National College of Ireland

Predicting Terrorism Attacks with Bitcoin Price Fluctuations using Machine Learning.

MSc Research Project
Data Analytics

Nisarg Shah
Student ID: x18137415

School of Computing
National College of Ireland

Supervisor :Dr. Muhammad Iqbal

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Nisarg Shah
Student ID:	x18137415
Programme:	Data Analytics
Year:	2019
Module:	MSc Research Project
Supervisor:	Dr. Muhammad Iqbal
Submission Due Date:	12/12/2018
Project Title:	Predicting Terrorism Attacks with Bitcoin Price Fluctuations using Machine Learning.
Word Count:	4645
Page Count:	19

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	28th January 2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

Submission Author	Nisarg Shah
Turnitin Paper ID (Ref. ID)	1232661981
Submission Title	x18137415_Research
Assignment Title	Submit the Research Paper style REPORT Here (PDF)
Submission Date	12/12/19, 00:05

Predicting Terrorism Attacks with Bitcoin Price Fluctuations using Machine Learning.

Nisarg Shah
x18137415

Abstract

The price variances in bitcoin has aroused the enthusiasm of numerous individuals towards it as a methods for fast increases, regardless of whether they are the deceitful components of the general public, for example, lawbreakers and terrorists. Terrorists have huge measure of money or assets which they can use in the fluctuating business sector of bitcoin to utilize strategies like pump and dump to rapidly build their additions and use them for subsidizing of their exercises. ISIS[1] is known for using Bitcoin as a method of accepting donations.

Objective: Does ISIS use pump and dump method to manipulate the Bitcoin prices. Do they do this when there is a terror attack in countries where ISIS is active.

Dataset: A publicly available dataset *Global Terrorism Database* maintained by Maryland State University has been used along with Bitcoin Price from Bitstamp Cryptocurrency exchange is used which is available on Kaggle.

Methodology: ARIMA[2], RNN[3] and LSTM[4] have been used to find the Bitcoin Price Prediction. ARIMA is used to find the number of people killed in Terror attacks. Patterns in fluctuations of price and terrorist attacks are found when all the data is visualized in Tableau.

Results: ARIMA had an Mean Absolute Percentage Error (MAPE) of 8% RNN had an MAPE of 6% and LSTM had the lowest MAPE of 3% for predicting Bitcoin price. Terrorism prediction had an MAPE of 33% using ARIMA.

1 Introduction

Bitcoin was introduced to the world of centralized physical currency in the year 2008 by a Satoshi Nakamoto. It is a peer to peer transaction system without the scrutiny of any government or banks. All the transactional records are maintained on a public ledger called Blockchain without any privacy invasion as they are maintained through a bitcoin address and not any other Know Your Customer (KYC) information. All the records are secure using cryptography as Nakamoto (2008) had developed it. The people who maintain the ledger and validate the transactions in a block of transactions get rewarded by new bitcoins, they are called Miners. Through this medium new bitcoins are introduced to the market. To control the market, the number of bitcoins generated

[1]Islamic State of Iraq and Syria
[2]Auto Regressive Integrated Moving Average
[3]Recurrent Neural Network
[4]Long Short Term Memory

gets halved by every 4 years. To reduce the supply and thereby increasing the demand for it. Roy et al. (2018). It is the most sought-after cryptocurrency. China is looking to bring its own version of cryptocurrency called China Coin, but it will be backed by Gold.

Bitcoin like some other finances exchange medium has its own positives and negatives. The constructive is individuals and substances having the option to move finances that doesn't include any banks and governments and alongside with them their over the top charges and various confinements or rules, yet this is being utilized by corrupt components of the general public and use bitcoin moves for illicit exchanging means, for example, weapons acquisition, drugs deal, sex entertainment, betting, tax avoidance, terrorists by abusing the benefits of obscurity from the financial guard dogs Seo et al. (2018). Terrorists were likewise found to have enormous stores in bitcoin by Ghost Security Group in Angela and Milad (2016). Another case of bitcoin being utilized by Cyber Criminals to extract money was in 2017 by North Korean cyber criminals by extricating ransoms in bitcoin by the spread of WannaCry Virus that encodes documents until the payment is paid. This affected around 2,00,000 individuals in 150 nations Oakley et al. (2018).

Countries such as Iraq, Syria, Libya, Yemen, Pakistan, Afghanistan where there is a high concentration of ISIS and other terror organizations and are also under the list made by the state department of United States of America for money laundering and some even designated as Safe Havens for terrorists. US et al. (2014) US et al. (2015) ISIS is also one the best funded terror organizations that it gets regular donations in bitcoin, cash, gold, oil etc. It also mints it own currency of gold and silver to further its funding. It is also famous for selling ancient relics on the black market and beheading of citizens when ransom demands are not met.

1.1 Motivation

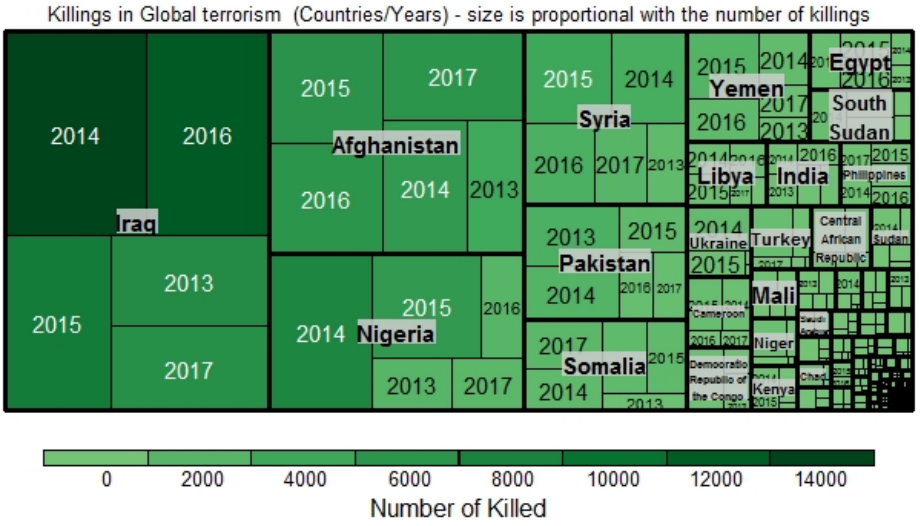

Figure 1: Number of people killed in various countries in Terror attacks over the years

The Figure 1 shows the number of people killed in the recent terror attacks shows how much active these guys are and hence we should put a stop to it as soon as possible to prevent loss of innocent lives.

