Blockchain Based Decentralized Technology For Internet Naming Systems

Apurva Tamhankar*
SoCE&MS
DIAT DRDO DU
Pune, India
apurvatamhankar@gmail.com

Sunita Dhavale*
SoCE&MS
DIAT DRDO DU
Pune, India
sunitadhavale@gmail.com

Arun Mishra
SoCE&MS
DIAT DRDO DU
Pune, India
arunmishra@diat.ac.in

Balaji Rajendran
CoE-DNS
CDAC
Bangalore, India
balaji@cdac.in

Gopinath Palaniappan
CoE-DNS
CDAC
Bangalore, India
gopinath@cdac.in

*corresponding author

2023 IEEE 11th Region 10 Humanitarian Technology Conference (R10-HTC) | 979-8-3503-2614-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/R10-HTC57504.2023.10461759

Abstract: **Domain Name Service (DNS) has become an essential element of the Internet in current era. The traditional DNS extends its authority down to the Top Level Domains (TLDs) and individual names before returning to the Root Server. To avoid the cons related to centralized authority scheme of the traditional DNS, recently many techniques based on the decentralized Internet with support of Blockchain (BC) are emerging. Hence, currently a variety of protocols and mechanisms are focusing on implementation of the Decentralized Naming Services which in turn supports concept of decentralized internet services. These Decentralized Naming Services are totally based on Blockchain architectures and provides various pros like resistance to single point of failure, resistance to censorship and permanent proof of ownership. Blockchain Domain Names act as Digital Identity in Decentralized Internet. Security is major concern in any DNS system and the similar challenges exists in the Blockchain DNS system too. Further, there is a lot of diversity being observed in decentralized internet space as a Domain name in a Blockchain DNS can refer to a website/portal or a wallet or a Non-Fungible Token (NFT) or simply be parked. Also, currently, there is rampant growth in development of decentralized applications with no standards implemented - neither across Blockchains nor regions. Hence, there is a need to detect security exploits carried out using malicious domains in Blockchain DNS system and implement mitigation measures accordingly. In this research work, we study and analyze malicious domain names in decentralized BC system. We explored Ethereum transaction dataset for detecting malicious transactions using Machine Learning (ML) and Deep Learning (DL) algorithms with good accuracy of 99% and 95% using Decision Tree and 1 Dimensional Convolutional Neural Network (CNN) respectively. We also applied ML techniques on Ethereum wallet dark list dataset for detection of domain names that were vii used for phishing attacks. We received 96% accuracy after handling data imbalance by Random Forest model. Model predicted nature of domain based on 17 features that were extracted from Ethereum wallet dark list dataset like number of consonants, vowels, digits, symbols and their ratios to length of domain.**

Keywords — *Blockchain, Domains, DNS, Web3, Decentralization*

I. INTRODUCTION

Around the year 1969, two complete computing systems were able to relay communication over the internet. It can be marked as birth of what we now term the Web 1.0. Of course, the evolution was not overnight and the same is true for further iterations of networking, namely Web 2.0 and Web 3.0. The first version was designed only for consuming and information flow was in single direction. Web 2.0 supported read and write operations and hence allowing information flow to be bidirectional. In Web 2.0, user's data was accepted, processed in real time and output was sculpted as per individual requirements. Smart interconnected technologies further assisted lives with day-to-day chores, with monitoring medical indicators, freight management and other user experiences. The plethora of new opportunities provided were also accompanied with various shortcomings.

The form of web and services which uses DNS as its core resource location service was not secure by design as evident from the number of attacks. DNS is the application layer protocol that enables internet users to make use of mapping between the Internet Protocol (IP) address where the resource files are hosted to meaningful memorable names. The new Web 3.0 development protocols and techniques propose to overcome the existing shortcomings of conventional DNS along with providing additional security measures. This work summarizes the flaws in the conventional DNS and gives insights into ongoing developments in shaping future web and possible attacks. The work is divided into following sections: (i) Literature Survey – It covers what conventional DNS is and what it suffers from as studied by researchers and academicians from India and around the globe through survey papers, research papers, reports and blogs. (ii) Blockchain Domains – This section covers the fundamentals on which blockchain is powering the interconnectivity of the future. (iii) Domain Exploits, which summarized how this system can be misused. (iv) Proposed System and Implementation – application of ML and DL to detect fraud. (v) Conclusion – summary of work and (vi) Acknowledgements.

