. In the fifth stage, the Hybrid prediction model is developed. The model consists of a stacked two hidden layers namely BiLSTM, BiGRU model to maximize the performance. Fig 8. Shows the neural network architecture of the proposed hybrid deep learning model.

Cross-validation of 10 folds has been done in stage 6. The bitcoin dataset along with the news articles sentiment scores appended dataset was divided into 10 segments and 8 segments out of it were taken for the train dataset and two part as the testing dataset in turns. Mean scores of all outputs were aggregated as used as an quality metric for the accuracy and efficiency of the model. The model is lastly validated through different performance measures.

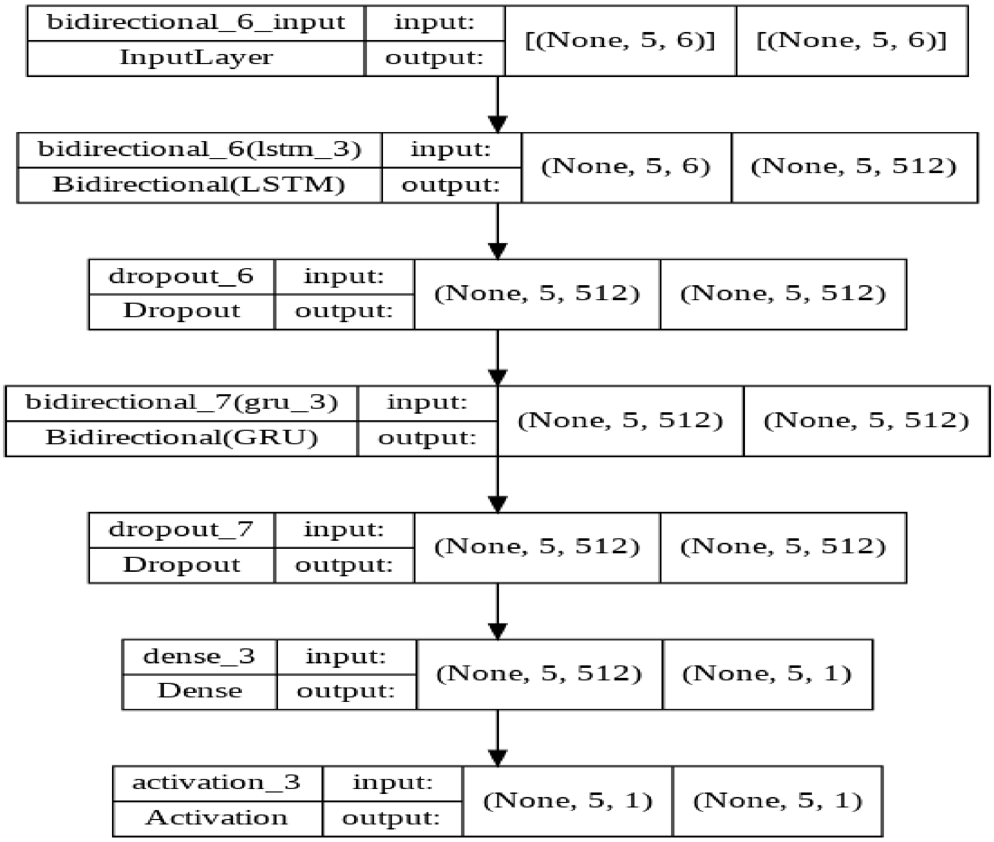


Fig 9. Hybrid model neural network architecture

4.1.2. IMPLEMENTATION OF A CRYPTOCURRENCY ATTACK

a. Reentrancy Attack

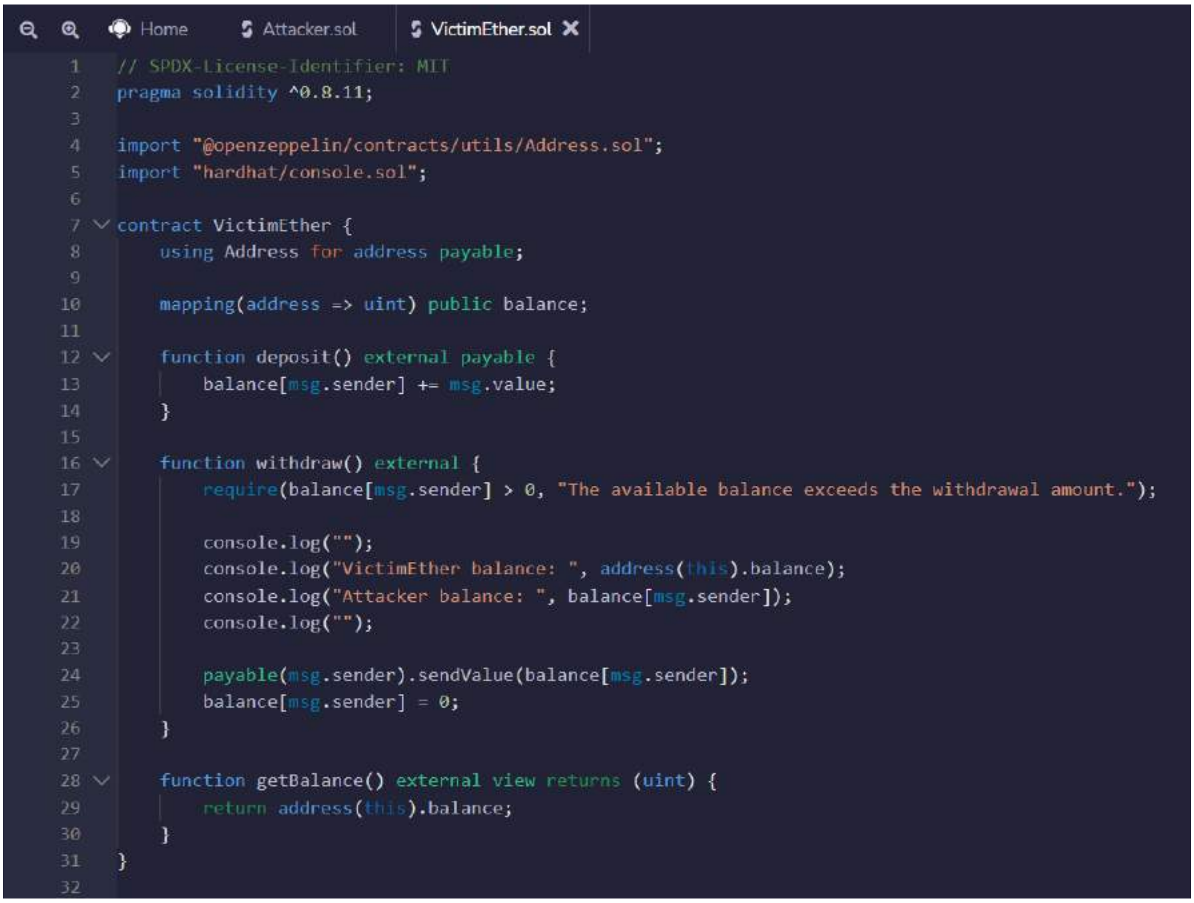
Interest in bitcoin is always increasing due to the opportunities that rapidly increase the investments, Which also involves high risk and challenges. Hackers are targeting cryptocurrency exchanges and online wallets in a huge number. If a hacker acquires access to cryptocurrency coins stored on a wallet, as well as the keys required to complete a transaction, they can steal them.

In August 2021, SurgeBNB reported a $4 million loss due to a reentrancy attack which is one of the most common reentrancy hacks. In recent years, there have been multiple reentrance smart contract attacks on cryptocurrency platforms.

An attack where malicious smart contracts drain all the funds from the victim contract. Reentrancy attacks happen when malicious contracts call the victim's contract in such a way that they gain more control over code execution, disturbing the victim's contract's state and modifying it in unanticipated ways. The attacker can call a withdraw function on a victim contract, which then transmits all the funds to the attacker. The attacker then takes the control of the code execution via the fallback function and can recursively call the victim's withdraw function before the Victim's balance is updated to reflect the withdrawal, and this continues until the attacker has successfully stolen all the funds from the victim's smart contract.

CODE SNIPPETS

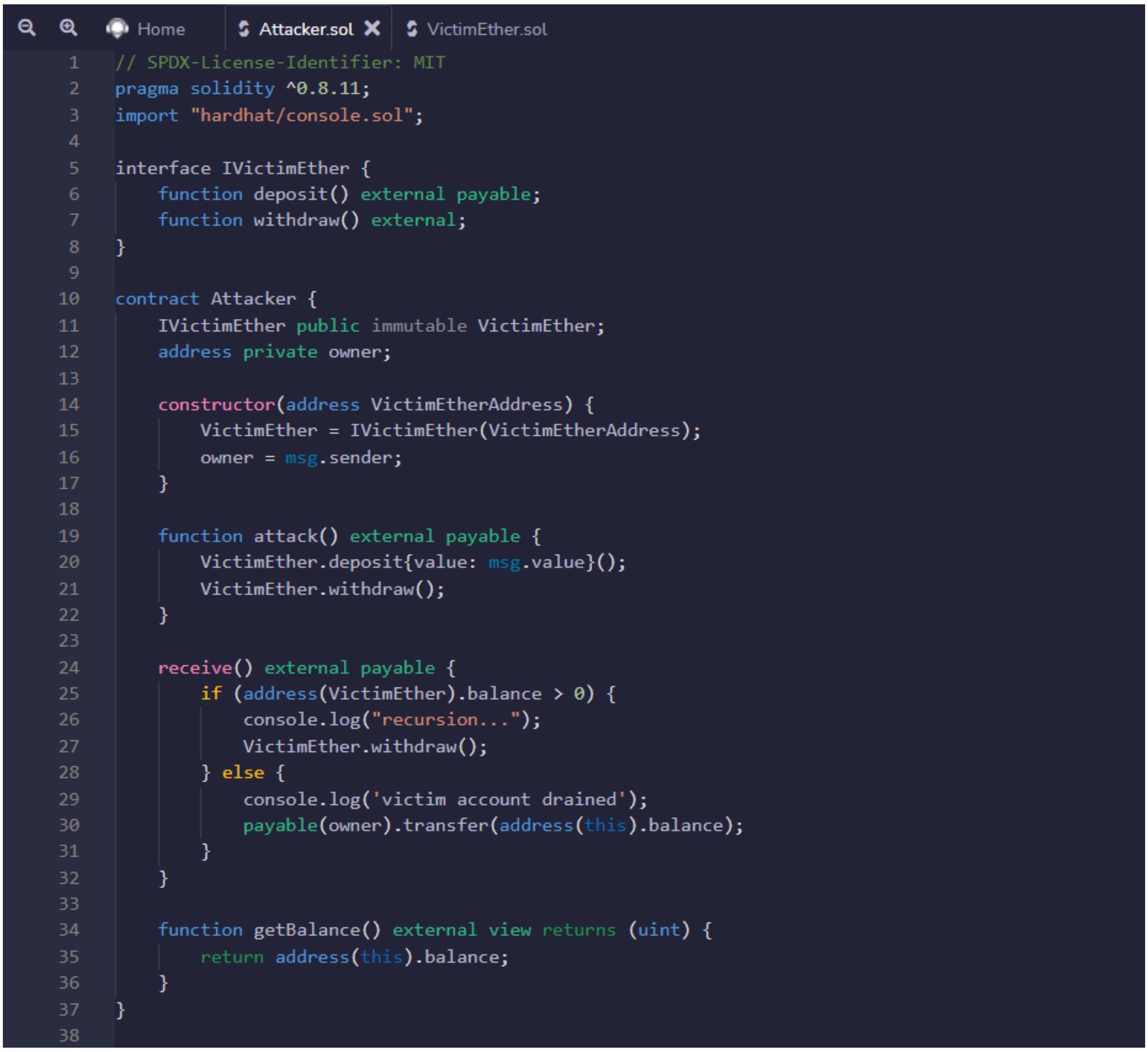
VictimEther.sol



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.11;

import "@openzeppelin/contracts/utils/Address.sol";
import "hardhat/console.sol";

contract VictimEther {
    using Address for address payable;

    mapping(address => uint) public balance;

    function deposit() external payable {
        balance[msg.sender] += msg.value;
    }

    function withdraw() external {
        require(balance[msg.sender] > 0, "The available balance exceeds the withdrawal amount.");

        console.log("");
        console.log("VictimEther balance: ", address(this).balance);
        console.log("Attacker balance: ", balance[msg.sender]);
        console.log("");

        payable(msg.sender).sendValue(balance[msg.sender]);
        balance[msg.sender] = 0;
    }

    function getBalance() external view returns (uint) {
        return address(this).balance;
    }
}
```

Fig 10. Code Snippet of Victim’s Smart Contract

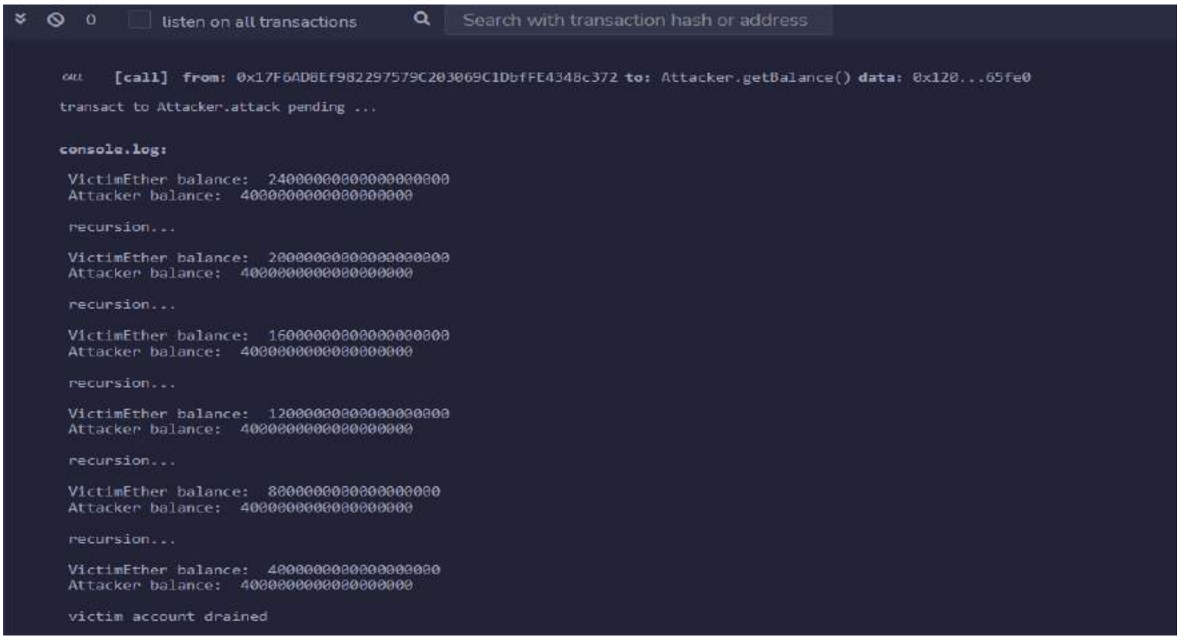
Attacker.sol