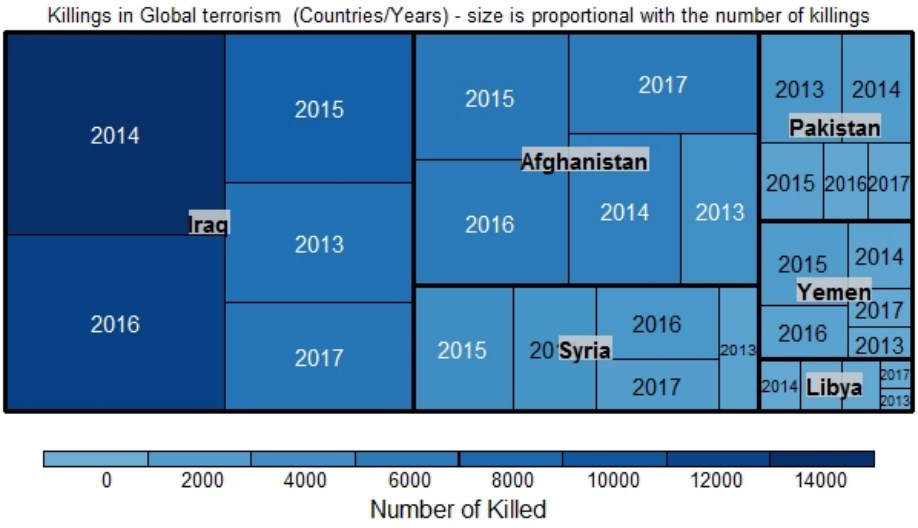

Figure 2: Number of people killed in various countries where ISIS is present

The Figure 2 shows the countries where ISIS is active and the number of people killed there in the mentioned years.

The next series of plots shows the direct correlation between Bitcoin' Price and the number of people killed. The Figure 3 shows an increase in the number of people killed increased and so did the price of Bitcoin and fell back again soon enough, proving the point that terrorist organizations use their excess cash for buying bitcoin in large quantities and then selling them when the price has increased enough and thus making the price fall.

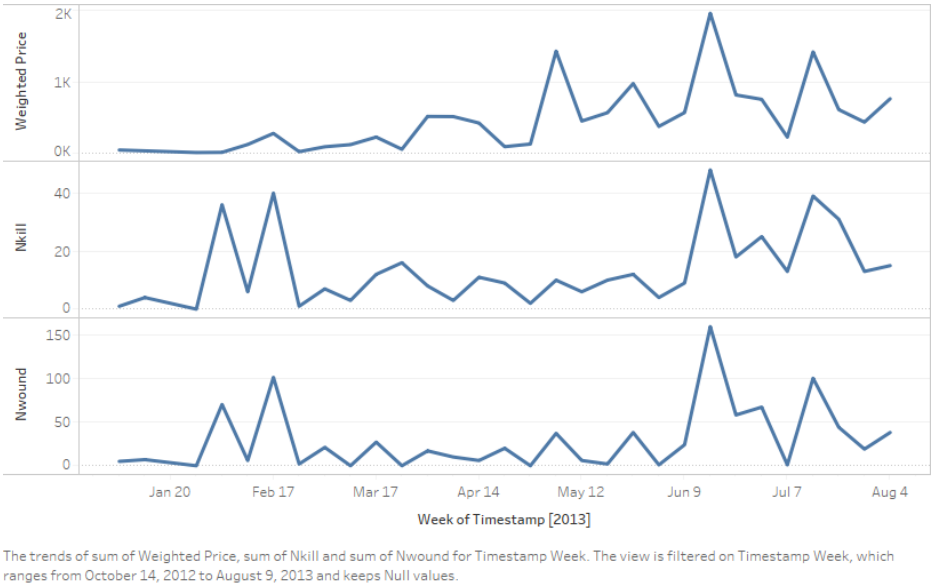

Figure 3: Initial analysis of the year 2013

As we can clearly in Figure 4 see that the trend continues even in the year 2017. This has motivated me to do this research project to help to bring an end to this unnecessary killings of innocent people.

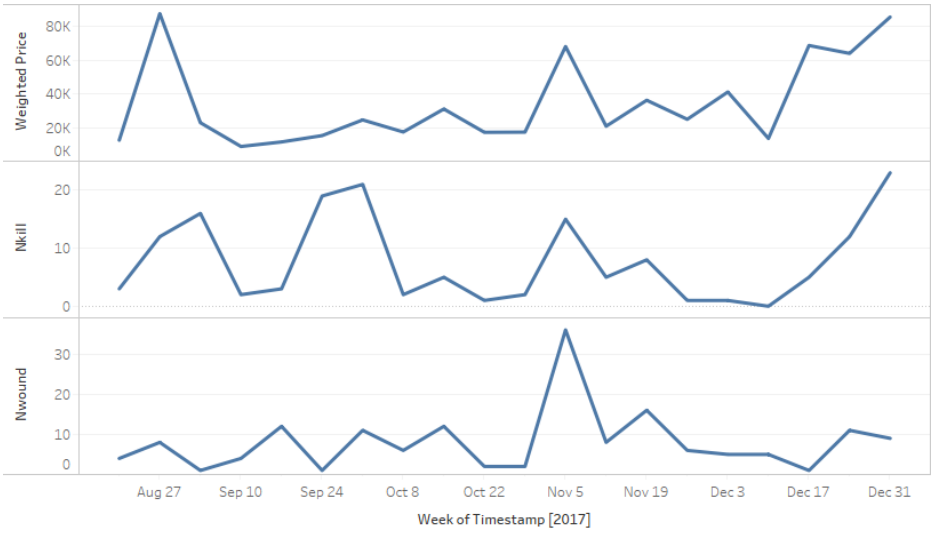

Figure 4: Initial analysis of the year 2017

Research Question : *How the daily price fluctuations in Bitcoin help in predicting terrorism attacks using machine learning algorithms for countries where ISIS is active?*

2 Related Work

Various predictions of bitcoin have been performed until this day. Bitcoin is a lucrative market for people with large amounts money to invest (whales) among other people have been behind crazy fluctuations in the recent bitcoin market. People have tried various methods to predict Bitcoin price but no one saw that even terrorists have large cash flow and have black money. They can use it to increase their funds by putting it in the bitcoin market.

The literature review is divided into 3 parts

- Bitcoin Predictions
- Bitcoin and its link to Terror activities
- Terrorism Prediction