II. LITERATURE SURVEY

Summary of work consisting of surveys, detection of threats and attacks in conventional hierarchical systems and Blockchain based systems and new threats to proposed solutions is presented here. Reference [1] notes that TTL can be altered in conventional systems making an expired record valid to be used and vice versa. DNS service being rendered unavailable because of DNS flaws in configurations is also

979-8-3503-2614-7/23/$31.00 ©2023 IEEE

mentioned. It proposes solution to mitigate intentional DoS attack by using Dynamic Round-Robin P2P solution built over Chord protocol. It provides alternate paths to resolve queries [2] talks about problems in maintaining and updating Blacklist of IP or websites which are malicious. It describes that phishing (a form of social engineering) is most popular attack and is used to trick users to steal critical login credentials and therefore establishing trust between entities of Internet is crucial. Therefore, they display reference implementation, a trustworthy Blockchain based DNS on Ethereum Quorum simulation which avoids redirection. Reference [3] highlights major attacks on DNS like Single Point of Failure because of hierarchical nature, data tampering and then the trends of usage of Blockchain in this sphere. It proposes decentralized blockchain to store domain name resolution zone files. In their solution system named DecDNS, they proactively invalidate multiple nodes and still claim their smooth functioning of resolution service without falsification of data or single point of failure. Moreover, they claim that their system is compatible with conventional DNS hierarchy.

To enable trust between domain owners, domain operators and others, the existing PKI relies on Certificate Authorities for authenticity. And Certificate Authority Authorization (CAA) indeed ensure no bogus CAs grant certificates. But ICANN has central control over these. So [4] present ”AuthLedger”, a domain authentication scheme using Ethereum Smart Contracts. Authors of [5] highlight major disruptions because of DNS Abuse and how Blockchain can limit or overcome those. Then they carry out comparative study of DNS attacks, how legacy solutions handle these and how Blockchain based solutions could handle these. Their work revolves around Identity Management, Distributed Storage, Decentralized Applications and Decentralized Internet. While there could be multiple ways by which existing flaws in hierarchical DNS systems can be overcome, [6] notes that non blockchain solutions like Local recursive DNS, Secure Distributed DNS and mDNS offer improvements in one dimension, not cover all. After comparing Namecoin, Blockstack and EmerDNS, they further point out that not all blockchain based solutions could be adopted easily and especially for resource constrained IoT systems. This paper provides theoretical solution which consists of improvements on work done in this field and an architecture compatible with IoT and other nodes. Reference [7] emphasizes the need for decentralized Name Resolution System for the future of Internet, i.e. Decentralized Web. They propose need for Universal Resolver after comparing Namecoin, Ethereum DNS, and Handshake. Reference [8] focusses on new challenges and opportunities that Blockchain and Decentralized File Storage (DFS) especially because of their immutability. The fully or pseudo anonymous nature of bitcoin address are favorable for ransom extortion and this issue is only tip of the ice berg. Use of DFS along with Blockchain enable applications with off-chain storage which can be used as permanent link to C&C server or spreading malware. Moreover data in such systems is immutable and cannot be assuredly deleted violating the Right to be forgotten and Privacy of GDPR. The security researchers of [9] state that Blockchain based DNS could solve various issues present in core Internet technologies today. But these systems have their own security flaws and they have presented threat landscape of such systems. They have been able to unravel domain extortion schemes and phishing attempts. They have studied how Blockchain based systems prove to be beneficial for Malwares as they avoid detection because they do not produce NXDomain responses as in traditional DNS where DGAs are used. Further, underlying bidding function may be exploited. Moreover complete lack of monitoring may lead to parallel Internets. Their work also highlights phishing attacks. Reference [10] provides good statistical analysis of Ethereum Name Service (ENS). The paper explains two bidding systems used namely The Initial Auction (Vickery Auction) and Short Names (English Auction). It explains Smart Contracts driving this - The Registry, Registrar and The Resolver. It then summarizes the flaws into Domain Squatting, Websites spreading Malware, Scam Addresses and Record Persistence Attacks.The attacks that can occur in conventional system are summarized in Table I.

