Computer Systems Science & Engineering
DOI:10.32604/csse.2022.025668
Article

Tech Science Press

Cooperative Detection Method for DDoS Attacks Based on Blockchain

Jieren Cheng[1,2], Xinzhi Yao[1,2,*], Hui Li[3], Hao Lu[4], Naixue Xiong[5], Ping Luo[1,2], Le Liu[1,2], Hao Guo[1,2] and Wen Feng[1,2]

[1]Hainan University, Haikou, 570228, China
[2]Hainan Blockchain Technology Engineering Research Center, Haikou, 570228, China
[3]Hainan Huochain Tech Company Limited, Haikou, 570100, China
[4]Research Office of Information Technology, Air Force Early Warning Academy, Wuhan, 430019, China
[5]Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, 74464, USA
*Corresponding Author: Xinzhi Yao. Email: yxz17771776160@163.com
Received: 01 December 2021; Accepted: 18 January 2022

Abstract: Distributed Denial of Service (DDoS) attacks is always one of the major problems for service providers. Using blockchain to detect DDoS attacks is one of the current popular methods. However, the problems of high time overhead and cost exist in the most of the blockchain methods for detecting DDoS attacks. This paper proposes a blockchain-based collaborative detection method for DDoS attacks. First, the trained DDoS attack detection model is encrypted by the Intel Software Guard Extensions (SGX), which provides high security for uploading the DDoS attack detection model to the blockchain. Secondly, the service provider uploads the encrypted model to Inter Planetary File System (IPFS) and then a corresponding Content-ID (CID) is generated by IPFS which greatly saves the cost of uploading encrypted models to the blockchain. In addition, due to the small amount of model data, the time cost of uploading the DDoS attack detection model is greatly reduced. Finally, through the blockchain and smart contracts, the CID is distributed to other service providers, who can use the CID to download the corresponding DDoS attack detection model from IPFS. Blockchain provides a decentralized, trusted and tamper-proof environment for service providers. Besides, smart contracts and IPFS greatly improve the distribution efficiency of the model, while the distribution of CID greatly improves the efficiency of the transmission on the blockchain. In this way, the purpose of collaborative detection can be achieved, and the time cost of transmission on blockchain and IPFS can be considerably saved. We designed a blockchain-based DDoS attack collaborative detection framework to improve the data transmission efficiency on the blockchain, and use IPFS to greatly reduce the cost of the distribution model. In the experiment, compared with most blockchain-based method for DDoS attack detection, the proposed model using blockchain distribution shows the advantages of low cost and latency. The remote authentication mechanism of Intel SGX provides high security and integrity, and ensures the availability of distributed models.

Keywords: Blockchain; smart contract; IPFS; DDoS attack

1 Introduction

Among the current types of network attacks, DDoS attacks have the characteristics of being easy to implement, destructive, difficult to resist and track, etc., so the harm is particularly significant [1,2]. According to data from Neustar, a well-known American communications service organization [3], compared with the fourth quarter of 2018, DDoS attacks in the fourth quarter of 2019 increased by 168% [4]. The largest mitigation threat is 587 Gbps, which is 31% larger than the largest attack in 2018, and the largest attack intensity observed in 2019 is 343 million packets per second (Mpps), which is a 252% increase from the most intense attack in 2018. In the first half of 2020, DDoS attacks have undergone major changes. Compared with the same period in 2019, the number of DDoS attacks has increased by 151%. These included the largest and longest sustained attacks that Neustar mitigated, at 1.17 Tbps per second and 5 days and 18 h, respectively. Big data environments such as customers, networks, service infrastructure, government organizations, and companies have increasingly become the key targets of DDoS attacks [5,6].

The current work to mitigate DDoS attacks mainly includes the following two: (1) By using legal services on Internet of Things (IoT) devices [7], for example, some simple service discovery protocols are used. However, the harm of DDoS attacks is amplified by this, making the defense problem more complicated and difficult, and causing more serious economic losses [8]. Among the mitigation plans currently proposed, most of the deployment work is extremely difficult to carry out, so only a very small number of plans can be deployed and implemented. For example, Internet Engineering Task Force (IETF) proposed the development of a collaboration protocol called DDoS Open Threat Signaling (DOTS) [9] to spread DDoS attacks. However, the complexity of the development of these new protocols and the high cost of maintenance have brought difficulties that are difficult to overcome in various aspects for the development of collaboration protocols. (2) Currently, DDoS protection schemes provided by companies such as Akamai [10] or CloudFlare [11] are gradually being adopted [12]. These cloud-based solutions to mitigate DDoS attacks [13] are solved by increasing capacity. In order to reduce the detection burden of attacked devices, the traffic in edge routers and switches is exported. When performing extra analysis in the cloud, packet filtering is used to balance, reroute, or drop traffic within the cloud. However, these schemes require protection from a third party, which means higher costs, lower service performance and greater credit problems [14]. However, the infrastructure of blockchain [15] and smart contracts can solve third-party problems and alleviate DDoS attacks.

