

Systematic Analysis of DDoS Attacks in Blockchain

Mohamad Arsalan Sheikh*, Gul Zameen Khan[†], Farookh Khadeer Hussain*

*School of Computer Science

Faculty of Engineering and Information and Technology

University of Technology Sydney, Broadway Ultimo, NSW 2007

mohamadarsalan.sheikh@student.uts.edu.au, farookh.hussain@uts.edu.au

[†] NLT Digital Solutions, Australia

gulzameenkhan@gmail.com

Abstract—With the expansion of the internet, the identification and recuperation of digital attacks have become a primary concern for digital businesses. Damage brought about by network attacks has caused far and wide concern. Distributed Denial of Service (DDoS) attack is a dangerous digital attack. It's an attack that annihilates the network and can cause multiple computers to be assaulted simultaneously, fizzling to perform service appropriately. A blockchain-based DDoS recognition model is proposed for the systematic evaluation of DDoS attacks to understand the vulnerabilities of the Blockchain better. The advantage of Blockchain is that Blacklisted IP addresses are effectively stored. The use of such a framework gives the benefit of additional security components over existing DDoS moderation frameworks. This paper has assessed the Tab Transformer, the XGBoost, and the Random Forest algorithm to discover the better classifying algorithm. Tree-Based classifier procedure utilized for feature selection to boost the computational time. Out of the three algorithms, the Tab Transformer gives an accuracy of about 97% real-time investigation of the attacks.

Index Terms—DDoS (Distributed Denial of Service), Blockchain, Machine learning (ML) Algorithm, Tab Transformer, Random Forest, XGBoost.

I. INTRODUCTION

As the number of resources associated with the web increases, the effect of Distributed Denial of Service (DDoS) attacks is expanding. As a profoundly damaging assault, the destruction and debasement of its service quality are capricious [1]. The top data transfer capacity of DDoS in 2013 has surpassed 300Gbps [2]. DDoS attacks are exceptionally destructive, making services reduced or even crashed [1]. Simple to execute and powerful innovation for attacking web assets. Before, there have been some large-scale attacks against notable websites [3]. Some preventive measures have been proposed to defend from these attacks. However, the expense of protection is high [4], [5], because DDoS detection was mostly centralized single-point detection, by examining nearby traffic highlights [6], which caused the DDoS attacks and couldn't be adequately shielded.

Contrasted and single-point protection systems [7] with the benefits of the disseminated guard has been demonstrated. For example, community-oriented interruption location frameworks, which permit data from different nodes of the interruption identification framework to communicate and gather data [8], yet this likewise directly prompted the issue of trust between members.

Denning proposed the general interruption discovery model [9] in 1987, and the interruption identification framework (IDS) has been well applied. However, with the development of Internet attack innovation, this traditional single-point recognition is effortlessly skirted by high attacks [10], so it is particularly essential to improve the adaptability of interruption location frameworks [11]. Altogether, to enhance the capacities of DDoS detection frameworks, some collaborative interruption recognition frameworks have been designed to permit data trade, and common assortment [8] between IDS. Despite the fact that IDS has existed and grown for nearly 40 years, it has been dealing with the issue of information sharing [12]. Since members don't confide in one another and involve privacy issues, they are hesitant to share information, which drives collaboration. The discovery framework can't gather information in time, and the communitarian location framework likewise faces internal information security issues brought about by inner attacks [10].

DDoS attacks are the most problematic and disruptive assaults that intrude on the administrations running over hours to days. There are several of DDoS assaults, out of which SYN Flood Attack, UDP Flood Attack and HTTP Flood Attack are the most common assaults. UDP Flood is an assault under which there are a colossal number of User Datagram Packets shipped off worker with an expectation of overpowering the objective assets and make them inert. There could be a firewall infringement and, thus, there might be a refusal of an authentic client demand. HTTP Flood is an assault wherein there are a gigantic number of HTTP demand shipped off workers with an objective to overpower the objective assets and make them inert. These assaults mostly focus on the OSI model application layer. The TCP-SYN Flood assault creates a huge traffic volume and makes worker assets difficult to reach. It works by more than once sending the SYN parcels (Initial Requests) and overpower every one of the ports on track gadget and making not to react to the traffic.

