



RESEARCH ARTICLE

A Decentralized Framework for DDoS Attack Mitigation Using Ethereum Smart Contracts and Crypto-economic Incentive Mechanisms

R. Akilandeswari^{1*}, Dr. S. Malathi²

Abstract

Inundating networks with traffic to cripple service accessibility defines a DDoS attack. Traditional defences, like firewalls and centralized scrubbing centres can suffer from single points of failure during large-scale attacks. Blockchain technology has emerged as a powerful technique, with Ethereum leading the way in decentralized solutions. Since Ethereum smart contracts enable DDoS detection and enforcement of validation rules, allowing events to be managed automatically, applying rewards or penalties without a central authority. In this way, it leverages the positive aspects of crypto-economic mechanisms and reputation systems, incentivizing people to act honestly while making abusing the system unprofitable, creating a trustless, transparent and resilient decentralized defence against cyber threats. This architecture includes a validated system that gating access to services includes a back-end gateway responsible for verifying transactions on the blockchain before processing user queries. The off-chain detection algorithm identifies unexpected traffic spikes that exceed a predefined threshold. Attackers were deterred by cost, the system itself stayed up and running, and the smart contract worked autonomously. The suggested approach maintained 96% access success for authorized users, successfully blocked 92% of DDoS traffic, and guaranteed 98% uptime during simulated attacks. All validated access attempts were 100% immutably recorded on-chain, and attackers had to pay 300% more employs transparent on-chain rules and Ethereum smart contracts to manage access. Because every access attempt is permanently documented on the blockchain, it is difficult to alter logs or stop denial-of-service attacks without detection.

Keywords: DDoS mitigation, Decentralized, Blockchain, Attackers, Threat Mitigation, Crypto-Economic Incentives, Authorized user, Ethereum smart contracts.

¹Research Scholar, Department of Computer Science, A. Veeriyar Vandayar Memorial Sri Pushpam College (Autonomous) (Affiliated to Bharathidasan University, Tiruchirappalli-24), Poondi, Thanjavur(dt), 613503, India

²Research Supervisor & Assistant Professor of Computer Science, Swami Dayananda College of Arts & Science, Manjakkudi (Affiliated to Bharathidasan University, Tiruchirappalli-24), Tiruvarur(dt), Tamil Nadu, India

***Corresponding Author:** R. Akilandeswari, Research Scholar, Department of Computer Science, A. Veeriyar Vandayar Memorial Sri Pushpam College (Autonomous) (Affiliated to Bharathidasan University, Tiruchirappalli-24), Poondi, Thanjavur(dt), 613503, India, E-Mail: akil10dhakshana@gmail.com

How to cite this article: Akilandeswari, R., Malathi, S. (2026). A Decentralized Framework for DDoS Attack Mitigation Using Ethereum Smart Contracts and Crypto-economic Incentive Mechanisms. *The Scientific Temper*, 17(6):6359-6366.

Doi: 10.58414/SCIENTIFICTEMPER.2026.17.6.06

Source of support: Nil

Conflict of interest: None.

Introduction

Distributed Denial of Service (DDoS) is arguably the most widespread and aggressive type of cyber threat, disrupting availability by overloading servers or entire networks. Defense mechanisms that people usually have at their top of the application are constructed on a centralized solution matrix — firewalls, intrusion detection systems, or even cloud-centred filtering services. However, these centralized installations are highly susceptible to a single point of failure and may not be able to withstand the pressure from overwhelming assaults.

Blockchain technology itself and especially Ethereum have created new opportunities for decentralized cybersecurity frameworks. This allows programmers to write programs that control particular operations on platforms like Ethereum. These programs become automated and tamper-proof smart contracts without needing a central authority.

In the DDoS attack scenario, router nodes generate a large number of requests directed toward the target server

to degrade its performance and disrupt service availability. The server continuously monitors its incoming traffic and receives the attack reports generated by consortium nodes. These reports are verified using predefined smart contract rules and rewards or penalties are assigned by the server based on these contracts.

