DDoS Prevention on Distributed application using Blockchain Smart Contracts and Machine Learning

[1]Aaditya Banchhiwal, [2]Jatin Bhardwaj, [3]M L Sharma, [4] V K Saini, [5]K C Tripathi

[1, 2, 3, 4, 5]Department of Information Technology, Maharaja Agrasen Institute of Technology, Rohini, Delhi 86.

Abstract

The effect of the threats posed by Distributed Denial of Service (DDoS) attacks on substantially large networks, such as a Blockchain network, demands effective detection and response methods due to the sheer enormity of the problems it causes. These methods are to be deployed not only at the network edge but also at its core. This paper gives an overview of a new solution that would prevent such attacks. It states that web applications can be prevented from DDoS attack by using a layered architecture based on blockchain and deep learning. This can prevent DDoS attack by capturing all the incoming traffic requests made to the server. The requests are redirected to a blockchain based architecture having computational capabilities of smart contracts. In this decentralized database, the dataset of various traffic requests are stored in the form of cryptographically secured chunks. The smart contract is used to filter out requests based on the type of request and some previously set parameters. The parameters are fed to the deep learning layer that is able to detect the anomalous request and differentiate between a genuine and a malicious user. The attack patterns show anomalies in the characteristics of the different selected packet attributes. Accuracy of detection and performance of the system is analyzed using live traffic traces from a variety of network environments ranging from points in the core of the network to those in an edge network.

Introduction

Distributed Denial of Service (DDoS) attack is a major threat to cyberspace. It originates from the network layer or the application layer of the attacker system which is a part of the network. The impact of this attack ranges from the simple inconvenience in using some particular service to causing grave failures at the targeted system. When there is a heavy traffic flow to a target server, it is necessary to classify the legitimate access and possible attacks[1].

Classification of DDoS attacks:

1. Classification by protocols: DDoS attacks are broadly classified into three groups: UDP, TCP and others. This classification is based on the main protocols that are used to transfer data over the internet whose vulnerabilities are exploited by malicious users to organize attacks.
2. OSI classification: OSI/ISO model consists of 7 layers. Every protocol of the network through which data of any kind is transmitted is referred to as a certain layer and DDoS attacks are aimed at Data Link Layer, Network, Transport and Application layers.
3. Mechanism of Action: There can be three groups based on attack mechanism of an attack which include: Attacks aimed at overloading the communication channels i.e. various types of flooding. Second group includes attacks exploiting the network protocol stack vulnerabilities. Third consists of application level attack.[2]

Blockchain and Distributed application:

A Blockchain is a chain of blocks or distributed ledger, consisting of data of a transaction happened between various parties. These blocks are linked via cryptographically secure hashes. Every block consists of a cryptographically secure hash of the previous block, a timestamp, and transaction data. This is generally stored represented as a Merkle Tree.

A Blockchain is resistant to modification of data by design. It essentially is an open and distributed ledger of data that can record transactions between parties efficiently. The blockchain network is a peer-to-peer network adhering to a protocol for inter-node communications and validation of new blocks. Once recorded, data cannot be altered retroactively in any block. Blockchain is considered to have been developed in stages or generations of modifications and improvements. Till now, there have been three major generations.

First generation blockchain networks: Bitcoin and digital currencies were the first generation of blockchain network in which blockchain is structured for the basic premise of a shared public ledger that supports a cryptographically secure currency in a network.

