Detect and Mitigate Blockchain-Based DDoS Attacks Using Machine Learning and Smart Contracts

Yaser Issam Hamodi[1], Aso Ahmed Majeed[2], Kamal H. Jihad[3], Banaz Anwer Qader[4]
E-mail: Yaserissam.hamodi@gmail.com, asoalsalihi@gmail.com, kamal.jihad@uokirkuk.edu.iq, banaz_2017@uokirkuk.edu.iq

[1]Department of Computer Engineering, Ministry of Higher Education and Scientific Research, Baghdad, Iraq
[2]Basic Sciences Branch, College of Nursing, University of Kirkuk, Kirkuk, Iraq
[3]College of Science, University of Kirkuk, Kirkuk, Iraq
[4]College of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq

Keywords: blockchain, DDoS attacks, ML, AI, smart contracts, SDN, EVM.

Received: February 2, 2022

The key target of Distributed Denial-of-Service (DDoS) attacks is to interrupt and suspend any available online services either executed for professional or personal gains. These attacks originate from the fast advancement in the number of insecure technologies. The attacks are caused due to the easy access to internet and advent of technology resulting to exponential growth of traffic volumes. DDoS attack remains most leading security risks to provisioning services. Also, the current embraced security mechanism for defense lacks flexibility and adequate resources to combat these attacks. Hence, there is need to embrace various other critical resources, where they can share the problem of mitigation. In addition, emerging technologies for instance smart contracts and blockchain offers for the sharing of these potential attacks information in an entirely automated and distributed manner. This paper recommends for a blockchain design which combines smart contracts and Machine Learning (ML) technologies, by presenting new ideal opportunities towards efficient DDoS mitigation solutions in variety of cooperative domains. Furthermore, the key advantage and benefits of this structure is deployment of still existing distributed and public infrastructure to blacklisted IP address or even advertise white, and the application of such an infrastructure with further defense mechanisms to current attacks of DDoS, deprived of considering distribution mechanisms or specialized registries, which facilitates the implementation of procedures across diverse domains. This paper further presents the demonstration and implementation features of this blockchain structure, discussion and study findings over these smart contracts and ML technologies. The study further concludes by recommending use of smart contract in collaborative block-chain design with ML for mitigating future attack of DDoS.

Povzetek: Ta dokument priporoča zasnovo blockchain, ki združuje nastajajoča orodja s pametnimi pogodbami in tehnologijami strojnega učenja, ki predstavlja nove idealne priložnosti za učinkovite rešitve za ublažitev DDoS-jev na različnih področjih sodelovanja.

1 Introduction

In the past few years, there has been an increase in DDoS cyberattacks, which has been very clear and easy to spot [1]. DDoS attacks are one of the most common and dangerous threats to both old and new network systems [2], which can affect the apps and devices that use them. DDoS attacks use a group of devices to attack a single target, making it hard for real people to use services like email and websites [3]. But these attacks seem to be trying to add to or even stop online services, especially on the internet, and the reasons behind them range from people's complaints to threats about politics [1]. They are the most common and dangerous attacks on and from devices connected to the Internet of Things (IoT), Cloud Computing, and fifth-generation (5G) communication networks [2, 3]. DDoS attacks on multiple servers and the Domain Name System (DNS), which is responsible for other system domains like Spotify, PayPal, and Twitter, were done in a coordinated way. Because of this, these signaling DDoS attacks made it so that some users in the US couldn't use services for a long time. One of the main reasons why DDoS attacks are happening more often is likely that there are more Internet of Things (IoT) home gateways or devices that are not properly set up or secured [1].

Nonetheless, by developing further legal issue concerning those technologies and devices such as using the Simple Service Discovery Protocol, whereby strength of DDoS, attacks gets more intensified, thus the issue the security mechanism creating further complex. Hence, the influence of attacks by DDoS fluctuates from minor problems to huge financial harms to companies and enterprises that depend on these available services [4]. Specific mitigations approaches and techniques have been recommended. But, only few elements more considered

for numerous scenarios due to implementation complexity and its effectiveness [5]. Machine learning (ML) is one way to handle more attacks, and ML classification techniques are used to handle different types of DDoS attacks [6]. Machine learning techniques are mostly used to figure out if a packet is malicious or not, since each attack uses a different protocol, as well as to find out if a normal packet is acting strangely and stop the attacks [6]. ML makes it easier for computers to build models from data samples to help people make decisions that are based on data [7]. However, this paper recommends for blockchain smart contracts, which offer robust defense deprived of maintaining further development and design challenges using protocols [5].

