DOI:

Journal of Computers and Intelligent Systems

Vol. 1, No. 1, 2023, pages 01 - 16

Journal Homepage:

https://journals.iub.edu.pk/index.php/JCIS/

ANN-Based Framework for Mitigation of Black Money Transactions in Crypto Exchanges

Muzzamil Mustafa[1*] Muhammad Zulkifl Hasan[2], Saad Hussain Chuhan[3], Muhammad Zunnurain Hussain[4], Nadeem Sarwar[5], Basit Sattar[6]

[1,6] Department of Artificial Intelligence, University of Management and Technology Lahore, Pakistan

[2]Faculty of Information Technology, Department of Computer Science, University of Central Punjab Lahore Pakistan

[3] Department of Computer Science National College of Business Administration and Economics, Lahore, Pakistan

[4,5]Department of Computer Science, Bahria University Lahore Campus, Pakistan

ARTICLE INFO

Article History:

Received:	February	16, 2024
Revised:	April	24, 2024
Accepted:	May	01, 2024
Available Online:	May	03, 2024

Keywords:

1.ANN
2. CNN
3. Neural Networks
4. BNB
5. Ethereum

Classification Codes:

Funding:

This research received no specific grant from any funding agency in the public or not-for-profit sector.

ABSTRACT

Cryptocurrencies have gained a lot of attention in the last 12 years after the launch of Bitcoin's decentralized system which allows direct online payments, Bitcoin opens up the way for many other digital currencies and coins like BNB, Ethereum, ETC (Ethereum Classic), XRP (Ripple), and many others. Many developed countries like America, Germany, France, and Belarus have started accepting payments from digital currency wallets, and their trade exchanges also allow trade through these digital coins and currencies, people of their countries use these currencies as digital financial assets, but many countries are even not ready to accept or legalize these digital currencies and coins due to chance of fraud, cyber security issues, anonymity, and privacy issues. In this paper, we have presented an ANN-based framework through which we can give a way to overcome these threats and vulnerabilities which will be helpful to countries who are looking to regularize it and who have security concerns over it. We have tested our dataset on two different models of Neural Networks, ANN and CNN. In the results CNN gives an accuracy of 81.97% on the other hand ANN gives the best accuracy of 96.72% on our dataset.

Corresponding Author's Email:

Citation:

1. Introduction

This paper proposed a research work applying Artificial Intelligence and machine learning techniques for improvement in the security system of crypto-currencies to mitigate illegal or black money transactions. Bitcoin was introduced at the end of 2008 as the first decentralized cryptocurrency that relies on the field of

cryptography for hashing and signing transactions. Bitcoin blockchain size reached 435GB in Oct 2022 [1]. This data is increasing day by day as the number of transactions increases day by day and there is a big need for automated tools to analyze this big amount of data we know AI tools can learn from that massive data by analyzing the patterns to decrease the chance of security threats. Artificial intelligence tools can learn from the patterns of money laundering and other transactions consisting of fraud and intimate the systems when these kinds of transactions are being performed to reduce security threats. In 2008 bitcoin was presented as an idea in a research paper by "Satoshi Nakamoto" [2] he introduced the peer-to-peer network technique for this digital currency and its value was 0.06 in 2010 and in 2021 it almost went up to $65000 means its increase more than 400000 times [3] from this we could think that how much importance it has for the countries which are in development phase. However, they are not taking any actions to make it regularized due to the chance of money laundering, fraudulent activities, and many other cyber issues. But it's not the main issue at all because as the world progresses day by day crimes also develop day by day like the technologies to detect these modern crimes are also becoming modern and mature day by day. According to them the only problem that could be faced by these countries is the shortage of power because these coins or crypto-currencies need the process of mining to make coins and for mining, we need a continuous and best supply of power, other than that all other security concerns are not a big problem when we already have AI algorithms. We will then provide a mechanism together with the ANN Algorithm that will cap and reduce illegal money transactions by ensuring that transactions are secure and not taking into cognizance whether the money being transacted is from legal entities or not. It is one the disadvantage of cryptocurrencies that certain people and officials of the government take the opinion that crypto transactions involve black money, which leads to their reluctance in regularizing it. The technology which is used in crypto-currencies is "Block Chain Technology" which is an advanced database mechanism or the process of recording transactions and tracking assets in a business network. Block Chain is helpful in making the transactions, orders, and payments completely transparent and confidential.

AI Algorithms in Crypto-Currencies

Crypto markets are using many techniques and algorithms of Deep learning (a type of AI) which are deep neural networks (used for solving industry problems) common implementation of DNL (Deep Neural network) is a Convolutional Neural network and this CNN used for solving Computer vision problems, NLP and audio processing. CNN is also helpful in reducing the subsampling problem and dimensionality problems because it also has a pooling layer. Many crypto trading agents and companies are using AI-based robots for the prediction of hikes in price and downfall some of the common Bots that are using AI for prediction using trends and patterns are mentioned below:-

i. 3Commas ii. Pionex iii. NAGA iv. EeToro v. CoinRule vi. CryptoHopper vii. TradeSanta viii. Shrimpy.io ix.Zignaly x. Botsfolio xi.HaasOnline xii. BitsGap xiii.Trality.

These trading bots are not only able to predict future trends they are also able to trade automatically. A study shows that almost 38% of people are using bots for crypto trading and 86% money of the crypto market circulates and trades through these bots [4]. But still, we are facing security problems in trading crypto-currencies.