Second generation blockchain networks: Smart Contracts were introduced as a result the computational properties were added to the blockchain technology by vitalik buterin as he created and launched ethereum with the concept of benefits in asset and trust agreements

Third generation blockchain networks: Ever emerging technology evolve each day and in third generation multiple chains can be conversed and it can be used as blockchain technological platform[4][5]

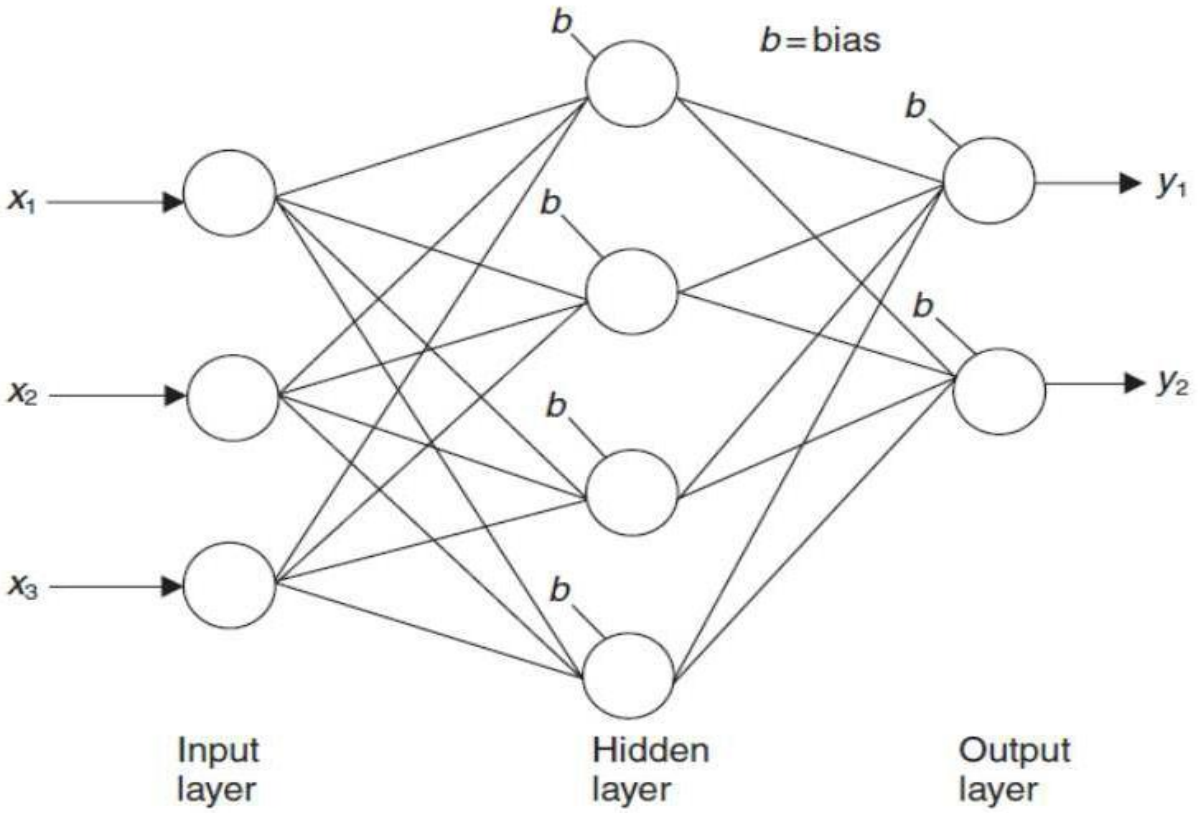
Blockchain, in-spite of being considered robust and secure, is not free of attacks as well. there have been many attacks in the past on blockchain networks as a whole that have made the users suffer. Some types of attacks on blockchain network are:

1. DDoS attacks are actually the most common type of attack on blockchain networks. While attacking a network, the hackers intend to bring down a server by consuming all its processing resources with enormous amount of requests. DDoS attackers aim to disconnect the mining pools, e-wallets, and other financial services of the network nodes. Entire blockchain network can be brought down by flooding full node operators with traffic via the Distributed Denial of Service attacks.
2. Majority attacks or 51% attacks are those attacks when the malicious user gain control over 51% of network block rate and create an alternative chain of blocks that finally supersede the authentic block although this vulnerability deemed as unrealistic but several blockchain based cryptocurrencies have suffered from this attack.
3. Mining pool attacks multiple miners collaborate their computational capabilities by creating a mining pool. Malicious user targets the mining pool and compromises the control over mining pool both externally and internally by exploiting vulnerabilities in conseys mechanism of blockchain.
4. Race attacks are executed when a malicious user creates two conflicting transactions. A transaction is first sent to the service provider who would accept the transaction and initiate the delivery of service without any confirmation of transaction. Simultaneously, an ambiguous transaction returning the same amount of cryptocurrency to the malicious user is broadcast to every node in the network which renders the original transaction illegitimate.