Software-defined Network (SDN) architecture is one of the best and most effective ways to use ML algorithms to spot DDoS attacks [2]. It facilitates customizable security services and policies in most active way. Centralized deployment and network control depends on the Command Line Interface (CLI) and Simple Network Management Protocol (SNMP). Therefore, with SDN the flow-rule may further get utilized which helps in blocking DDoS attacks and other close malicious packets dropped to prevent the occurrence of DDoS attacks [8].

This paper illustrates proposed architecture of collaborative blockchain, utilizing smart contract and explores ways of mitigating DDoS attack in entirely decentralized system. Therefore, any interested service provider in public system or using shared protections, reveal unable to detect the incidence of DDoS attacks, also share mitigation and detection ways [8]. Also, this paper presents easy-to-manage and automated DDoS mitigation ways. Also, this technique recommends an implementation and architecture to any black listed IP address, and signaling white in diverse domains depending on smart contracts and blockchain.

2 Related Works

2.1 Blockchain and Machine Learning Techniques

Machine learning (ML) methods, which have been shown to be helpful in cybersecurity, are one of the many ways to protect against DDoS attacks. Many ML-based methods have been suggested for detecting DDoS. These include supervised, unsupervised, and hybrid methods, which combine the first two methods [9]. This section gives an overview of some new ideas for how to do things in this area [10].

Najafimehr et al. [10] came up with a new method that combined supervised and unsupervised algorithms. This method was called a hybrid method. They used a clustering algorithm and several flow-based features to separate the strange traffic from the normal data. Then, a classification algorithm is used to give the clusters names based on certain statistical measures. We use a framework for processing big data to evaluate. The results showed that this method's Positive Likelihood Ratio (LR+) is about 208% higher than that of the ML classification algorithms.

Marcelo et al. [2] set up an SDN-based architecture that was flexible and made of small parts. Multiple Machine Learning (ML) and Deep Learning (DL) models are used to find transport and application layer DDoS attacks. They were right more than 99 percent of the time when identifying traffic they hadn't seen (testing set). Also, they showed high detection rates, above 98 percent for transport-layer DDoS attacks and up to 95 percent for application-layer DDoS attacks.

Manikumar and Maheswari [6] came up with a plan for a system that would add more security to the existing DDoS mitigation models. It uses machine learning algorithms to figure out if an incoming packet is malicious or not, and it uses Blockchain technology to keep track of the IP addresses that should be blocked. To find the best algorithm for classifying, three different ones are used: the KNN Classifier, the Decision Tree Classifier, and the Random Forest algorithm. A technique called Tree-Based Classifier is used for Feature Selection to speed up the time it takes to do calculations. Random Forest is about 95% accurate at analyzing traffic in real time.

Almaraz-Rivera et al [3]. Built a new Intrusion Detection System based on Machine Learning and Deep Learning models. Where, the best ways to find DDoS and DoS attacks on IoT networks were the Decision Tree and Multi-layer Perceptron models. It uses the Bot-IoT dataset to fix the problem of a class imbalance. With the Decision Tree and the Random Forest, it got a score of 100 percent for accuracy, precision, recall, and F1 score for several different combinations of Normal flows vs. DDoS/DoS protocols.

2.2 Blockchain and Smart Contracts

Review studies shows that smart contract works as designed software used to foster performance or negotiation of contract, capable to enforce, verify, and implement on its own. Besides, a smart contrast solely does not make “smart” since it requires additional infrastructure which may enforce, verify, and implement the performance or negotiation of any contract through specific computer protocols [11]. Research also shows that this technique has acquired greater consideration in the setting of blockchain that offer decentralized design to verify, execute and run a smart contract. Hence, smart contract require being ran on blockchain design that ensures; (a) hindrances to manipulate context of the contract and (b) ensure its long-lasting storage [4]. However, a participating node in blockchain often operates smart contract performing the script, authenticating any script outcome, accommodating outcomes in a block and the contract [12]. Besides, conducted a study that proposed DDoS attack defense technique based on block for IoT technologies. The experimental outcomes specified that the recommended setup is cost effective and efficient.