To address various kinds of DDoS assaults, the vital use of machine learning approaches is to recognize abnormal behavior of the network traffic. Each attack uses specific methods to introduce irregularities in the network and can be detected over time by capturing the traffic and analyzing the traffic for these anomalies. The machine learning approaches can be effectively used to deal with anomalies with high accuracy

and high precision, and recall. As a first very important step, feature engineering for every attack, we have utilized a Tree-Based classifier.

We utilize various state-of-the-art machine learning models, including Tab Transformer, to recognize DDoS attacks. The performance is compared with Random Forest and XGBoost algorithms. The Tab Transformer is a model based on Natural Language Processing and used effectively in language modeling to capture contextual information. The use of such a model encourages us to capture the time-varying information effectively that helps us identify various kinds of DDoS attacks.

This paper is organized as follows: Section II summed up the previous work. The section III presents the proposed methodology utilized in this paper. The section IV presents the experimental analysis of the machine learning approaches. The Section V summarizes and dissects results and validation. The section VI conclude the paper with discussion.

II. LITERATURE REVIEW

This section reviews some of the work done in DDoS attacks detection and machine learning approaches to analyze the different types of attacks. The Balkanli et al [13] used Bro and Corsaro systems and CART (Classification and Regression Trees) to detect DDoS attacks. The work mainly focused on two classification problems without using IP addresses and port numbers as a features. The authors have introduced a methodical examination of the DDoS assaults.

Kumar et al. [11] proposed a plan of utilizing DenS recognition in entropy in an Internet Service Provider (ISP) area. Seeing that the past traffic checking and examination for DDoS is carried out by the aggressor on a single connection of the ISP, this not only expands the memory and figuring pressure yet also makes it defenseless against assault itself, so the author proposed A appropriated strategy dependent on traffic dissemination between ISPs and POPs is distinguished. Chen et al. [12] proposed a new distributed traffic stream identification strategy for distinguishing DDoS flood assaults. They utilize the shared participation between the change conglomeration tree area workers in the ISP space to aggregate the flood reports of course reports.

Robinson et al. [14] proposes DefCOM for a distributed network, particularly for insurance against DDoS attacks. The DefCOM is introduced on all organization hubs. It has capacities to separate the errands between the nodes. Each organization node may either take assignments like arrange whether the packet is noxious, Rate Limitation, Generation of alarms to different nodes in a network. Nodes take up the undertakings at which they are great. The system has another usefulness that makes it to help message prioritization. When utilized inside a solitary substance, the System is an ideal methodology, however not so reasonable when utilized as an instrument for dividing information among organizations. DefCOM's functioning model is to such an extent that it offers a lightweight design that empowers collaboration between

hubs, as opposed to presenting an alternate type of DDoS defence defense framework.

Ni et al. [15] proposed a technique to distinguish DDoS Attacks caused at the application layer utilizing Time Series Analysis. They proposed a design for Bandwidth and Resource Exhausting DDoS attacks. Their commitments incorporate HTTP GET demands per source IP address to distinguish DDoS assaults. A recognition strategy utilizing an SVM classifier creates high proficiency and adaptability in distinguishing attacks. Rashidi et al. [16] proposed a DDoS guard component called CoFence, which included unique asset assignment devices in the area, permitting the organization to help each other to face DDoS assaults through resource sharing. The primary idea of collective identification for DDoS is data sharing between framework individuals and asset assignment assistance. This is a smart approach for the recognition of disseminated disavowal of service. Distributed Denial of Service (DDoS) guard framework itself isn't safe to enormous scale attacks. Rodrigues, Bocek and Stiller [17] proposed BLOSS-an approach to work on DDoS by sending shared network hardware The new arrangement of assault flagging shows that the blockchain framework has the decentralization highlight and the support of shrewd agreements, and it is feasible to participate to defend against DDoS helpful assaults by improving on the operability and interoperability between Autonomous Systems. However, for such frameworks, security and framework performance are key issues to consider.