In the current work on mitigating DDoS attacks using blockchain and smart contracts, the mainstream approach is the architecture and implementation method of using blockchain [16] and smart contracts to transmit attack information (whitelist or blacklist IP address signals) across multiple domains [1]. However, DDoS attacks are large-scale attacks, the number of whitelisted and blacklisted IPs for DDoS attacks is extremely large, and there is a risk of critical data leakage. The blockchain is a distributed structure composed of multiple blocks. The transmission of huge data using the blockchain will seriously affect the time overhead, bring extremely high transmission costs, and greatly reduce the transmission efficiency. Therefore, distributing the DDoS attack detection model can well alleviate the problems of high transmission cost and time overhead, and ensure that key data is not leaked. In order to ensure the security of the model, after the DDoS attack detection model is trained, we use Intel SGX [17] to protect the model to ensure the security of the DDoS attack detection model before distribution. In this paper, our goal is to leverage blockchain and IPFS to distribute DDoS attack detection models. We propose a blockchain-based DDoS attack collaborative detection method, which uses blockchain and IPFS to distribute a DDoS attack detection model to reduce more costs and significantly reduce time overhead. The contributions of this article are:

- A model distribution mechanism is proposed to further improve the timeliness of the entire framework while ensuring that key data is not leaked.
- This article is not limited to a small technological breakthrough, but turns its attention to providing a valuable and implementable overall framework for mitigating DDoS attacks. This article provides a new application scenario for blockchain and a strong guarantee for the distribution mechanism. This scene has a wide range of commercial applications.

2 Background

2.1 Blockchain

Blockchain technology [18] can build a reliable data model that is collectively maintained under the condition of decentralization and no prior trust of service providers. Make data transfer between service providers through encryption algorithms, consensus mechanisms, and specific data storage methods. Miyachi et al. [19] proposed a modular hybrid privacy protection framework, using off-chain and on-chain blockchain system design to be applied to three different reference models. Manogaran et al. [20] proposed a blockchain-assisted data offloading method for maximum availability (BDO-AM), which is to prevent the non-probabilistic (NP) difficult problem of data availability due to prolonged backlog. Nguyen et al. [21] deployed blockchain technology to create a safe and reliable data exchange platform between multiple data providers, in which IoT data is encrypted and recorded in a distributed ledger. Lucas et al. [22] proposed a DR registration framework and implemented it as a proof of concept on Hyperledger Fabric, using real assets in a laboratory environment to study its feasibility and performance. Sun et al. [23] proposed a new model of social network public opinion dissemination based on blockchain technology. This model considers the impact of a reasonable quantitative value contribution on the incentive mechanism generated by the dissemination of information in such social networks, and constructs a profit-risk matrix under different dissemination behaviors. [24] proposed the concept of a blockchain-based remote data integrity check (RDIC) scheme for big data. The new concept uses blockchain technology to greatly improve the efficiency and security of RDIC. Wang et al. [25] first analyzed the security risks of data storage in sensor networks, and then proposed using blockchain technology to ensure the security of data storage in sensor networks. Veeramakali et al. [26] proposed a security framework for data communication based on the Internet of Things using blockchain. In terms of processing time and writing time, the proposed system and the existing system based on the Internet of Things were evaluated for performance. Chinaei et al. [27] use blockchain as a distributed platform to implement on-demand verification schemes. This scheme allows the authorities to automatically conduct transactions with connected devices for witness services.

2.2 Smart Contract

Smart contract is an event-driven, stateful code and algorithm contract [28]. With the continuous development of blockchain technology, the current blockchain technology has gradually surpassed the era of programmable currency and entered the era of smart contracts. Jain et al. [29] designed a joint resource allocation and pricing scheme using blockchain smart contracts. Ziar et al. [30] provide a privacy protection solution for permissionless blockchains to authorize users to control transaction data in the open ledger. Xu et al. [31] proposed a distributed health monitoring system based on blockchain technology to achieve data security, information transparency, efficient sharing and autonomous decision-making through smart contracts. Lakhan et al. [32] proposed to develop a new, cost-effective and stable IoMT framework based on Wuyun supporting blockchain. Estevam et al. [33] proposed a new decentralized timestamp service that combines smart contracts and different time providers. Chen et al. [34] proposed an incentive compatible reasonable secret scheme to construct a game tree with imperfect

information to facilitate our analysis and proof, and directly eliminate the strict control strategy to simplify the game tree. Spataru et al. [35] proposed a blockchain architecture with different semantics, which introduced a new type of node, the purpose of which is to enhance the storage used by smart contracts and an efficient storage model combined with a hybrid compression mechanism. Khan et al. [36] proposed a secure decentralized LMS based on a private blockchain network, called a blockchain-based learning management system (BLMS). Kamboj et al. [37] proposed an RBAC model that uses blockchain-based smart contracts to manage user role permissions in organizations.

2.3 Distributed Denial of Service Attack Detection

Currently, there is no way to completely eliminate DDoS attacks, but we can mitigate DDoS attacks through DDoS attack detection, and quickly restore business and provide services after suffering a DDoS attack. Liu et al. [38] aimed at the existing flow-based DDoS attack detection methods that face non-negligible time delays, and they are not universal for different types and different rates of DDoS attacks. They proposed a fast data packet-based method. DDoS attack detection method (FAPDD). Amaizu et al. [39] proposed a composite and efficient DDoS attack detection framework for 5G and B5G. The proposed detection framework consists of a composite multilayer perceptron, which is combined with an efficient feature extraction algorithm. Not only can it detect DDoS attacks, but it can also return the type of DDoS attacks encountered. Cui et al. [40] proposed a DDoS attack detection and defense mechanism based on self-organizing mapping (SOM) in an SDN environment. Yu et al. [41] proposed a collaborative DDoS attack detection scheme based on entropy and integrated learning. The method established a coarse-grained preliminary detection module based on entropy in the edge switch to monitor the network status in real time. If an abnormality is found, then Report to the controller. Gadekallu et al. [42] proposed a blockchain-based solution to secure datasets generated from IoT devices for e-health applications.

3 Blockchain-based Collaborative Detection Framework for Distributed Denial of Service Attacks

3.1 The Structure of the Framework

The blockchain-based DDoS attack collaborative detection framework proposed in this paper is divided into three parts, as shown in Fig. 1. The first part includes many clients at the outermost layer, the second part is the middle-level service provider, and the third part is the outer blockchain network. Data with valuable meaning, sharing requirements, collaborative processing requirements, and auditing requirements are suitable for uploading to the blockchain. The model meets the above characteristics and occupies less resources, so it is very suitable to upload the model and distribute it.