```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.11;
import "hardhat/console.sol";

interface IVictimEther {
    function deposit() external payable;
    function withdraw() external;
}

contract Attacker {
    IVictimEther public immutable VictimEther;
    address private owner;

    constructor(address VictimEtherAddress) {
        VictimEther = IVictimEther(VictimEtherAddress);
        owner = msg.sender;
    }

    function attack() external payable {
        VictimEther.deposit{value: msg.value}();
        VictimEther.withdraw();
    }

    receive() external payable {
        if (address(VictimEther).balance > 0) {
            console.log("recursion...");
            VictimEther.withdraw();
        } else {
            console.log('victim account drained');
            payable(owner).transfer(address(this).balance);
        }
    }

    function getBalance() external view returns (uint) {
        return address(this).balance;
    }
}

```

Fig 11. Attacker's Side Code to Execute an Attack

Output


0
listen on all transactions
Search with transaction hash or address

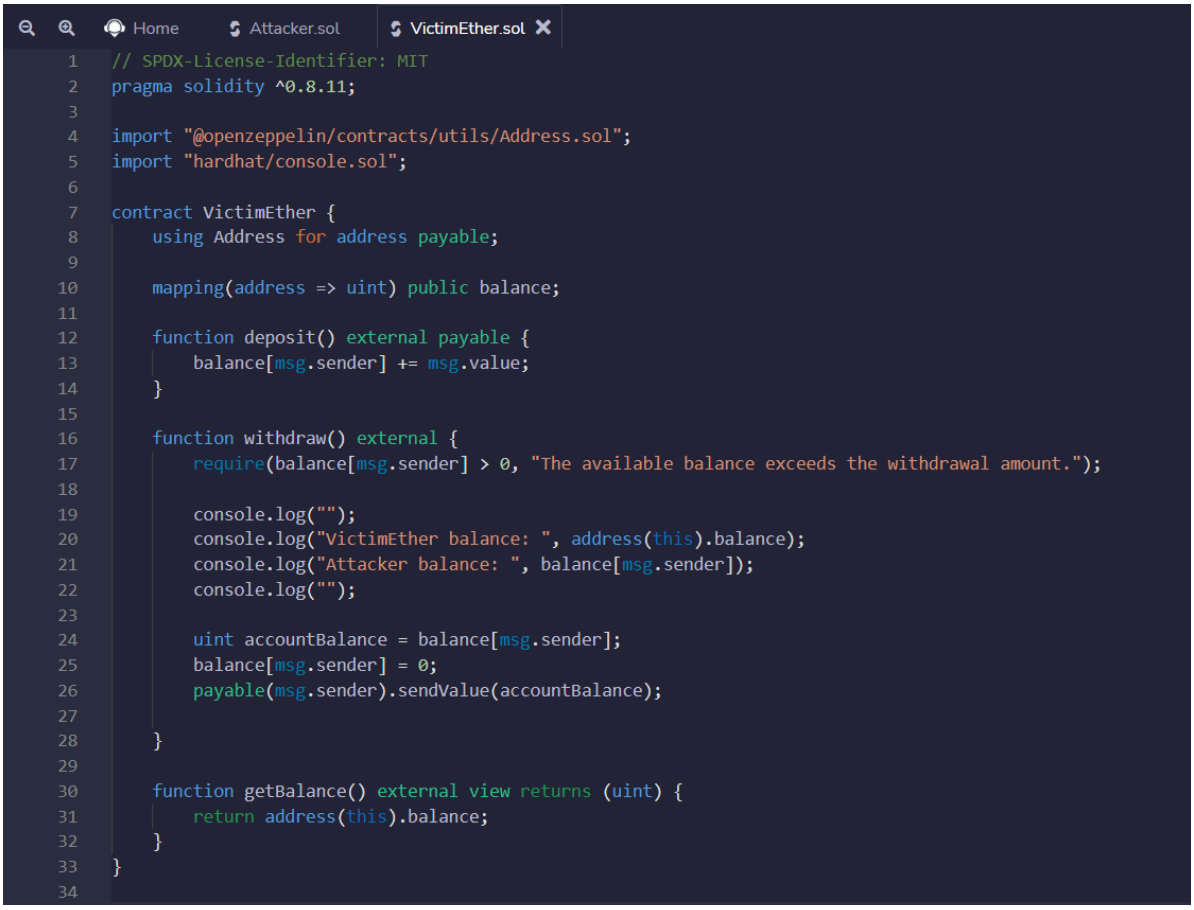
```
call    [call]  from: 0x17F6AD8Ef982297579C203069C1DbfFE4348c372 to: Attacker.getBalance() data: 0x120...65fe0
transact to Attacker.attack pending ...

console.log:
 VictimEther balance:  24000000000000000000
 Attacker balance:  4000000000000000000

 recursion...

 VictimEther balance:  20000000000000000000
 Attacker balance:  4000000000000000000

 recursion...

 VictimEther balance:  16000000000000000000
 Attacker balance:  4000000000000000000

 recursion...

 VictimEther balance:  12000000000000000000
 Attacker balance:  4000000000000000000

 recursion...

 VictimEther balance:  8000000000000000000
 Attacker balance:  4000000000000000000

 recursion...

 VictimEther balance:  4000000000000000000
 Attacker balance:  4000000000000000000

 victim account drained
```

Fig 12. Code Snippet of Hacked Victim’s Account

Prevention

One way to avoid this is to create a temporary variable to hold up the victim's account balances before transferring payments. If we reset the balance to zero then there is nothing to send. As a result, if an attacker tries to call the withdraw function repeatedly, the initial require function in the attacker's withdraw function will fail since the victim's account balance is set to zero.

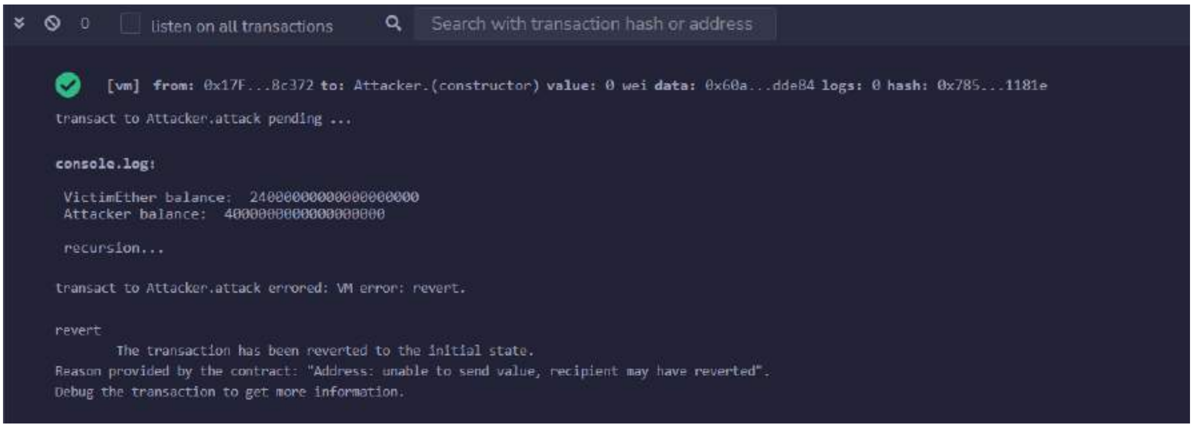
VictimEther.sol



```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.11;

import "@openzeppelin/contracts/utils/Address.sol";
import "hardhat/console.sol";

contract VictimEther {
    using Address for address payable;

    mapping(address => uint) public balance;

    function deposit() external payable {
        balance[msg.sender] += msg.value;
    }

    function withdraw() external {
        require(balance[msg.sender] > 0, "The available balance exceeds the withdrawal amount.");

        console.log("");
        console.log("VictimEther balance: ", address(this).balance);
        console.log("Attacker balance: ", balance[msg.sender]);
        console.log("");

        uint accountBalance = balance[msg.sender];
        balance[msg.sender] = 0;
        payable(msg.sender).sendValue(accountBalance);

    }

    function getBalance() external view returns (uint) {
        return address(this).balance;
    }
}

```

Fig 13. Prevention Code Snippet of Victim’s account

Output


0
listen on all transactions
Search with transaction hash or address

```
[vm] from: 0x17F...8c372 to: Attacker.(constructor) value: 0 wei data: 0x60a...dde84 logs: 0 hash: 0x785...1181e
transact to Attacker.attack pending ...

console.log:

 VictimEther balance:  24000000000000000000
 Attacker balance:  4000000000000000000

 recursion...

transact to Attacker.attack errored: VM error: revert.

revert
        The transaction has been reverted to the initial state.
Reason provided by the contract: "Address: unable to send value, recipient may have reverted".
Debug the transaction to get more information.
```

Fig 14. Output of Prevented Victim’s Account

b. A new cryptocurrency attack that could be performed in the future

Despite the fact that blockchain use is still growing, an increase in cyber assaults on the technology has a negative influence. An attack that might be carried out in the future on the cryptocurrency platform is explained.

Blockchain explorer is a tool that displays information about all the transactions that take place on the blockchain network. We can view all of the addresses used to make the transaction in the blockchain and can also check the transaction's status, destination addresses, and wallet balance. In Fig 15. , Type 1, By using this blockchain explorer a hacker or a scammer can send cryptocurrency to multiple addresses and monitors the transactions that are made by them. And develops a strategy to obtain their information. If successful, attackers use this knowledge against their targets via threats or phishing attacks, or other new approaches to steal their funds.

Software most commonly has vulnerabilities, and when the developers identify those they develop a new solution and release a new update. In Type 2, Hackers can detect this before developers and can use this to their advantage by launching an attack. They could follow a variety of methodologies to steal the funds from the investors.

Architecture

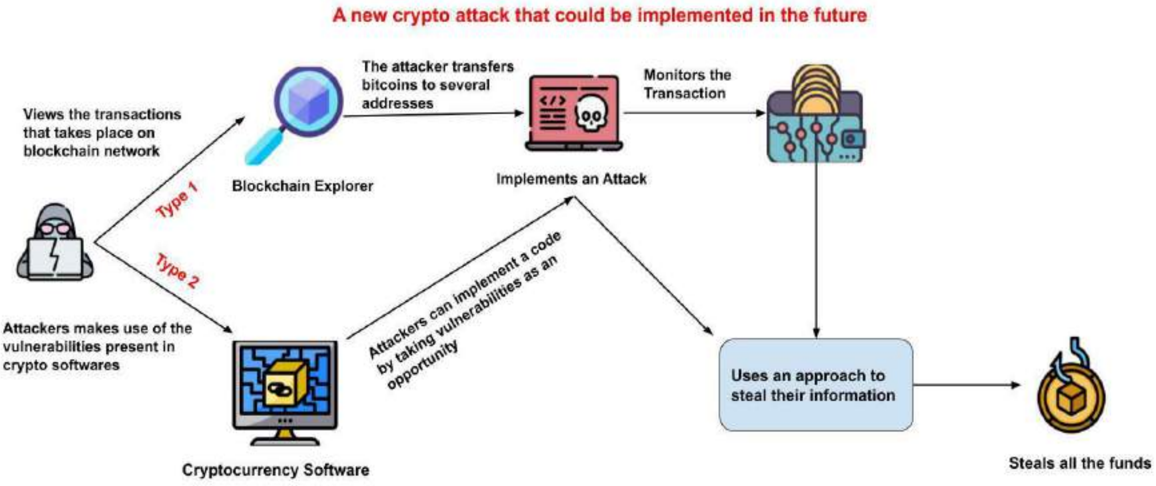
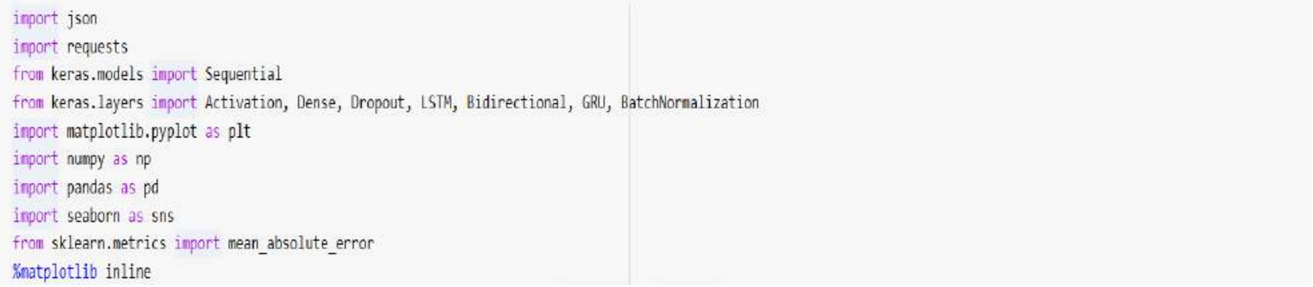

A new crypto attack that could be implemented in the future
Views the transactions that takes place on blockchain network
Type 1
Blockchain Explorer
The attacker transfers bitcoins to several addresses
Implements an Attack
Monitors the Transaction
Type 2
Attackers makes use of the vulnerabilities present in crypto softwares
Cryptocurrency Software
Attackers can implement a code by taking vulnerabilities as an opportunity
Uses an approach to steal their information
Steals all the funds

Fig 15. Architecture of new Crypto Cyber-attack

4.2. CODES AND STANDARDS

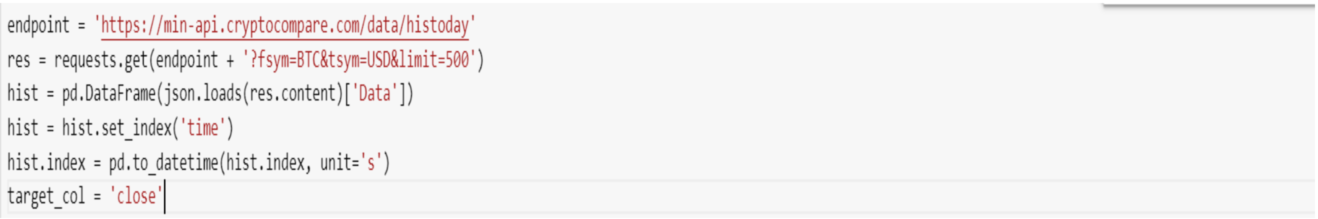
4.2.1. LIBRARIES USED