2.1 Bitcoin Predictions

Bitcoin predictors have taken various approaches just like Yogeshwaran et al. (2019) suggests grabbing bitcoin data from the website poloniex.com SVM is used for classification of data. To reassure they deployed linear regression as well to find the general trend in values. They used CNN and RNN as a deep learning model to predict the next day's closing price. The results suggested that a difference of 5% between real world prices and predicted prices. This was achieved using CNN with 3 layers. A web application was used to display the results using python code. Phaladisailoed and Numnonda (2018) do a comparison of many machine learning models to predict bitcoin price. 1-minute intervals

data was used. LSTM was used to overcome the problem of vanishing gradient in RNN but did not achieve high accuracy which is overcome by Gated Recurrent Unit (GRU). It has a reset and update gate to determine how much data should be forgotten and how much should be taken into consideration. The best results were obtained by GRU in the optimum time. McNally et al. (2018) also use RNN and LSTM to predict the values of bitcoin from the data they got from Coindesk. They did not get high accuracy from both the results, ranging from around 50% and time required for this was also high, so they used GPU processing to reduce the processing timing by almost 50%. RNN worked best when the prediction time period was 24 days. The work by Roy et al. (2018) is also good as they got around 90% accuracy by using ARIMA and its sub products of AR and MA. The prediction done was just for the next 10 days, which is less so it's high levels of accuracy is questionable since bitcoin market is highly unpredictable. Work by Pant et al. (2018) uses tweets as a secondary tool or medium to support its bitcoin price prediction. They collect tweets then classify it as a positive or a negative tweet and put it through an RNN predictor. Multiple methods are used to classify the tweets as positive and negative like, Naïve Bayes, Multinomial Naïve Bayes, Bernoulli Naïve Bayes and Random Forest. It achieved 78.49% accuracy using RNN along with LSTM. Some researchers like Sin and Wang (2017) demonstrate their accuracy made an exchanging system dependent on the earlier day pattern and producing 85% returns through back testing technique. ANN are utilized alongside Ensemble Learning. A Multi Layered Perceptron consisting of 5 layers is made. Because of the multifaceted nature of back testing the MLP is prepared with a regulated calculation known as Levenberg-Marquardt (LM) calculation, as it demonstrated impressive improvement over heuristic calculations as far as speed and exactness. It gave a precision scope of 58 to 63%.

What's more, in conclusion Radityo et al. (2017) shows the utilization of various kinds of neural systems. It utilizes different ANN strategies and of ANN it utilizes Backpropagation Neural Network (BPNN), Genetic Algorithm Neural Network (GANN), Genetic Algorithm Backpropagation Neural Network (GABPNN) to anticipate the following day closing price. GABPNN has the least MAPE at 1.833 yet the preparation time was the most elevated of all. Second best was BPNN at 1.998 however with the most reduced preparing time expected of all. Subsequently it is the best performing technique for them all. This one-day expectation done by the framework is only for transient use however can't be utilized all things considered for long haul financial investors.

2.2 Link of Bitcoin to Terror Activities

Bitcoin has been utilized by Criminal Institutions like Terrorists because of it secrecy and practically guideline free from the AML/CTF guidelines as referenced in Angela and Milad (2016). Criminals requires an enormous income to continue themselves. Phantom Security Group an extremist gathering that claims to keep an eye on ISIS records and give data on to the authorities, they subsequent to doing chain investigation on the bitcoin exchanges discovered 2 bitcoin wallets with $4.7 and $15.7 million in them and purportedly have a place with the ISIS. They additionally affirmed that ISIS which purportedly has $2 billion in its coffers broadly utilizes bitcoin. Militant associations have been distinguished to utilize internet games as a medium to source bitcoin gifts. Another significant wellspring of unlawful bitcoin exchange is Bitcoin ATM's which can be utilized by psychological militant associations to deposit money in one finish of the globe and pull back at opposite finish of the globe, taking care of their money issue and keeping

up their identiy hidden also. Criminal institutions can even purchase their own bitcoin ATM for as modest as $6,500 and do exchanges in under 15 seconds. WannaCry was an infection that reason significant disturbance as it was a ransomware that influenced a large number of individuals as it encoded people groups document and except if a specific sum was paid by the individual in bitcoin, the records were not unscrambled. This was accepted to be another strategy by insane cybercriminal amassing riches for psychological warfare exercises. It utilized a secondary passage in old Microsoft frameworks who had not refreshed their frameworks, and this influenced in excess of 2,00,000 individuals in excess of 150 nations. Oakley et al. (2018) referenced somebody made a programmed bot for twitter that revealed the sum that was saved into the record of the individual and the sum in dollars too. Till now 20.041 Bitcoins have been gotten in it and afterward further moved to two other bitcoin wallets, this was then part and re split and moved to different records, in absolute more than 10 bitcoin wallets have been utilized for the equivalent. This methodology referenced by them gives a knowledge regarding how lawbreakers or psychological oppressors worked in the bitcoin biological system. Toward the finish of 2017, it was attested by USA, UK and Australia that North Korea was behind the assault to raise money for their nuclear missile project.

Criminal on the hidden web or dark web have numerous apparatuses in convenient to keep their obscurity from the investigation of the legislature and white programmers. Seo et al. (2018) called attention to that criminal on the tor organize utilized blending administrations to conceal their character and move their bitcoin to their goal. Blending administrations utilize a contribution of different bitcoin senders and afterward blends the location and assets to conceal the sender or shroud the sending deliver and send to various bitcoin accepting location. To be specific some bitcoin blending administrations accessible on the tor are: Bitcoin Fog, Coin Mixer, Crypto Mixer, Bitcoinmix. What's more, in conclusion Michel (2008) brought up that criminal associations utilize numerous technique to expand their benefits made by unlawful exercises. Some of them are, Pump and dump, Money Laundering, False Documentation, Extortion. The fundamental fascinating purpose of the all being Pump and dump. Since the paper is before the dispatch of bitcoin administration, they didn't think about this reality by any means. Siphon and dump are a strategy used to siphon all the cash and afterward when all is good and well dump every one of the benefits and pull back all money. This technique benefits select not many and unaware individuals and their reserve funds are lost all the while. Concerning we presently think about how criminal institutions may utilize bitcoin to build their benefits and if there is any connection between bitcoin value variances and Terror attacks or assults on inncoent public.

2.3 Terrorism Analysis and Prediction

(Baghel and Yogesh; 2018) recovered information from Kaggle with respect to the assaults led by criminal institutions on different nations and from the earliest starting point of 1970, the information sub separated by year from 1970 to 2000 and from 2001 to 2016, the lion's share being in the last mentioned. Right off the bat, the information is put through fast excavator and bunching of the equivalent is performed. The outcome got was k implies was actualized which gave the ideal Davies Bouldin Index. Numerous visual investigations were directed to show which variable is influenced. Kim et al. (2018) utilize profound taking in based named element acknowledgment from the GTD (Global Terrorism Database). They utilized semantex, a standard based framework to

mark the information with custom names to produce preparing information for profound neural system. Along these lines they created a marking technique to naturally name the information automatically.

Talreja et al. (2017) needs to anticipate the culprit by doing investigation on the GTD. They have partitioned the dataset into Training and Testing, yet before doing that they envisioned the information onto India with respect to which district has the most elevated dread assaults. They embedded the information into Rapid miner and run many AI models on it. Fast excavator is an apparatus that will run numerous approach's on it and give the best strategy for that information. They run K-implies grouping, Boruta Analysis, and C4.5 or Decision Tree, SVM or Support vector machine was the best one as they physically made changes in the information and actualized experimentation till they found the most elevated precision of 78%.

The exploration done by Mo et al. (2017) and Gohar et al. (2014) shows the utilization of GTD alongside information mining procedure with Support Vector Machine (SVM), Naïve Bayes (NB), and Logistic Regression (LR). Right off the bat, the information is handled to expel any undesirable things and clear the spaces in the information for consistency. Next the component is chosen from a rundown of highlights, the thought being the less element the higher the precision in forecast of terror assaults. Thirdly doing all arrangement strategies on them to locate the one with most elevated exactness. For this situation Logistic relapse has the most noteworthy exactness of 78.41% because of the seven chose highlights from the GTD and accomplishing 92.75% precision in the last mentioned.