Client computer. The outermost layer contains many visitors, many visitors include normal clients and malicious attackers (normal clients are blue dots, and malicious attack machines are red dots). Normal clients have normal access to the service provider, while malicious attackers have organized abnormal access to the service provider.

Service provider. The service provider is responsible for receiving the visits of the outermost visitors, and is responsible for the tasks of keeping visit records, training models, using SGX to protect the models and uploading the models to the blockchain. The task of service providers is particularly important. Therefore, it is very important for service providers to reach an agreement in advance to form an alliance before receiving numerous client visits.

Blockchain network. Before receiving visits from many clients, service providers jointly formed a blockchain network to form an alliance so that service providers could help each other without the risk of key data leakage. While service providers are distributing models to each other, the models are also being updated over time, and the latest models are distributed through the blockchain, so as to achieve more efficient collaborative detection purposes.

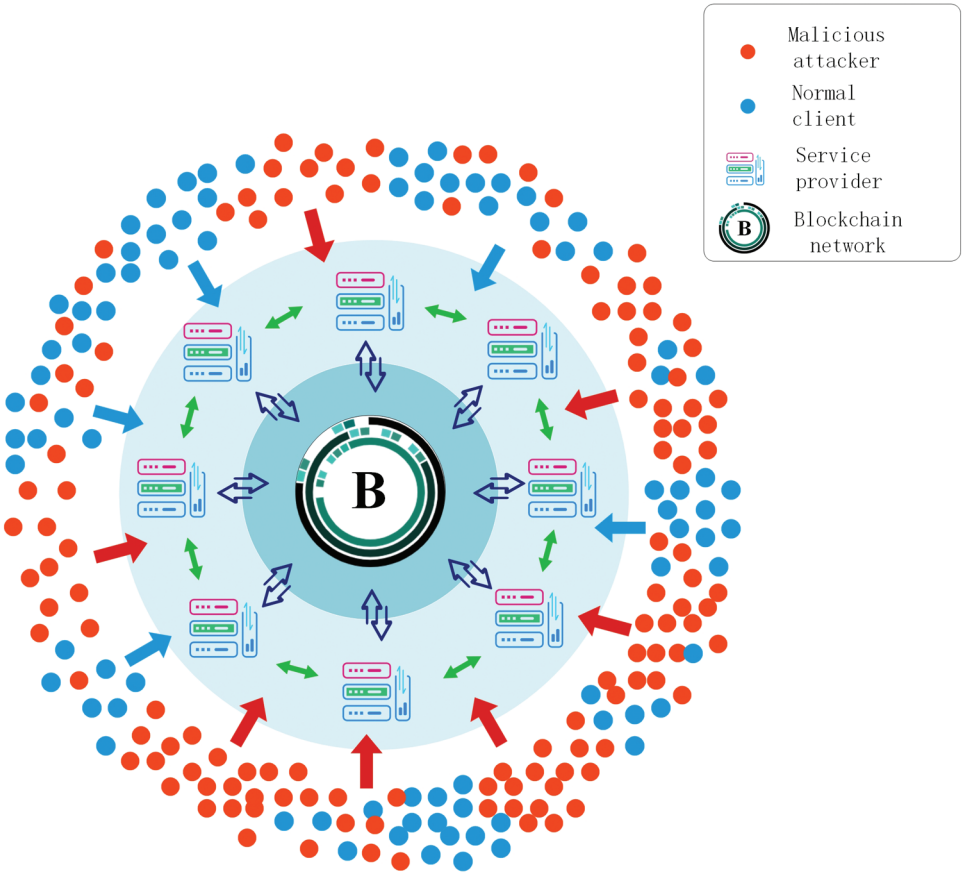

Figure 1: Blockchain-based collaborative detection framework for DDoS attacks

3.2 Distributed Denial of Service Attack Collaborative Detection Process

The main purpose of the blockchain-based collaborative detection framework for DDoS attacks is to conduct collaborative detection of DDoS attacks by using the characteristics of the blockchain. Among them, The blockchain can ensure that the model is not tampered with, and the size of the CID generated by IPFS can ensure that it does not affect the efficiency of the blockchain. SGX provides protection locally for the trained DDoS attack detection model. SGX can effectively prevent the model from being maliciously tampered with before uploading to the blockchain. As shown in Fig. 2, the details of the system architecture are as follows:

- **Step 1.** Clients access the service provider, including both normal clients and malicious attackers. Normal clients normally access the service provider and receive services from the service provider. Many malicious attackers launch DDoS attacks on service providers in an active or manipulated state, in an attempt to cause serious damage to the service provider's business.
- **Step 2.** The service provider has access records after normal clients and malicious attack machines have visited, and the service provider sends the access records to the model training machine.
- **Step 3.** The model training machine uses the access records sent by the service provider to train the DDoS attack detection model.
- **Step 4.** After training the DDoS attack detection model, the training machine uses SGX to protect the model locally to prevent the model from being tampered with.

- **Step 5.** The training machine uploads the DDoS attack detection model protected by SGX to IPFS. After receiving the model, IPFS generates CID and uploads the CID to the blockchain. Note that this blockchain network is composed of service providers in the same industry.
- **Step 6.** When the CID is uploaded to the blockchain network, other service providers on the blockchain will download the CID from the blockchain network. Other service providers use CID to download the model on IPFS and detect the visiting clients.
- **Step 7.** If other service providers in the blockchain network have also suffered DDoS attacks, the model can be updated and distributed according to the above steps.