```
import json
import requests
from keras.models import Sequential
from keras.layers import Activation, Dense, Dropout, LSTM, Bidirectional, GRU, BatchNormalization
import matplotlib.pyplot as plt
import numpy as np
import pandas as pd
import seaborn as sns
from sklearn.metrics import mean_absolute_error
%matplotlib inline
```

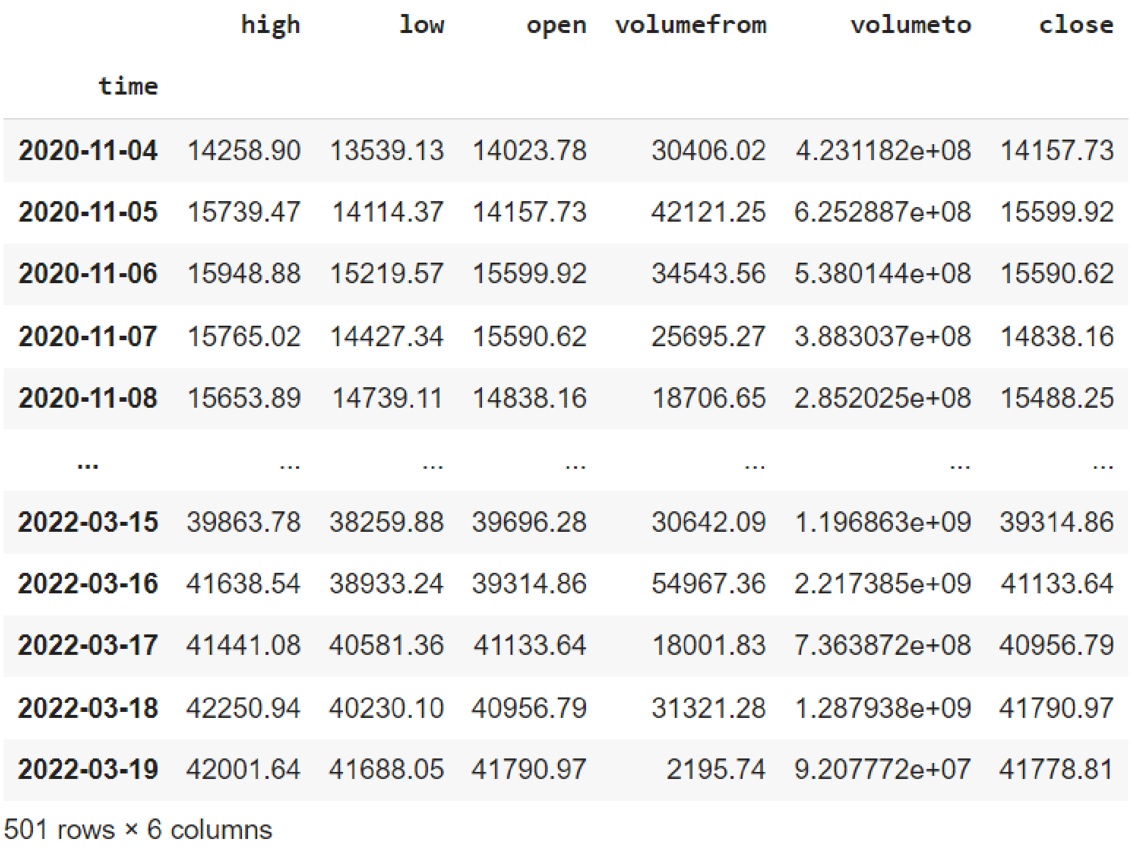
Fig 16. Libraries used in modeling

4.2.2. SCRAPING BITCOIN HISTORICAL DATASET USING API KEYS



```
endpoint = 'https://min-api.cryptocompare.com/data/histoday'
res = requests.get(endpoint + '?fsym=BTC&tsym=USD&limit=500')
hist = pd.DataFrame(json.loads(res.content)['Data'])
hist = hist.set_index('time')
hist.index = pd.to_datetime(hist.index, unit='s')
target_col = 'close'
```

Fig 17. API Scraping of Bitcoin Dataset

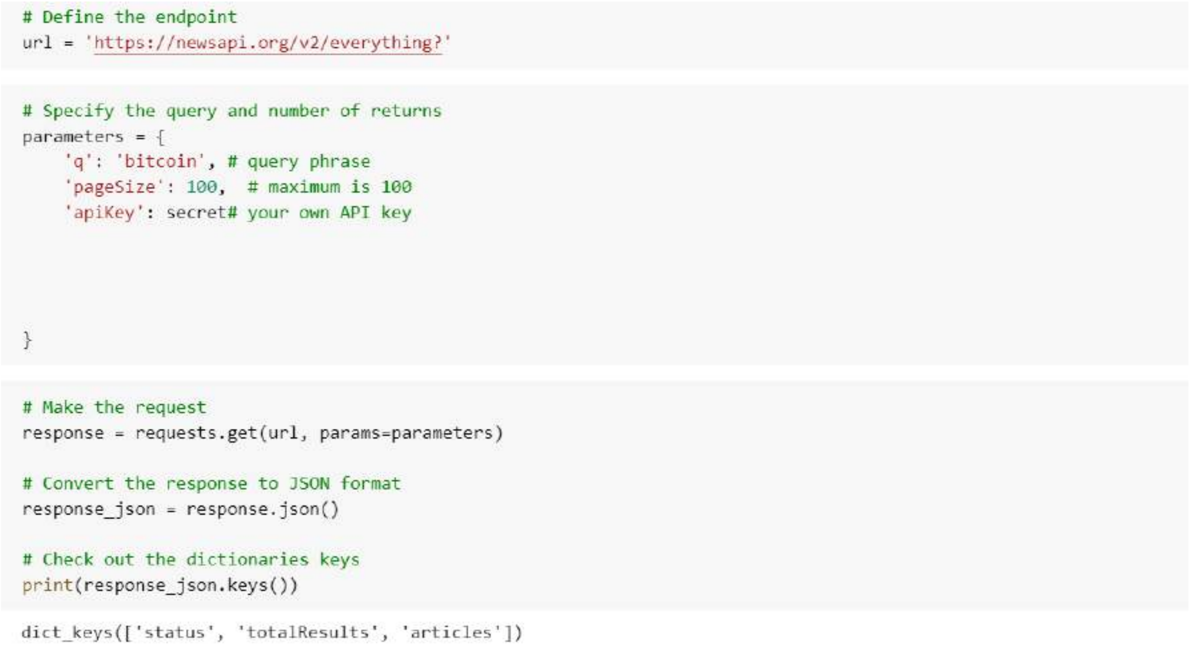


	high	low	open	volumefrom	volumeto	close
time						
2020-11-04	14258.90	13539.13	14023.78	30406.02	4.231182e+08	14157.73
2020-11-05	15739.47	14114.37	14157.73	42121.25	6.252887e+08	15599.92
2020-11-06	15948.88	15219.57	15599.92	34543.56	5.380144e+08	15590.62
2020-11-07	15765.02	14427.34	15590.62	25695.27	3.883037e+08	14838.16
2020-11-08	15653.89	14739.11	14838.16	18706.65	2.852025e+08	15488.25
...	...	...	...	...	...	...
2022-03-15	39863.78	38259.88	39696.28	30642.09	1.196863e+09	39314.86
2022-03-16	41638.54	38933.24	39314.86	54967.36	2.217385e+09	41133.64
2022-03-17	41441.08	40581.36	41133.64	18001.83	7.363872e+08	40956.79
2022-03-18	42250.94	40230.10	40956.79	31321.28	1.287938e+09	41790.97
2022-03-19	42001.64	41688.05	41790.97	2195.74	9.207772e+07	41778.81

501 rows × 6 columns

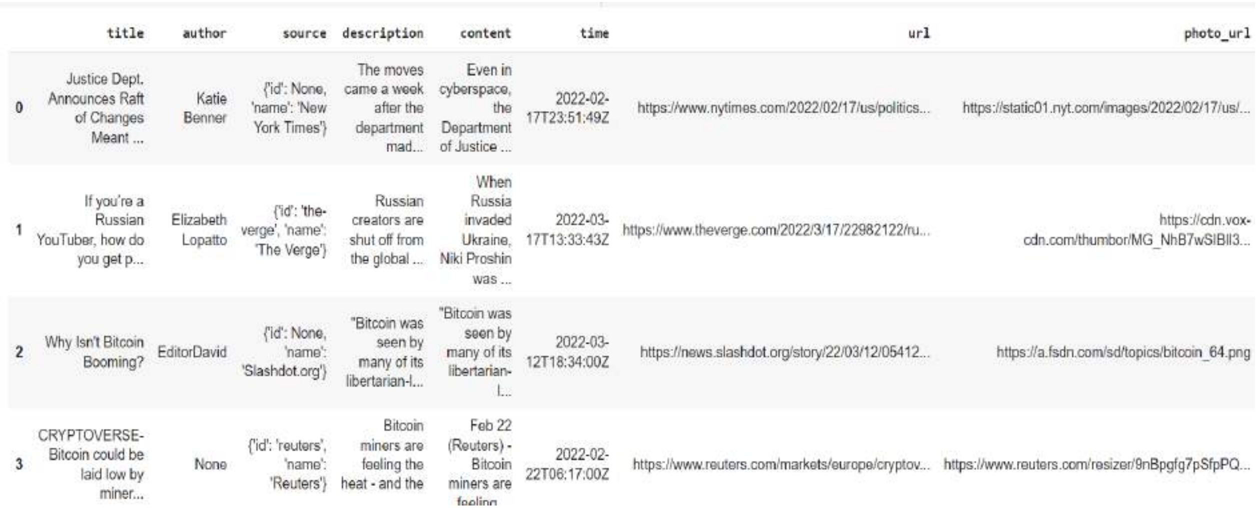
Fig 18. Bitcoin Historical Dataset

4.2.3. SCRAPING NEWS ARTICLES DATASET USING API KEYS



```
# Define the endpoint
url = 'https://newsapi.org/v2/everything?'

# Specify the query and number of returns
parameters = {
    'q': 'bitcoin', # query phrase
    'pageSize': 100,  # maximum is 100
    'apiKey': secret# your own API key




}

# Make the request
response = requests.get(url, params=parameters)

# Convert the response to JSON format
response_json = response.json()

# Check out the dictionaries keys
print(response_json.keys())

dict_keys(['status', 'totalResults', 'articles'])
```

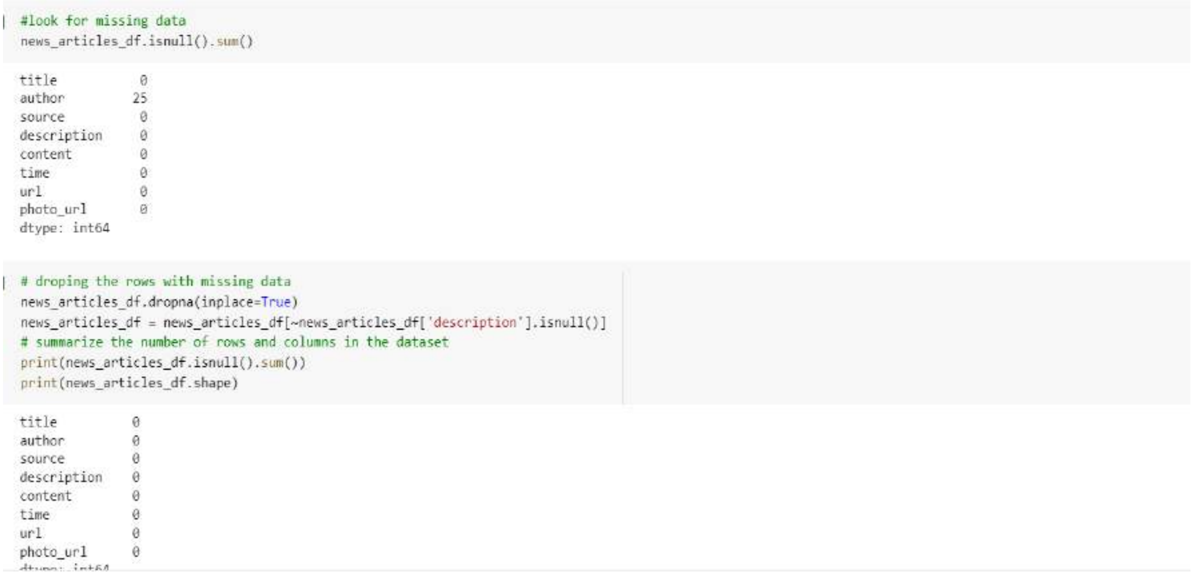
Fig 19. API Scraping of News Articles Dataset



	title	author	source	description	content	time	url	photo_url
0	Justice Dept. Announces Raft of Changes Meant ...	Katie Benner	{'id': None, 'name': 'New York Times'}	The moves came a week after the department mad...	Even in cyberspace, the Department of Justice ...	2022-02-17T23:51:49Z	https://www.nytimes.com/2022/02/17/us/politics...	https://static01.nyt.com/images/2022/02/17/us/...
1	If you're a Russian YouTuber, how do you get p...	Elizabeth Lopatto	{'id': 'the-verge', 'name': 'The Verge'}	Russian creators are shut off from the global ...	When Russia invaded Ukraine, Niki Proshin was ...	2022-03-17T13:33:43Z	https://www.theverge.com/2022/3/17/22982122/ru...	https://cdn.vox-cdn.com/thumbor/MG_NhB7wSIBII3...
2	Why Isn't Bitcoin Booming?	EditorDavid	{'id': None, 'name': 'Slashdot.org'}	"Bitcoin was seen by many of its libertarian-l...	"Bitcoin was seen by many of its libertarian-l...	2022-03-12T18:34:00Z	https://news.slashdot.org/story/22/03/12/05412...	https://a.fsdn.com/sd/topics/bitcoin_64.png
3	CRYPTOVERSE-Bitcoin could be laid low by miner...	None	{'id': 'reuters', 'name': 'Reuters'}	Bitcoin miners are feeling the heat - and the	Feb 22 (Reuters) - Bitcoin miners are feeling	2022-02-22T06:17:00Z	https://www.reuters.com/markets/europe/cryptov...	https://www.reuters.com/resizer/9nBpgfg7pSfpPQ...

Fig 20. News Articles Dataset

4.2.4. CLEANING NEWS ARTICLES DATASET