TABLE I. ATTACKS ON AND USING HIERARCHICAL DNS

Attacks on DNS Infrastructure	Attacks using DNS Infrastructure
Cache Poisoning	DDoS
Registry Hijacking	DNS Tunnelling
Zone Transfer	Cyber Squatting
Physical Attack	Phishing

III. BLOCKCHAIN DOMAINS

The internal security provisions would be overshadowed unless the connectivity endpoints to external networks are secured. Hence the internet access mechanisms need to be secured by design. This is leveraged by the use of Blockchain Technology in the backend. This technology is built over strong cryptographic fundamentals like hash and encryption.

Digital Signatures ensure authenticity, integrity and non-repudiation of transactions. For this purpose asymmetric key encryption is used. The user authorizes blockchain transaction using wallets which hold the public and private key.

The three properties of hash are: A) The Pre Image Resistant property which does not allow detection of data for which hash was calculated supporting anonymity. B)Second Pre-Image Resistant and C) Collision Resistant which ensures that data cannot be replaced with other data that produces same output. Or that computational time required to find another input producing same output is astronomical. Moreover, since hash is fixed smaller length output as compared to large sized input, it’s economical to store, transfer or compare. The data structure implemented is Merkle Patricie tree which is hash tree. If two sets of transactions need to check for equality, then only their roots be compared as modification of any data would result in totally different roots.

The early version of locating wallet address required remembering the hash values associated with wallet addresses. An Ethereum address of user called Wallet Address (WA) or that of a smart contract called Externally Owned Address (EOA) are last 160 bit of Keccack (NIST standard of Secure Hash Algorithm SHA3) hash of public key. Secp256k1 Elliptic Curve Digital Signature Algorithm (ECDSA) is implemented by Bitcoin. But, now that Blockchains are supporting wide variety of functionalities because of programs residing on blockchains called Smart Contracts. The support for human meaningful and memorable names have replaced these addresses. These domain names act as unique account identifiers for crypto asset payments. Each blockchain has token trackers or block explorers that allow searching via

Block Number, Transaction Number, Transaction Receipt, wallet address, contract address or domain name. The tokens supported by Ethereum are of primarily three types – ERC20 which is totally fungible meaning that the value of two different tokens is exactly same with no difference of value if exchanged. Another is ERC1155 which mints tokens which are like certificates - individual credibility but in same format. These are given as proof of attendance / proof or completion or as a gate pass. The third type ERC721 or Non-Fungible Token standards produce unique tokens that are differentiated with metadata. Twitter officially allows setting NFT domains as handles. The web domains themselves have variety of applications including but not limited to using domains to log in on social media platforms while keeping personally identifiable information safe. Block chat is secure messaging platform native to Blockstack browser and Blockchain [11]. Nestree for Android and iPhone/iPad is reward based messenger powered by Polygon [12]. Ethereum Name Service developed over Ethereum allows these web3 domain addresses to store text records that are links to social media like reddit, discord, github, Instagram and more, unique visual digital representation "avatar" as well as addresses for crypto coin transfers of other blockchain networks like Solana, Polygon, Bitcoin etc. Web3 domain names can be used as mail addresses. Hashmail provides support for 170+ wallets user can enter Ethereum, Ethereum Name Service, and Unstoppable Domain, Lens or other wallet address as receiver address. Reference [13] As the world is progressing, there is also a paradigm shift in gaming industry models. From offline gaming beating once's previous record to Massively Multiplayer Online Role Playing Games (MMORPG) exhibiting "Play to Win" model, there is shift to "Play to Win" model with blockchain powered games. Games like Cryptokitties on Flow [14] and Axie Infinity on Ronin Network, a side chain of Ethereum blockchain [15] require wallet funds and have been fundamental in building traction to blockchain gaming industry. Domains of favourite gaming characters fair higher in NFT markets. Blockchain is not ideal for storing large volumes of data, so actual content for consumption is uploaded on peer to peer, decentralized file storages (DFS). These are content addressable networks which map resources using Distributed Hash Table (DHT). It can be used as pointer to decentralized storage like IPFS. Emercoin Name Value System (NVS) allows storage of key value pairs on Bitcoin Blockchain. EmerDNS service of Emercoin[16] efficiently supports .emc, .coin, .lib, .bazar DNS zones. The resolution of Blockchain Domain Names is provisioned by Wallet Extensions. Table II summarizes popular Blockchain Domain Extensions, Browsers, and domain support.