Another study conducted, proposed a biologically motivated collaborative DDoS detection model utilizing fuzzy neural networks, smart contract, and blockchain. However, each of the collaborators domains hosted specifically on a private blockchain by not sharing data or privacy with various other collaborators [12]. However, the research findings revealed that smart contract can effectively detect any attacks by DDoS information, data and further generates irregular chains in the nodes. Also, the study results showed that while sharing data synchronized, perhaps good outcomes may be realized as a collaborative detection system.

A research study established that though the Bitcoin blockchain reveal as the initial completely decentralized digital currency and a distributed ledger. It is usually intended to transfer digital wallet or digital assets and appears as a non-Turing-complete (i.e. necessarily fails to hold loops). For instance, Turing-complete in smart contract language provides specific rules for either blocking or allowing any IP address understood using a Software-defined Network (SDN) controller [13]. Ethereum blockchain, smart contracts often operate in sand-boxed typical EVM and each executed operations within each EVM gets paid mainly to help inhibit DDoS.

Another reviewed study shows that SDN-based solutions also lead to improved alertness to implement decisions which need universal network. Hence, intra-domain defense mechanism and policies react to and prevent DDoS attack. However, this is realized by combining the inter-domain benefit offered by smart contract and blockchain and intra-domain capabilities provisioned by SDN [4]. Results of the study shows improved effectiveness in mitigation of DDoS attack in intra and inter-domains.

A study conducted by [13], embraced a related approach and demonstrated four ranges of categories of defense mainly against DDoS attacks which encompass; (i) attack prevention (ii) attack source identification (iii) attack detection, and (iv) attack-reaction. The study findings also reveal that such attack mitigation aims to inhibit any potential attacks before they develop to big issue. The results revealed that any attack source identification being utilized once the attack has been detected and reveal as an essential step to efficiently re-route or contain the potential attacks as near to its source. The eventual step (attack reaction) encompass considering appropriate measures against the potential attacks.

Other related works in this study include the cooperative security mechanism against DDoS attack. But, it still remains as an open concern because DDoS attacks appear gradually increasing in frequency, duration, complexity, and scale [14]. For instance, the Internet Engineering Task Force (IETF) shows currently recommending unique protocol known as DDoS Open Threat Signaling (DOTS), which covers both communications in inter-organization and intra-organization mainly to publicize potential attacks. Indeed, this protocol needs clients DOTS agents and servers, well-structured in both distributed and centralized architecture specifically to advertise white listed or black addresses.

However, rather than utilizing current infrastructure, for instance the smart contracts and blockchain, approaches stated above recommend development of certain protocols such as gossip-based. In the view, integration and deployment of appropriate solution gets more complicated because the current resolution requires being further changed to fully support the proposed protocol [14]. Besides, IETF plan emphasizes on systematizing better protocol that foster effective deployment. Hence, the needs may get acquired from normal SDN, smart contract, and blockchain (s), to prevent obstacles of adoption.

Table 1 shows a summary of past studies that used blockchain algorithms, smart contracts, and other technologies like SDN and EVM. It compares the proposed systems in terms of their features, limitations, and the new technologies they use.

Study	Designed Model	Techniques Used	Characteristic	Drawbacks	Result	Mitigation levels
Rodrigues et al. (2017) [4]	Design and develop a collaborative architecture to broadcast and mitigate DDoS attacks.	Public blockchains, smart contracts, EVM	Infrastructure is added to DDoS defense systems without altering them.	Only static IPs should be blockable. The smart contract only supports one hierarchy.	Deploying a public, distributed infrastructure to broadcast white or blacklisted IP addresses enables rule enforcement across numerous domains.	Multiple
Singh et al. (2020) [11]	Present a study and comparison among DDoS attacks solutions	Public and Private blockchains and SDN	Helps build research projects in blockchain's growing field.	Solutions unable to scale in size, cost, or efficacy, and they do not account for false positives and negatives.	Blockchains are prone to DoS attacks, thus researchers must fix them before using them.	Multiple