```
#look for missing data
news_articles_df.isnull().sum()
```

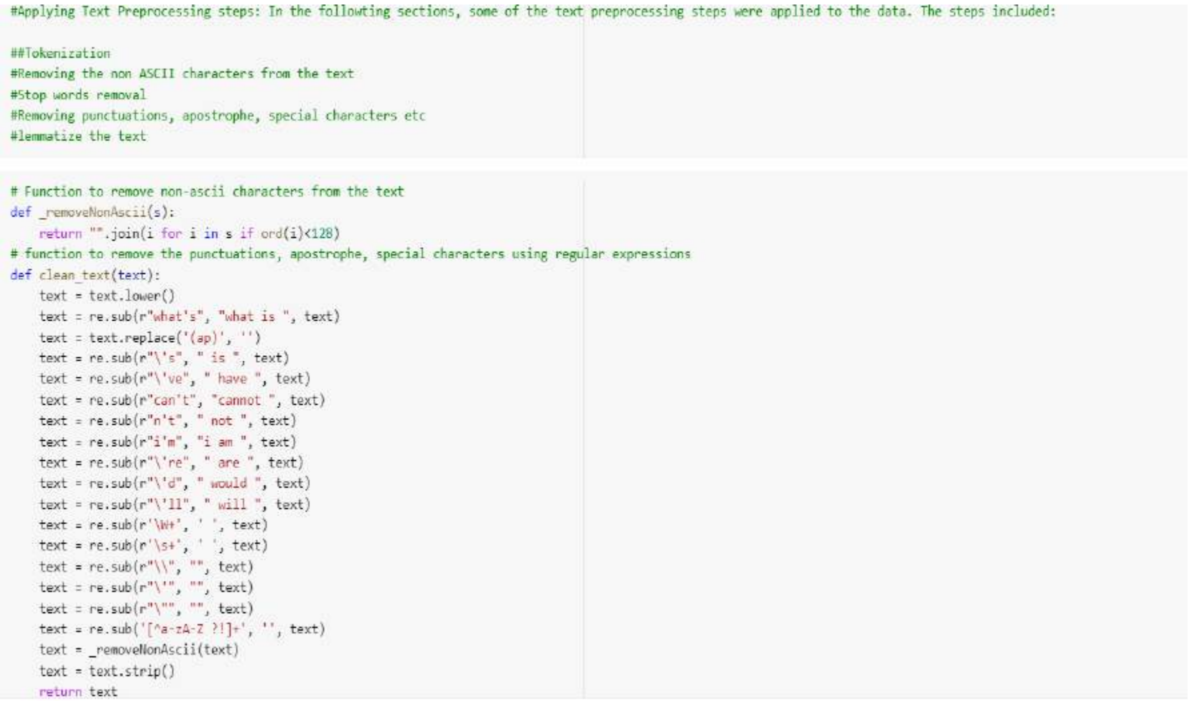
```
title          0
author        25
source         0
description    0
content        0
time           0
url            0
photo_url      0
dtype: int64
```

```
# droping the rows with missing data
news_articles_df.dropna(inplace=True)
news_articles_df = news_articles_df[~news_articles_df['description'].isnull()]
# summarize the number of rows and columns in the dataset
print(news_articles_df.isnull().sum())
print(news_articles_df.shape)
```

```
title          0
author         0
source         0
description    0
content        0
time           0
url            0
photo_url      0
dtype: int64
```

Fig 21. Cleaning News Articles Dataset

4.2.5. NEWS ARTICLES DATASET PREPROCESSING

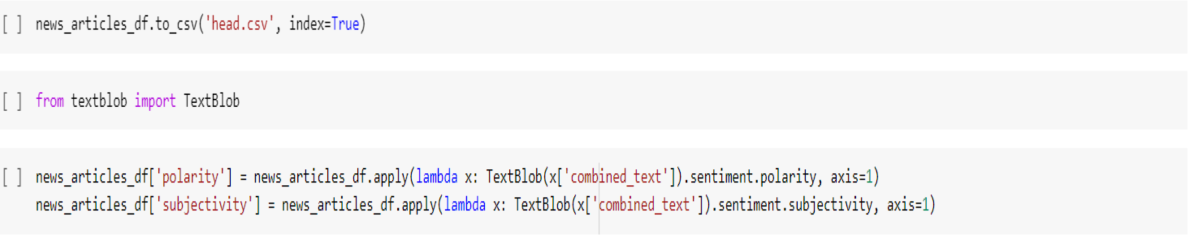


```
#Applying Text Preprocessing steps: In the followting sections, some of the text preprocessing steps were applied to the data. The steps included:

##Tokenization
#Removing the non ASCII characters from the text
#Stop words removal
#Removing punctuations, apostrophe, special characters etc
#lemmatize the text
```

```
# Function to remove non-ascii characters from the text
def _removeNonAscii(s):
    return "".join(i for i in s if ord(i)<128)
# function to remove the punctuations, apostrophe, special characters using regular expressions
def clean_text(text):
    text = text.lower()
    text = re.sub(r"what's", "what is ", text)
    text = text.replace('(ap)', '')
    text = re.sub(r"\'s", " is ", text)
    text = re.sub(r"\'ve", " have ", text)
    text = re.sub(r"can't", "cannot ", text)
    text = re.sub(r"n't", " not ", text)
    text = re.sub(r"i'm", "i am ", text)
    text = re.sub(r"\'re", " are ", text)
    text = re.sub(r"\'d", " would ", text)
    text = re.sub(r"\'ll", " will ", text)
    text = re.sub(r'\W+', ' ', text)
    text = re.sub(r'\s+', ' ', text)
    text = re.sub(r"\\", "", text)
    text = re.sub(r"\'", "", text)
    text = re.sub(r"\"", "", text)
    text = re.sub('[^a-zA-Z ?!]+', '', text)
    text = _removeNonAscii(text)
    text = text.strip()
    return text
```

Fig 22. News Articles Dataset Preprocessing

4.2.6. SENTIMENT ANALYSIS ON NEWS ARTICLES DATASET

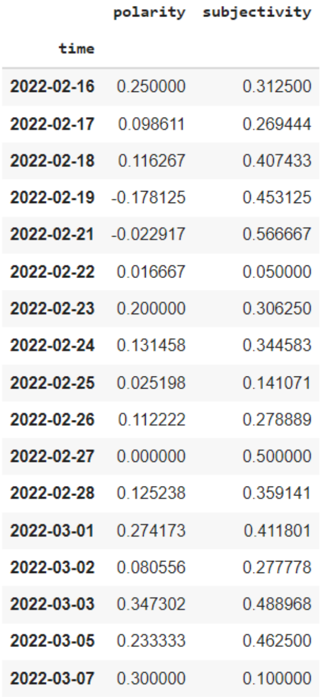


```
[ ]  news_articles_df.to_csv('head.csv', index=True)
```

```
[ ]  from textblob import TextBlob
```

```
[ ]  news_articles_df['polarity'] = news_articles_df.apply(lambda x: TextBlob(x['combined_text']).sentiment.polarity, axis=1)
     news_articles_df['subjectivity'] = news_articles_df.apply(lambda x: TextBlob(x['combined_text']).sentiment.subjectivity, axis=1)
```

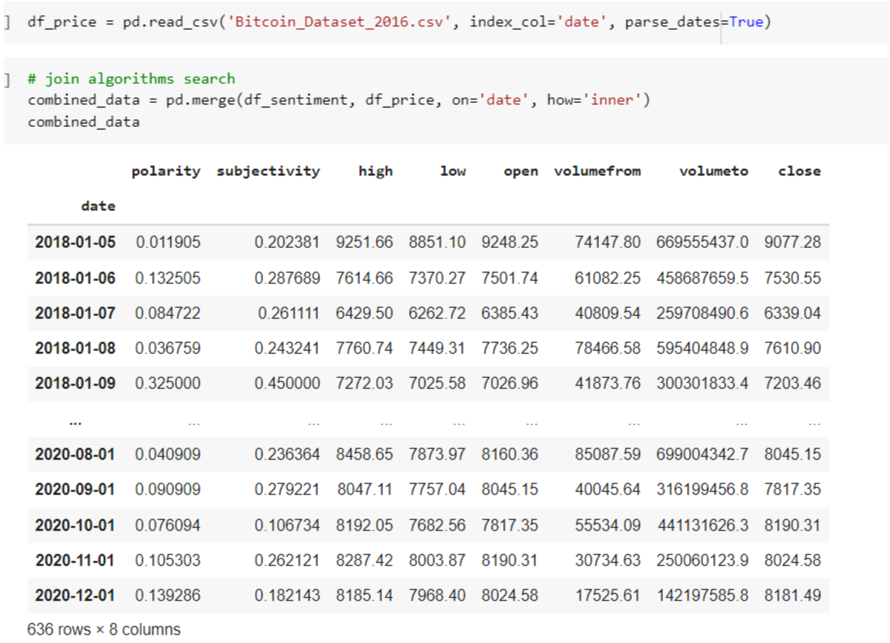
Fig 23. TextBlob Sentiment Analysis



time	polarity	subjectivity
2022-02-16	0.250000	0.312500
2022-02-17	0.098611	0.269444
2022-02-18	0.116267	0.407433
2022-02-19	-0.178125	0.453125
2022-02-21	-0.022917	0.566667
2022-02-22	0.016667	0.050000
2022-02-23	0.200000	0.306250
2022-02-24	0.131458	0.344583
2022-02-25	0.025198	0.141071
2022-02-26	0.112222	0.278889
2022-02-27	0.000000	0.500000
2022-02-28	0.125238	0.359141
2022-03-01	0.274173	0.411801
2022-03-02	0.080556	0.277778
2022-03-03	0.347302	0.488968
2022-03-05	0.233333	0.462500
2022-03-07	0.300000	0.100000

Fig 24. News Articles Sentiment Scores

4.2.7. APPEND SENTIMENT SCORES TO BITCOIN DATASET



```
df_price = pd.read_csv('Bitcoin_Dataset_2016.csv', index_col='date', parse_dates=True)
```

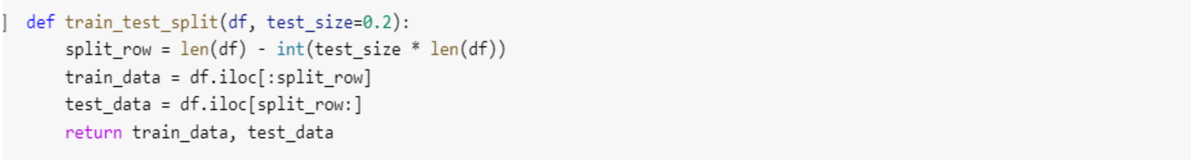
```
# join algorithms search
combined_data = pd.merge(df_sentiment, df_price, on='date', how='inner')
combined_data
```

date	polarity	subjectivity	high	low	open	volumefrom	volumeto	close
2018-01-05	0.011905	0.202381	9251.66	8851.10	9248.25	74147.80	669555437.0	9077.28
2018-01-06	0.132505	0.287689	7614.66	7370.27	7501.74	61082.25	458687659.5	7530.55
2018-01-07	0.084722	0.261111	6429.50	6262.72	6385.43	40809.54	259708490.6	6339.04
2018-01-08	0.036759	0.243241	7760.74	7449.31	7736.25	78466.58	595404848.9	7610.90
2018-01-09	0.325000	0.450000	7272.03	7025.58	7026.96	41873.76	300301833.4	7203.46
...	...	...	...	...	...	...	...	...
2020-08-01	0.040909	0.236364	8458.65	7873.97	8160.36	85087.59	699004342.7	8045.15
2020-09-01	0.090909	0.279221	8047.11	7757.04	8045.15	40045.64	316199456.8	7817.35
2020-10-01	0.076094	0.106734	8192.05	7682.56	7817.35	55534.09	441131626.3	8190.31
2020-11-01	0.105303	0.262121	8287.42	8003.87	8190.31	30734.63	250060123.9	8024.58
2020-12-01	0.139286	0.182143	8185.14	7968.40	8024.58	17525.61	142197585.8	8181.49

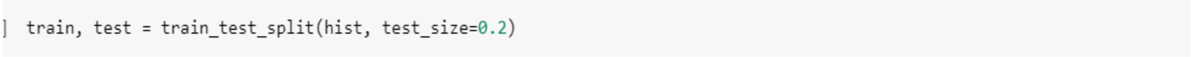
636 rows × 8 columns

Fig 25. Merged Dataset

4.2.8. DATASET TRAIN TEST SPLIT

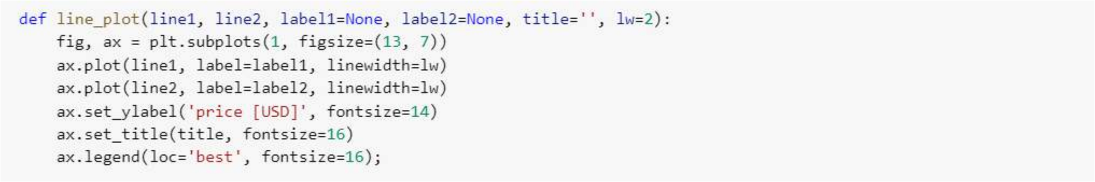