Toure and Gangopadhyay (2016) states building up a standard based expectation framework where they have set principles to increment or decrements the danger of an assault in the coming 10 days or not. For this they utilized information from different areas like Mali, Yemen, Nigeria, Kenya and Libya. On testing for the 6 principles they had set out they watched a most extreme exactness of 96.3% which is extraordinary.

A crime forecast model was created to unravel past unsolved cases by Ozgul et al. (2009) and it worked incredible on smaller criminal organization's activities as they pursue a comparative Modus Operandi than bigger gatherings with a precision of 81% since they continue changing their MO to maintain a strategic distance from recognition among authorities and complete their assignments.

3 Methodology

The methodology applied in this research is widely used when the information you are trying to gather is relatively new and no progress has been made in that field. For such a scenario we use Knowledge Discovery in Databases (KDD).

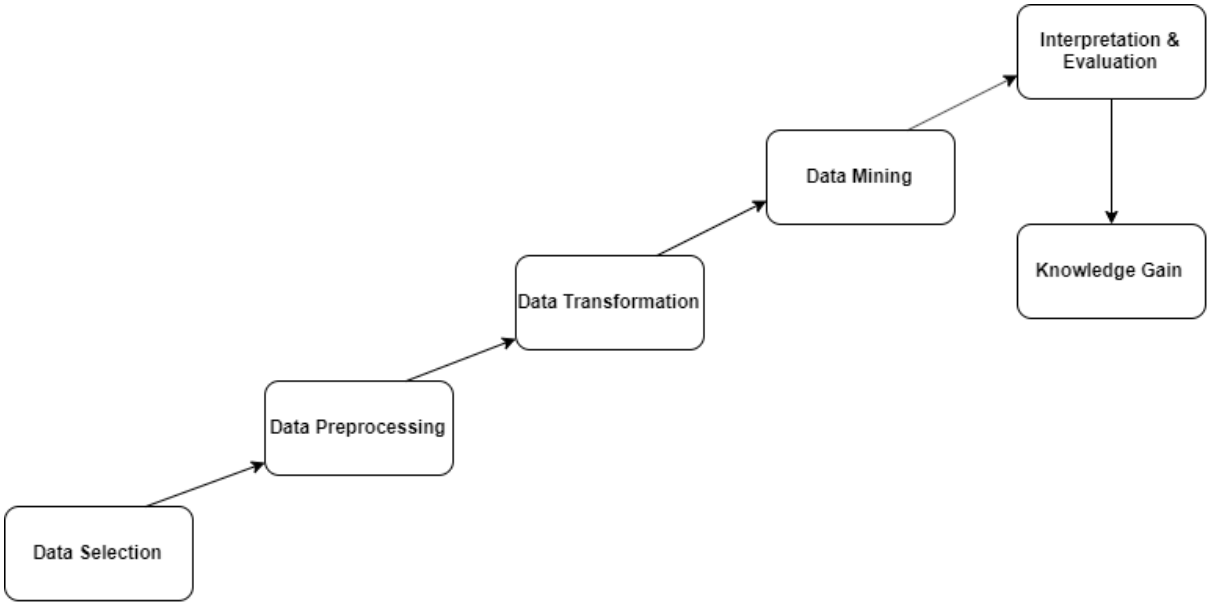

Figure 5: Knowledge Discovery in Databases

3.1 Data Acquisition

Data of both Bitcoin and Terrorism is downloaded from kaggle.com and then further processed. This is done as the data is regularly updated and many guidance tutorial are available from it.

3.2 Data Preparation

	Timestamp	Open	High	Low	Close	Volume_.BTC.	Volume_.Currency.	Weighted_Price
0	1325317920	4.39	4.39	4.39	4.39	0.455581	2.000000	4.390
1	1325346600	4.39	4.39	4.39	4.39	48.000000	210.720000	4.390
2	1325350740	4.50	4.57	4.50	4.57	37.862297	171.380338	4.535
3	1325350800	4.58	4.58	4.58	4.58	9.000000	41.220000	4.580
4	1325391360	4.58	4.58	4.58	4.58	1.502000	6.879160	4.580

Figure 6: Bitcoin Data

Bitcoin Data is loaded onto Jupyter Notebook. The timestamp of Bitcoin data is in UNIX format and hence is converted into Date format so that further operations can be conducted over it. Weighted Price is found after calculations made from the Open, High, Low and Close price to find an average price during a single day. Volume of Bitcoin and Volume Currency is not used and are removed from the data frame further on. Bitcoin data is then re sampled into daily, weekly, monthly, quarterly, and yearly to show how the data looks when it is plotted.

	Date	country_txt	nkill	nwound
0	2013-01-01	Pakistan	0	0
1	2013-01-01	Iraq	1	5
2	2013-01-01	Iraq	0	5
3	2013-01-01	Iraq	0	2
4	2013-01-01	Pakistan	0	0

	nkill	nwound
2013-01-01	48	77
2013-01-02	15	36
2013-01-03	78	152
2013-01-04	8	25
2013-01-05	40	63

Figure 7: Terror Data Before and After

Terrorism Data is loaded onto Rstudio for removing of unnecessary columns and then filtered by a year basis since bitcoin begun in the year 2013 and hence just that data is taken. Countries are filtered out with just those in with ISIS is active. After that Terrorism Data is loaded into Jupyter Notebook to convert it into a time series format data.

Data is summed up into single values: such as many attacks can happen on a date, These values are added up into a single date. Some days there aren't any attacks. So a new index is created and 0 value is place in front of the date. This helps us to create a time series format data. The 0 values are filled by using a 'ffill' function that take the average values from above and below the data frame to fill it.

This is further re sampled into weekly format to match the Bitcoin data and also to smooth-en the data.

3.3 Business Understanding

Bitcoin price fluctuations causes gains of some select few people and loss of many unfortunate people who don't know what they are getting into as they are just caught up in the greed of gaining some extra money due to peer pressure. Terror organizations use this as a unique opportunity to multiply their funds. A co-relation is found between an terror attack happening and the price of bitcoin rising and falling back. This as mentioned in Angela and Milad (2016) that terror organizations like ISIS have large funds in Bitcoin wallets.

3.4 Modelling

In this research several time series and machine learning models are used to predict the bitcoin price and terrorism attacks. After running them all ARIMA, RNN, LSTM gave good results to find the bitcoin price and ARIMA gave good results to predict the number of people killed in terror attacks.

3.4.1 ARIMA

Auto Regressive Integrated Moving Average is a famous time series prediction algorithm since it take the previous values to predict the future values.Roy et al. (2018) got 90%

accuracy using ARIMA but seasonal factor was not considered we can get better accuracy for the same using SARIMA model to get even better results.