Security Concerns of block-chain Technology:

As blockchain technology becomes more secure day by day the attacks are also changing their ways of attack following are the few types of attacks that can occur on a block-chain technology network [5].

i. Sybil Attack

Hackers generate fake network nodes by using these nodes they will acquire majority consensus and disrupt the chain of transactions.

ii. Endpoint Vulnerabilities

It's the most visible problem of blockchains in which hackers keep an eye on the acts of the user and electronic devices i.e. mobile/computers to steal the user's key by targeting his/her device it mostly happens when the user saves block-chain keys or passwords on their devices.

iii. 51% Attack

This attack mostly occurs when a hacker acquires the hash rate of a system and seizes control of the whole system after this hacker changes the order of transactions and forestalls them from being confirmed and even the hacker could reverse previously completed transactions that could lead to double-spending.

iv. Phishing attacks

It's the most common security concern of every field the main goal of hackers in phishing attacks is to steal the credentials of the user the main reason for it is the un-awareness of a user to IT (field) because it mostly happens by clicking on unknown or malicious or spammed links.

v. Routing attacks

A blockchain network and application rely on the real-time movement of massive amounts of knowledge. Hackers can use an account's anonymity to intercept data because it's being transmitted to internet service providers. In the case of these attacks, blockchain participants are usually unaware of the threat because data transmission and operations proceed as was common. The danger is that these attacks will frequently expose confidential data or extract currency without the user's knowledge.

The main reasons for this are the following:

a. Not using encryption
b. Not changing passwords regularly or not having a strong password
c. Not using secure routing protocols

vi. Private Keys

Private keys are also known as Seed Phrases and these phrases are to your funds if private keys are weak then a hacker can easily guess them and steal your funds.

vii. Scalability Issues

This implies that the network will solely handle a restricted variety of transactions at any given time. These issues are due to the infancy of block-chain technologies due to which quantifiability problems are occurring.

viii. Malicious Nodes

This mostly happens when a malicious company or individual floods the network with plenty of transactions or when they try to reverse valid transactions.

Paper Contributions:

This paper contributes in the field of Digital Currencies and gives a way to those who want to regularize the digital currencies in their countries. It also contributes how AI can help in the matter of regularizing Digital currencies (i.e crypto-currencies), and also contributes the security mechanism which should be adapted to overcome black money transactions over the crypto exchanges. Proposed framework with the help of AI & IoT not only detect the black money transactions it will also help to eradicate that kind of transactions.

Challenges in Crypto-Currencies

According to the study of different researchers, these are some important challenges that we are facing in crypto-currencies:

a. Security
b. Fraud Detection
c. Mining
d. Anonymity & Privacy
e. Volatility Prediction

f. Price Prediction

And some other major challenges to these crypto-currencies according to many economic experts many money launderers use these currencies to turn their black money into white and some of the experts even say that these currencies just came into being for money launderers [6]. In this, we will also discuss how we can overcome the issue of money laundering through crypto-currencies using AI methods.

a. Security

Security issues were highlighted when two large markets of digital currencies were hacked and caused their bankruptcy one was of Tokyo named Mt. Gox which was hacked in February 2014 and $477 Million worth of bit-coins was theft and Mt.Gox was declared bankrupt and the other was Flex coin which was bitcoin storage company of Canada it was hacked in March 2014 and $65000 worth bitcoins theft approximately.

The other major issue was highlighted in 2012 but verified in September 2014 by the FBI, American drug supplier company Silk Road (Addictive Drug selling Company) started an online drug-selling bazaar and received payments through bitcoin exchanges. These issues raised a big question on the authenticity of currencies/coins like bitcoin and the need for proper laws and regulations and updates in security structure arises. However, the security of these currencies now become very fair but it still needs Artificial intelligence to become more secure [7].

b. Fraud Detection

As it is well known these digital currencies didn't have a proper transaction record in the beginning so many frauds we performed using Bitcoin payment methods and fraudulent persons are not been identified yet. The most common example of fraudulent activities was published by the American Department of Justice where they reported Fake IDs and Passports are used to sell non-existent high-value vehicles priced generally between $ 10,000 to $45,000 and the fraudulent sellers received payments through crypto-currencies to avoid arrest. Now the transaction method is much better and exchanges like Binance, and CoinBase take better initiatives to overcome this [8].

c. Mining

It's also mentioned above many underdeveloped countries that do have not enough power resources cannot mine because to mine any coin or to mine a new coin we need more and more powerful resources the more power the more coins we can make and the other effect of mining is on the temperature but it has solution, which is that under-developed and other countries use the areas which are too cold to live in this way the problem of temperature rise could be prevented but the power issues need better strategies for power production [9].

d. Anonymity & Privacy

All transactions that are performed in the crypto marketplace are not encrypted from address to address so anyone can know how much coin is held by the specific address which causes many Anonymity and privacy issues [10].

e. Volatility Prediction

In the crypto crisis of 2021, many people lost their money due to the logical failure of all predictors who were not able to predict the situation of the market causing losses to many traders and local traders. Also, crypto is known as more unpredictable than stocks and bonds [11].

f. Price Prediction:

This challenge also arises in the crypto crises of 2021 when almost all price prediction bots of crypto gave the wrong predictions due to uncertainty and volatility in the market and this raises a big question about the AI techniques of Bots.

Security Layers of Crypto-currency:

The crypto-currency is secured with three layers of security

i. ICO (Initial Coin Offering)
ii. Exchanges
iii. Wallets

While choosing the currency you're taking the risk related to protocols, if some anonymous person exploits the flaws in protocol then he/she could exploit the whole network. The exchanges are a web service for the exchange of tokens & coins (i.e. bitcoin EOI & MOBI etc) and in the past, we have had many incidents that show the importance of knowing about the credibility of an exchange before choosing it for your block-chain trades the recent incident was in February 2018 when Hackers steal approximately $195 million from cryptocurrency exchange named as BitGrail Wallets can be a security risk if you are using a hot Wallet because the hot wallet is in the control of your exchange which means that if someone reached your exchange system he or she could easily steal a coin from your wallet.