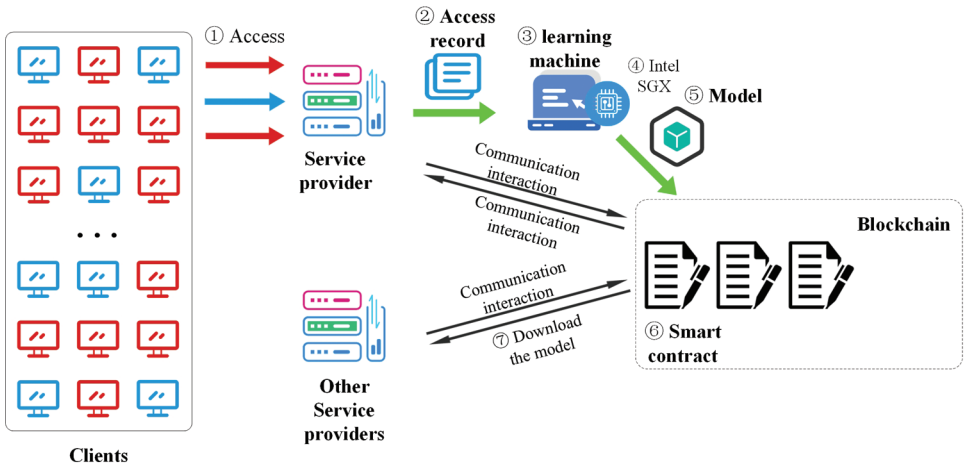

Figure 2: Blockchain-based DDoS attack collaborative detection architecture

Assuming that model f_i and data f_D, the relationship between model f_i and data f_D is that $f_i < f_D$. Since the time cost of distributing files is proportional to the size of the files to be transmitted, the relationship between model f_i and data f_D is shown in (1):

$$t_i(f_i) < t_i(f_D) \tag{1}$$

The blockchain-based DDoS attack collaborative detection architecture has a total of i service providers, and each service provider can distribute the model. Because $t_i(f_i) < t_i(f_D)$, The relationship between the total cost of the distribution of model f_i and data f_D in a fixed period of time is shown in (2):

$$\sum_{i=1}^{n} t_i(f_i) < \sum_{i=1}^{n} t_i(f_D) \tag{2}$$

Before implementing model distribution, service providers need to train the DDoS attack detection model in advance. There are various ways of training the DDoS attack detection model. We give an example and show it in Algorithm 1.

Algorithm 1: Establishment of the recognition model

Input: Network traffic x, label y

Output: The learned parameter θ

1: **for** epochs *1, 2, 3,...,MAX_EPOCH* **do**

2: **for** interaction *1, 2, 3,...,MAX_ITER* **do**

(Continued)

Algorithm 1: (continued)

3: Sample data batch B

4: Put the data batch to network

5: Get the Output of the network

6: Compute the cross entrophy loss l_{ce}

7: Update the network on B

8: **end for**

9: **end for**

3.3 Model Distribution Process

3.3.1 Model Distribution Architecture

This article uses IPFS to complete the task of uploading the model to the blockchain. The reasons for choosing IPFS to chain are shown in Part 4. The service provider uploads the trained model from the training machine to IPFS, and IPFS will feed back the CID corresponding to the model. The service provider then uploads the CID to the blockchain through a smart contract to achieve the purpose of model distribution. Since the size of the CID has always been in a fixed interval, and the size of this interval is in bytes, the model will save a lot of cost through IPFS on the chain than directly on the chain. The distribution architecture of the model is shown in Fig. 3.

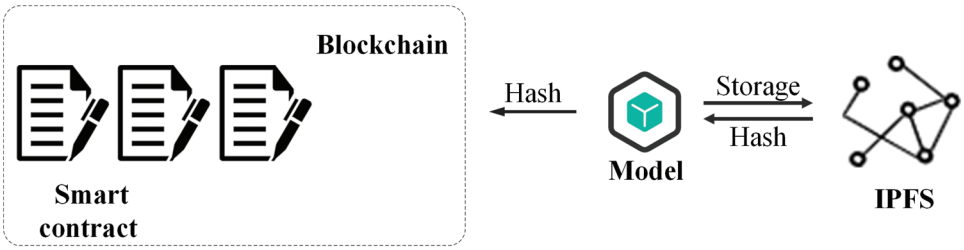

Figure 3: Model distribution architecture

3.3.2 Model Upload Process

The process of uploading the model to IPFS is shown in Fig. 4. The steps required are as follows:

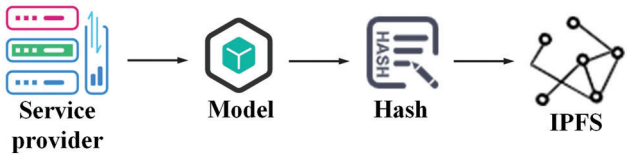

Figure 4: Model upload process

- **Step 1.** The service provider encounters a DDoS attack and has trained the model, and needs to upload the model to IPFS.
- **Step 2.** The service provider stores the model in its working directory.
- **Step 3.** The service provider informs IPFS that it wants to add a model, and the system generates the CID of the model (the CIDs generated by IPFS all start with Qm).

- **Step 4.** The model already exists in the IPFS network.

The model utilizes the IPFS upload and confirmation functions explained in Algorithm 2.