Related Work

Traditional Anomaly based DDoS detection systems construct a profile of the traffic normally seen in a network, and then identify the anomalies whenever traffic behaviour deviates from normal profile behaviour beyond a threshold limit. This extent of deviation is usually not utilized[5]**.** This extent of deviation from detection threshold is used as an input to ANN model for predicting the number of zombies in the network.[5} A real time estimation of the number of zombies in an attack scenario is very helpful for suppression of the effect of attack by choosing the predicted number of most suspicious attack sources for either filtering or rate limiting.[5]

Botnets have always been an issue to deal with any DoS/DDoS network based attack. [5] helps in giving a good method to predict and determine the network of zombies using ANN model training. This approach still has limitations since it cannot be implemented in a blockchain or distributed systems. The request-response cycle of the particular is of immense importance when it comes to financial transactions online, and delays in them will cause issues in the working of the project itself.



Paper [8] studied the source code of some popular DDoS attack bots, namely, Agobot, SDBot, RBot and Spybot etc. to get full knowledge about such attacks which is useful for designing efficient approaches for the detection and mitigation of DDoS attacks. These previous attacks were measured on the basis of backbone internet traffic, activities of the botnets and changes in routing. Based on these analyses, the author concluded that in many attacks, these attackers acted in a non-state. They were able to use huge numbers of botnet nodes efficiently and effectively to begin massive DoS attacks causing huge damages.[8]

Dangers of these Botnet-based DDoS attacks that originated at the application layer were studied by Alomari et al. [10]. These attacks created immense losses of revenue of many business sites and government websites.[10]

Kumarasamy and Asokan [11] put forward a puzzle solving mechanism for pushing back requests to the core routers rather than sending them to the target server. In order for them to avoid the attackers, the victim server gave a puzzle to the client which is sending the traffic. If the client solves the puzzle, then it is considered as authentic, allowing the traffic from the client into the server. In case the puzzle solving client was flagged as malicious, then the target gave a more complicated puzzle. For identifying the DDoS attack, combined puzzle sending and push back mechanism was used by the authors.[11] This by far is the most simple and widely used method employed to prevent attack vectors and used by giants like Google as well.

Most of the standard applications use the well-known port numbers (0 to 1023). Since ports are listening for a long time for acknowledgements from the users, this makes such attacks easier. Hence, pseudo-random port-hopping and synchronization between communicating parties is required to reduce attacks.[14] But time servers are susceptible to attacks themselves, and a further level of security needs to be implemented on them too, which becomes a shortcoming for this strategy.

Mirkovic et al. [18] has proposed a defense system called "DefCOM". According to this, some selected nodes in the network-called DefCOM nodes-are situated at some distance from the source, victim and core networks. These nodes operate as an overlay to find and cut the attacks. These defense nodes strain the attacker traffic, and protect the resources of the victim, and also help to identify the valid traffic along the suspicious traffic and make its correct delivery to the victim. This strategy is useful in understanding the attacks and response methods on a distributed system.

Companies like Akamai [19] and CloudFlare [20] provide DDoS protection services, the adoption of which is increasing [21]. These cloud-based solutions absorb all DDoS attacks by increasing the capacity of servers and taking the burden of detection away from the victim device by exporting flow records away from edge routers and switches. Cloud performs additional analysis. Packet filtering is employed to balance, reroute, or drop the traffic inside the cloud. However, such solutions require a third party Protection Service provider, which implies additional costs and decrease in service performance of the victim application.