Gu et al. [18] built an alliance blockchain structure for malware location and evidence extraction in cell phones, shared by the detection federation chain shared by test individuals and clients. The public chain is made and effectively accomplishes higher accuracy. Dobson et al. [19] carried out Random Forest, Logistic regression, KNN and Gradient boost algorithm on interruption recognition NSL-KDD dataset. They looked at the outcomes accomplished by AI calculations with profound learning calculations and closed profound learning calculations had accomplished high exactness and accuracy. Othman et al. [1] carried out SVM on Interruption identification benchmark datasets by utilizing Chi-square feature selection method technique to decrease the preparing time. Oikonomou et al. [20] proposed a gossip based correspondence model that gives data of different digital attacks. In this model when one framework got attack different system will be educated with the attacker data. Henceforth, it assists different frameworks with dealing with the assaults. The frameworks are associated in a distributed model to divide the aggressor data between different nodes.

Dheeraj et al. [21] proposed a communitarian system which utilizes Blockchain and keen agreements to moderate DDoS attacks across various Areas. It utilizes a circulated and decentralized stockpiling which helped in fostering a proficient synergistic engineering against DDoS attacks. Devendra Prasad et al. [22] proposed a framework utilizing Stochastic angle boosting calculation to recognize DDoS attacks. It gave a superior presentation results contrasted with KNN, Choice Tree and Arbitrary Timberland. Filho et al. [23] proposed a

framework and assessed the exhibition on interruption recognition datasets to be specific, CIC-DDoS, CICDDoS2017, and CICDDoS2018, and had the option to arrange different kinds of DDoS attacks. A. A. T. Blameless et al. [24] proposed a framework for Blockchain innovation with protection by including a novel improvement for secure calculation conventions. The information inside Blockchain can be ensured utilizing keyless cryptosystem which might be an add-on to security in Blockchain [25]. A. Pasumpundian et al. [26] proposed a framework which is a blend of neural organizations and SVM calculation to distinguish DDoS assault. The framework contains two modules i.e., memory and learning modules used to recognize pernicious packets.

Further Zhang et al. [27] contend that vindictive code identification is considered an example acknowledgment and can be settled by a neural network that doesn't need a numerical portrayal of how the yield is practically reliant upon the information to estimate the capacity. Fuzzy logic and neural networks are complementary, so they propose a fuzzy neural organization-based malware discovery calculation and it is demonstrated that this method can successfully distinguish malevolent paired code. The connection between them leads to iteratively improve the quality of issue arrangements additional time [28]. The molecule swarm advancement calculation used as Multitude knowledge (SI) is an arbitrary pursuit algorithm that recreates creature rummaging conduct and uses group collaboration as a fundamental segment. It very well may be considered a multi-specialist enhancement framework. MAOS). Since the particle swarm improvement calculation has a generally quick relative convergence rate in the beginning phase, it is barely noticeable the optimal arrangement in the quick hunt cycle and accordingly fall into the local ideal, so Eberhart and Shi [29] will change the inertia weight in the molecule swarm optimization calculation. We will provide proactive defences that can protect against attacks that have several vulnerabilities; on the other hand, also reactive defences that defend themselves against attacks that exploit a few vulnerabilities.

III. PROPOSED SOLUTION

We proposed a framework for the systematic evaluation of DDoS attacks in the context of Blockchain. The machine learning/deep learning models are trained on data from attacks and genuine traffic. The framework will enable the trigger for flagging white or boycotted IP addresses and identify the attacks targeting the network.

In a normal TCP connection, the first step is the TCP connection establishment which is a 3-way handshake. In a 3-way handshake, the client sends a SYN packet, the server sends a SYN+ACK packet after receiving the SYN packet. When the client receives the SYN+ACK packet, it sends an ACK packet. In the framework, three computers are used as attack computers that send TCPSYN requests from different source IP addresses targeting a victim server which is listening on port 80. This floods the server with TCPSYN requests

as the Server will send SYN+ACK packet to each TCPSYN packet.