Algorithm 2: Add and verify file functions

Input: model, CID

Add file: push the model to the CID

Verify file: calculate the array length and assign it to *G* variable

1: **for** $j \leftarrow 0$ to G **do**
2: **if** CID was stored with the model **then**
3: $FileConfirm = 1$
4: **end if**
5: **break**
6: **end for**
7: **if** $FileConfirm = 1$ **then**
8: **return true**
9: **else**
10: **return false**
11: **end if**

4 Case Study

In this section, we will introduce the implementation and explain that the cost of each aspect of the solution is within a reasonable range. Compared with mainstream methods of mitigating DDoS attacks, our solution has obvious advantages in terms of cost, time, and security. Compared with direct transmission, this solution has greater advantages in terms of security, credibility, and feasibility. Our implementation environment is carried out on a Dell Precision 3630 desktop computer, this desktop computer supports Intel SGX, the processor is Intel(R) Core(TM) i7-9700K CPU, 16G memory, the Ubuntu version is Ubuntu 9.3.0-17ubuntu1~20.04, The Linux kernel version is 5.11.0-38-generic (buildd@lgw01-and64-041), Ganache is used to create a blockchain environment, and the Ubuntu version of IPFS Desktop.

4.1 Cost Overhead

This experiment aims to compare the cost of choosing IPFS to upload to the blockchain and directly uploading to the blockchain, so as to prove the correctness of choosing IPFS in this article. Since the blockchain is distributed, the size of each block is only about 1 M. When the amount of data that needs to be uploaded is large, the use of blockchain transmission is not only extremely inefficient and costly (the cost here is in gas units). We compare 10 data uploaded to the blockchain via IPFS with the data directly uploaded to the blockchain. The size of the data directly uploaded to the blockchain is 10 K, as shown in Fig. 5. We can clearly observe from Tab. 1, since the size of the generated CID (Content-ID) is always in a small range after the data is uploaded to IPFS. However, uploading only 10 K of data directly to the blockchain consumes 231,943 gas. so in terms of transaction overhead, using IPFS to upload to the blockchain will consume less gas. In October 2021, 1ether will be approximately 3642 U.S. dollars. Therefore, the smaller the gas, the lower the chain cost.

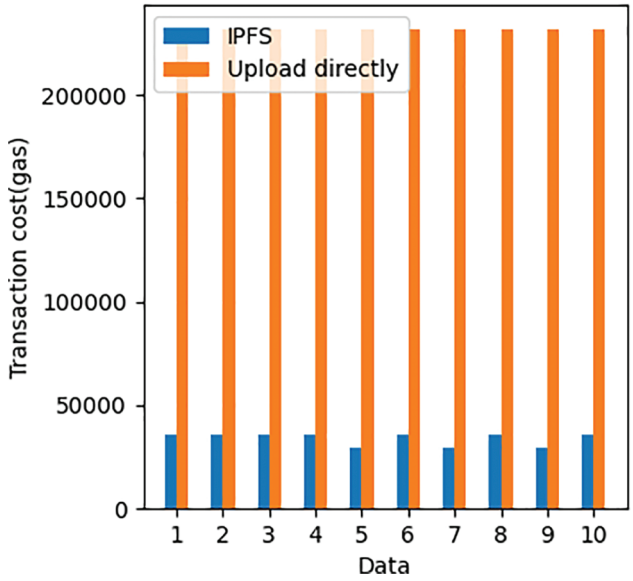

Figure 5: Comparison of the cost of using IPFS and uploading data directly to the blockchain

Table 1: Comparison of the cost of using IPFS and uploading data directly to the block chain

Data size (MB)	Transaction cost (gas)
12.8	35934
25.6	35934
38.4	35934
51.2	35934
64	28874
76.8	35934
89.6	28874
102.4	35934
115.2	28874
128	35934
0.0097	231943

4.2 Model Distribution

This experiment aims to demonstrate the advantages of the blockchain-based DDoS attack collaborative detection framework, which is mainly reflected in the time overhead. Distributing the DDoS attack detection model to other service providers that make up the blockchain through the blockchain-based DDoS attack collaborative detection framework can solve the problem of time overhead. We have taken the experimental data of 30 consecutive uploads and downloads, which are shown in Figs. 6 and 7. Fig. 6 shows the comparison [43] of the upload time of the model and large data through the smart contract in the blockchain distribution process. It takes 11.18881 and 16.27832 s to upload 1.5G and 2G data. In the process of uploading the same data, the time overhead for the first upload will be very large, and

subsequent uploads will be accompanied by certain fluctuations. But the upload time cost of the model is smooth and efficient.

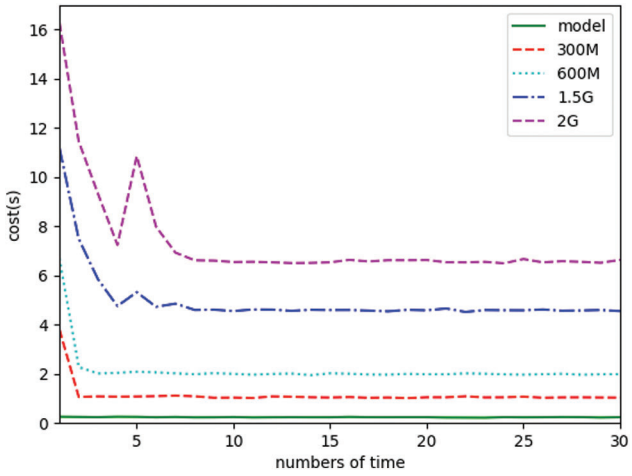

Figure 6: Comparison of the time cost of uploading data between models and large data