TABLE II. WEB3 DOMAIN RESOLUTION

Browser Extension	Browsers	Domains Supported
Peername.com	Firefox, Chrome, Opera	.bit, .emc,.coin,.lib,.bazar
Unstoppable Domains	Firefox, Chrome, Opera, Edge Brave	.crypto, .zil, .wallet, .blockchain, .bitcoin, .x, .888, .nft, .dao, .klever, .zil, .hi
Metamask	Firefox, Chrome	.eth

For resolution, the appropriate extension needs to be downloaded by user. As an example, to resolve Apurva.bdn, user simply can type http://Apurva.bdn or Apurva.bdn/ and results from decentralized websites will be produced. If the dnstext record pointing to content has is set, then the domains can also be resolved by adding ".limo" or ".link" as suffix[17]. Blockchain based DNS solutions are Decentralized, and because resources are distributed, they work great against Single Point of Failure, Censorship or Distributed Denial of Service Attacks. Also, blockchains have been known to provide Security and Privacy of users.

IV. DOMAIN EXPLOITS

Blockchain DNS evolved to cater the rising need for decentralized internet. Even though Blockchain DNS was introduced with the plan to overcome the limitations of traditional DNS, it does have its own security concerns and issues. A major security issue that exists is common between Blockchain DNS and traditional DNS is that of malicious domains. Malicious domains exist in Blockchain backed system too and are more prevalent due to the ease in creation of domain names in a Blockchain DNS ecosystem. Also because there are no standard policies or guideline for operating the services and so each of the providers operate individually and differently.

In the Blockchain DNS ecosystem, in addition to namespace registrar the users can also create their own TLD. It is understood that OpenNIC which is a universal domain resolver (Catering to both traditional and blockchain DNS) had withdrawn support for .bit because plenty of malicious domains were created in it. This freedom to create TLDs creates a larger room for domain squatting attacks in blockchain DNS when compared to that in traditional DNS. Mixers are dark web of the crypto world. The transactions that happen over blockchain are private meaning that one can derive the transacting entities' addresses but those addresses cannot be mapped to individual real world identities. Mixers erase this transaction link making tracing actual flow impossible. Tornado Cash, one such mixer has been sanctioned by the strictest Office of Foreign Assets Control for inability to prohibit laundering frauds. Only few blockchains have support for Anti Money Laundering (AML), Know Your Customer (KYC) and Know Your Business (KYB). The others support total anonymity, making it impossible to trace the miscreants. Wallets (especially private keys) need to be secure always as exposure of such may lead to irrecoverable loss of digital gold. Smart Contracts interaction should be done with caution and preferrable with only once passing Security Audits. Although the blockchain technology supports privacy, and does not collect Personally Identifiable Information (PII), some technologies may collect network information including IP address. Since there is no check/validation on who creates what and where, blockchain domains can be used for spreading malware. Also, the ecosystem does not support Right to Be Forgotten as data once uploaded cannot be taken down. Smart Contracts need to be heavily tested for any bugs or vulnerabilities, as once the contract is deployed, it cannot be changed and if incorrectly coded may lead to huge loss of assets.

V. PROPOSED SYSTEM AND IMPLEMENTATION

A. Part I

We analyze Ethereum Fraud Detection Dataset [18] which is labelled dataset consisting of 9841 samples with 51 features.

The features include address of Ethereum Account, average time difference between sent and received transaction, time difference between first and last transaction, number of initiated and receipted transactions, number of transactions which included contract creation, unique accounts which account sent and received transactions, minimum, maximum and average values of Ether (native token) tokens sent and received. The minimum, maximum and average values sent and received to contracts. The similar features are recorded for ERC 20 tokens. A sample of transactions are shown in Fig. 1. Sample Token Transactions The 'FLAG' field indicated genuine transaction as '0' and '1' otherwise.

Algorithm:

1. Gather transactions data
2. Preprocess
3. Split data 8:2 for training and testing.
4. Train Model using ML and DL algorithms on
5. Test Model
6. Select Best Model and Deploy for actual predictions.