Han et al. (2020) [12]	Proposed a shared DDoS detection system based on consortium chain.	Smart contract and private blockchains	Smart contracts can recognize DDoS data and build abnormal chains.	Every member has its own chain. The privacy of members is not compromised. The public chain stores abnormal data, so it can't be changed. Members can get reliable info without a third-party source.	The system can secure user data since it takes such little time to build an exception chain and share information.	Multiple
Wang. et al. (2019) [13]	Proposed a 6-layer smart contract research framework.	Smart contract and blockchains	Smart contracts allow untrusted parties to implement contract conditions without a trusted authority or central server.	Smart contract performance is poor, it cannot handle sophisticated logic execution and high-throughput data, and it can't implement cross-chain.	Layer 1 ensures smart contract correctness. Layer 2: Off-chain smart contract computations. Layer 3: Blockchain and IoT connect the physical and virtual worlds.	Three
El Houda et al. (2019) [14]	Cochain-SC includes intra-domain (I-ES, I-BS, and I-DM) and inter-domain (Ethereum's smart contract for SDN) DDoS mitigation.	Blockchains, Smart contract, and SDN	Cochain-SC detects illicit flows with flexibility, efficiency, security, cheap cost, quick deployment, and high accuracy.	Unable to stop IP-based real-source assaults.	It uses Ethereum's Ropsten test network. The proposed work reduces the cost of forwarding packets over numerous domains, making it a promising DDoS mitigation strategy.	Two

Table 1: The summary table of related works.

3 Blockchain Structure Design

A scenario is illustrated in Figure 1 in the appendixes illustrating the proposed blockchain structure. Web server is presented at around AS, while C based on DDoS attack and other hosted device at specific domains i.e. (A, B, C, ASes). However, with non-collaborative approach of DDoS mitigation, web server depends on security mechanism executed at AS, which in several instances could appear distanced from source of the attacks traffic, thus overburdening numerous domains with the attack traffic [14].

Notably, collaborative defense participants (customers and ASes) first require developing a smart contract, properly connected with a smart contract which is registry-based. Hence, when potential attackers try to overload the used web server, AS and customer attack protects IP address in any potential attacks within blockchain smart contract [14]. However, in Ethereum blockchain there is creation of blocks in about each 14 seconds, thereby pledged ASes gets restructured address list ready to get blocked and authorize potential attacks and exploring statistics of traffic and confirming target address legitimacy [15]. In deployment encompassing numerous domains, immediately collaborative security node gets information concerning potential attack, and then these may utilize better mitigation, measures and actions consistent with security policies.

DDoS attacks mostly vary and increase based on trends and patters, requirement of coordinated reactions further grows and bypass the attack resourcefully. It is essential to understand that the existing relationships between ASes and customers reveal as additional technique in the current security mechanism. Figure 2, shows the blockchain architecture that include three key components [16].

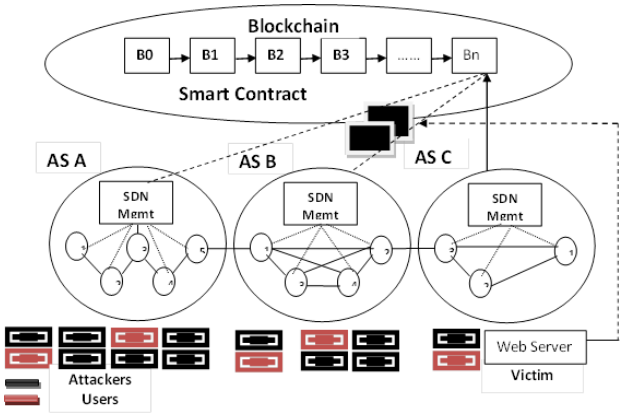

Figure 1. The Blockchain Design

Customers: - reports any blacklisted and white listed IP address to applied Ethereum blockchain, and in this case through smart contract.