```
def train_test_split(df, test_size=0.2):
    split_row = len(df) - int(test_size * len(df))
    train_data = df.iloc[:split_row]
    test_data = df.iloc[split_row:]
    return train_data, test_data
```

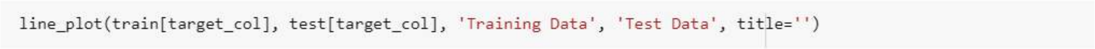


```
train, test = train_test_split(hist, test_size=0.2)
```

Fig 26. Train and Test Datasets



```
def line_plot(line1, line2, label1=None, label2=None, title='', lw=2):
    fig, ax = plt.subplots(1, figsize=(13, 7))
    ax.plot(line1, label=label1, linewidth=lw)
    ax.plot(line2, label=label2, linewidth=lw)
    ax.set_ylabel('price [USD]', fontsize=14)
    ax.set_title(title, fontsize=16)
    ax.legend(loc='best', fontsize=16);
```



```
line_plot(train[target_col], test[target_col], 'Training Data', 'Test Data', title='')
```

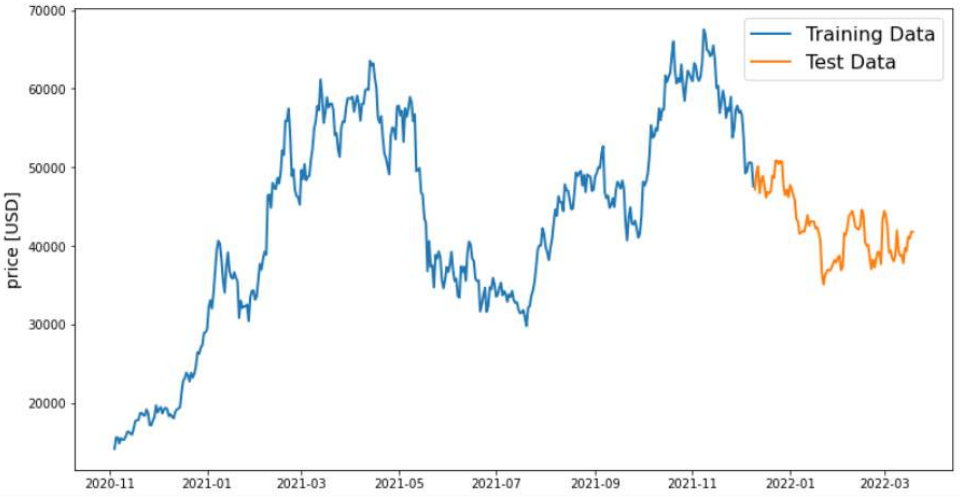
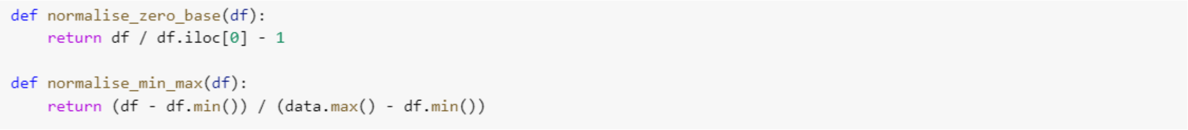
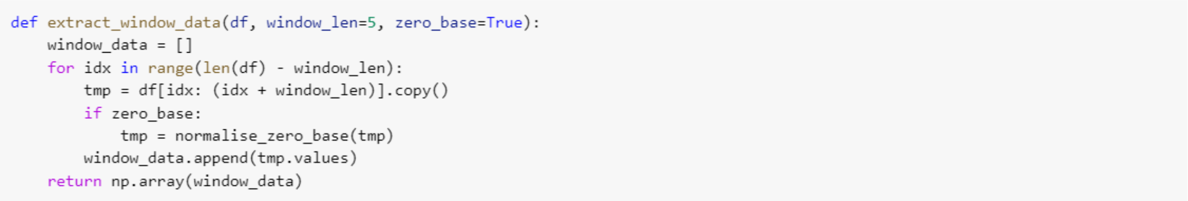


Fig 27. Time Frame of Train and Test Datasets

4.2.9. BITCOIN HISTORICAL DATASET PREPROCESSING



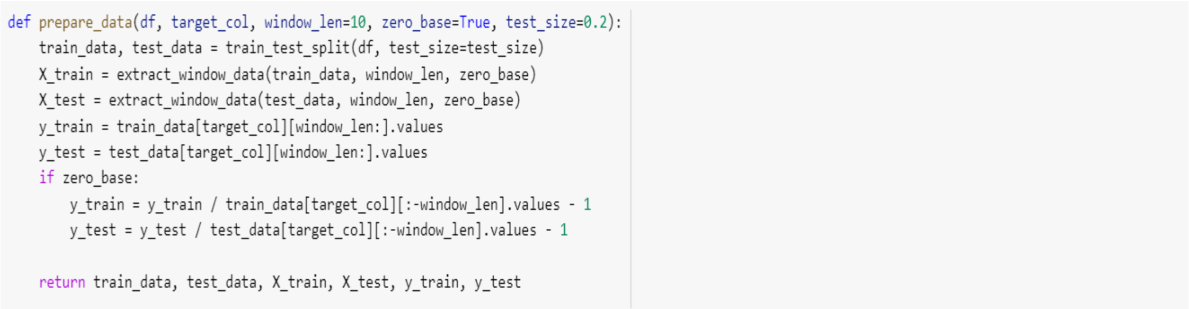
```
def normalise_zero_base(df):
    return df / df.iloc[0] - 1

def normalise_min_max(df):
    return (df - df.min()) / (data.max() - df.min())
```



```
def extract_window_data(df, window_len=5, zero_base=True):
    window_data = []
    for idx in range(len(df) - window_len):
        tmp = df[idx: (idx + window_len)].copy()
        if zero_base:
            tmp = normalise_zero_base(tmp)
        window_data.append(tmp.values)
    return np.array(window_data)
```

Fig 28. Preprocessed Bitcoin Dataset

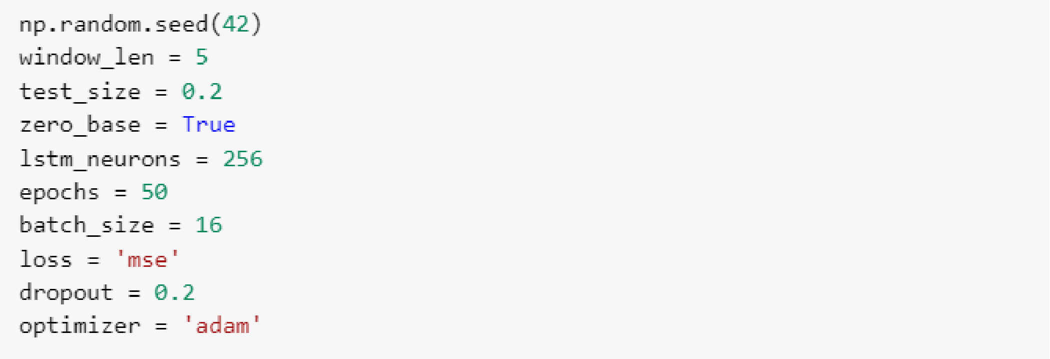
4.2.10. CONVERTING TIME-SERIES DATASET TO SUPERVISED LEARNING DATASET USING SLIDING PROTOCOL



```
def prepare_data(df, target_col, window_len=10, zero_base=True, test_size=0.2):
    train_data, test_data = train_test_split(df, test_size=test_size)
    X_train = extract_window_data(train_data, window_len, zero_base)
    X_test = extract_window_data(test_data, window_len, zero_base)
    y_train = train_data[target_col][window_len:].values
    y_test = test_data[target_col][window_len:].values
    if zero_base:
        y_train = y_train / train_data[target_col][:-window_len].values - 1
        y_test = y_test / test_data[target_col][:-window_len].values - 1

    return train_data, test_data, X_train, X_test, y_train, y_test
```

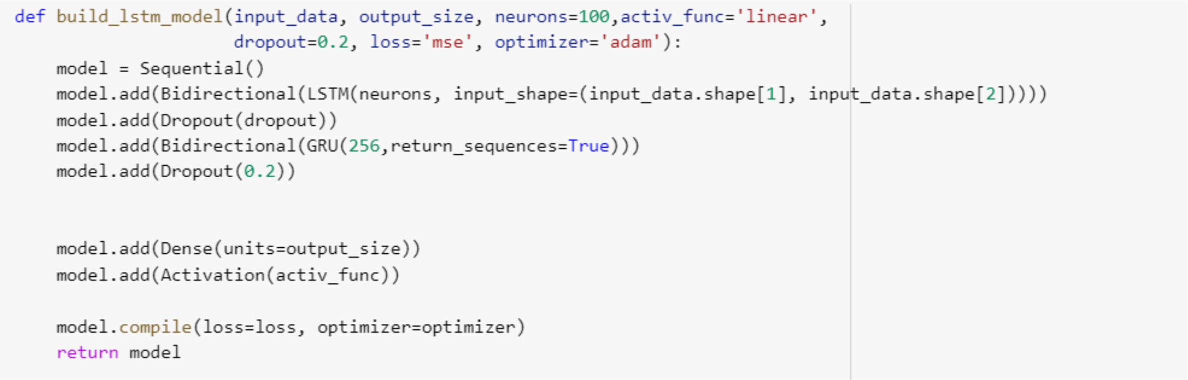
Fig 29. Sliding Window Protocol

4.2.11. BUILDING THE HYBRID-NN MODEL



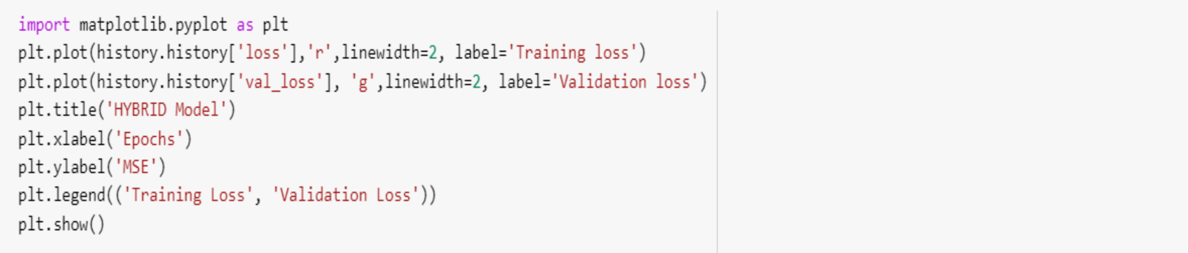
```
np.random.seed(42)
window_len = 5
test_size = 0.2
zero_base = True
lstm_neurons = 256
epochs = 50
batch_size = 16
loss = 'mse'
dropout = 0.2
optimizer = 'adam'
```

Fig 30. Hyperparameters used



```
def build_lstm_model(input_data, output_size, neurons=100,activ_func='linear',
                     dropout=0.2, loss='mse', optimizer='adam'):
    model = Sequential()
    model.add(Bidirectional(LSTM(neurons, input_shape=(input_data.shape[1], input_data.shape[2]))))
    model.add(Dropout(dropout))
    model.add(Bidirectional(GRU(256,return_sequences=True)))
    model.add(Dropout(0.2))


    model.add(Dense(units=output_size))
    model.add(Activation(activ_func))

    model.compile(loss=loss, optimizer=optimizer)
    return model
```

Fig 31. Hybrid Model Layers