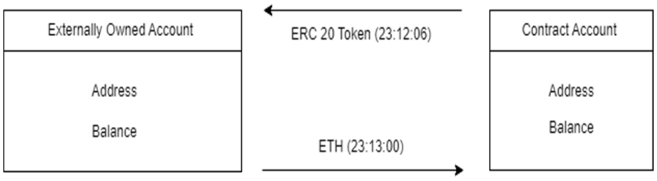
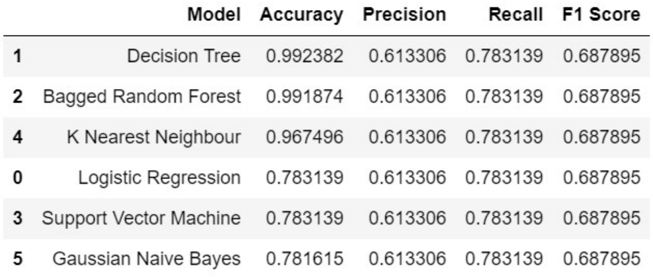


Fig. 1. Sample Token Transactions

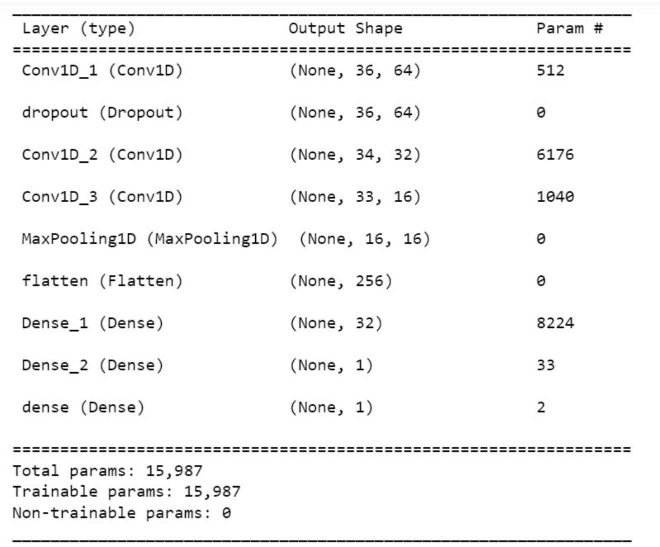
The initials steps included replacing missing and 'NaN' values with zero. The heatmap of correlation of features was plotted and highly corelated or redundant features were removed like 'ERC20 max value sent contract', 'ERC20 avg time between contract txn' and associated maximum and average values. String values were label encoded and all features were converted to float data type. After all pre-processing steps, the modified dataset contained 9841 samples with 43 features. The dataset was split into train and test portion in 8:2 ratio. 6 machine learning models were fit into training data. Fig. 2. summarizes the comparison of model performance using Precision, Accuracy, Recall and F1 score.



	Model	Accuracy	Precision	Recall	F1 Score
1	Decision Tree	0.992382	0.613306	0.783139	0.687895
2	Bagged Random Forest	0.991874	0.613306	0.783139	0.687895
4	K Nearest Neighbour	0.967496	0.613306	0.783139	0.687895
0	Logistic Regression	0.783139	0.613306	0.783139	0.687895
3	Support Vector Machine	0.783139	0.613306	0.783139	0.687895
5	Gaussian Naive Bayes	0.781615	0.613306	0.783139	0.687895

Fig. 2. Model Comparison on Transaction Predictions

Further, we tried to training using Deep Learning – one dimensional convolutional neural network. The same initial pre-processing steps were followed. Then the train data, train label, test data and test label were all converted initially to numpy arrays. Data had to be reshaped to be fed to 1D-CNN model. After reshaping, shape of data was (7872, 42, 1). Fig. 3. represents model summary.



```
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 Conv1D_1 (Conv1D)           (None, 36, 64)            512

 dropout (Dropout)           (None, 36, 64)            0

 Conv1D_2 (Conv1D)           (None, 34, 32)            6176

 Conv1D_3 (Conv1D)           (None, 33, 16)            1040

 MaxPooling1D (MaxPooling1D)  (None, 16, 16)           0

 flatten (Flatten)           (None, 256)               0

 Dense_1 (Dense)             (None, 32)                8224

 Dense_2 (Dense)             (None, 1)                 33

 dense (Dense)               (None, 1)                 2

=================================================================
Total params: 15,987
Trainable params: 15,987
Non-trainable params: 0
_________________________________________________________________
```

Fig. 3. Model Summary

For all except last layer, Rectified Linear Unit (ReLU) was used. But since it's a binary class classification problem, Sigmoid function is used in last layer along with binary cross entropy as loss function and metrics used is accuracy. The same model was compared for three optimizers. The accuracy plot after training is shown in Fig. 4., Fig. 5. and Fig. 6. for ADAM, RMS PROP with parameter 0.001 and RMS PROP with parameter 0.01 respectively. Test accuracy and loss is also summarized in Fig. 7.