Security Levels of Block-Chain Technologies:

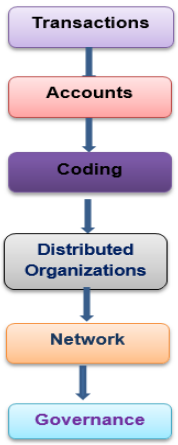

Fig 1: Security Levels of Crypto

Transactional Level:

It's the minimum required level for better blockchain technology in this level block-chain technology needs to validate the transactions to confirm the finality of a transaction.

Account Level:

Accounts have two types in block-chain technologies:

1. Account managed by self via a private wallet
2. Account managed by Exchange or by a Bot.

Bitfinex Attack is a popular attack in blockchain technologies that happens on exchanges, and the DAO replay attack is popular for private wallet hacking.

Exchanges can overcome it by working hard on security and users need to avoid private wallets because they can easily be hacked by phishing attacks.

Programming Level:

This happens when contracts or scripts could be compromised. Smart contracts can have vulnerabilities that can be compromised or can exploited, which causes the disappearance of funds.

Distributed Organizations Level:

This is related to laws of block-chain it's important for organizations who want to become autonomous. Autonomy has its risks, but firstly the organization itself must be verified and the organization must be strong before it gets a chance to run autonomously.

Network Level:

As we know blockchain technologies run on peer-to-peer network technology physically and virtually. 51% of the attack mostly happens at the network level and transactions become "hijacked" at the network level [12]. It's concerned with the soundness of algorithms, and protocols used by the blockchain.

Governance Level:

This is the most important area where work is not done means many countries have no decentralized governance, policies, and laws due to this many cyber-crimes are happening.

Security Algorithms Used by Different Crypto-Currencies

Name	Year of Adoption	Used By	Description
SHA-256 [13]	2002	Bitcoin, Peer Coin, MazaCoin, Bitcoin Cash	It's the most complicated algorithm as compared to others but It's most extensively used because data is processed through data blocks so no chance of error in it.
ECDSA	2005	Ripple, XRP	This algorithm ensures that the money is spent by their trusted owners.
SCRYPT [14]	Sep 2011	LTC, Dogecoin, Latium, Elacoin	It needs vast memory on mining devices and it is measured in KH/s (Kilo Hashed Per second).
Crypto Note [14]	July 2012	BCN, XMR, DNC, XDN	It is a proof-of-work algorithm. It is developed for ordinary mining through CPUs.
Ethash	2013	Ethereum, ETC	
X11	2014	DP, CYC, CRYPT, ADZ	It is more usable than Scrypt because it is energy efficient.
PIVX	Jan 2016	Blockchain development	PIVX Algorithm is used for the development of blockchains, this is also an energy-efficient POW (Proof of work) algorithm.
EquiHash	Feb 2016	Ethereum	It is an asymmetric, memory-driven POW algorithm that demands extreme RAM requirements to bottleneck proof generation, making ASIC advancement impracticable, just like Ethereum.

2. Related Work

Year	Technique	Contribution
2013	ML-based clustering & Classification [15]	Identifying properties of a client who performs anonymous behavior through classifying clients who exhibit suspicious activities.
2014	ML-based microstructuring techniques [16]	Reveals the chains that are committing fraud through MMT (Mobile Money Transfer System).
2016	Unsupervised ML Techniques [17]	It was developed to detect anomalies in Bitcoin transactions
2016	ML-based multifaceted approach [18]	Used K-means & Kd-trees to detect fraud in Bitcoin transactions.
2016	Clustering-based method/stress test [19]	Clustering based technique was deployed to reduce the DoS (Denial of Service) attack.
2017	Supervised ML Technique [20]	Demonstrates how large nodes are related in the Bitcoin network for cybercrime in the Bitcoin network and nodes relevant to malicious activities.
2017	ML adoption for Graphical threat detection [21]	Provides human operators with an initiative way to derive insights about the blockchain system by gathering the system's features into a group of characters that are graphically rendered.
2017	ML-based network analysis technique [22]	Used community detection of bitcoin on a network of weak signals.
2018	Data Mining Technique [23]	Detect the wallet address of bitcoin in the network to detect accounts related to Ponzi Scheme
2018	An ML-based Ransomware detection [24]	This solution was based on an analysis of ransomware dataset families to provide a layered defense system against Cryptographic Ransomware in the Cryptocurrency system.
2018	An NLP and ML-based phishing ring DNS style detection [25]	Introducing a detection scheme for phishing ring DNS style through ML and NLP techniques where the detection mechanism relies on the observation of newly registered domains.
2019	Present micro-blockchain-based dynamic intrusion detection [26]	The scope of application of block-chain was discussed
2019	Present genetic algorithm implementation to block-chain [27]	It's to cover the future applications of blockchain
2020	ML techniques of Linear Regression Intrusion decision system, Binary Neural Networks [28]	The system will evaluate and ensure the integrity of smart contracts, Execution time, and Transactional delay.
2022	Real-Time Sequential Deep Extreme Learning Machine [29]	Used smart contracts and verified control lists to provide more security to transactions.
2023	KryptosChain—A Blockchain-Inspired, AI-Combined, DNA-Encrypted Secure Information Exchange Scheme [30]	Use IDS (Intrusion Detection System) for secure Information Exchange in crypto Exchanges and their model gives an accuracy of 95.84%