According to the framework shown in Fig.1, the raw features are fed to the ExtraTreeClassifier to obtain the important features relevant to the classification task. The classification task is a three-class classification task: Benign, UDP flood, and TCPSYN flood attacks. The important features selected from the raw dataset are illustrated in fig.2

- As shown in fig 2, destination IP address of the victim computes shows strong correlation of almost 16% in the feature selection to detect the TCP flood attack. Thus from a network attack's point of view the traffic destined to a TCP server needs to be scrutinized based on the destination IP address. This could be achieved by employing an Intrusion detection and prevention system to monitor the source and destination IP addresses and triggering a notification if traffic flows from several source IP addresses to a particular destination address.
- The second feature is TTL (Time to Live) which is an 8-bit field in the IP packet header. As TCP traffic is sent as an IP packet, a default TTL value (255) is added to all the TCP traffic in the IP header. In the case of benign traffic the TTL value will be different as the Source computers could be located at different locations with different router hops to the victim server. In the case of an attack, the TTL values are the same as they are generated on the same network which could be used as an indicator of a TCP flood attack.
- Similarly, SYN is an important feature in detecting the attack with a correlation of almost 14% as shown in Fig.2. If there are several SYN packets with different source IP addresses and same destination address, it could be an attack to the given destination IP address. As a result the server will attempt to process the attacker's fake SYN requests and becomes unresponsive to legitimate TCP requests, preventing the completion of the handshake.

The following selected machine learning algorithms are used for the experimentation.

1) *Extreme Gradient Boosting (XGBoost)*: Extreme Gradient Boosting (XGBoost) [30] is an efficient open-source project implementation of the gradient boosting algorithm. Gradient boosting is a class of ensemble machine learning used extensively for predictive analytics and work very well for unstructured data. In general, the ensemble is constructed from the addition of decision tree models one at a time to reduce prediction error using a gradient descent optimization algorithm. The XGBoost optimizes gradient boosting by effective parallelization, hardware optimization, and regularization. The algorithm is highly scalable with higher computational speed on memory-constrained systems.

2) *Tab Transformer*: [31] The Transformer is widely used for contextual modeling in Natural Language Processing (NLP). The Tab Transformer is the adaptation of the Transformer for tabular data. The Tab Transformer utilizes a sequence of multi-head attention-based Transformer layers to take input and convert it into contextual embeddings to bridge