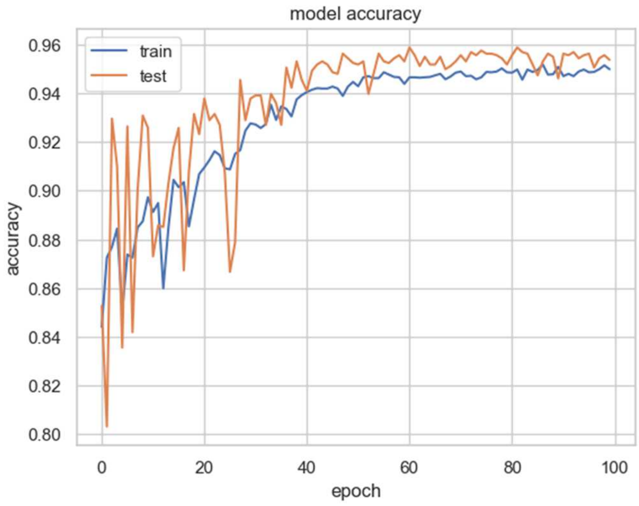


Fig. 4. Accuracy plot of ADAM

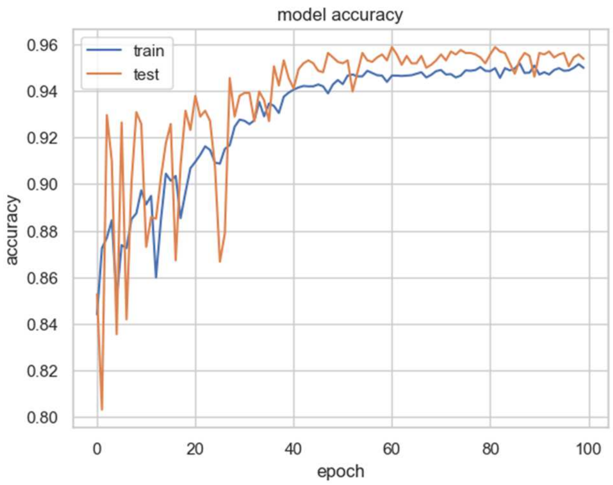


Fig. 5. Accuracy plot of RMS PROP 0.001

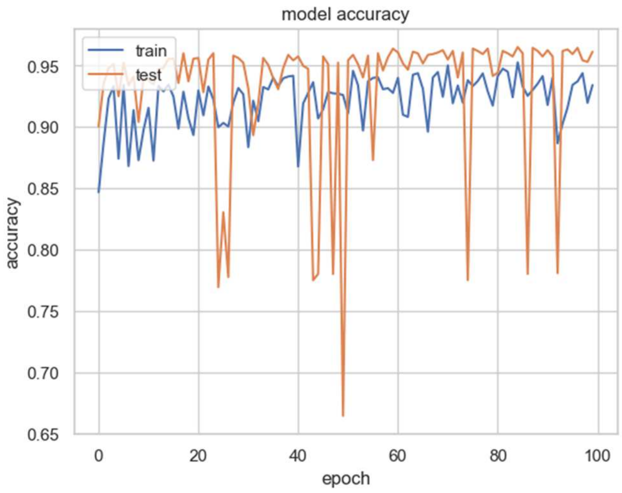
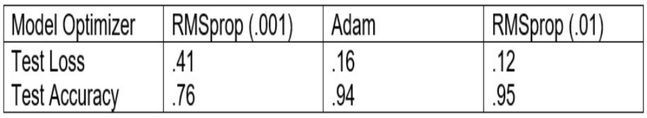


Fig. 6. Accuracy plot of RMS PROP 0.01



Model Optimizer	RMSprop (.001)	Adam	RMSprop (.01)
Test Loss Test Accuracy	.41 .76	.16 .94	.12 .95

Fig. 7. Test Accuracy and Loss Summarization

Decision tree predicted the result with accuracy of 99%. A sample decision tree with max dept 4 which produces 5 layers is shown in Fig. 8.