3.4.2 RNN

Recurrent Neural Network has 3 layers namely, input layer, hidden layer and output layer. It reserves all the data from the previous layers and aids in finding better results. It reserves the values in the previous layers which aids in giving better accuracy. It does take a lot of time to run the model as it did in (McNally et al.; 2018)

3.4.3 LSTM

Long Short Term Memory an extension of RNN is a feed forward system. It has 3 gates input, output and forget gate. It gives good results for classification, processing and making predictions for time series.

3.5 Evaluation

Evaluation is performed separately using Mean Squared Error(MSE), Mean Absolute Error(MAE), Root Mean Square Error(RMSE), Mean Absolute Percentage Error(RMSE) error rate. The lowest the MAPE the better the model is at predicting values as shown in Radityo et al. (2017)

4 Implementation

Figure 8 shows the implementation of the research project. It starts with Data Collection where the data is downloaded from kaggle[5] in R and Python, where it is further processed for machine learning algorithms are applied and then evaluated and then visualized using Tableau and python.

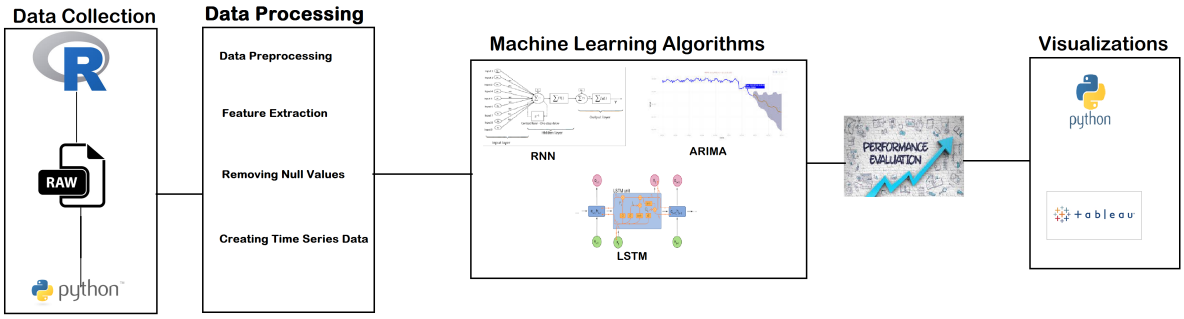

Figure 8: Implementation Flow Diagram

4.1 Data Collection

The data is collected from kaggle and then downloaded onto the local system where it is loaded either in Rstudio and Python based on the work that is easier and faster depending

[5]www.kaggle.com

on the software like where Tree maps for initial analysis can be made using RStudio and not Python.

4.2 Data Processing

Data is processed using both RStudio and Jupyter notebook.

4.2.1 Feature Extraction

Finding which columns have an effect on the final prediction, such as there are 4 prices in Bitcoin data, such as High, Low, Open, Close. Another column of 'Weighted_Price' is added to take an average value of the day. Similarly for Terror data, the number of people killed and wounded data was enough to warrant which attack was a large one or a small one.

4.2.2 Removing Null Values

Null values can be completely removed or can be replaced. In this case the null values were replaced with an 'ffill' method so they can take an average value of the cell above and below it.

4.2.3 Creating Time Series Data

The Terror Data was not in a time series format. There were days when multiple attacks took place and some days there were none. The total was added up based on the date. The missing values were replaced as 0 to complete the time series data.

4.3 Machine Learning Algorithms

Several Machine Learning Algorithms were applied on the 2 sets of different data on which prediction was supposed to be made. SARIMA algorithms were used to predict the value of Bitcoin and Terrorism with their own pre processing required. Complete data was fed to the algorithm and a separate prediction is plotted along with it.

RNN the data was split into training and testing. with the testing part having just the last 50 days of the whole dataset. 5 layers of RNN is run. After this Tensor flow is used to get the predictions, epochs of size 100 is used and batches of 64 is used to get better accuracy. The original plot of 50 days is plotted along side the predictions of the RNN system.

LSTM there is no need of the initial processing of data as it is continuation of RNN. Directly we run Tensor Flow, epoch size of 100 and batch size of 32 is used to get better accuracy. The information generated is plotted, the original value against the predicted values.

4.4 Performance Evaluation

Evaluation is done using New Mean Squared Error (MSE), Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), Mean Absolute Percentage Error (MAPE)

4.5 Visualizations

All the data that was generated was initially visualized in jupyter notebook. But to find the correlation between them. All the data i.e Weighted price of Bitcoin prediction and Number of kills of Terror Prediction is plotted together filtered on a weekly basis in Tableau to show how one affects another.

5 Evaluation

As the past research done by Radityo et al. (2017) among others have showcased the use of MAPE as a method to check the accuracy of the system after comparing it with the actual values along with the values generated by the system. As mentioned in the Table 1 below LSTM gave the highest accuracy @ 97%. Of all the bitcoin prediction methods ARIMA is lowest at 92% but it take all the data. where as RNN and LSTM predict the values of just 50 days.

Model	Accuracy
ARIMA Bitcoin	92%
RNN	94%
LSTM	97%
ARIMA Terror	67%

Table 1: Models and their Accuracy

5.1 Experiment 1: ARIMA Bitcoin

Evaluations	Accuracy
MSE	192851.83
MAE	184.4
RMSE	439.15
MAPE	0.08

Table 2: Evaluation of ARIMA Model on Bitcoin Data

As seen in Table 2 the evaluation measures of ARIMA model which was run on Bitcoin data, the MAPE error is of 0.08 i.e it has an accuracy of 92%. This high accuracy is achieved since all the data was considered into making this prediction.

5.2 Experiment 2: RNN

As seen in Table 3 the evaluation measures of RNN model which was run on Bitcoin data, the MAPE is of 0.06 i.e it has an accuracy of 94%. This high level of accuracy was achievable due to using Tensor flow and predicting values of just 50 days.

Evaluations	Accuracy
MSE	706317.44
MAE	700.53
RMSE	840.42
MAPE	0.06

Table 3: Evaluation of RNN Model on Bitcoin Data

5.3 Experiment 3: LSTM

As seen in Table 3 the evaluations of LSTM model run on Bitcoin data. The MAPE is 0.03 i.e the model has 97% accuracy the highest of all 3 models that have been run on the Bitcoin data. This high level of accuracy is acheievable due to Tensor Flow and predicting values of just 50 days.

Evaluations	Accuracy
MSE	245533.15
MAE	379.42
RMSE	495.51
MAPE	0.03

Table 4: Evaluation of LSTM Model on Bitcoin Data

5.4 Experiment 4: ARIMA Terror

Evaluations	Accuracy
MSE	2606.19
MAE	19.49
RMSE	51.05
MAPE	0.33

Table 5: Evaluation of ARIMA on Terrorism Data

6 Results and Discussion

6.1 ARIMA Bitcoin

The Bitcoin prediction using ARIMA was possible because of converting the 'timestamp' available in the dataset. It was in UNIX format and had to converted into 1 day format. It was not able to give the best accuracy in daily format due to the high fluctuations and some values were missing in it as well. Hence the data was re sampled into weekly format. The data had seasonality as well, which is obvious in financial type of data. This is a plus point in getting higher accuracy if used properly. Hence we thought of implementing the SARIMAX model that uses Seasonal data to improve predictions. The plot 9 shows the original values and the predicted values.