Additionally, an even more long term decentralized DDoS mitigation system could use a network of distributed nodes all acting in collaboration to detect and neutralize malicious traffic patterns. Instead of a single point of authority in the form of a traditional centralized board vendor, nodes on the network will share traffic intelligence, alter bad behaviour by consensus, decide on and launch a global response such as rate limiting or blacklisting offending sources. This way of building a decision-making strategy makes more resilient because the attacker cannot target a single point to overwhelm the defense solution. Likewise, due to the transparency of blockchain, anyone can examine their work, this leads to greater certainty and auditability through immutable records at every stage of action and decision by participants.

In addition to this, the design of crypto-economic incentives within a system works as both disincentives against malicious behavior and incentives for honest participation. In this way, nodes that provide false information or acquire malicious action are penalized, and accurate ones that assist in defending against attacks are rewarded with tokens. However, the reason this incentive structure is important is that it effectively strengthens the defensive network. The unique incorporation of decentralized design, smart contract executes automated enforcement, and financial incentive mechanisms enabled by blockchain technology. It provides scalability and reliability for DDoS mitigation and serves as a more suitable replacement for conventional security mechanisms. Therefore, the proposed framework is well positioned to fill an infrastructure gap in the emerging ecosystem of IoT systems.

Related Works: A Brief Review

The Incorporation of crypto-economic models, including token-based incentives, reputation systems, and staking mechanisms can encourage incentivize ongoing participation while discouraging low-quality contributions through economic disincentives. This decentralized approach enhances system fault tolerance, improve transparency and also facilitate a more equitable distribution of responsibilities associated with cybersecurity defense. Blockchain has advanced applications in cryptocurrency, smart contracts, healthcare delivery, communication networks, the Internet of Things, financial services and censorship-resistance platforms, electronic voting system and, decentralized provenance tracking. These applications demonstrate the potential of blockchain to improve security, trust, and operational efficiency across

distributed environment. Owing to its open nature and wholly decentralized peer-to-peer framework, transactions recorded on a blockchain cannot be altered once they have been added to the ledger. Consequently, records maintained on the blockchain are protected from tampering and accessible for public verification (Mauri et al., 2018). Bitcoin employs the open and immutable properties of blockchain technology in order to enable fast and reliable verification of financial transaction without the need for a centralized authority.

DDoS attacks have become increased in frequency over the past few years, their primary is to disrupt or stop Internet services. The motivations for these attacks span the spectrum from political objectives to personal vendettas and extortion. For example, a major DDoS attack in October 2016 targeted DNS service providers hosting popular domains, including Twitter, PayPal and Spotify, resulting in widespread service disruptions that affected users across the United States. To enable real-time threat signaling and mitigation across networks, the Internet Engineering Task Force (IETF) has proposed a cooperative protocol called DDoS Open Threat Signaling (Rodrigues et al., 2020). As the authors of the study explain, the proposed framework provides a decentralized solution that utilizes Ethereum smart contracts to mitigate DDoS attacks. The framework incorporates blockchain-based logic to recognize attack patterns and respond automatically using event-driven approaches. It integrates crypto-economic incentives, whereby participating nodes are rewarded with tokens for reporting authentic attack-related data (Mohanty et al., 2021).

Decentralized consensus is used by a hybrid blockchain framework to identify and address DDoS attacks in Internet of Things networks. The study demonstrates the importance of distributed consensus for attack detection, although it is not Ethereum-specific (Sharma et al., 2018). The study focuses on automating the monitoring and mitigation of anomalous traffic patterns from IoT nodes using Ethereum-deployed smart contracts. It describes a lightweight protocol appropriate for settings with limited resources (Yadav et al., 2020). In a decentralized DDoS defense system, the work suggests a crypto-economic defensive paradigm that rewards cooperation and penalizes false reporting. The approach could be combined with smart contracts for enforcement, and it is based on game theory (Wu et al., 2021). According to the study (Diro et al., 2019), Secure Chain is a distributed firewall that uses blockchain technology to mitigate malicious activity and block suspect IP addresses. The concept can be applied to Ethereum using smart contracts for comparable policy enforcement, even though it makes use of Hyperledger.