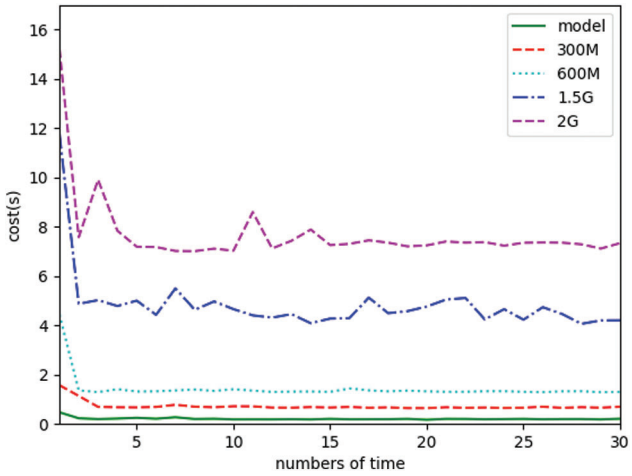

Figure 7: Comparison of the time cost of downloading data between model and large data

Fig. 7 shows the comparison of the download time of the model and large data through the smart contract in the blockchain distribution process. It can be concluded from Fig. 7 that the blockchain-based DDoS attack collaborative detection framework can greatly reduce the download time overhead of various service providers. In the process of downloading the same piece of data, the time overhead for the first download will also be large, and subsequent downloads will be accompanied by certain fluctuations. But the download time overhead of the model is very efficient.

The above experiments clearly show that the blockchain-based DDoS attack collaborative detection framework not only solves the problem of high time overhead for detecting DDoS attacks on the current blockchain, but also improves the detection efficiency of various service providers and reduces all aspects of costs.

4.3 Time Cost of Model in Software Guard Extensions

This experiment aims to compare the time spent in SGX between models and data of different sizes. We tested the time spent on SGX for 7 different data (models are also a type of data), where the time spent is the sum of the time spent on reading, encrypting, decrypting, transmitting and writing text. We used 7 different data (including models and gradually increasing data). Tab. 2 compares our experimental results with the time spent in SGX [44] for data of different sizes obtained from preliminary research. It can be clearly derived from Fig. 8 that the time cost of the model is much smaller than the time cost of gradually increasing data. This experiment proves that the distribution model can not only improve the efficiency of collaborative detection, but also significantly reduce the burden of security and transmission without reducing its performance. Note that a model with too simple functions will lead to a decrease in the detection effect.

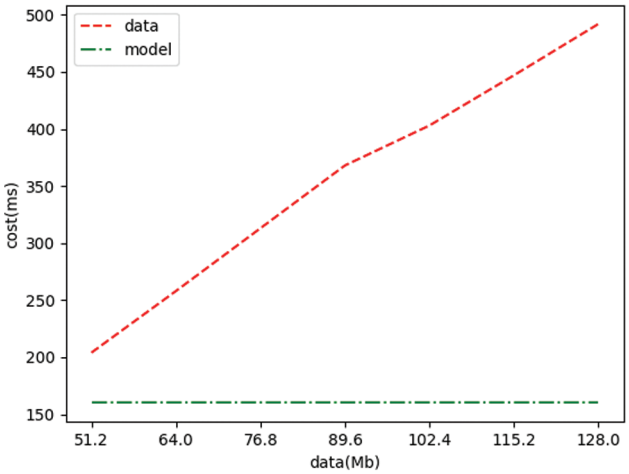

Figure 8: Comparison of the time cost of model and data in SGX

4.4 Overall Transmission Time Overhead

This experiment aims to compare the time overhead of a blockchain-based DDoS attack collaborative detection framework and the transmission model without using the blockchain. It can be clearly drawn from Tab. 3 that compared with the two, the total transmission time of this method is not too far behind without blockchain transmission while ensuring the safety and stability. Although the time overhead of direct transmission without using the blockchain is small, other hidden dangers are worrying. Therefore, the advantages of the blockchain-based collaborative detection framework for DDoS attacks appear to be particularly prominent.

Table 2: Comparison of the time cost of model and data in SGX

Data size (MB)	Cost (s)
51.2	0.2036
64	0.2580
76.8	0.3127
89.6	0.3678
102.4	0.4030
115.2	0.4466
128	0.4924

Table 3: Comparison of model transmission time overhead with or without blockchain

Transfer method	Cost (s)
Transmission using blockchain	1.31181
Transmission without blockchain	0.65046

4.5 Summary

Through the above experiments, it can be proved that the blockchain-based DDoS attack collaborative detection framework has the characteristics of low cost, low time efficiency, high efficiency, security and comprehensiveness. This framework solves the problem of poor timeliness and high cost in today's blockchain detection of DDoS attacks. Part 4.1 proves the low-cost characteristics of the blockchain-based DDoS attack collaborative detection framework using smart contracts and IPFS to distribute the model. Part 4.2 proves the low timeliness and high efficiency of the model when using the blockchain-based DDoS attack collaborative detection framework to transmit. Section 4.3 proves the low timeliness, high efficiency and security of the DDoS attack collaborative detection framework based on blockchain. Part 4.4 proves the comprehensiveness of the blockchain-based DDoS attack collaborative detection framework.

5 Conclusion

The scale of DDoS attacks expands rapidly with the increase in the number of network devices, and the problem of detection efficiency of DDoS attacks is becoming more and more prominent. The use of blockchain to detect DDoS attacks is one of the current mainstream, but most detection methods have the problems of time overhead and high cost. This work distributes the DDoS attack detection model through the blockchain, which is helpful to the existing research on using the blockchain to detect DDoS attacks. The DDoS attack detection model has the characteristics of value, small amount of data, and security, and is very suitable for distribution using the blockchain, which significantly reduces the time and cost. In this article, first of all, we introduce a blockchain-based DDoS attack collaborative detection method, so that the model is distributed through the blockchain to solve the problem of high time and cost of detecting DDoS attacks on the existing blockchain. Secondly, the research results reported in this article bring new enlightenment to the method of using blockchain to detect DDoS attacks, and it helps to improve the timeliness, security and practicability of the method. Finally, the evidence of this research shows that our solution can provide low-cost, low-latency and secure model storage for DDoS attack detection using blockchain.