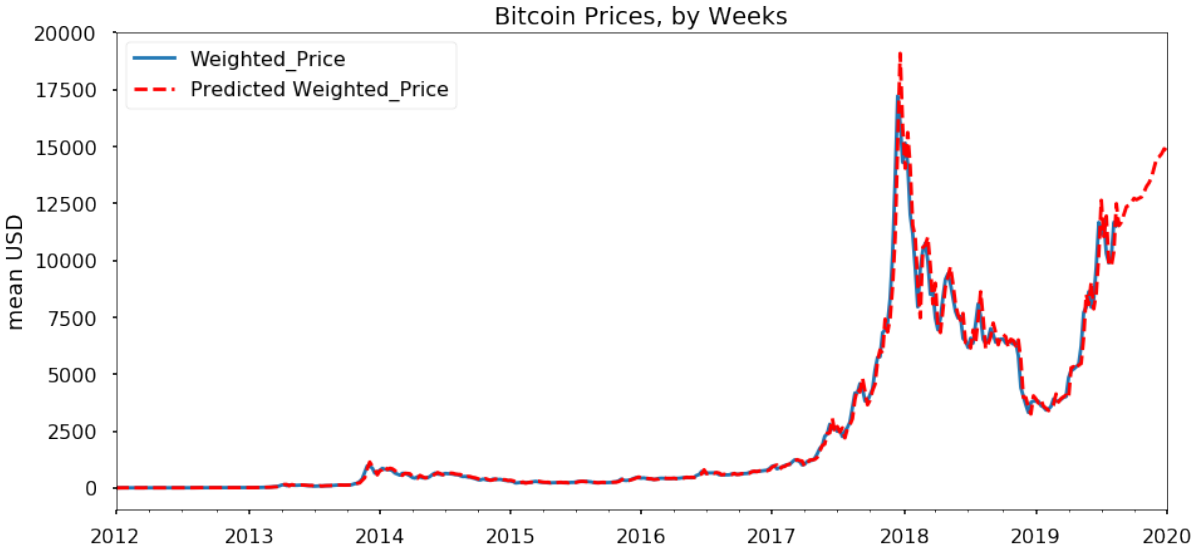

Figure 9: Bitcoin ARIMA result

6.2 RNN Bitcoin

The Bitcoin price prediction using RNN is done by running on a timeslice of 50 days using Tensor flow.

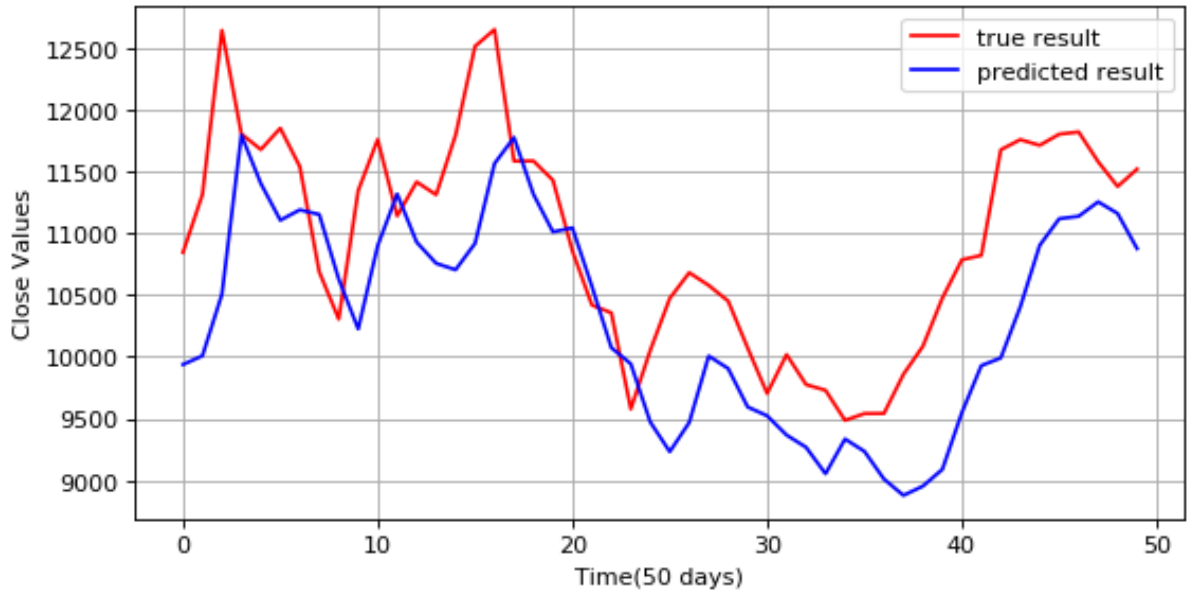

Figure 10: Bitcoin RNN result

6.3 LSTM Bitcoin

The Bitcoin price prediction using LSTM is done by running on a timeslice of 50 days using Tensor Flow.