This mechanism's fundamental principle is to employ blockchain technology as a decentralized, immutable ledger

for securely storing transaction data. Each transaction is linked to its predecessor and encrypted, creating an irreversible chain of records (Kabla et al., 2022). This distributed ledger significantly reduces the risk of fraudulent activity by ensuring that changing transactional records is almost impossible without the consent of the majority of network participants. Recurrent neural networks (RNNs), convolution neural networks (CNNs), and long short-term memory (LSTM) networks are examples of advanced deep learning models that are used to analyze historical transaction data stored on the blockchain (Chatterjee et al., 2023; Kim et al., 2023; Xu et al., 2020). Trained on massive amounts of data, these models can detect complex patterns and abnormalities, enabling the identification of suspicious behavior and the prediction of potential fraudulent activities in real-time (Javaid et al., 2022).

An energy-efficient chaotic sparrow search algorithm based clustering protocol for wireless sensor network communications (EE-CCSAC) technique was proposed by (Hema, 2022) based on the integration of chaotic maps into the traditional sparrow search algorithm to improve the network speed.

An ensemble deep learning model was proposed by (Malathi et al., 2024) for precise identification of cyberattacks, such as DDoS, in Internet of Things networks. By successfully identifying malicious nodes, their work improves trustworthiness. It does not, however, have automatic response systems or decentralized coordination. This presents an opportunity to integrate such detection algorithms into blockchain-based systems using smart contracts and crypto-economic incentives to connect for effective DDoS mitigation. A GI time-frequency technique was proposed by (Kuppusamy et al., 2011) to identify and stop DDoS attacks. Their approach focuses on traffic pattern analysis for early attack detection. However, it relies on centralized systems. This limitation highlights the need for decentralized blockchain-based approaches to DDoS detection and mitigation.

Prevention of distributed denial of service attacks based on target customer activity pattern exploitation was proposed by (Kuppusamy et al., 2012). In order to detect such attacks, it uses anomaly-based monitoring system. However, it depends on centralized monitoring methods. This implies that decentralised blockchain solutions are

needed for broader, better DDoS mitigation. To control and mitigate DDoS attacks, (Akilandeswari et al., 2022) proposed a framework using a blockchain-based approach leveraging Ethereum and Bitcoin. In their work, blockchain is leveraged to prevent attacks and offer secure monitoring. It brings decentralization in the management of DDoS attacks which is in line with the usage of crypto-economic incentives and smart contracts for proper DDoS defense purposes.

Ensemble Deep Learning Algorithm for DDoS Attack Detection and Prevention in cloud environments was proposed by (Dheepika et al., 2024). In this method, the authors discussed optimised models that improve detection accuracy. However, it relies on a centralized cloud-based structure. This necessitates decentralized blockchain-based DDoS mitigation solutions using smart contracts and/or financial incentives. An ensemble model based on RPL was proposed by (Sakthiraman et al., 2025). In this work, the authors combined RNNs with Random Forest (RF) and Support Vector Machine classifier for detecting DDoS attack on the IoT-WSN systems. They presented a hybrid machine learning approach for improving detection. It relies upon decentralized processing and for the analysis it heavily depends on centralized processing. This proves the requirement for decentralized framework based resilient approaches with scalability to mitigate DDoS.

The authors proposed an explainable deep learning framework based on attention-based neural networks to protect the IoT systems from various cyber threats such as DDoS (Begum et al., 2026). Over the years, DDoS attacks have become extremely common and represent a first-class challenge to the availability, reliability & performance of web services.

However, existing DDoS mitigation solutions based on blockchain are either not fully-automated or have a scalability limited by high operational costs. This paper attempts to design and construct a decentralized DDoS mitigation system with Ethereum smart contracts and crypto-economic processes which will realize an automated, tamper-proof and cooperation-based defense method to large scale attacks.

The main objectives of this research are

- To detect DDoS attacks within the network using a fully decentralized approach.
- To design a blockchain-based mitigation model

Table 1: Comparative Analysis of review of literature

<i>Paper</i>	<i>Technology</i>	<i>Smart contract</i>	<i>Incentive mechanism</i>	<i>Limitations</i>
Sharma et al. (2018)	Blockchain and IoT	No	No	Centralized response triggers
Yadav & Malviya (2020)	Ethereum	Yes	No	No crypto-economic model
Wu et al. (2021)	Game Theory and Blockchain	No	Yes	No on-chain implementation
Mohanty et al. (2021)	Ethereum	Yes	Partial	Not tested for scalability
Diro & Chilamkurti (2019)	Hyperledger	No	No	Permissioned blockchain

leveraging both Ethereum and Bitcoin technologies, using probabilistic methods for effective attack identification and response.