```
import matplotlib.pyplot as plt
plt.plot(history.history['loss'],'r',linewidth=2, label='Training loss')
plt.plot(history.history['val_loss'], 'g',linewidth=2, label='Validation loss')
plt.title('HYBRID Model')
plt.xlabel('Epochs')
plt.ylabel('MSE')
plt.legend(('Training Loss', 'Validation Loss'))
plt.show()
```

Fig 32. Hybrid Model Loss

5. SCHEDULE , TASKS AND MILESTONES

5.1. SCHEDULE-TASKS TABLE

Table 13. Schedule-Tasks table

Task	Description	Timeline	Duration
Problem Statement	The aim and objectives of the capstone project were defined.	03-01-2022 To 15-01-2022	12 days
Literature Survey	The existing state-of-art models in the domain were studied.	16-01-2022 To 31-01-2022	15 days
Datasets Collection	The bitcoin and news articles datasets were scraped using API keys from various crypto platforms and news aggregators.	01-02-2022 To 15-02-2022	14 days
Datasets Preprocessing	The datasets were preprocessing using text processing and min max normalization and the data was cleaned.	16-02-20222 To 25-02-2022	9 days
Learning RNN models	Various RNN models were studied.	26-02-2022 To 15-03-2022	17 days
Developing RNN models	Existing state-of-art RNN bitcoin price	16-03-2022 To	15 days

	prediction models were developed on the datasets collected.	31-03-2022	
Limitations identified	The limitations were identified from the state-of-art RNN models for bitcoin price prediction	01-04-2022 To 16-04-2022	14 days
Developing Hybrid Model	The hybrid-NN bitcoin price prediction model was developed using BiLSTM and BiGRU.	16-04-2022 To 10-05-2022	24 days
Performance analysis	The efficiency and accuracy of the developed hybrid model was evaluated using various performance metrics.	11-05-2022 To 16-05-2022	5 days
Cyber-attacks on crypto identified	The existing prevalent cyber-attacks on crypto platforms were identified and analyzed as a research to understand their impact on Cryptocurrency platforms.	17-05-2022 To 25-05-2022	9 days
Implementation of a	A Cryptocurrency	26-05-2022	6 days

Cryptocurrency Attack	Cyber-attack has been implemented manually on the Ethereum platform along with a prevention method.	To 31-05-2022	

Table 13. describes the tasks included in the study, their respective descriptions with their timeline and durations.

5.2. GANTT CHART

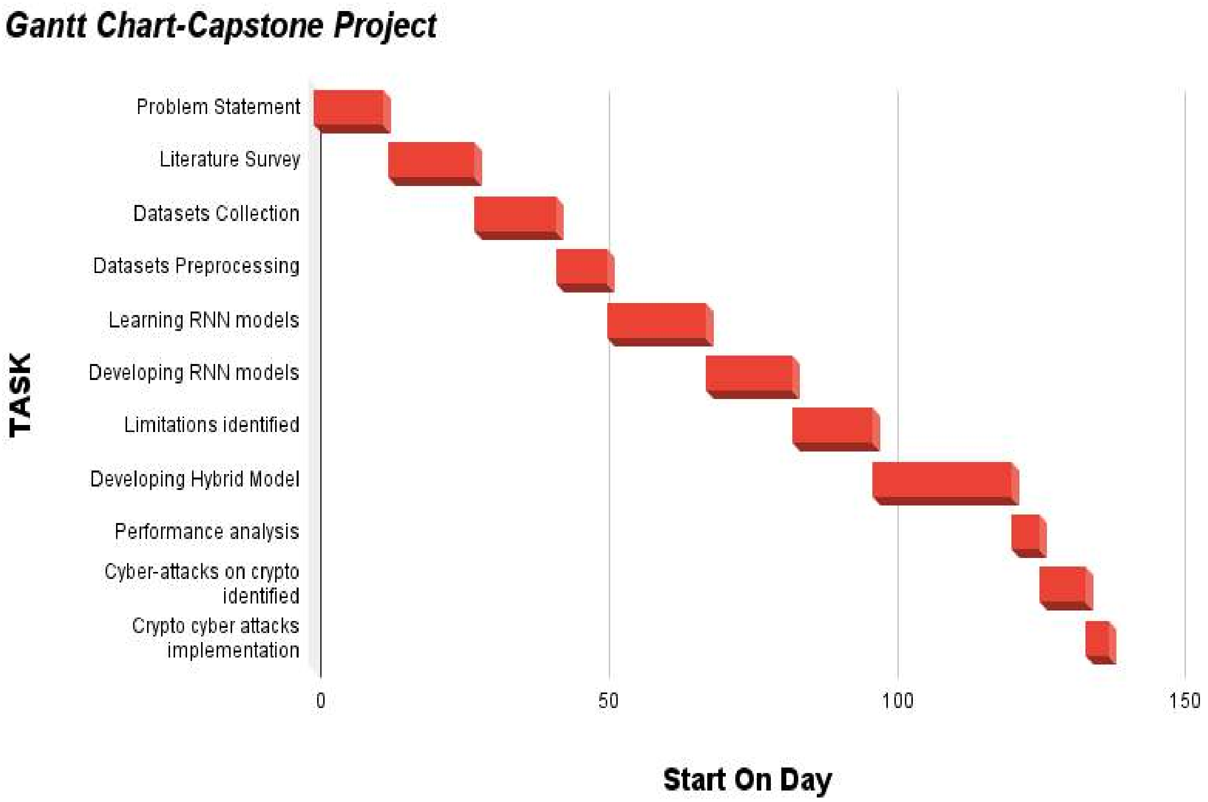


Fig 33. Gantt chart

Fig 33. shows the gantt chart of the proposed work.

5.3. TIMELINE CHART

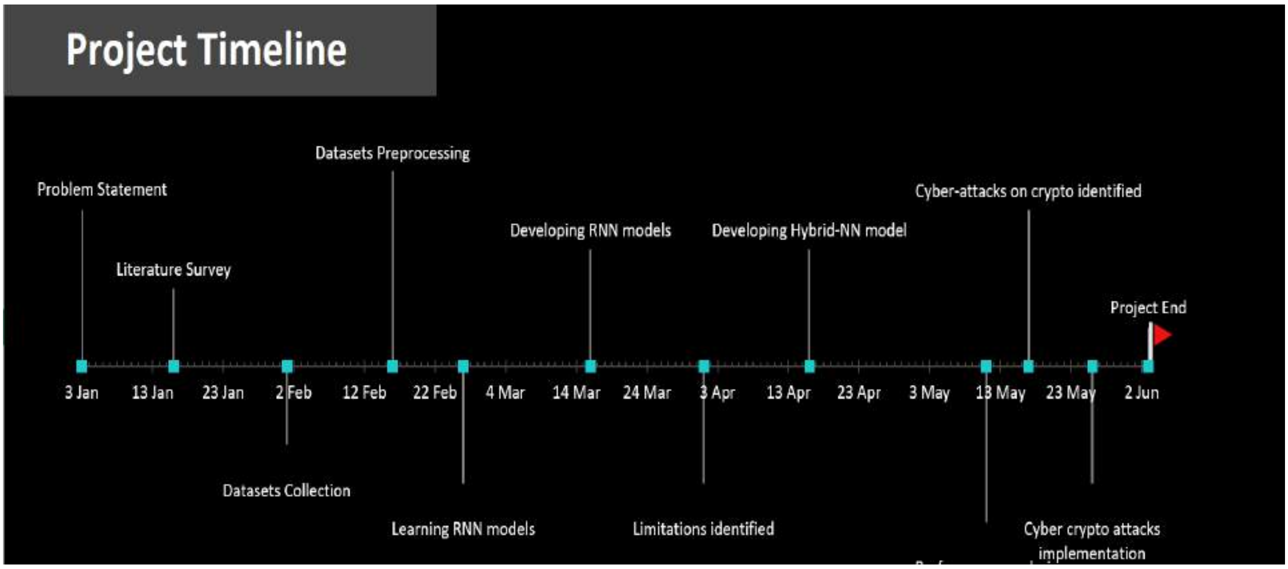


Fig 34. Project Timeline chart

Fig 34. Shows the project timeline chart and the milestones represent the start day of the tasks.

6. PROJECT DEMONSTRATION

Various RNN models such Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), Bidirectional Long-Short Term Memory (BiLSTM), Bidirectional Gated Recurrent Units (BiGRU) were developed for bitcoin price prediction with news articles sentiment analysis. The performance analysis of the models has been done using performance metrics such as precision, recall, accuracy and mean-squared error (MAE). Fig 35. Shows the accuracy scores of the RNN models. Fig 36. Shows the precision scores of the RNN models. Fig 37. Shows the F1-scores of the RNN models. Fig 38. Shows the MSE values of the RNN models. Fig 39. Shows the line graph of 90 days bitcoin price prediction using BiLSTM. Fig 40. Shows the line graph of 90 days bitcoin price prediction using BiGRU.

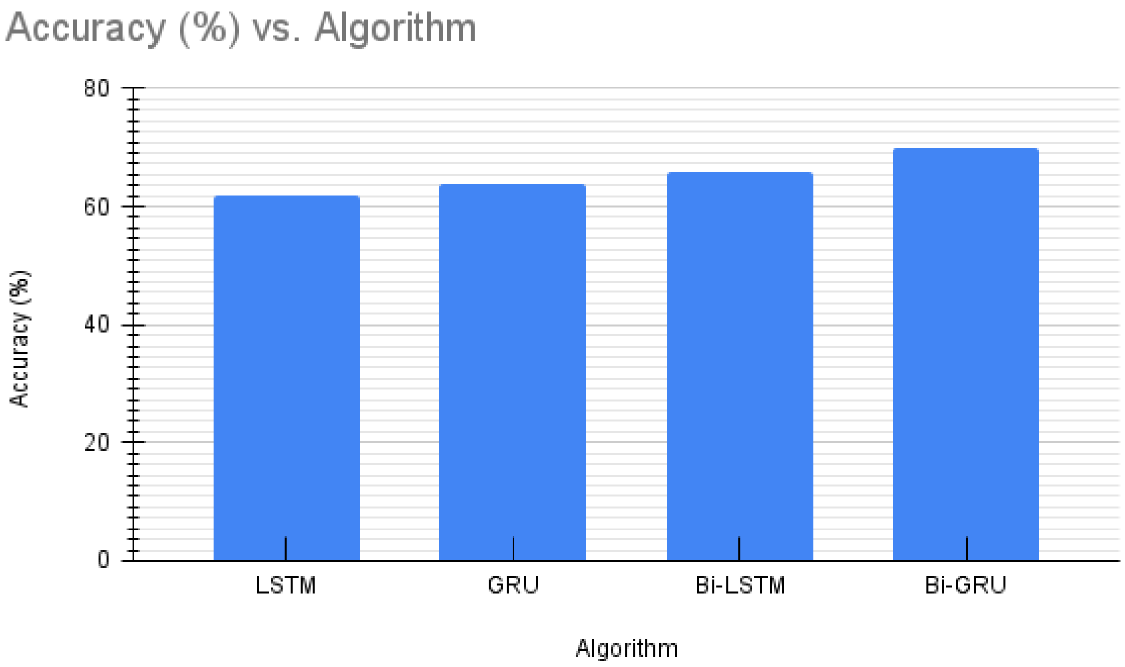


Fig 35. Accuracy vs. Algorithm of RNN models

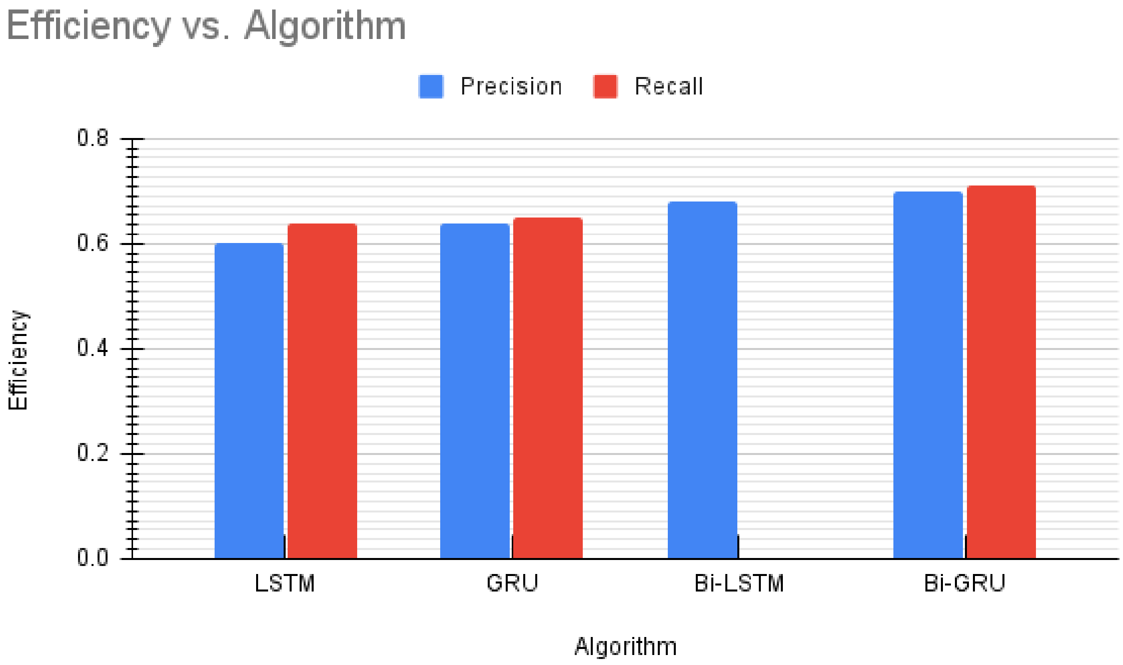


Fig 36. Efficiency vs. Algorithm of RNN models

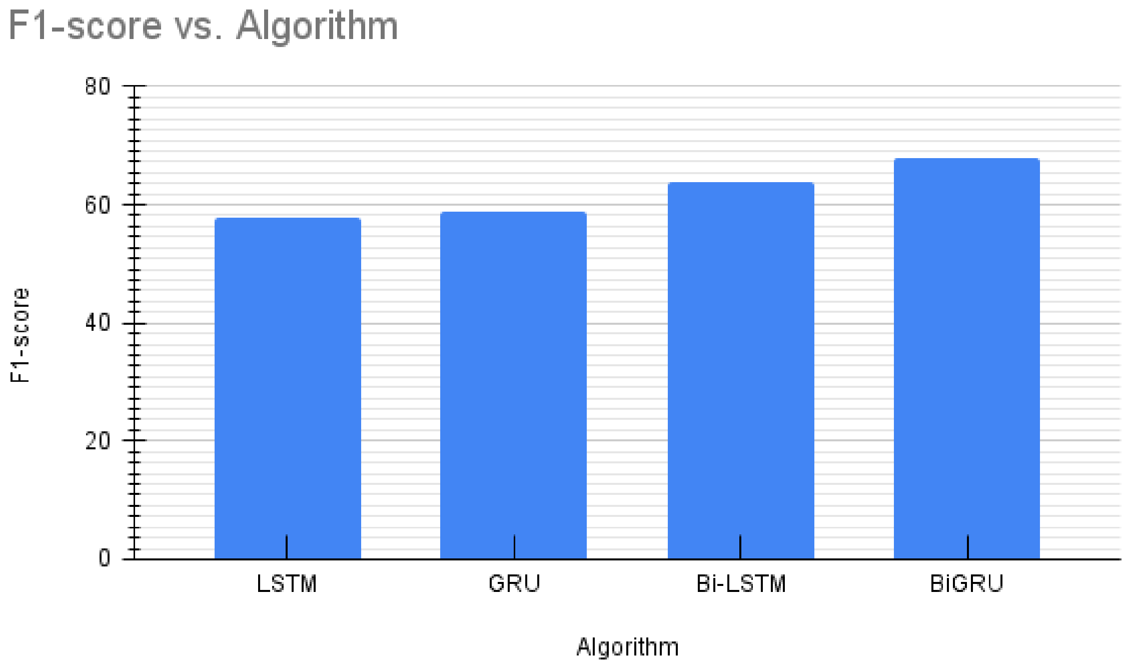


Fig 37. F1-score vs. Algorithm of RNN models

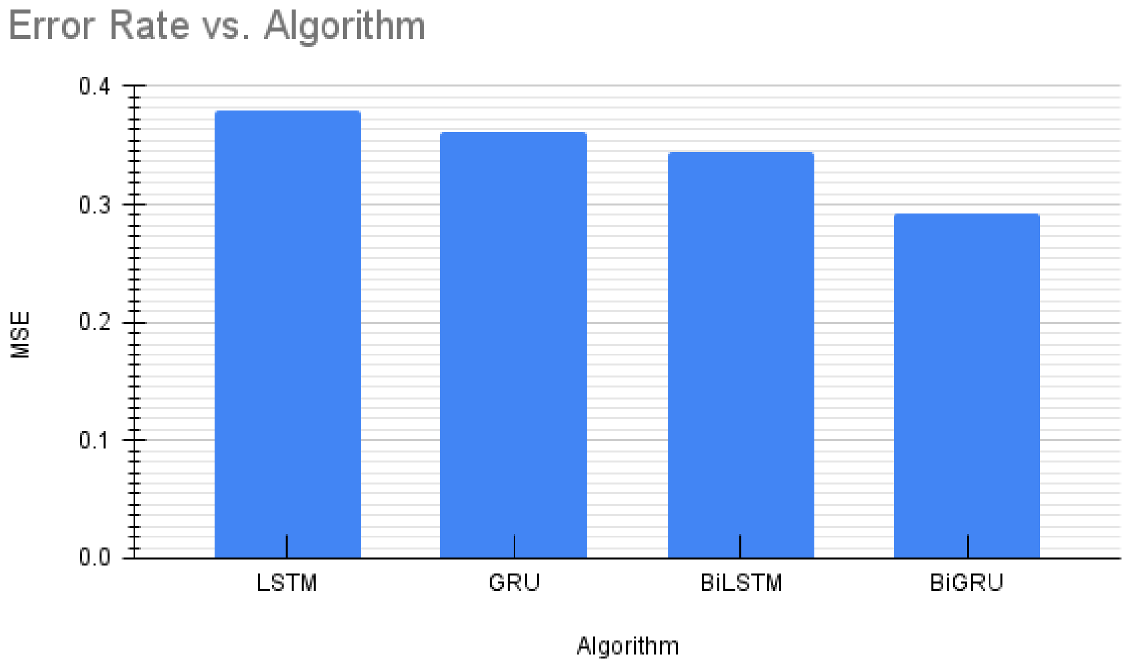


Fig 38. MSE vs. Algorithm of RNN models

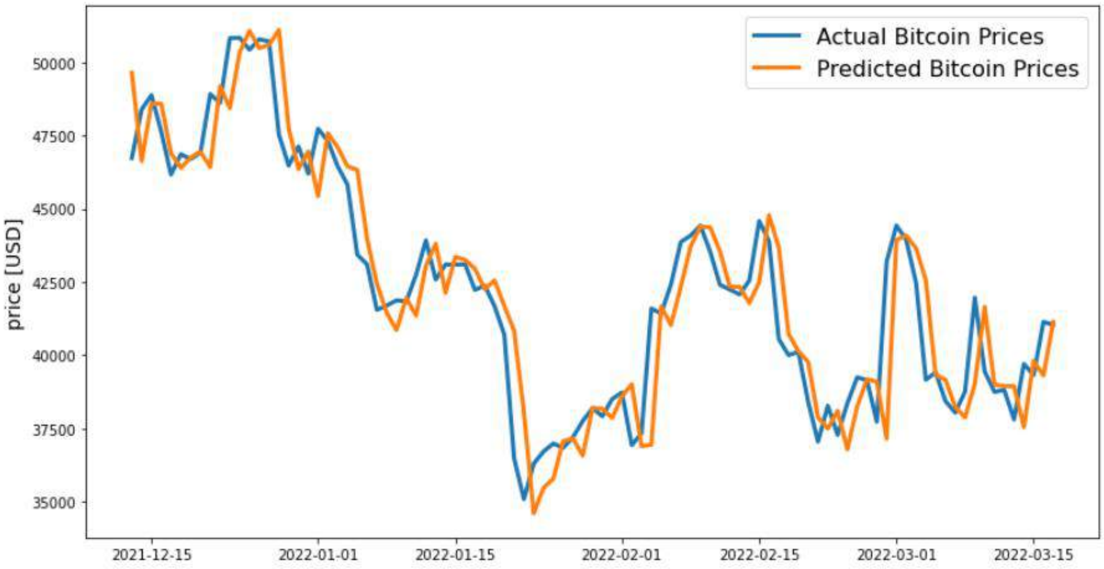


Fig 39. 90 days Bitcoin price prediction using BiLSTM

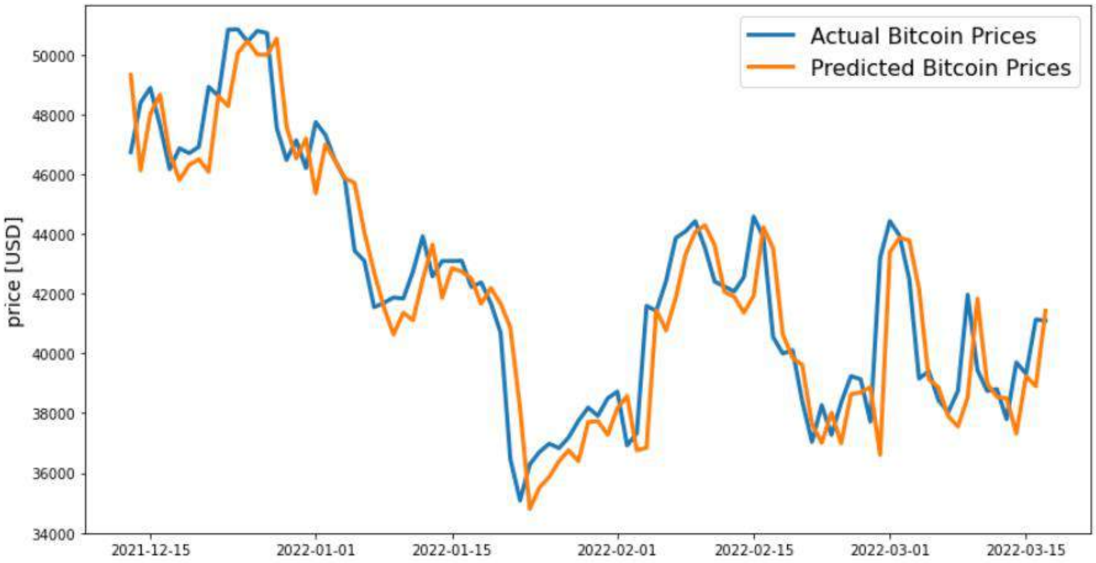


Fig 40. 90 days Bitcoin price prediction using BiGRU

Analysis of the RNN Prediction models

- The bidirectional neural networks BiLSTM and BiGRU offer better accuracy and performance than the unidirectional LSTM and GRU because the input sequences are processed from forwards and backwards for each cell state. The information can be stored for a longer duration of time without vanishing.

- BiGRU is better and faster than BiLSTM since it directly transmits the hidden state to the next neural state whereas the BiLSTM needs to use the cell state to transmit the hidden info to the next state.

- Thus, for Bitcoin Price Predictions it is advisable to use BiLSTM, BiGRU or a hybrid of the two models.

7. RESULTS AND DISCUSSION

7.1. MOTIVATION FOR THE HYBRID-NN MODEL

- For our Experimental Modeling for various RNN algorithms, we found that BiLSTM and BiGRU have the least MAPE scores.
- Thus, we intend to make a hybrid model which makes use of both BiLSTM and BiGRU layers.
- RNN models can work with 1 input layer, 1 hidden layer and 1 dense output layer.