Evaluation of machine learning models

Fig. 1. Block diagram of Machine Learning model

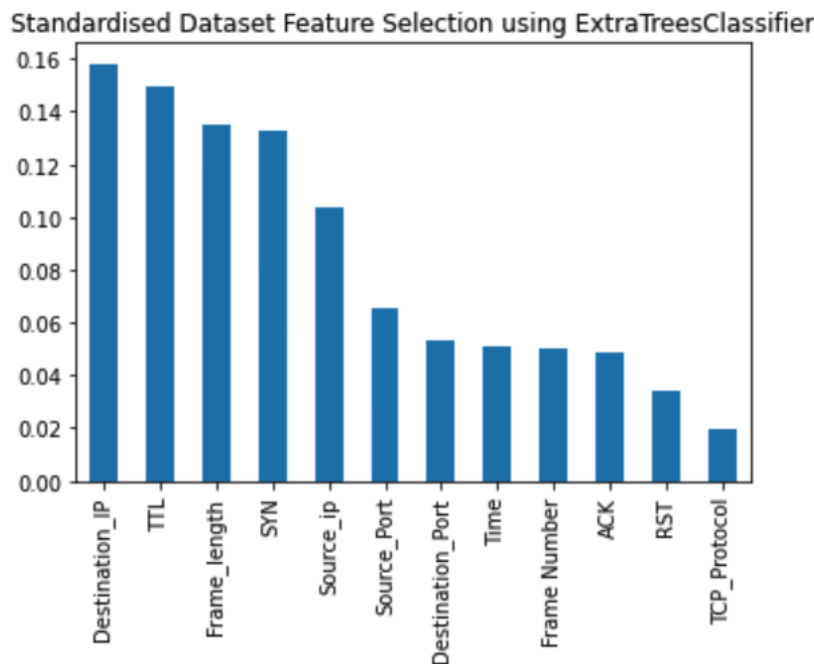


Fig. 2. Feature Engineering using Extra Trees Classifier

the gap between baseline MLP and GBDT models. The highly correlated features in the same column and cross column result in an embedding vector close to euclidean distance. There is no such relationship that exists in context-free embedding. The Tab Transformer is highly robust to the random missing and noisy data.

3) *Random Forest*: Random Forest uses a set of decision trees selected randomly from the bootstrap sample of the training dataset. The vote is aggregated from all the decision trees, and the final score of classification is given. The classifier is efficient with a big dataset and can handle a large number of input variables. Moreover, it avoids overfitting and improves generalizations. During the forest building, it produces the estimate of unbiased generalization of error. The best experimental parameters of the classifier are: There were 120 estimators with minimum sample leaves as 1, and 120 estimators with minimum sample split as 3 were used for best classification accuracy. The Gini criterion is used to measure the quality of the split.

IV. EXPERIMENTAL ANALYSIS

A. Dataset

The dataset [32] used in this research study is comprised of two types of attacks, i.e., TCPSYN and UDP flood attacks, and the attacks are directed towards the server attached to the backbone network of the campus. The router is attached to a blockchain-based network. There are three computers used for attacking the network, and the traffic is captured using the hping3 software. The attack packets contain spoofed source IP addresses and are generated randomly that appear to the router as if the traffic is coming from various sources. In this study, we investigate the behavior of such attacks at the router and the peer-to-peer level. The traffic is captured from the router and peer-to-peer network by mirroring the traffic to the computer for storage. The saved traffic is used for further analysis and evaluation of intrusion detection systems.

B. EVALUATION CRITERIA

1) *Accuracy*: Accuracy is a widely used criterion for the evaluation of machine learning algorithms. Our dataset is

TABLE I
THE ACCURACY AND PARAMETER SETTINGS FOR MACHINE LEARNING MODELS.

Model	Accuracy Score	Parameter Settings
Tab Transformer	97%	Embedding dimension=32, No of layers=6, attention heads=8
Random Forest	94.3%	criterion='gini', samples split=2
XGBoost	94.8%	criterion='friedman mse', loss='deviance'

TABLE II
F1-SCORE OF MACHINE LEARNING MODELS.

Features	Tab Transformer	Random Forest	XGBoost
Benign	1.00	0.98	0.99
TCPSYNC	0.90	0.80	0.85
UDPFLOOD	0.91	0.81	0.84

imbalanced with more Benign traffic compared to TCPSYNC and UDPFLOOD attacks. Therefore, we will be looking into some other popular criteria to assess the machine learning model's performance. The formula for Accuracy is given below.

$$Accuracy = (TP + TN) / (TP + FN + FP + TN)$$

2) *Precision*: It is defined as the ratio of correctly classified items to actually classified items.

$$Precision = TP / (TP + FP)$$

3) *F1-Score*: The F1-Score is also known F-Measure that calculates the harmonic mean of Precision (P) and Recall(R) to find the score. The maximum value for F1-score is 1 known as Dice similarity coefficient. The formula for F1-Score is given below.

$$F1 = 2 * (P * R / P + R)$$

Where P and R represent Precision and Recall, respectively.

V. RESULTS AND VALIDATIONS

This section will discuss the performance of different machine learning algorithms on predicting DDoS attacks from benign traffic in the context of Blockchain. We analyze the traffic for DDoS attacks at the hierarchical level, firstly at the router level and then at the peer-to-peer level. The accuracy of Tab Transformer is around 97% shown in Table I. The accuracy of XGBoost and Random Forest is mostly comparable, having accuracy 94.3% and 94.8% respectively. The dataset has been labeled with three classes of TCPSYNC, UDPFLOOD, and mixed with normal traffic labeled as Benign traffic.