3. Proposed flow of Working*:*

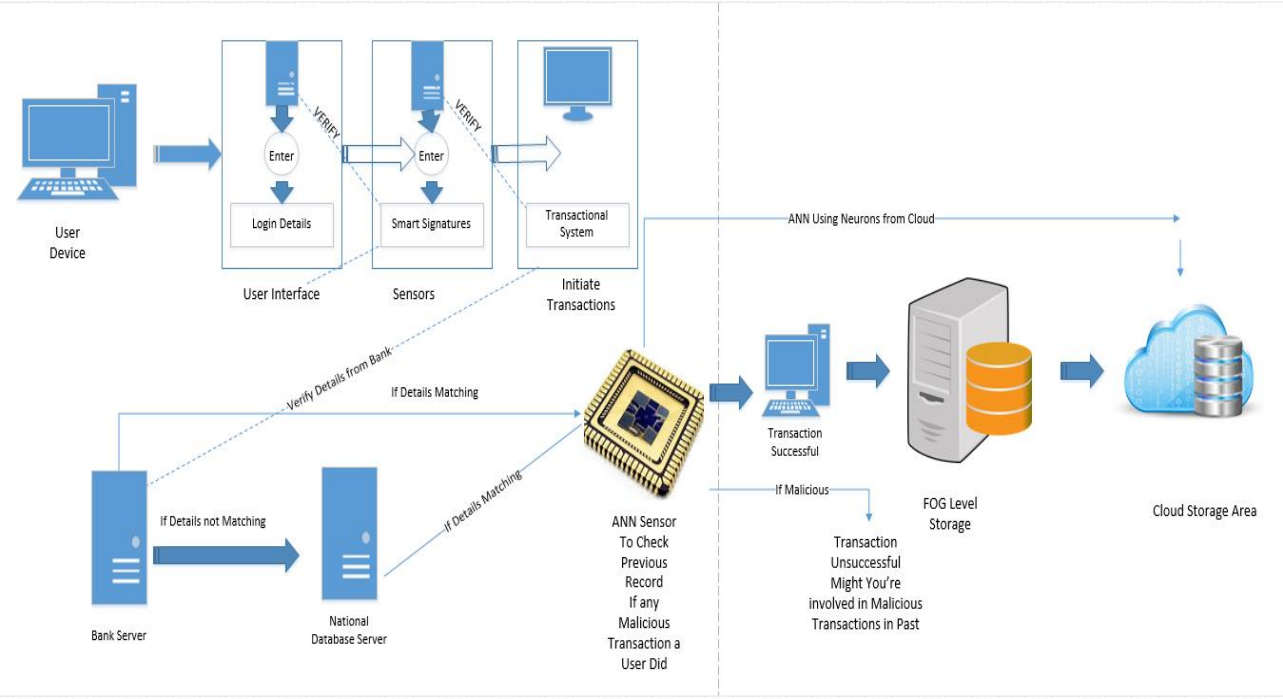

Figure 2: Proposed framework

Implementation of Proposed Framework:

As most attacks happen at the transaction level and using previous data which is stored in the server we are going to introduce a system based on IOT devices and ML Algorithms to protect the transactional level of Block-chain and we will also use some cloud security techniques to secure previous data from breaching. For effective Implementation we don't only needs the IoT and AI we also need some governing organizations and banks who involves in the whole process of transactions.

Our proposed methodology will consist of the following entities:

i. User Devices
ii. Blockchain
iii. IoT Sensors
iv. Artificial Neural Network (ANN)
v. Secure Cloud Storage

i. User Devices:

It means that the devices which are using blockchain exchanges to buy and sell digital currencies over the system will take data from these devices and the main work starts from here.

ii. Block-Chain Exchanges:

Blockchain will identify the login credentials and allow or disallow the user login after successful login user have access to all transactional options whether buy or sell. It may be **Binance** of **CoinBase** or any other Exchange.

iii. IOT Sensor:

If a user initiates a transaction whether buying or selling a coin IoT Sensors will use the following databases/APIs to check the authenticity of a user:

a. Concerned Bank:

At this level, IOT sensors will check the bank data and identify whether a user has enough funds in his/her official bank account or not if his transaction is not matching with his account statement then this user may have black money or user investing money of other persons, and maybe the other persons is using his black money on the name of this user.

b. Concerned Record-Keeping Authorities:

In case of the above failures means if the bank statement is not match the number of transactions then IoT sensors of Block-chain Exchanges take data from record keeping authority of the relevant user country to check if this user may have other sources of money I.e. properties or shares of the market if a user doesn't have it IoT sensors generate a message on systems of Money Laundering Control Agencies of that country to take necessary actions if this money is black.

iv. Artificial Neural Network Model:

As most of the attacks are on the transactional level and the above solutions are not implemented yet and even after the implementation of the above-recommended solutions we need some algorithms which can use the previous data to learn about vulnerabilities and solutions of it. ANN will check whether the person is involved in attacks on exchanges, or the user was involved in an illegal transaction or scam if a user is involved user will automatically be banned. As ANN can also do classification so in our system ANN will classify original and fake transactions.

transactions.