ASes: - Distributes any blacklisted or white listed IP address, and further recover lists holding the available IP address, and also execute DDoS security mechanism.

Smart Contract/Blockchain: - in this component, shared EVM node within the Ethereum blockchain as they run additional smart contract, and encompass sense to reporting any IP address within blockchain [15].

The architecture considered below principles:

i- DDoS mitigation and detection countermeasures provisioned as on-demand services through third-party services, or ASes;

ii- To receive/report any attacks of information. However, it's essential that each domain allows other nodes linked to blockchain.

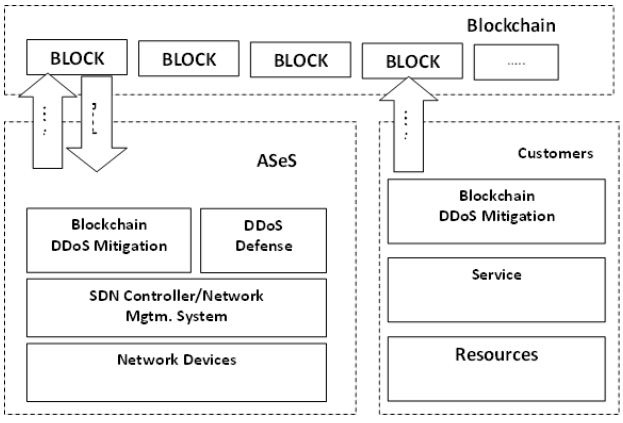

Figure 2. Proposed Blockchain Architecture

iii- To efficiently support synchronized response to potential attacks, blockchain DDoS mitigation modules run on the components (ASes or customers) thereby reporting IP address and also snooping to the entire blockchain.

iv- Only ASes or customers with evidence of ownership of IP address could identify such address to used smart contract.

To effectively mitigate any DDoS attacks first techniques may be embraced upon detection by customers or ASes and encompass analyzing internet traffic using detection algorithms then filtering [17]. Secondly, both on ASes and customer are simpler as using Ethereum is used publicly and there is an available device using smart contracts to mitigate attacks of DDoS. The smart contract and ML classification mechanism are illustrated in figure 3. The flowchart is mainly applied as harmonizing idea in the current DDoS security mechanism of mitigation.

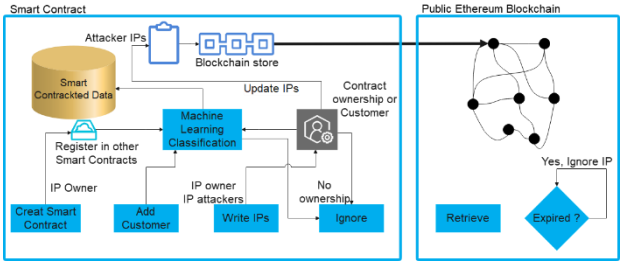

Fig 3. The Proposed System

The data traffic which arrives at AS and customer may get further filtered and analyzed utilizing monitoring tools such as custom SDN, sFlow, and Net Flow implementations. However, the blockchain may also be effectively deployed as further security mechanism in system which executes information or device to advertise white/blacklisted IP address within blockchain. Classification, analysis, and filtering of traffic within gateway get further enabled through SDN; hence these techniques reveal designed with monitoring structures depending on considered Open Flow protocol.

4 Discussion and Comparative Study

Blockchain implementation feature identified in this smart contract is that it stores various sources of IP addresses perhaps which should be allowed or blocked. However, to avoid complexities, the only addresses include the IPv4 address. In this case, either the AS or the customer may develop the smart contract, whereby it is necessary to have an IP ownership certificate. In contrast, for the case of customers, the certificate may be then developed using automated system (challenge-response), whereas AS needs matching certificates with the AS registration entry [18]. Also, the accounts owner that established the contract may then include additional addresses and which are authorized to include IPs for blocking. However, before such additional addresses are further included, they are first checked to ensure the parent subnet matches with the addresses.