6 Limitation and Future Research

In this section, we describe the limitations of this paper and the scope of future work.

The limitations of this paper are:

- **Intel SGX.** Currently, SGX has a memory limit of 128 MB, which limits the amount of important data that can be stored. If the total amount of data that needs to be protected is much larger than the memory limit of SGX, then the efficiency of SGX will drop significantly.
- **Blockchain.** Currently, the use of smart contracts to transfer data on the blockchain is still limited. The size of data directly uploaded to the blockchain using smart contracts is still not ideal, and the transmission efficiency on the blockchain still needs to be improved.

Our future scope of work:

- **Reputation Assessment.** Even if the service provider distributes the trained latest DDoS attack detection model, there is still the issue of the authenticity of the distribution model. Therefore, it is necessary to use the reputation evaluation mechanism to constrain each service provider to ensure the validity of the distributed model.
- **Model safety.** According to the latest research, the detection model has the risk of leaking key data. How to protect the model before it is distributed is another research direction.

Funding Statement: This work was supported by the Key Research and Development Program of Hainan Province (Grant No. ZDYF2020040, ZDYF2021GXJS003), Major science and technology project of Hainan Province (Grant No. ZDKJ2020012), National Natural Science Foundation of China (NSFC) (Grant No. 62162022, 62162024 and 61762033), Hainan Provincial Natural Science Foundation of China (Grant No. 620MS021), and Opening Project of Shanghai Trusted Industrial Control Platform (Grant No. TICPSH202003005-ZC).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Z. Houda, A. Hafid and L. Khoukhi, "Co-IoT: A collaborative DDoS mitigation scheme in IoT environment based on blockchain using SDN," in *2019 IEEE Global Communications Conf.*, Waikoloa, HI, USA, pp. 1–6, 2019.

[2] B. Rodrigues, E. Scheid and C. Killer, "Blockchain signaling system (BloSS): Cooperative signaling of distributed denial-of-service attacks," *Journal of Network and Systems Management*, vol. 28, no. 1, pp. 953–989, 2020.

[3] M. Snehi, "Vulnerability retrospection of security solutions for software-defined cyber-physical system against DDoS and IoT-DDoS attacks," *Computer Science Review*, vol. 40, pp. 100371, 2021.

[4] A. Bhardwaj, V. Mangat and R. Vig, "Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions," *Computer Science Review*, vol. 39, pp. 100332, 2021.

[5] L. Yeh, P. Lu and S. Huang, "SOChain: A privacy-preserving DDoS data exchange service over SOC consortium blockchain," *IEEE Transactions on Engineering Management*, vol. 69, no. 4, pp. 1487–1500, 2020.

[6] G. Spathoulas, N. Giachoudis and G. P. Damiris, "Collaborative blockchain-based detection of distributed denial of dervice attacks based on internet of things botnets," *Future Internet*, 2019, vol. 11, no. 11, pp. 226–250.

[7] A. Hakiri and A. Gokhale, "A software-defined blockchain-based architecture for scalable and tamper-resistant IoT-enabled smart cities," Communication Technologies for Networked Smart Cities, pp. 275–300, 2021. [Online]. Available: https://digital-library.theiet.org/content/books/10.1049/pbte090e_ch12.

[8] S. Vetha and K. V. Devi, "A trust-based hyervisor framework for preventing DDoS attacks in cloud," *Concurrency and Computation: Practice and Experience*, vol. 33, pp. 32–47, 2019.

[9] K. Nishizuka, L. Xia and J. Xia, "Inter-domain cooperative DDOS protection mechanism," July 2016. [Online]. Available: https://tools.ietf.org/html/draft-nishizuka-dots-inter-domain-mechanism-02.

[10] Akamai, "How to protect against DDoS attacks-stop denial of service," 2017. [Online]. Available: https://www.akamai.com/us/en/resources/protect-against-ddos-attacks.jsp.

[11] CloudFare, "Cloudflare advanced DDoS protection," 2016. [Online]. Available: https://www.cloudflare.com/static/media/pdf/cloudflare-whitepaper-ddos.pdf.

[12] B. B. Gupta and C. Chaturvedi, "Software defined networking (SDN) based secure integrated framework against distributed denial of service (DDoS) attack in cloud environment," in *2019 Int. Conf. on Communication and Electronics Systems (ICCES)*, Coimbatore, India, pp. 1310–1315, 2019.

[13] V. Kansal and M. Dave, "Proactive DDoS attack mitigation in cloud-fog environment using moving target defense," arXiv preprint arXiv:2012.01964, 2020.

[14] R. Saxena and S. Dey, "DDoS attack prevention using collaborative approach for cloud computing," *Cluster Computing*, vol. 23, no. 2, pp. 1329–1344, 2020.

[15] T. R. Gadekallu, Q. V. Pham and D. C. Nguyen, "Blockchain for edge of things: Applications, opportunities, and challenges," *IEEE Internet of Things Journal*, vol. 9, pp. 964–988, 2021.

[16] B. Prabadevi, N. Deepa and Q. V. Pham, "Toward blockchain for edge-of-things: A new paradigm, opportunities, and future directions," *IEEE Internet of Things Magazine*, vol. 4, pp. 102–108, 2021.

[17] W. Zhang, Y. Wu and X. Wu, "A survey of intel SGX and its applications," *Frontiers of Computer Science*, vol. 15, pp. 153808, 2021.

[18] B. Bordel, R. Alcarria, D. Martín and Á. Sánchez-Picot, "Trust provision in the internet of things using transversal blockchain networks," *Intelligent Automation & Soft Computing*, vol. 25, no. 1, pp. 155–170, 2019.