- Adding stacked hidden layers can add to the complexity of the situation.
- Make the input layer as BiLSTM. This is because BiLSTM can show more variability in the data and it has more expressive power.
- Make the hidden layer as BiGRU since they have fewer parameters(i.e they have lesser number of gates) and the model can be trained faster.
- BiLSTM hidden layers shows greater volatility through its gradient descent compared to BiGRU owing to the greater number of gates.

7.2. PERFORMANCE ANALYSIS OF THE PROPOSED HYBRID-NN MODEL

Various performance measures are used to evaluate the proposed hybrid-NN model. The performance measures used are Mean Absolute Error (MAE), Mean Squared Error (MSE), Root Mean Squared Error (RMSE), Mean Absolute Error Percentage (MAPE).

Table 14. Performance measures of the proposed hybrid-NN model.

ALGORITHM	**MAE**	**MSE**	**RMSE**	**MAPE(%)**
Proposed Hybrid-NN Model	0.0263	0.0014	0.0380	1.7817

Table 14. shows the performance measures of the proposed hybrid-NN model. The hybrid-NN model shows better performance than the state-of-art models. The proposed hybrid-NN model is able to achieve a lowest MAPE(%) score of 1.7817 surpassing the state-of-art models.

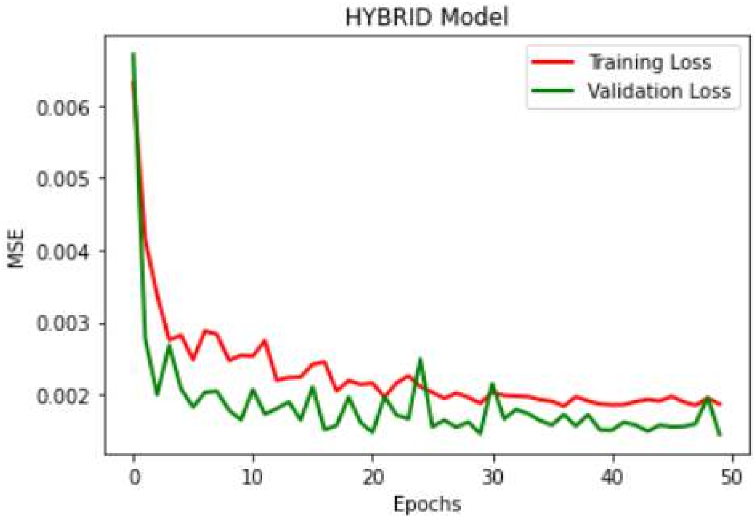


Fig 41. MSE vs. Epochs of Hybrid-NN model

Fig 41. Shows the loss vs. epochs of the proposed hybrid-NN model.

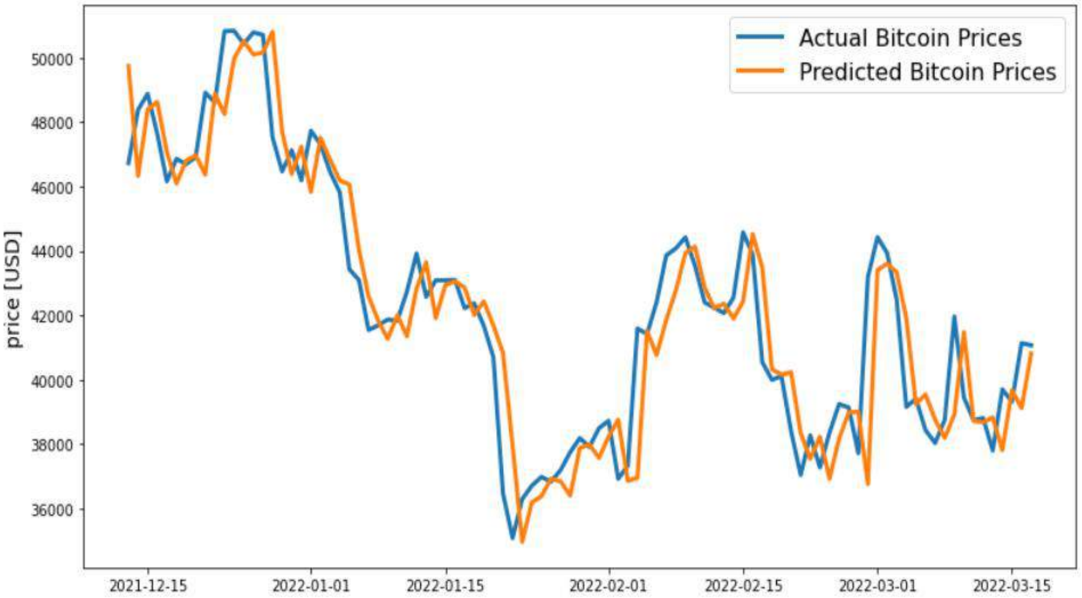


Fig 42. 90 days bitcoin price prediction using proposed Hybrid-NN model

Fig 42. Shows the 90 days bitcoin price prediction using proposed Hybrid-NN model.

7.3. CRYPTOCURRENCY PRICE PREDICTION APP

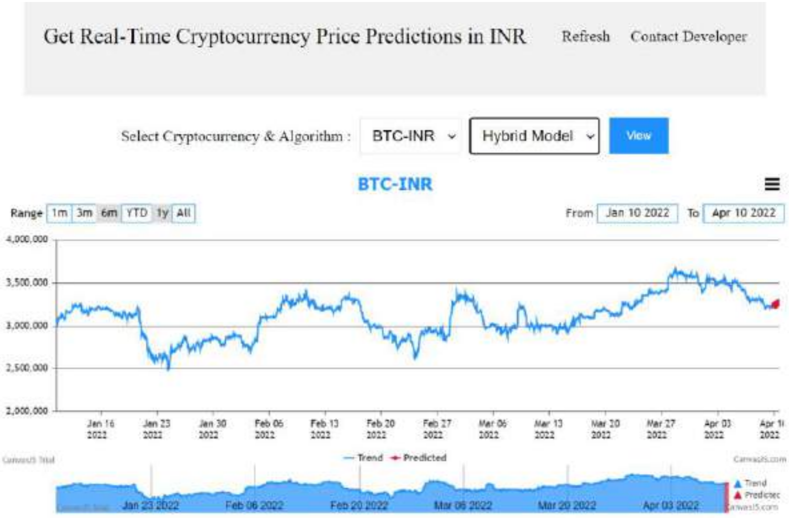
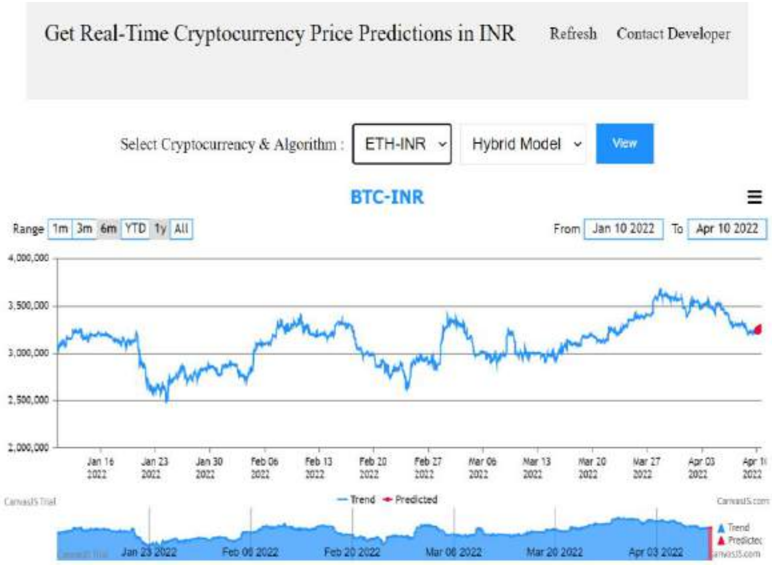


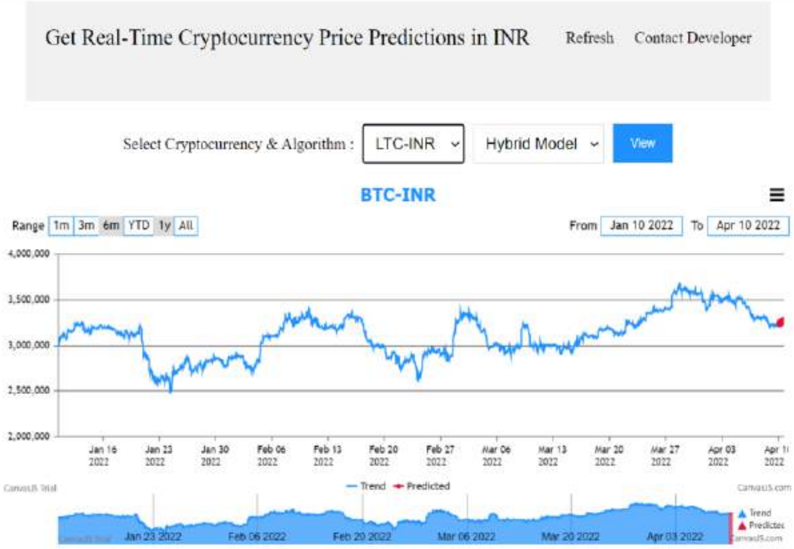
Fig 43. Real-time bitcoin price prediction using hybrid-NN model



Get Real-Time Cryptocurrency Price Predictions in INR Refresh Contact Developer

Select Cryptocurrency & Algorithm : ETH-INR Hybrid Model View

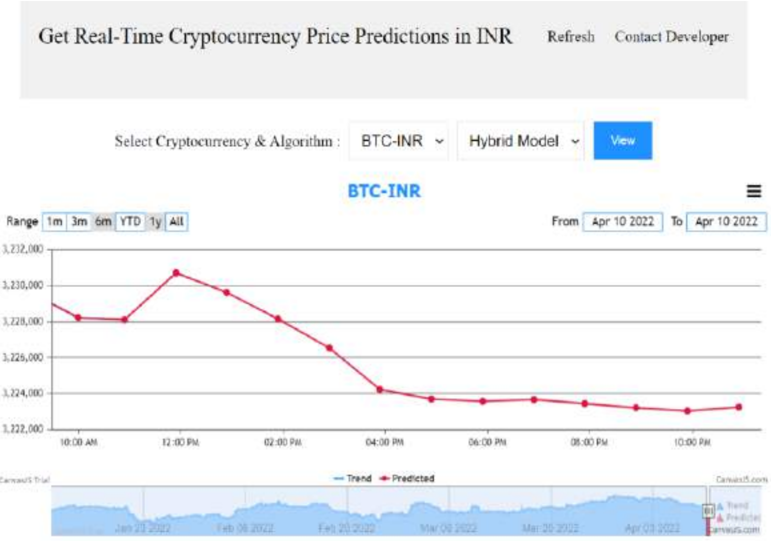
Fig 44. Real-time Ethereum price prediction using hybrid-NN model



Get Real-Time Cryptocurrency Price Predictions in INR Refresh Contact Developer

Select Cryptocurrency & Algorithm : LTC-INR Hybrid Model View

Fig 45. Real-time Litecoin price prediction model using Hybrid-NN model



Get Real-Time Cryptocurrency Price Predictions in INR

Select Cryptocurrency & Algorithm : BTC-INR Hybrid Model

Range: 1m 3m 6m YTD 1y All

From Apr 10 2022 To Apr 10 2022

Fig 46. Real-time hourly bitcoin price prediction

8. SUMMARY

In this study, we have developed a Hybrid Deep Learning Bitcoin Price Prediction Model by News Sentiment Analysis. Experimental Analysis shows that the proposed hybrid model outperforms the various other state-of-art models News headlines data collected Covid-19 era. This model can even be adopted after the Covid-19 pandemic to help investors and traders in their decision-making. Future research would include considering the impact of other factors on the bitcoin market movement such as Covid-19. Various different sentiment analysis techniques can also be used to improve the model. This paper also examined the known attacks on the blockchain, how they can take place on any bitcoin platform, and its basic defensive methods. The recent attacks on the blockchain system were also reviewed. Implementation of a cryptocurrency attack along with a prevention method on Ethereum platform and written a new attack that could be performed in the future. In our future work as part of cyber security, we would like to extend our study to review other types of cyber-attacks on Wallets, initial coin offering scams, and also in-depth study on improving the security protocol and working on the proof of activity.

References

[1] X. Tan and R. Kashef, "Predicting the Closing Price of Cryptocurrencies: A Comparative Study," 2019, doi: 10.1145/3368691.3368728.

[2] A. Ibrahim, R. Kashef, M. Li, E. Valencia, and E. Huang, "Bitcoin Network Mechanics: Forecasting the BTC Closing Price Using Vector Auto-Regression Models Based on Endogenous and Exogenous Feature Variables," *J. Risk Financ. Manag.*, vol. 13, no. 9, 2020, doi: 10.3390/jrfm13090189.

[3] A. Ibrahim, R. Kashef, and L. Corrigan, "Predicting market movement direction for bitcoin: A comparison of time series modeling methods," *Comput. Electr. Eng.*, vol. 89, p. 106905, 2021, doi: https://doi.org/10.1016/j.compeleceng.2020.106905.

[4] A. F. Ibrahim, L. Corrigan, and R. Kashef, "Predicting the Demand in Bitcoin Using Data Charts: A Convolutional Neural Networks Prediction Model," in *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2020, pp. 1–4, doi: 10.1109/CCECE47787.2020.9255711.

[5] O. Kraaijeveld and J. De Smedt, "The predictive power of public Twitter sentiment for forecasting cryptocurrency prices," *J. Int. Financ. Mark. Institutions Money*, vol. 65, p. 101188, 2020.