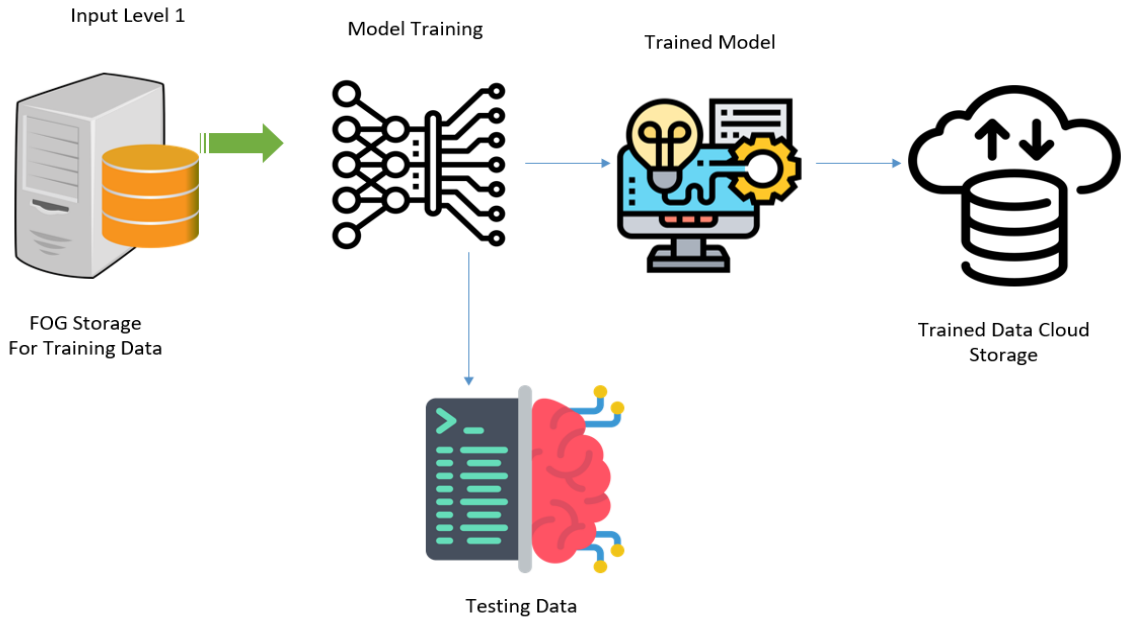

Figure 3: ANN Model Training and Neurons Storage Area

Figure 3 shows the flow of working of our model. ANN will take malware transactional data from FOG storage, and match them with testing data after that our model will store its neuron in Cloud storage to detect malware transactions in the future.

v. Secure Cloud Storage Area:

We have two storage areas one is at the FOG Computing level and one is at the Cloud level to prevent data loss in case of anonymous attacks. We are using cloud storage because the files stored on cloud servers are encrypted, which means that they're scrambled which makes have for cybercriminals to attack or access them. And cloud will also be used as storage of trained model predictions of ANN as shown in Fig 2.

Dataset/Data Collection:

The dataset of Bitcoin Heist Ransomware Dataset from the Kaggle dataset containing the address, year, time, looped, neighbor, income, and label following the model shape we got from MATLAB. The link to data is as follows: https://www.kaggle.com/datasets/sapere0/bitcoinheist-ransomware-dataset. This dataset contains the fields of name, year, address, length, weight, neighbors, count, and looped. A few fields like income neighbors are collected through different datasets because these fields are required to generate threats in our proposed system. We have tested this data set on two different models of NN (Neural Networks). This dataset also holds the data of accounts that are involved in illegal business or have done illegal transactions.

Training & Results of Model:

We have used MATLAB2023a to train and test our model of ANN & CNN models are trained and tested on different inputs to check the accuracy of our models and the results are explained below.

CNN:

- Accuracy: 81.97%
- Precision: 73.12%
- F1 Score: 73.12%

ANN:

- Accuracy: 96.72%
- Precision: 94.31%
- F1 Score: 94.31%

CNN gives us the Accuracy of 81.92% with precision of 73.12% and F-1 Score of 73.12% on the other hand ANN performed best on our data set with the accuracy of 96.72% Precision of 94.3% and F-1 score of 94.3% the full result classification of ANN is provided as under.

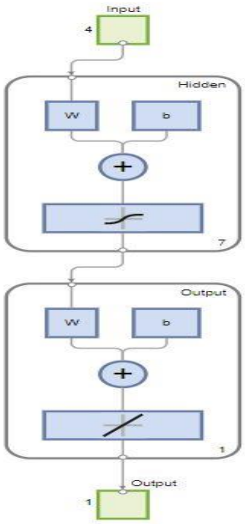

Fig.4 (ANN Model)

Following Results we obtain from this model:

Layer Size = 7

	Observation	MSE	R
Training	943717	6.6927e+22	0.1348
Validation	0	NaN	NaN
Test	104858	3.7834e+22	0.2199

Running Performance:

Training Process

Unit	Initial Value	Stopped Value	Target Value
Epoch	0	1000	1000
Elapsed Time	-	00:30:45	-
Performance	6.76e+27	6.69e+22	0
Gradient	1.08e+28	3.34e+21	1e-07
Mu	0.005	50	1e+10
Validation Checks	43	36.6	0
Sum Squared Param	55	79.2	0

In above tables we have mentioned the training testing and validation results of our ANN model that shows an efficient accuracy of 96.72% in predicting vulnerable transactions over the cryptocurrencies networks.

Gradient Plot:

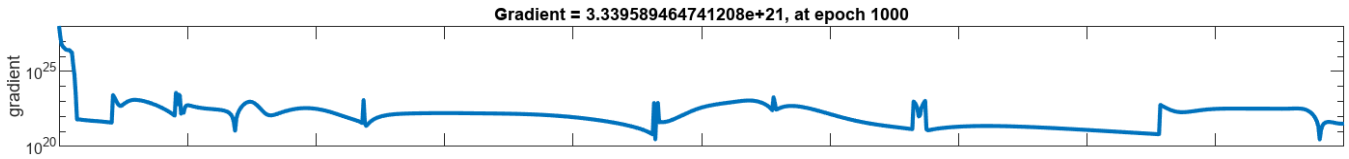

Fig 5: Gradient of Model

The gradient shows that how our model have reduced it error rate while training upon different parameters. This figure is representing the optimization process of our model. This figure is providing that how our models learning and adjusting its parameters to reduce errors over different iterations.

Mu Plot:

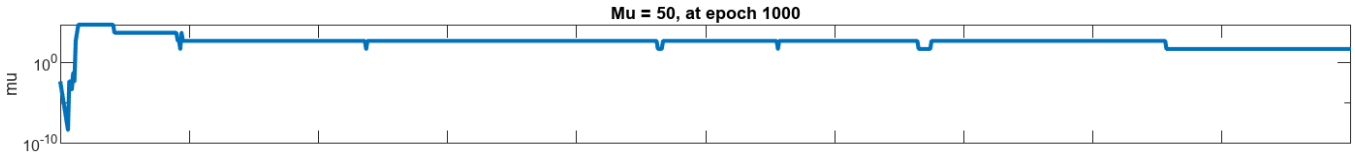

Fig 6: Memory Utility of Model

As this figure is representing the memory utility model of our ANN model this plot is providing information about the dynamics of training of ANN model. A consistent reduction in the curve suggesting that the model's parameters are being updated smoothly, leading to stable convergent towards an optimized solution.