[19] K. Miyachi and T. K. Mackey, "hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design," *Information Processing & Management*, vol. 58, no. 3, pp. 102535, 2021.

[20] G. Manogaran, S. Mumtaz and C. Mavromoustakis, "Artificial intelligence and blockchain-assisted offloading approach for data availability maximization in edge nodes," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2404–2412, 2021.

[21] B. L. Nguyen, E. L. Lydia, M. Elhoseny, I. V. Pustokhina, D. A. Pustokhin *et al.,* "Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 87–107, 2020.

[22] A. Lucas, D. Geneiatakis and Y. Soupionis, "Blockchain technology applied to energy demand response service tracking and data sharing," *Energies*, vol. 14, no. 7, pp. 1–17, 2021.

[23] G. Sun, S. Bin, M. Jiang, N. Cao, Z. Zheng *et al.,* "Research on public opinion propagation model in social network based on blockchain," *Computers, Materials & Continua*, vol. 60, no. 3, pp. 1015–1027, 2019.

[24] H. Wang, D. He and J. Yu, "RDIC: A blockchain-based remote data integrity checking scheme for IoT in 5G networks," *Journal of Parallel and Distributed Computing*, vol. 152, no. 12, pp. 1–10, 2021.

[25] J. Wang, W. Chen, L. Wang, R. S. Sherratt, O. Alfarraj *et al.,* "Data secure storage mechanism of sensor networks based on blockchain," *Computers, Materials & Continua*, vol. 65, no. 3, pp. 2365–2384, 2020.

[26] T. Veeramakali, R. Siva and B. Sivakumar, "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model," *The Journal of Supercomputing Volume*, vol. 77, pp. 9576–9596, 2021.

[27] M. H. Chinaei, H. H. Gharakheili and V. Sivaraman, "Optimal witnessing of healthcare IoT data using blockchain logging contract," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 10117–10130, 2021.

[28] A. H. Lone and R. N. Mir, "Applicability of blockchain smart contracts in securing internet and IoT: A systematic literature review," *Computer Science Review*, vol. 39, no. 1, pp. 100360, 2021.

[29] V. Jain, B. Kumar, "Combinatorial auction based multi-task resource allocation in fog environment using blockchain and smart contracts," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 3124–3142, 2021.

[30] R. A. Ziar, S. Irfanullah and W. U. Khan, "Privacy preservation for on-chain data in the permission less blockchain using symmetric key encryption and smart contract," *Mehran University Research Journal of Engineering and Technology*, vol. 40, no. 2, pp. 305–313, 2021.

[31] J. Xu, H. Liu and Q. Han, "Blockchain technology and smart contract for civil structural health monitoring system," *Computer-Aided Civil and Infrastructure Engineering*, vol. 36, no. 10, pp. 1288–1305, 2021.

[32] A. Lakhan, M. A. Mohammed and A. N. Rashid, "Smart-contract aware ethereum and client-fog-cloud healthcare system," *Sensors*, vol. 21, no. 12, pp. 4093–4113, 2021.

[33] G. Estevam, L. M. Palma and R. S. Luan, "Accurate and decentralized timestamping using smart contracts on the ethereum blockchain," *Information Processing & Management*, vol. 58, no. 3, pp. 102471, 2021.

[34] Z. Chen, Y. Tian and C. Peng, "An incentive-compatible rational secret sharing scheme using blockchain and smart contract," *Sciece China. Information Sciences*, vol. 64, no. 10, pp. 106587, 2021.

[35] A. L. Spataru, C. P. Pungila and M. Radovancovici, "A high-performance native approach to adaptive blockchain smart-contract transmission and execution," *Information Processing & Management*, vol. 58, no. 4, pp. 102561, 2021.

[36] M. Khan and T. Naz, "Smart contracts based on blockchain for decentralized learning management system," *SN Computer Science*, vol. 2, no. 4, pp. 1–9, 2021.

[37] P. Kamboj, S. Khare and S. Pal, "User authentication using blockchain based smart contract in role-based access control," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 1–16, 2021.

[38] X. Liu, J. Ren and H. He, "A fast all-packets-based DDoS attack detection approach based on network graph and graph kernel," *Journal of Network and Computer Applications*, vol. 185, no. 2, pp. 103079, 2021.

[39] G. Amaizu, C. I. Nwakanma and S. Bhardwaj, "Composite and efficient DDoS attack detection framework for B5G networks," *Computer Networks*, vol. 188, no. 1, pp. 107871, 2021.

[40] J. Cui, M. Wang and Y. Luo, "DDoS detection and defense mechanism based on cognitive-inspired computing in SDN," *Internet Technology Letters*, vol. 97, pp. 275–283, 2021.

[41] S. Yu, J. Zhang and J. Liu, "A cooperative DDoS attack detection scheme based on entropy and ensemble learning in SDN," *EURASIP Journal on Wireless Communications and Networking*, vol. 90, pp. 1–10, 2021.

[42] T. R. Gadekallu, M. K. Manoj and K. S. Sivarama, "Blockchain based attack detection on machine learning algorithms for IoT based E-health applications," *IEEE Internet of Things Magazine*, vol. 4, pp. 30–33, 2020.

[43] B. Rodrigues, T. Bocek and A. Lareida, "A Blockchain-based architecture for collaborative DDoS mitigation with smart contracts," in *IFIP Int. Conf. on Autonomous Infrastructure, Management and Security*, Zurich, Switzerland, vol. 10356, pp. 16–29, 2017.

[44] J. Cheng, J. Li and N. Xiong, "Lightweight mobile clients privacy protection using trusted execution environments for blockchain," *Computers, Materials & Continua*, vol. 65, no. 3, pp. 2247–2262, 2020.