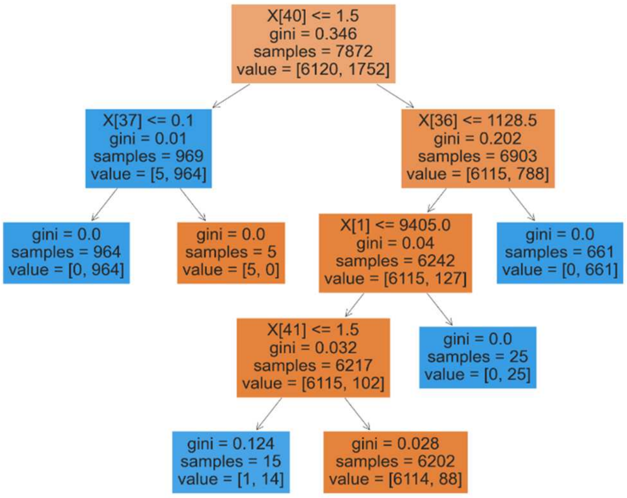
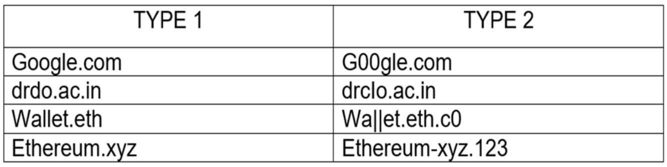


Fig. 8. Decision Tree

B. Part II

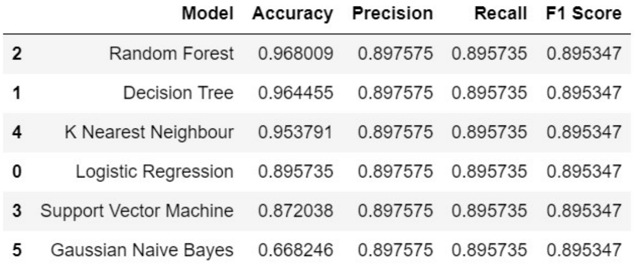
The genuine domains names are distinguishable from that used in malicious activities. The difference may not be obvious to human eye and therefore identification of such is attempted using ML algorithms. Fig. 9. provides evidence for domains possibly used for good (TYPE 1) and bad intentions (TYPE 2) and the number of vowels, consonants, digits and symbols differ.



TYPE 1	TYPE 2
Google.com	G00gle.com
drdo.ac.in	drclo.ac.in
Wallet.eth	Wa||et.eth.c0
Ethereum.xyz	Ethereum-xyz.123

Fig. 9. Difference in String Features

For the above objective, labelled URLs mostly found in Phishing Wallets were extracted [19]. These are based out of Ethereum blockchain and are flagged. String functions were applied to eliminate unnecessary portions in Python. The domain list was parsed using python script to calculate 17 features. The features are flag indicating genuineness of domain. Rest of the features are length, number of digits, number of unique digits, number of characters, number of unique characters, number of symbols, number of vowels, number of consonants, number of alphanumeric characters, number of dots, number of underscores, number of unique characters, ratio of letters to length, ratio of unique letters to length, ratio of unique letters to unique characters, ratio of unique digits to unique characters. Synthetic Minority Oversampling Technique (SMOTE) was used to handle the imbalance of minority class. The result is summarized in Fig. 10.



	Model	Accuracy	Precision	Recall	F1 Score
2	Random Forest	0.968009	0.897575	0.895735	0.895347
1	Decision Tree	0.964455	0.897575	0.895735	0.895347
4	K Nearest Neighbour	0.953791	0.897575	0.895735	0.895347
0	Logistic Regression	0.895735	0.897575	0.895735	0.895347
3	Support Vector Machine	0.872038	0.897575	0.895735	0.895347
5	Gaussian Naive Bayes	0.668246	0.897575	0.895735	0.895347

Fig. 10. Model Comparison of Domain Predictions

Random Forest predicted genuineness of domain best with accuracy of 96%.

VI. CONCLUSION:

Out of all ML/DL models trained, Decision Tree Model was able to classify a transaction as genuine or not best with an accuracy of 99%. We also applied ML techniques on Ethereum wallet dark list dataset that contained domain names based on Ethereum Blockchains that were used for phishing attacks and for genuine purposes. We received accuracy of 96% by using Random Forest after handling data imbalance. Data imbalance was handled using SMOTE. The models predicted a domain as fraudulent or not based on 17 various extracted from Ethereum wallet dark list dataset domains. The detected fraud transaction's address may be blacklisted from further interaction. A proactive approach is essential as blockchain is immutable ledger where transactions cannot be reversed. This study will be useful for anyone who wants to develop Decentralized Applications using suitable Blockchain as per use cases.