Num Parameters Plot:

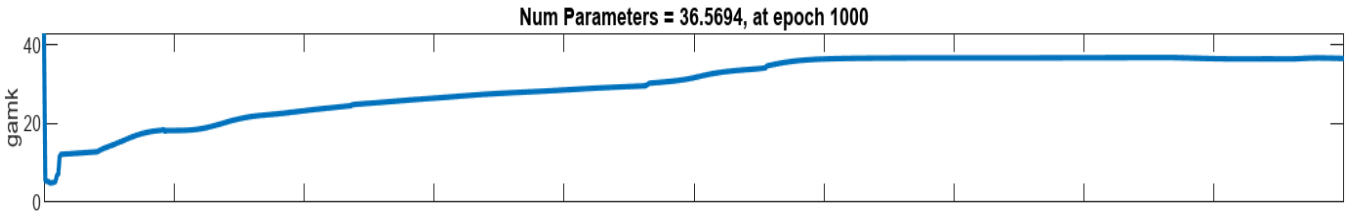

Fig 7:Num Parameters Plot

The above figure of Num Parameters providing insight into the structural characteristics of the model. This plot showing the number of parameters as a function of the depth or the number of layers in the model.

Sum Squared Parameters Plot:

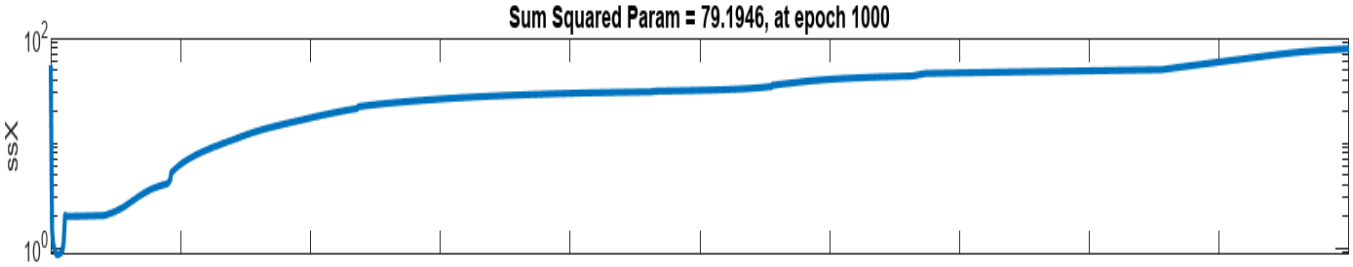

Fig 8: Sum of Squared Parameters of Datasets

The plot of SSP providing insight about the connections of ANN model between layers and neurons. As our dataset have large size of data so the smooth increase in the curve representing that the size of dataset is large and there are many connections between neurons and layers. It also shows that the performance of models is stable in complex situations.

Regression Plot:

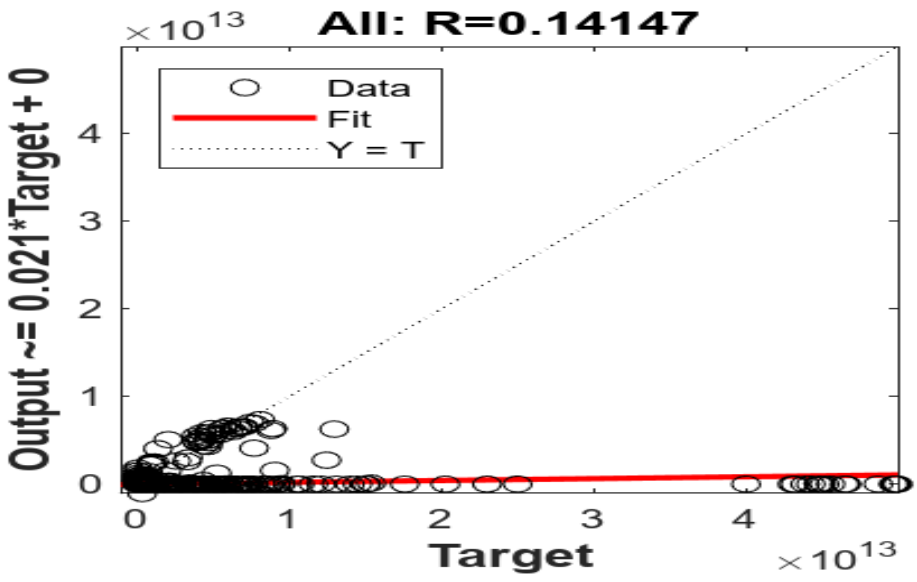

Fig 9: Overall Regression Plot

As regression show that how the model predicted values matching the actual parameters this above figure representing that our model have strong linear relationship between actual parameters and predicted Parameters.