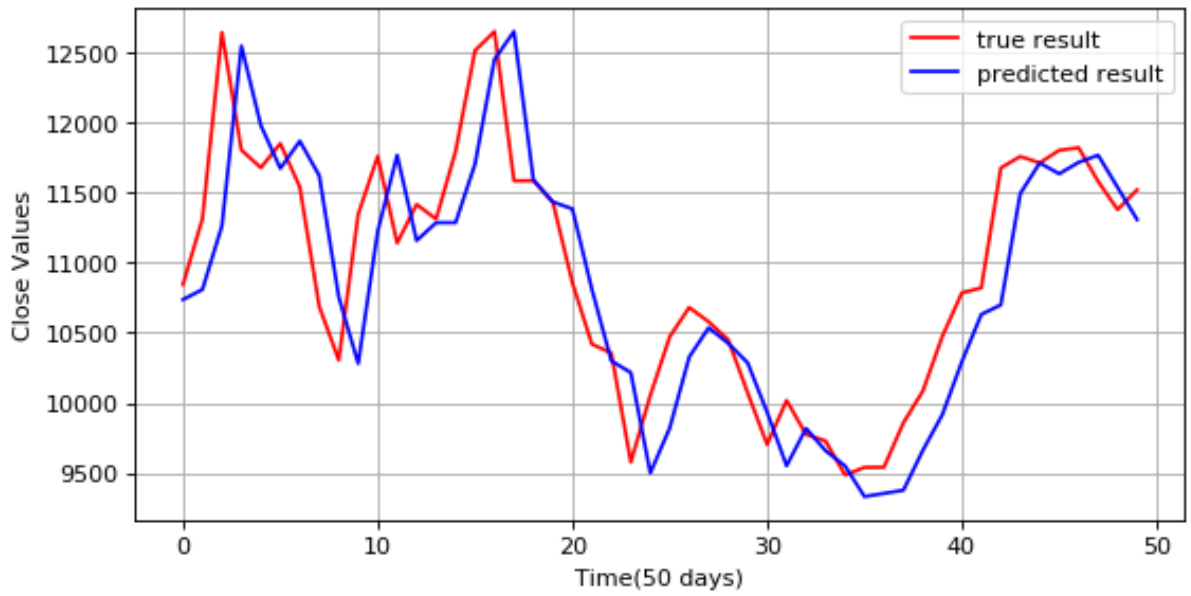

Figure 11: Bitcoin LSTM result

6.4 ARIMA Terror

The ARIMA prediction of Terror was done with a lot of pre processing. Initially the data is converted into a time series format by adding all the values based on the time of the event There have been a lot of days when there were no attacks hence the value was 0. This was handled by ffill method. Since there were many large fluctuations of values. The data was re sampled into a weekly format to match the Bitcoin Output.The plot 12 shows the original values and the predicted values.

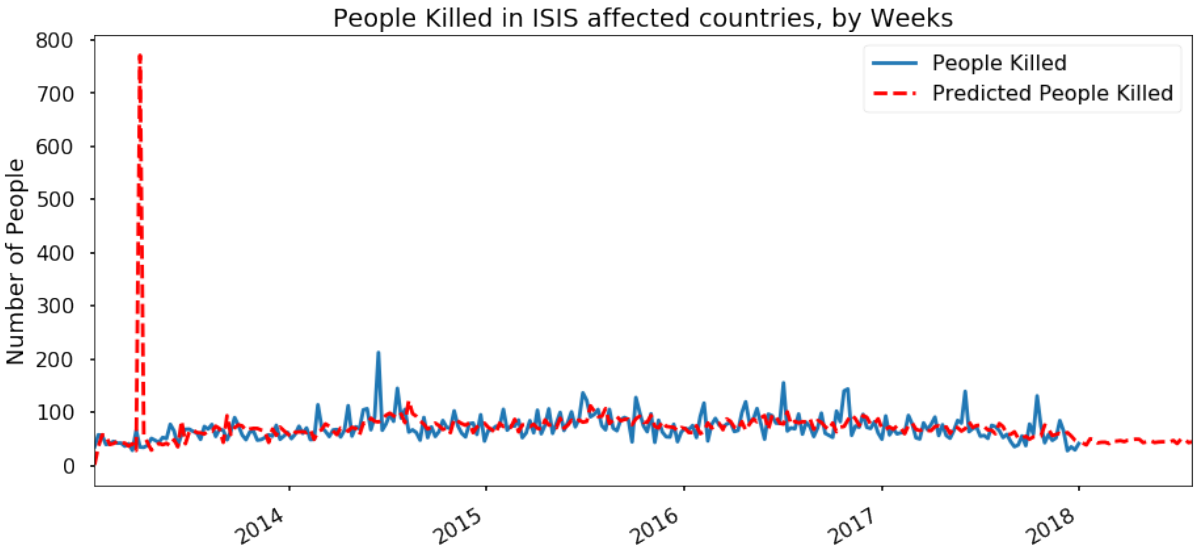

Figure 12: Terror ARIMA result

6.5 Final Result

6.5.1 Original Values

The Original values of Bitcoin Price and Number of people killed in terror attack is plotted in Figure 13

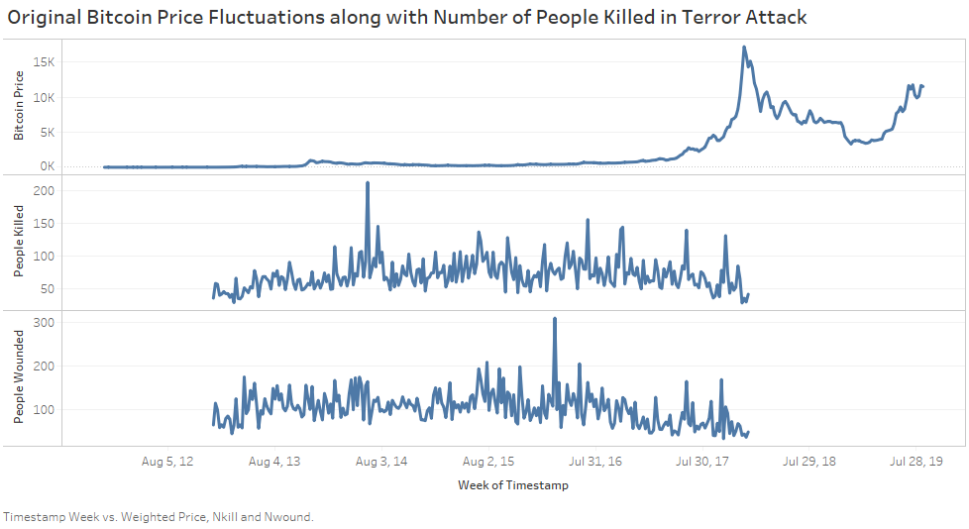

Figure 13: Original Values Graph

6.5.2 Predicted Values

The Predicted values of Bitcoin Price and Number of People killed in terror attacks is plotted in Figure 14

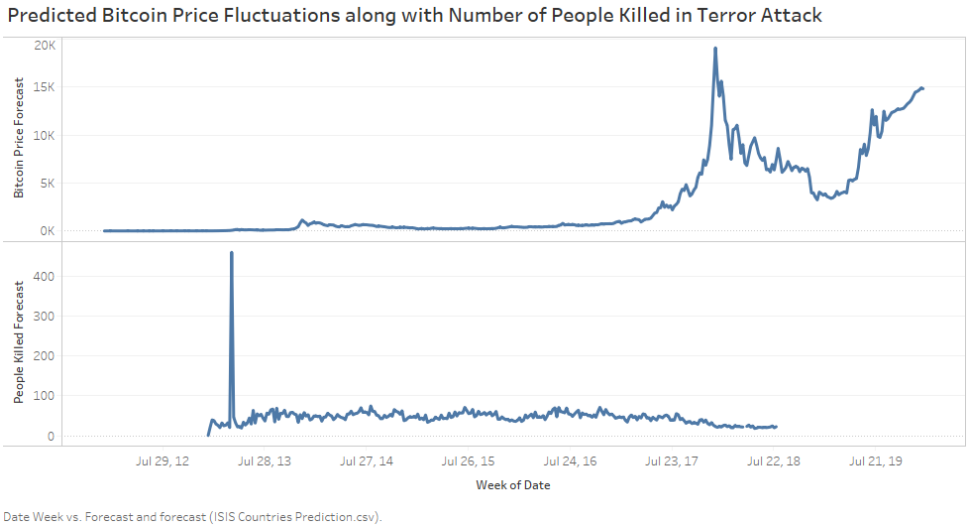

Figure 14: Predicted Values Graph

6.5.3 Original Values week wise

The original values are shown week wise to show the direct co- relation between Bitcoin price fluctuations and the number of people killed in Figure 15