ACKNOWLEDGEMENTS

This work is done under collaboration of DIAT DRDO DU and CDAC Bangalore and I sincerely thank both institutes for giving me opportunity to intern at CDAC Bangalore.

REFERENCES

[1] Abu-Amara, M., Azzedin, F., Abdulhameed, F.A., Mahmoud, A., Sqalli, M.H.: DYNAMIC PEER-TO-PEER (P2P) SOLUTION TO COUNTER MALICIOUS HIGHER DOMAIN NAME SYSTEM (DNS) NAMESERVERS.

[2] Hsieh, W.-B., Leu, J.-S., Takada, J.-I.: Use chains to block DNS attacks: A trusty blockchain-based domain name system. Journal of Communications and Networks. 24, 347–356 (2022). https://doi.org/10.23919/jcn.2022.000009.

[3] Liu, J., Li, B., Chen, L., Hou, M., Xiang, F., Wang, P.: A data storage method based on blockchain for decentralization DNS. In: Proceedings - 2018 IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018. pp. 189–196. Institute of Electrical and Electronics Engineers Inc. (2018). https://doi.org/10.1109/DSC.2018.00035.

[4] Guan, Z., Garba, A., Li, A., Chen, Z., Kaaniche, N.: AuthLedger: A novel blockchain-based domain name authentication scheme. In: ICISSP 2019 - Proceedings of the 5th International Conference on Information Systems Security and Privacy. pp. 345–352. SciTePress (2019). https://doi.org/10.5220/0007366803450352.

[5] Karaarslan, E., Adiguzel, E.: Blockchain based DNS and PKI solutions. IEEE Communications Standards Magazine. 2, 52–57 (2018). https://doi.org/10.1109/MCOMSTD.2018.1800023.

[6] de Klerk, L., Ays¸en, A., Erkin, Z.: Blockchain-based DNS and PKI to solve issues of trust, security and censorship in the context of the IoT.

[7] 2022 IEEE Region 10 Symposium (TENSYMP). IEEE.

[8] Casino, F., Politou, E., Alepis, E., Patsakis, C.: Immutability and Decentralized Storage: An Analysis of Emerging Threats. IEEE Access. 8, 4737–4744 (2020). https://doi.org/10.1109/ACCESS.2019.2962017.

[9] Patsakis, C., Casino, F., Lykousas, N., Katos, V.: Unravelling Ariadne's Thread: Exploring the Threats of Decentralised DNS. IEEE Access. 8, 118559–118571 (2020). https://doi.org/10.1109/ACCESS.2020.3004727.

[10] Xia, P., Wang, H., Yu, Z., Liu, X., Luo, X., Xu, G., Tyson, G.: Challenges in Decentralized Name Management: The Case of ENS. In: Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC. pp. 65–82. Association for Computing Machinery (2022). https://doi.org/10.1145/3517745.3561469.

[11] Zhang, A., Shah, S., Elmandjra, Y., Decesare, M., Hanna, M., Snyder, S.: I. Cover Page BlockChat: A Decentralized Messenger on the Blockchain.

[12] Nestree to scale blockchain integrated messaging app using Matic Network — Polygon | Blog, https://polygon.technology/blog/nestree-to-scale-blockchain-integrated-messaging-app-using-matic-network, last accessed 2023/02/10.

[13] Hasmail, https://www.hashmail.dev/, last accessed 2023/02/10.

[14] Cryptokitties, https://www.cryptokitties.co/, last accessed 2023/02/10.

[15] Axie Infinity, https://axieinfinity.com/, last accessed 2023/02/10.

[16] Emercoin Services, https://emercoin.com/en/documentation/blockchain-services/introduction-to-emercoin-services/, last accessed 2023/02/10.

[17] Publish content path, https://docs.ipfs.tech/concepts/dnslink/#publish-content-path, last accessed 2023/02/10.

[18] Ethereum Fraud Detection, https://www.kaggle.com/datasets/vagifa/ethereum-frauddetectiondataset, last accessed 2023/04/05.

[19] GitHub - MyEtherWallet/ethereum-lists, https://github.com/MyEtherWallet/ethereum-lists, last accessed 2023/04/05.