Error Histogram:

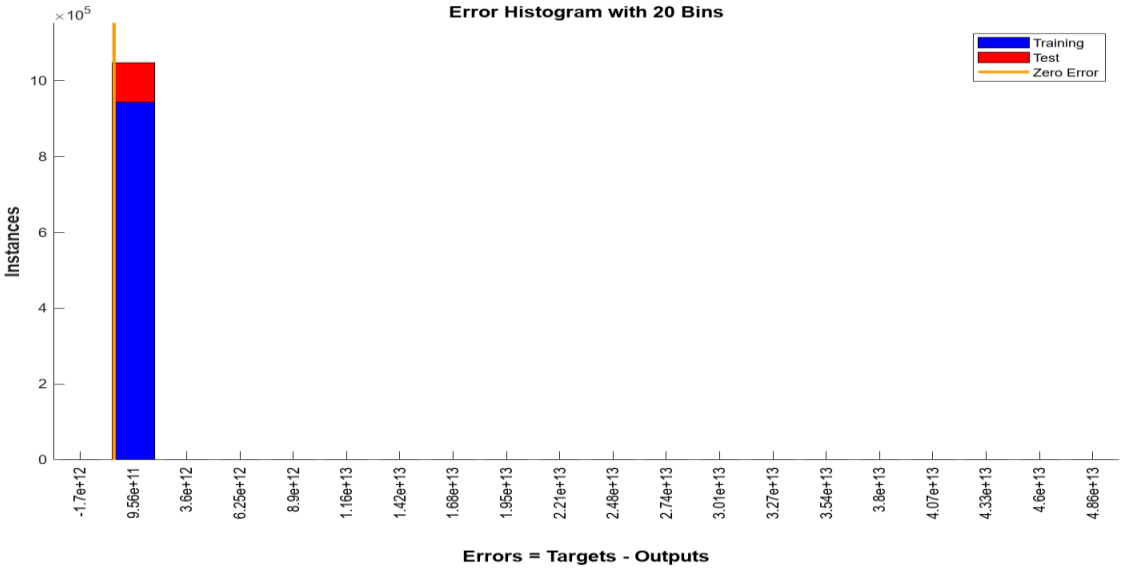

Fig 10: Error Histogram

As the accuracy of our ANN model is 96.72% and this accuracy is calculated from this error histogram which contains 20 bins and have 9.56e+11(0.0328) error rate.

Performance & Accuracy Measurement:

The below Plotting is showing the performance of our system for the detection of malware transactions

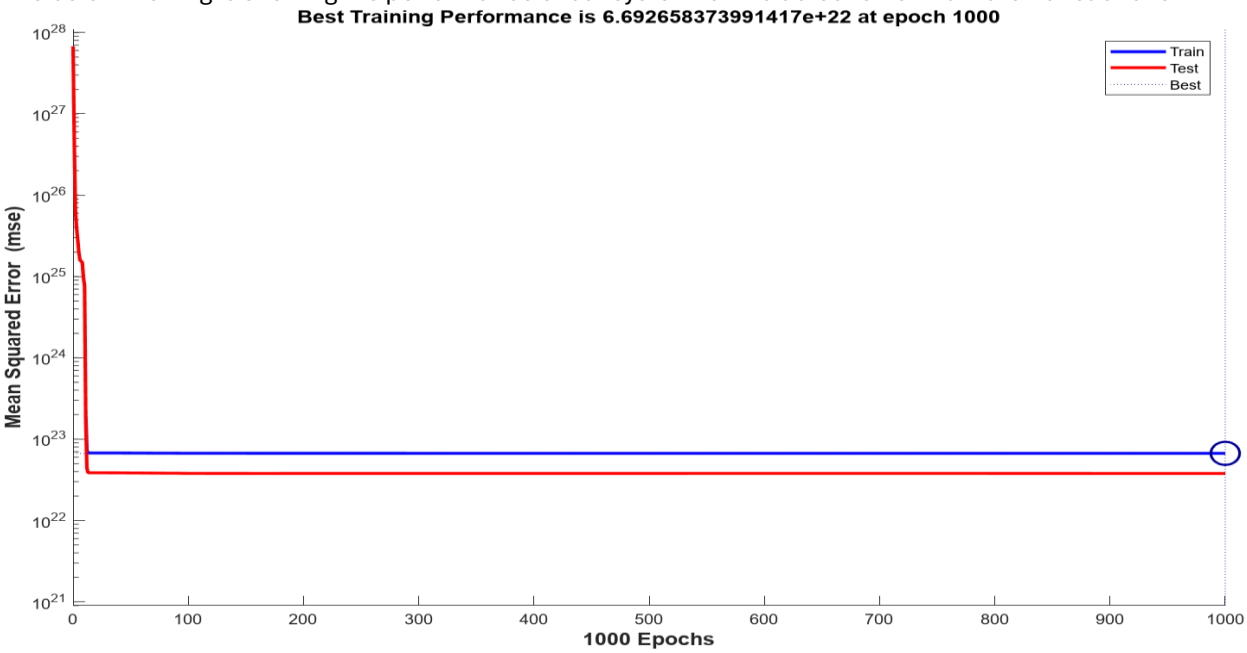

Fig 11: Performance Analysis Graph of ANN Model

This performance and results obtained after the training of the ANN model at 1000 Epochs and the most popular and most accurate algorithm of ANN "**Levenberg Marquardt"** is used to obtained those results. After that ANN will store this data in the cloud as shown in **Fig:3** The accuracy of the model is calculated as (1-Error rate), the above system has accuracy of 96.72% i.e (1-0.0328).

4. Conclusions:

We propose an innovative framework on Artificial Intelligence (AI) and Machine Learning (ML) technologies, which enhances the security of cryptocurrencies transactions. In contrast to cryptocurrencies revolutionary nature, serious security problems exist like fraud and privacy. To detect and stop illegal transactions, our research combines AI techniques which are primarily Artificial Neural Networks (ANN). Our model demonstrated a strong performance with an accuracy of 96.72% that is higher than competitors like Convolutional Neural Networks (CNN). We provide powerful layers of protection by combining the blockchain technology, IoT sensors, and a secure cloud storage. As a proactive procedure to the crucial issue of fraud detection and mining vulnerabilities we build up the authority trust of user and regulators. Our efforts promote the use of safe digital financial systems and help in the growth of trust and transparency in the bitcoin ecosystems.

5. Acknowledgements

We thank our beloved teachers whose priceless guidance and undisputed support have been indispensable in this journey of research. Through their guidance and expertise, our knowledge about Artificial Intelligence, machine learning, and blockchain technologies has been broadened. We cannot fail to thank them for their encouragement and significant contribution towards the success of our study through their critical analysis.