Before getting to retrieve IP pairs (destination or even the source), and then verify function requires being called

for to ensure the IP address on target has evidence of ownership. The certificate issuance (i.e. certOwnerIPv4) reveal as the only outstanding key entity within the architecture. Also, it is essential for the smart contract to first register itself within a different smart contract Registry, thus allowing entire applicable smart contracts to be detected [18]. Therefore, an AS often snoops for such changes, and any other additional may be assessed and monitored mainly against the AS network properties and utilize the rule of blocking if appropriate.

In comparison to the Application of Ethereum Virtual Machine (EVM) and Blockchain designs offers diverse cooperative domains particularly involved in any potential attacks scenario to raises specific functions in smart contract and help in preventing future attacks. That make Blockchain better than the EVM because it allows the address cross multiple problems. It makes the use of already infrastructures that already exist to spread the rules without use of specialized registries [19]. However, supporting black/whitelisted IP address reveal as key decision which relies on security, and policies mechanism available in every cooperative domain. Hence, smart contract appeared initially established in supporting white and blacklisted IP by utilizing a flag specifying the nature of address being reported. Besides, EVM smart contracts facilitate in native decentralized to controlling users when identifying DDoS attack, and name of attackers.

The outcomes represents a more better and sophisticated application of Blockchain design in the process of mitigating the DDoS in IETF plan (i.e. DOTS protocol) rather than using current infrastructure for instance the smart contracts and blockchain, the IETF recommends from scratch the establishment of those protocols with numerous requirements such as resilience and extensibility to get properly deployed within distributed blockchain architecture [19]. Hence, to maintain the complexity of the blockchain architecture reduced, only data requires being stored within the contract.

Our study's collaborative architecture leveraging block chain and smart contracts mitigates DDoS attacks in multiple domains, as demonstrated in Table 1. This structure is efficient and collaborative. It can be used to bolster DDoS defenses. The Ethereum Virtual Machine (EVM) in study [4] allows numerous domains involved in an attack scenario to call functions in a smart contract reporting attacks or maintaining a list of trusted white and black IP addresses. EVM smart contracts decentralize and natively control who reports an attack and who attacks. Comparative research [11] suggests that public blockchain solutions don't scale in size, cost, or efficacy. In [12], a collaborative DDoS detection system based on consortium chain was presented to monitor an attacker's information. It absolutely protected privacy. Public chain stores abnormal data. Each member uses its own private chain, so information isn't shared. It established that blockchain's strong encryption protects data and prevents tampering. The study [13] offered a basic research framework of smart contracts based on a revolutionary six-layer architecture suggesting that smart contracts will change several traditional industries, such as finance, management, and IoT. Smart contract nodes can provide decentralized data structures and interaction mechanisms for distributed social systems and AI. Cochain-SC in study [14] provided a safe, easy-to-deploy, low-cost, efficient, and flexible DDoS assaults mitigation method based on Ethereum employing smart contracts with two domains: intra-domain and inter-domain. Despite the option of using alternative blockchains, such as EOS, Cochain-SC prefers Ethereum because it is the most popular blockchain that supports smart contracts and has the most committed developers.

5 Conclusions

The paper recommends a collaborative design architecture mainly utilizing block chain and smart contracts to facilitate mitigation of DDoS attacks in diverse domains. However, as primarily public and distributed storage, the blockchain further help in determining an efficient and non-complex structure to establish a collaborative model in mitigation of DDoS. Recommended blockchain architecture may be effectively deployed as added security device in the current DDoS defense plans. Another key aspect considered towards feasibility of the approach reveal as the fairness amongst some of the diverse cooperative domains. Hence, this applicable factor requires further details in future work to recommend a reputation plan depending on the cooperative architecture.

References

[1] B. Rodrigues and B. Stiller, “Cooperative signaling of DDoS attacks in a blockchain-based network,” *in Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos*, *New York*, 39–41, 2019, https://doi:10.1145/3342280.3342300.

[2] N. M. Yungaicela-Naula , C. Vargas-Rosales, and J. A. Perez-Diaz, “SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning”, *IEEE Access*, vol. 9:108495–108512, 2021, https://doi:10.1109/ACCESS.2021.3101650 .

[3] J. G. Almaraz-Rivera , J. A. Perez-Diaz, and J. A. Cantoral-Ceballos, “Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models”, *sensors (MDPI)*, 22(9):1-18, 2022, https://doi:10.3390/s22093367.