VI. CONCLUSION

This paper explores the performance of the current state-of-the-art machine learning models such as Tab Transformer to detect and identify DDoS attacks in the context of Blockchain networks. The performance of machine learning and deep

learning approaches largely depends on selecting features for the required task. The insightful analysis of the dataset is fundamental before choosing the machine learning/deep learning model. In our case, the Tab transformer [31] model learns the contextual information, thus showing superior performance in identifying the DDoS attacks.

REFERENCES

- [1] S. M. Othman, F. M. Ba-Alwi, N. T. Alsohybe, and A. Y. Al-Hashida, "Intrusion detection model using machine learning algorithm on big data environment," *Journal of Big Data*, vol. 5, no. 1, pp. 1–12, 2018.
- [2] F. Wang, X. Wang, J. Su, and B. Xiao, "Vicsifter: a collaborative ddos detection system with lightweight victim identification," in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2012, pp. 215–222.
- [3] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Transactions on Computer Systems (TOCS)*, vol. 24, no. 2, pp. 115–139, 2006.
- [4] A. D. Keromytis, V. Misra, and D. Rubenstein, "Sos: An architecture for mitigating ddos attacks," *IEEE Journal on selected areas in communications*, vol. 22, no. 1, pp. 176–188, 2004.
- [5] X. Yang, D. Wetherall, and T. Anderson, "A dos-limiting network architecture," *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 4, pp. 241–252, 2005.
- [6] Z. Han, X. Wang, F. Wang, and Y. Wang, "Collaborative detection of ddos attacks based on chord protocol," in *2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012)*. IEEE, 2012, pp. 1–4.
- [7] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan, "Cossack: Coordinated suppression of simultaneous attacks," in *Proceedings DARPA information survivability conference and exposition*, vol. 1. IEEE, 2003, pp. 2–13.
- [8] Y.-S. Wu, B. Foo, Y. Mei, and S. Bagchi, "Collaborative intrusion detection system (cids): a framework for accurate and efficient ids," in *19th Annual Computer Security Applications Conference, 2003. Proceedings*. IEEE, 2003, pp. 234–244.
- [9] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on software engineering*, no. 2, pp. 222–232, 1987.
- [10] C. Duma, M. Karresand, N. Shahmehri, and G. Caronni, "A trust-aware, p2p-based overlay for intrusion detection," in *17th International Workshop on Database and Expert Systems Applications (DEXA'06)*. IEEE, 2006, pp. 692–697.
- [11] K. Kumar, R. Joshi, and K. Singh, "A distributed approach using entropy to detect ddos attacks in isp domain," in *2007 International Conference on Signal Processing, Communications and Networking*. IEEE, 2007, pp. 331–337.
- [12] Y. Chen, K. Hwang, and W.-S. Ku, "Collaborative detection of ddos attacks over multiple network domains," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 12, pp. 1649–1662, 2007.