6. References

[1] T. Li, "Bitcoin and Blockchain," *Bitcoin and Blockchain: Security and Privacy,* pp. 10-15, 2020.

[2] S. Nakamoto, "Bitcoin A Peer-to-Peer Electronic Cash System," *IEEE,* p. 9, 2008.

[3] T. Navamani, "A Review on Cryptocurrencies Security," *Journal of Applied Security Research,* p. 23, 2021.

[4] F. Sabrina, "A Blockchain based Secured IoT System using Device Identity Management," *Sensors,* p. 17, 2022.

[5] T. Navamani, "A Review on Cryptocurrencies Security," *Journal of Applied Security Research,* vol. 6, p. 21, 2021.

[6] T. Choithani, "A Comprehensive Study of AI and Cybersecurity on Bitcoin, Crypto Currency and Banking System," *Annals of Data Science,* p. 33, 2022.

[7] T. L. S. M. I. M. W. M. Ehab Zaghloul, "Bitcoin and Blockchain: Security and Privacy," *IEEE Internet of Things Journal ,* vol. 7, p. 26, 2020.

[8] H.-N. D. C. a. H. W. Zibin Zheng and Shaoan Xie, "Blockchain challanges and opportunities: a survey," *Int. J. Web and Grid Services, No. 4,,* vol. 14, pp. 352-376, 2018.

[9] N. E. Villanueva, "Blockchain Technology Application: Challenges, Limitations and Issues," *Journal of Computational Innovations and Engineering Applications ,* pp. 8-14, 2021.

[10] M. A. A. a. W. S. Bhaya, "Blockchain Technology's Applications and Challenges: an overview," *AIP Conference Proceeding,* p. 10, 2020.

[11] M. C. V. a. M. C. Shipra Chhina, "Challenges and opportunities for Blockchain Technology: A systematic Review," *Austrailian Conference on Information System,* p. 10, 2019.

[12] F. F. 1. A. V. DAZA2, "SoK: Network-Level Attacks on the Bitcoin P2P Network," *IEEE Access,* vol. 10, no. 2022, pp. 94924 - 94265, 2022.

[13] Y.-C. B. Zeinab Shahbazi, "Analysis of Security and Reliabilty of Cryptocurrency system using Knowledge Discovery and ML Methods," *MDPI,* p. 15, 2022.

[14] M. S. V. M. A. Dr Arvind Kumar, "CRYPTOCURRENCY SECURITY," *YMES,* p. 12, 2020.

[15] Q. B. P. P. A. K. P. K. S. Sudeep Tanwar, "ML Adoption in Block-Chain Based Smart Appilations: The Challenges, and a Way forward," *IEEE Access,* p. 15, 2020.

[16] K. X. N. G. Mohamed Rahouti, "Bitcoin Concepts, Threats and Machine-Learning Security," *IEEE Access,* p. 18, 2018.

[17] T. P. a. S. Lee, "Anomly Detection in bitcoin network using Unsupervised Learning method," *IEEE,* p. 15, 2016.

[18] V. M. a. B. T. P.M Monamo, "A multifaceted approach to bitcoin fraud detection: Global and local outliers," *IEEE Conference ICMLA 2016,* p. 8, 2016.

[19] D. H. D. M. a. N. W. K. Baqer, "Stressing Out: Bitcoin aAIJstress testingaAI," *Springer Conferece ICFCDS 2016,* pp. 3-18, 2016.

[20] H. Y. a. R. Vatrupa, "A first Estimation of the proportion of cybercriminal entities in the bitcoin Ecosystem and supervised ML," *IEEE Conference ICBD (Big Data) ,* pp. 3690-3699, 2017.

[21] A. Bonger, "Seeing is Understanding: Anomly detection in blockchainswith visualized features," *ACM Conference on IJCPUCPISWS 2017,* pp. 5-8, 2017.

[22] B. R. a. L. M. C. Remy, "Tracking Bitcoin users activty using community detection on a netwrok of weak signals," *Spring Internation Workshop on Complex Networks and their Applications,* pp. 166-177, 2017.

[23] B. P. a. S. S. M. Bartoletti, "Data Mining for detecting bitcoin ponzi schemes," *arXiv,* 2018.

[24] S. S. a. V. Ribeiro, "Ramsomwall: A layered defense system against cryptographic ransomare attacks using machine learning," *IEEE Conference ICOMSNETS,* pp. 356-363, 2018.

[25] A. H. a. J. O'Connor, "Coinhoarder: Traking a ukranian bitcoin phising ring dns style," *IEEE Conference APWG Sysposium on Electronic Crime Research,* pp. 1-5, 2018.

[26] M. R. N. N. a. A. A.-F. K. Salah, "Blockchain for AI: Review and open research challenges," *IEEE Access,* vol. 7, p. 15, 2019.

[27] T. D. a. C. P. F. Casino, "A systematic Literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Inform,* vol. 36, pp. 55-81, 2019.

[28] Q. B. P. P. A. K. P. K. S. a. W.-C. H. Sudeep Tanwar, "Machine Learning Adoption in Blockchain-Based Smart Applications: The challenges and a way forward," *IEEE Access,* vol. 7, p. 15, 2020.

[29] M. A. K. A. R. M. U. R. a. H. S. K. Amir Haider, "A Real-Time Sequential Deep Extreme Learning Machine Cybersecurity Instrusion Detection," *CMC,* p. 14, 2022.

[30] C. P. H. K. T. Pratyusa Mukherjee, "KryptosChain—A Blockchain-Inspired, AI-Combined, DNA-Encrypted Secure Information Exchange Scheme," *MDPI,* p. 29, 2023.

[31] E. Karger, "Combining Blockchain and AI - Literature Review and State of the Art," *ICIS,* p. 9, 2020.