[4] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, “A blockchain-based architecture for collaborative DDoS mitigation with smart contracts,” *in IFIP International Conference on Autonomous Infrastructure, Management and Security*, *Springer*, vol. 10356:16–29, 2017, https://doi:10.1007/978-3-319-60774-0_2.

[5] M. Chen, X. Tang, J. Cheng, N. Xiong, J. Li, and D. Fan, "A DDoS Attack Defense Method Based on Blockchain for IoTs Devices," *in International Conference on Artificial Intelligence and Security, (ICAIS), Springer, Singapore, Communications in Computer and Information Science*, vol. 1253: 685–694, 2020, https://doi:10.1007/978-981-15-8086-4_64.

[6] D. V. V. S. Manikumar and B. U. Maheswari, "Blockchain Based DDoS Mitigation Using Machine Learning Techniques", *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), India*, pp. 794-800, 2020, https://doi: 10.1109/ICIRCA48905.2020.9183092.

[7] B. A. Qader, K. H. Jihad, and M. R. Baker, "Evolving and training of Neural Network to Play DAMA Board Game Using NEAT Algorithm", *Informatica*, 46(5):29-37, 2022, https://doi:10.31449/inf.v46i5.3897

[8] Subardono and I. K. Hariri, "Monitoring and Analysis of Honeypot System Performance using Simple Network Management Protocol (SNMP)," *Journal of Internet and Software Engineering*, 2(1):1–8, 2021.

[9] Sh. Al-Otaibi, and A. Al-Rasheed, "A Review and Comparative Analysis of Sentiment Analysis Techniques", *Informatica*, 46(6): 33–44, 2022, https://doi.org/10.31449/inf.v46i6.3991.

[10] M. Najafimehr, S. Zarifzadeh, and S. Mostafavi, "A hybrid machine learning approach for detecting unprecedented DDoS attacks", *J Supercomput.*, 78(6):8106–8136, 2022, https://doi:10.1007/s11227-021-04253-x.

[11] R. Singh, S. Tanwar, and T. P. Sharma, "Utilization of blockchain for mitigating the distributed denial of service attacks," *Security and Privacy*, 3(3):96, 2020, https://doi:10.1002/spy2.96.

[12] X. Han, R. Zhang, X. Liu, and F. Jiang, "Biologically Inspired Smart Contract: A Blockchain-Based DDoS Detection System," *in 2020 IEEE International Conference on Networking, Sensing and Control (ICNSC), China*, pp. 1–6, 2020, https://doi:10.1109/ICNSC48988.2020.9238104.

[13] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(11):2266–2277, 2019, https://doi:10.1109/TSMC.2019.2895123.

[14] Z. Abou El Houda, A. S. Hafid, and L. Khoukhi, "Cochain-SC: An intra-and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract," *IEEE Access*, vol. 7:98893–98907, 2019, https://doi:10.1109/ACCESS.2019.2930715.

[15] Gruhler, B. Rodrigues, and B. Stiller, "A reputation scheme for a blockchain-based network cooperative defense," *in 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pp. 71–79, 2019.

[16] M. H. Jumaa, and A. Ch. Shakir, "Iraqi E-Voting System Based on Smart Contract Using Private Blockchain Technology", *Informatica*, 46(6):87–94, 2022, https://doi.org/10.31449/inf.v46i6.4241.

[17] N. D. Wirasbawa, Ch. T. P. Widjaja, Ch. I. Wenji, and S. Hansun, "Expert API for Early Detection of TB Disease with Forward Chaining and Certainty Factor Algorithms", *Informatica*, 46(6):117–124, 2022, https://doi.org/10.31449/inf.v46i6.3947.

[18] Rashidi, C. Fung, and E. Bertino, "A collaborative DDoS defence framework using network function virtualization," *IEEE Transactions on Information Forensics and Security*, 12(10):2483–2497, 2017, https://doi:10.1109/TIFS.2017.2708693.

[19] T. Bocek and B. Stiller, "Smart contracts–blockchains in the wings," *in Digital marketplaces unleashed, Springer*, pp. 169–184, 2018.