- [13] E. Balkanli, J. Alves, and A. N. Zincir-Heywood, "Supervised learning to detect ddos attacks," in *2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*. IEEE, 2014, pp. 1–8.
- [14] M. Robinson, J. Mirkovic, S. Michel, M. Schnaider, and P. Reiher, "Defcom: defensive cooperative overlay mesh," in *DARPA Information Survivability Conference and Exposition*, vol. 3. IEEE Computer Society, 2003, pp. 101–101.
- [15] T. Ni, X. Gu, H. Wang, and Y. Li, "Real-time detection of application-layer ddos attack using time series analysis," *Journal of Control Science and Engineering*, vol. 2013, 2013.
- [16] B. Rashidi, C. Fung, and E. Bertino, "A collaborative ddos defence framework using network function virtualization," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2483–2497, 2017.
- [17] B. Rodrigues, E. Scheid, C. Killer, M. Franco, and B. Stiller, "Blockchain signaling system (bloss): Cooperative signaling of distributed denial-of-service attacks," *Journal of Network and Systems Management*, vol. 28, no. 4, pp. 953–989, 2020.
- [18] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," *IEEE Access*, vol. 6, pp. 12 118–12 128, 2018.
- [19] A. Dobson, K. Roy, X. Yuan, and J. Xu, "Performance evaluation of machine learning algorithms in apache spark for intrusion detection," in *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE, 2018, pp. 1–6.
- [20] G. Oikonomou, J. Mirkovic, P. Reiher, and M. Robinson, "A framework for a collaborative ddos defense," in *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*. IEEE, 2006, pp. 33–42.
- [21] J. Dheeraj and S. Gurubharan, "Ddos mitigation using blockchain," *International Journal of Research in Engineering, Science and Management*, vol. 1, no. 10, pp. 622–626, 2018.
- [22] Z. Martinasek, "Scalable ddos mitigation system for data centers," *Advances in Electrical and Electronic Engineering*, vol. 13, no. 4, pp. 325–330, 2015.
- [23] M. D. Prasad, V. P. Babu, and C. Amarnath, "Machine learning ddos detection using stochastic gradient boosting," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 4, pp. 157–16, 2019.
- [24] Q. Li, L. Meng, Y. Zhang, and J. Yan, "Ddos attacks detection using machine learning algorithms," in *International Forum on Digital TV and Wireless Multimedia Communications*. Springer, 2018, pp. 205–216.
- [25] A. A. T. Innocent and G. Prakash, "Blockchain applications with privacy using efficient multiparty computation protocols," in *2019 PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS)*. IEEE, 2019, pp. 1–3.
- [26] P. Gopalakrishnan and B. U. Maheswari, "Keyless cryptosystem for secure primitive pairing of mobile devices," *Journal of Computational and Theoretical Nanoscience*, vol. 15, no. 5, pp. 1607–1614, 2018.
- [27] P. Karunakaran, "Deep learning approach to dga classification for effective cyber security," *Journal of Ubiquitous Computing and Communication Technologies (UCCT)*, vol. 2, no. 04, pp. 203–213, 2020.
- [28] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proceedings of ICNN'95-international conference on neural networks*, vol. 4. IEEE, 1995, pp. 1942–1948.
- [29] R. C. Eberhart and Y. Shi, "Comparing inertia weights and constriction factors in particle swarm optimization," in *Proceedings of the 2000 congress on evolutionary computation. CEC00 (Cat. No. 00TH8512)*, vol. 1. IEEE, 2000, pp. 84–88.
- [30] T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, 2016, pp. 785–794.
- [31] X. Huang, A. Khetan, M. Cvitkovic, and Z. Karnin, "Tabtransformer: Tabular data modeling using contextual embeddings," *arXiv preprint arXiv:2012.06678*, 2020.
- [32] D. Erhan and E. Anarim, "Boğaziçi university distributed denial of service dataset," *Data in brief*, vol. 32, p. 106187, 2020.

Mohammad Arsalan Sheikh received a bachelor's degree in computer science from Delhi University India in 2014 and a master's degree by research in computer science from University of Technology Sydney (UTS) Australia in 2019. He is currently pursuing his PhD studies in computer science from UTS Australia. Mr. Sheikh is also working as a Solution Architect with AWS Australia and has completed several challenging projects successfully. His main area of research is blockchain security and AI. He is a member of IEEE.

Gul Zameen Khan received a bachelor's degree in computer systems engineering from UET Peshawar Pakistan in 2007 and a master's degree in computer engineering from Hanyang university South Korea in 2011. He completed his PhD in networks and security from Griffith University Australia in 2017. Dr. Khan has worked in the academia, industry, and R&D for 14 years in well reputed organization across different parts of the world.

Farookh Hussain received his PhD degree from Curtin university Australia in 2006. He is highly experienced researcher both in practical industrial research and theoretical research in fog and cloud computing, blockchain and data analytics. Prof. Dr. Hussain is currently working as the head of the discipline software engineering and as a professor in the department of computer science in UTS Australia.