Proposed Solution

The idea consists of a multi-phase modular structure which works as a safeguarding mechanism to protect applications from an attack similar to the DDoS attack. This would require making of a decentralized application hosted on the web and protection mechanism requires another blockchain application with deployed smart contract and deep learning algorithm. It would require traffic classification and learning algorithms on the same using smart contracts for initial classification.

Blockchain and Smart Contracts:

All the traffic incoming to a blockchain based core application are redirected to the blockchain (database) on which an initial smart contract will be instantiated. This smart contract will filter out requests based on the type and a few previously set parameters. This Layer is made in order to ensure that request-response cycle for the application does not suffer due to processing time of the classifier. If initial parameters are satisfied then the request will immediately go to the server for processing. Remaining suspicious requests will be sent to the Machine learning classifier.

While several projects try to address these issues, the Ethereum [23] blockchain is the most popular that supports a Turing-complete contract language, empowering more sophisticated smart contracts. In Ethereum, smart contracts run in a sand-boxed Ethereum Virtual Machine
(EVM) and every operation executed in the EVM has to be paid for to prevent Denial-of-Service (DoS) attacks.

Machine Learning Algorithm Classifier:

Those requests that are labelled suspicious and need to be thoroughly verified whether or not it is a part of a Botnet, a malicious request or a DoS attempt, are sent to ML classifier that employs deep learning techniques to verify

whether the incoming traffic is malicious or not. Safe traffic is sent to the server for processing and Malicious traffic is discarded and a log file created to store the malicious IP/MAC addresses.

Classifier first determines anomalies coming in a network in real time. For this, network is studied to learn the behaviour of regular packets. Anomalies occurring in real time are monitored and suspicious packets are labelled accordingly. These suspicious packets are then classified based on characteristics like:

The type of request

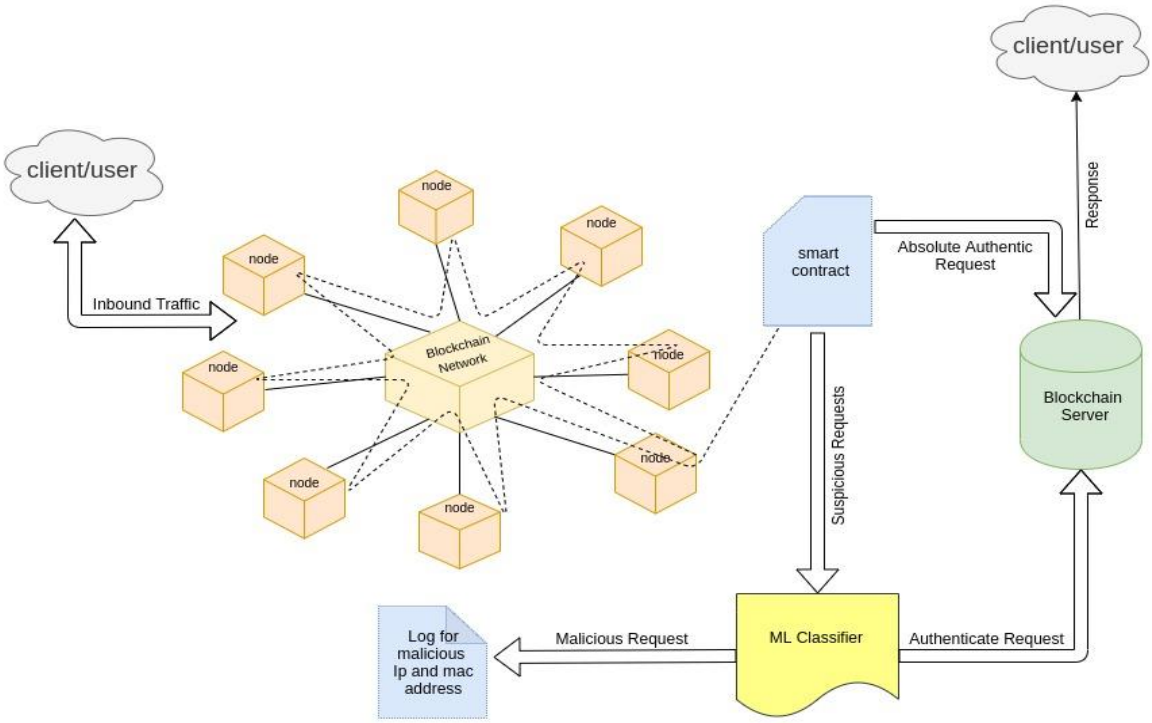
Source of the request

Type of resource accessed by the request

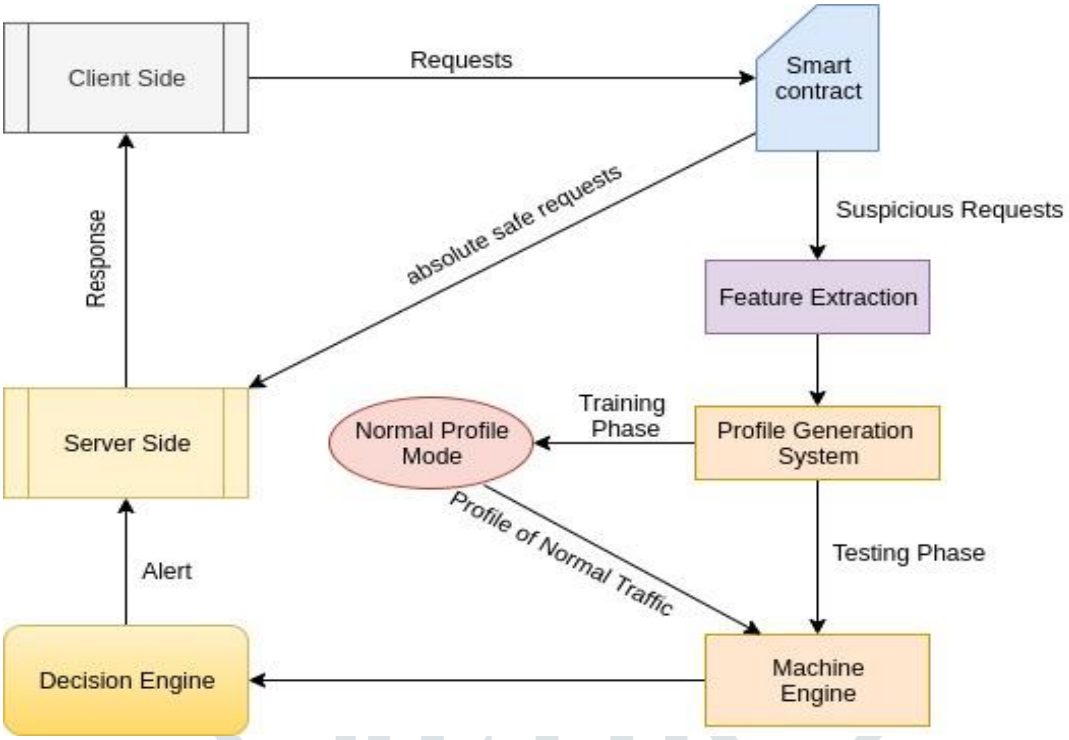
Packet size

Possible Scripts embedded inside packet

Blocked packets are blacklisted and the smart contract along with the classifier checks for the presence of these malicious IP sources in the Log file for further reducing the request response time. Thus, useability is enhanced.



Architecture of DDoS prevention System



Scope and Relevance of Project

In order to distinguish DDoS attacks and network attack flow, this research shall put forward the attack detection using machine learning and classify user as confirmed attacker or a genuine user. Though technology has improved and many number of filtering methods are used to identify the legitimate access and the flooding created by the attackers, there still is a need for a novel solution that considers prevention of all the attacks. This paper puts forward an approach that improves traditional approaches and is a step forward in creating that novel solution. Although further improvements can be incorporated, the scope of this paper involves only the detection and prevention of Distributed Denial of Service attacks, of the type - overflow attack. The performance of the classification is compared by the detection rate and False Positive Rate (FPR). The model can be further improved on getting more improved, cleaner dataset and refining the parameters.