[6] T. R. Li, A. S. Chamrajnagar, X. R. Fong, N. R. Rizik, and F. Fu, "Sentiment-Based Prediction of Alternative Cryptocurrency Price Fluctuations Using Gradient Boosting Tree Model," *Front. Phys.*, vol. 7, 2019, doi: 10.3389/fphy.2019.00098.

[7] S. Mohapatra, N. Ahmed, and P. Alencar, "KryptoOracle: A Real-Time Cryptocurrency Price Prediction Platform Using Twitter Sentiments." 2020.

[8] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 858–880, 2019, doi: 10.1109/COMST.2018.2863956.

[9] S. Kamiya, J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz, "Risk management, firm reputation, and the impact of successful cyberattacks on target firms," *J. financ. econ.*, vol. 139, no. 3, pp. 719–749, 2021, doi: https://doi.org/10.1016/j.jfineco.2019.05.019.

[10] S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

[11] C. Li, D. He, S. Li, S. Zhu, S. Chan, and Y. Cheng, "Android-based Cryptocurrency Wallets: Attacks and Countermeasures," in *2020 IEEE International Conference on*

Blockchain (Blockchain), 2020, pp. 9–16, doi: 10.1109/Blockchain50366.2020.00010.

[12] R. Zhang, R. Xue, and L. Liu, “Security and Privacy on Blockchain,” *ACM Comput. Surv.*, vol. 52, pp. 1–34, 2019, doi: 10.1145/3316481.

[13] Myung and S. C. Kim, “A survey on blockchain cybersecurity vulnerabilities and possible countermeasures,” 2019.

[14] A. Jain, S. Tripathi, H. D. Dwivedi, and P. Saxena, “Forecasting Price of Cryptocurrencies Using Tweets Sentiment Analysis,” in *2018 Eleventh International Conference on Contemporary Computing (IC3)*, 2018, pp. 1–7, doi: 10.1109/IC3.2018.8530659.

[15] S. Symeonidis, D. Effrosynidis, and A. Arampatzis, “A comparative evaluation of pre-processing techniques and their interactions for twitter sentiment analysis,” *Expert Syst. Appl.*, vol. 110, pp. 298–310, 2018, doi: https://doi.org/10.1016/j.eswa.2018.06.022.

[16] H. Lyu, L. Chen, Y. Wang, and J. Luo, “Sense and Sensibility: Characterizing Social Media Users Regarding the Use of Controversial Terms for COVID-19,” *IEEE Trans. Big Data*, vol. 7, no. 6, pp. 952–960, 2021, doi: 10.1109/TBDATA.2020.2996401.

[17] W. Yiying and Z. Yeze, “Cryptocurrency Price Analysis with Artificial Intelligence,” in *2019 5th International Conference on Information Management (ICIM)*, 2019, pp. 97–101, doi: 10.1109/INFOMAN.2019.8714700.

[18] M. Rizwan, S. Narejo, and M. Javed, “Bitcoin price prediction using Deep Learning Algorithm,” in *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, 2019, pp. 1–7, doi: 10.1109/MACS48846.2019.9024772.

[19] N. P, R. J. Tom, P. Gupta, A. Shanthini, V. M. John, and V. Sharma, “Prediction of Bitcoin Price Using Bi-LSTM Network,” in *2021 International Conference on Computer Communication and Informatics (ICCCI)*, 2021, pp. 1–5, doi: 10.1109/ICCCI50826.2021.9402427.

[20] R. Gupta and M. Chen, “Sentiment Analysis for Stock Price Prediction,” in *2020 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, 2020, pp. 213–218, doi: 10.1109/MIPR49039.2020.00051.

[21] M. Saad *et al.*, “Exploring the Attack Surface of Blockchain: A Comprehensive Survey,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020, doi:

10.1109/COMST.2020.2975999.

[22] J. Dai and C. Chen, “Text classification system of academic papers based on hybrid Bert-BiGRU model,” in *2020 12th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)*, 2020, vol. 2, pp. 40–44, doi: 10.1109/IHMSC49165.2020.10088.

[23] I. Bakagiannis, V. C. Gerogiannis, G. Kakarontzas, and A. Karageorgos, “Machine learning product key performance indicators and alignment to model evaluation,” in *2021 3rd International Conference on Advances in Computer Technology, Information Science and Communication (CTISC)*, 2021, pp. 172–177, doi: 10.1109/CTISC52352.2021.00039.

[24] M. Gharib and A. Bondavalli, “On the Evaluation Measures for Machine Learning Algorithms for Safety-Critical Systems,” in *2019 15th European Dependable Computing Conference (EDCC)*, 2019, pp. 141–144, doi: 10.1109/EDCC.2019.00035.

[25] C. Kaplan, C. Aslan, and A. Bulbul, “Cryptocurrency Word-of-Mouth Analysis viaTwitter,” 2018.

[26] R. Khan, F. Rustam, K. Kanwal, A. Mehmood, and G. S. Choi, “US Based COVID-19 Tweets Sentiment Analysis Using TextBlob and Supervised Machine Learning Algorithms,” in *2021 International Conference on Artificial Intelligence (ICAI)*, 2021, pp. 1–8, doi: 10.1109/ICAI52203.2021.9445207.

[27] C. Kariya and P. Khodke, “Twitter Sentiment Analysis,” in *2020 International Conference for Emerging Technology (INCET)*, 2020, pp. 1–3, doi: 10.1109/INCET49848.2020.9154143.

[28] L. Li, A. Arab, J. Liu, J. Liu, and Z. Han, “Bitcoin Options Pricing Using LSTM-Based Prediction Model and Blockchain Statistics,” in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 67–74, doi: 10.1109/Blockchain.2019.00018.

[29] S. Tanwar, N. P. Patel, S. N. Patel, J. R. Patel, G. Sharma, and I. E. Davidson, “Deep Learning-Based Cryptocurrency Price Prediction Scheme With Inter-Dependent Relations,” *IEEE Access*, vol. 9, pp. 138633–138646, 2021, doi: 10.1109/ACCESS.2021.3117848.