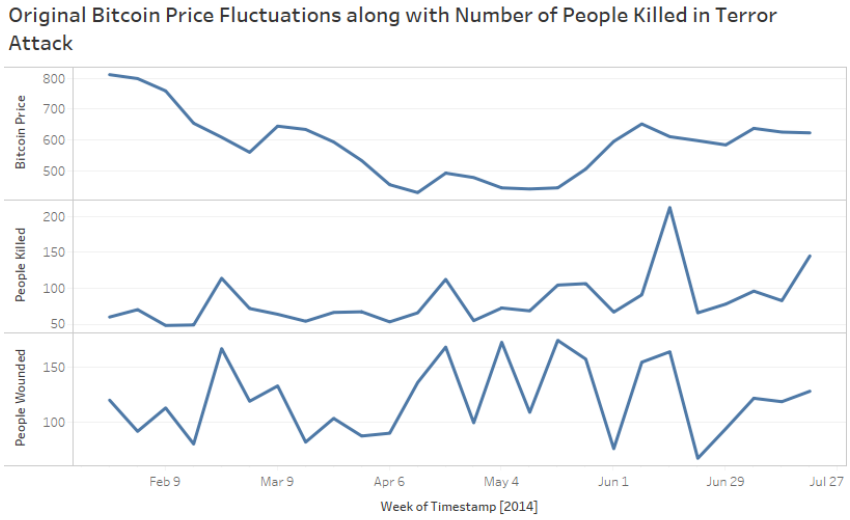

Figure 15: Original Values week wise graph

6.5.4 Predicted Values week wise

The values predicted by the system are plotted for the same days as above original values in Figure 16.

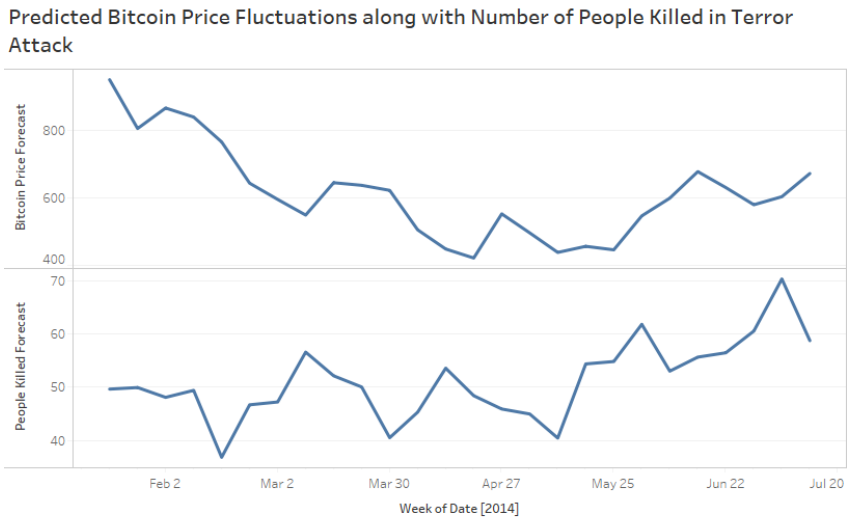

Figure 16: Predicted values week wise graph

7 Conclusion and Future Work

In this research we set out to find the answer to the question, *How the daily price fluctuations in Bitcoin help in predicting terrorism attacks using machine learning algorithms for countries where ISIS is active?* We have successfully found that Bitcoin price fluctuations have a direct link to the terror attacks in countries where ISIS have a presence. The system faces issues because of missing data and when converting data to time series.

We believe this research has opened many eyes with respect to bitcoin and how they use the public to increase the bitcoin prices and while they make the majority of the profits at others expenses. It has its own limitations because of the high level of fluctuations in data.

In the future we could create a new dataset from the above data and give a counter whenever the Bitcoin price rises and falls when there is a terror attack and do analysis through that way. we could use Neural networks to perform the same. As they have higher understanding to trends and time series. However the results of this research are high and able to find the trends as well in data.

References

Angela, S. and Milad, I. (2016). The use of crypto-currencies in funding violent jihad, *Journal of Money Laundering* **4**: 407–425.

Baghel, S. and Yogesh (2018). Detecting future terrorism trend in india using clustering analysis, *ICRITO* .

Gohar, F., Butt, W., Qamar, U. and Haider, W. (2014). Terrorist group pediction using data classification, *AIPR* .

Kim, I., Pottenger, W. M. and Behe, V. (2018). Can a student outperform a teacher? deep learning-based named entity recognition using automatic labeling of the global terrorism database, *HST* .

McNally, S., Roche, J. and Caton, S. (2018). Predicting the price of bitcoin using machine learning, *PDP* .

Michel, P. (2008). Financial crimes: the constant challenge of seeking effective prevention solutions, *Journal of Financial Crime* **15**(4): 383 – 397.

Mo, H., Meng, X., Li, J. and Zhao, S. (2017). Terrorist event prediction based on revealing data, *ICBDA* .

Nakamoto, S. (2008). Bitcoin : A peer to peer electronic cash system, *www.bitcoin.org* .

Oakley, J., Worley, C., Yu, L. and Skjellum, A. (2018). Unmasking criminal enterprises: An analysis of bitcoin transactions, *MALWARE* .

Ozgul, F., Erdem, Z. and Bowerman, C. (2009). Prediction of past unsolved terrorist attacks, *ISI* .

Pant, D. R., Neupane, P., Poudel, A., Pokhrel, A. K. and Lama, B. K. (2018). Recurrent neural network based bitcoin price prediction by twitter sentiment analysis, *ICCCS* .

Phaladisailoed, T. and Numnonda, T. (2018). Machine learning models comparison for bitcoin price prediction, *ICITEE* .

Radityo, A., Munajat, Q. and Budi, I. (2017). Prediction of bitcoin exchange rate to american dollar using artificial neural network methods, *ICACSIS* .

Roy, S., Nanjiba, S. and Chakrabarty, A. (2018). Bitcoin price forecasting using time series analysis, *ICCIT* .

Seo, J., Oh, M. and Lee, K. (2018). Money laundering in the bitcoin network: Perspective of mixing services, *ICTC* .

Sin, E. and Wang, L. (2017). Bitcoin price prediction using ensembles of neural networks, *ICNC- FSKD* .

Talreja, D., Nagaraj, J., Varsha, N. J. and Mahesh, K. (2017). Terrorism analytics: Learning to predict the perpetrator, *ICACCI* .

Toure, I. and Gangopadhyay, A. (2016). Real time big data analytics for predicting terrorist incidents, *HST* .

US, State and Department (2014). 2014 international narcotics control strategy., *INCSR* .

US, State and Department (2015). Country reports on terrorism.

Yogeshwaran, S., Kaur, M. and Maheshwari, P. (2019). Project based learning: Predicting bitcoin prices using deep learning, *EDUCON* .