Result and Conclusion

This paper presents a comprehensive and literature review concerning DoS/DDoS attack detection using machine learning and blockchain smart contract techniques. It is not surprising that ANN and SVM play a dominant role in many researches because of the accuracy and robustness. This work has some limitations. This study only contains papers that were published from 2007 to 2017. We now focus on gathering more articles from other online resources/journals in order to further improve upon the idea.

Implementing the mentioned idea shall require more research in the field and capabilities of smart contracts and their limitations in dealing and manipulating the network traffic.

References

[1] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. Kalita, “Detecting distributed denial of service attacks: Methods, tools, and future directions,” The Computer Journal,2013. pp 1-20

[2] S. Umarani, D. Sharmila "Predicting Application Layer DDoS Attacks Using Machine Learning Algorithms", World Academy of Science, Engineering and Technology, January, 2016 pp 1-6.

[3] Brij Bhooshan Gupta, Ramesh Chand Joshi, and Manoj Misra, "ANN Based Scheme to Predict Number of Zombies in a DDoS Attack", International Journal of Network Security, January 2011 pp 216-225

[4] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System". October 2008 pp. 1-11

[5] Thing, Vrizlynn L., Morris Sloman, and Naranker Dulay. "A survey of bots used for distributed denial of service attacks." New Approaches for Security, Privacy and Trust in Complex Environments. Springer US, 2007, pp. 229-240.

[6] Dr. Gavin Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger Byzantium Version",What is block of blockchain, June 2018, pp 5

[7]Alomari, Esraa, et al. "Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art." arXiv preprint arXiv:1208.0403 2012, pp. 24-32

[8]Kumarasamy, S., & Asokan, R. (2012). Distributed Denial of Service (DDoS) Attacks Detection Mechanism. arXiv preprint arXiv:1201.2007, pp. 41-49.

[9]Bhuyan, Monowar H., et al. "Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions." The Computer Journal 2013, pp. 1-20.

[10]Gu, Q., & Liu, P. Denial of service attacks. Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, Volume 3, 2007, pp. 454-468

[11]Fu, Z., Papatriantafilou, M., & Tsigas, P. (2008, October). Mitigating distributed denial of service attacks in multiparty applications in the presence of clock drifts. In Reliable Distributed Systems, 2008. SRDS'08 pp. 63-72.

[12] J. Dheeraj, S. Gurubharan, 2017 "Multi-domain DDoS Mitigation Based on Blockchains" Research gate, June 2017. pp. 185-190 DOI: 10.1007/978-3-319-60774-0_19

[13] L. Mauri, S. Cimato, and E. Damiani, "A comparative analysis of current cryptocurrencies,"International Conference on Information Systems Security and Privacy, 2018 pp 127-138,

[14] Braian A Ho, "Transforming Commerce, Information Storage and Exchange: The Threats and Opportunities of Blockchain Technology" 2019 pp 1-17

[15] Mirkovic, Jelena, et al. "Distributed defense against DDOS attacks." University of Delaware CIS Department Technical Report CIS-TR-2005-02, 2005, pp. 1-12.

[16] Akamai: "How to Protect Against DDoS Attacks - Stop Denial of Service" (2016). https://www.akamai.com/us/en/resources/protect-against-ddos-attacks.jsp. Accessed 10 Jan 2017 pp 1-13

[17] Jonker, M., Sperotto, A., van Rijswijk-Deij, R., Sadre, R., Pras, A.: "Measuring the adoption of DDoS protection services." In: Proceedings of the 2016 ACM on Internet Measurement Conference, IMC 2016, Santa Monica, California, USA (2016) p 1-21