- To enable collaborative protection by developing an automated and easily manageable DDoS mitigation framework.

Proposed Decentralized System for Ethereum Smart Contracts and Crypto-Economic Incentives

The proposed architecture consists of two phases. The first phase is DDoS mitigation service on Ethereum. It consists of distributed detection nodes, detect secure aberrations in traffic patterns, smart contracts that define how validation and mitigation will work, a reputation system to determine whether nodes are trustworthy or not and a token-based rewards mechanism.

The next phase involved writing and deploying smart contracts using Ethereum test networks such as Ganache and Goerli. These contracts would be used to: (1) maintain a registry of nodes, (2) log suspicious activities, (3) identify and validate malicious behaviour and, (4) assist mitigation techniques such as automatically blacklisting misbehaving IP directly into the contract.

A new framework was developed using these two phases to incentivize positive, cooperative interaction across all layers of the network. Participants who successfully reported DDoS attacks were rewarded with tokens, where as those who submitted false reports faced penalties in the form of reduced stakes or reputation scores. This framework was evaluated using simulated DDoS traffic to replicate real attack conditions. Similarly, the smart contracts were tested at different loads using tools such as Truffle, Remix and Hardhat while Python scripts. In the case of anomaly detection, these scripts would call contract functions which on-chain performs a full end-to-end validation of resiliency and efficiency of the system.

A number of important metrics are used to evaluate the

efficiency and effectiveness of the proposed decentralized DDoS mitigation system. The detection accuracy measures the degree to which the system can correctly identify actual DDoS attacks, and it captures information about true positive, false positive and false negative rates. Response time indicates how quickly the system reacts in real time by calculating the time between anomaly detection and execution of mitigation actions through smart contracts. Gas consumption is analyzed to measure the cost-effectiveness of simulating smart contract operations on the Ethereum blockchain to ensure the sustainable of the financial model. Finally, scalability is evaluated by establishing how well the system handles large-scale situations, such as a high intensity of attacks or many participating nodes involved, demonstrating its robustness and flexibility.

The proposed method provides decentralized, transparent and automated approach against DDoS attacks. It is designed to identify potential DDoS attack patterns, store such attack events onto the blockchain in a permanent manner and enforce mitigation based on pre-set logic. It has a crypto-economic model that promotes trust while correcting for falsified or malicious reporting through punitive measures on malevolent activity and rewards of cooperative behavior.

The proposed design supports the following goals. Discovering new abnormal patterns that may indicate DDoS attacks, enabling decentralized reporting and coordination regarding these detections, providing automatic mitigation using Ethereum based mechanisms such as traffic flagging and IP banning, incentivizing accurate detection, utilizing blockchain logs to ensure transparency and tamper resistance. Figure 1 illustrates the workflow of the proposed system.

The proposed architecture consists of six primary components. Detection nodes run off-chain and continuously listen to network traffic for any abnormalities with the help of probabilistic or threshold-based algorithms.

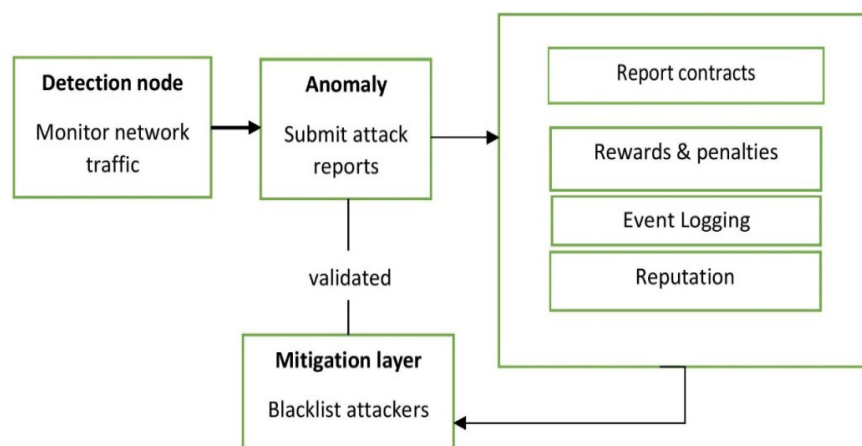


Figure 1: Flow chart of the Proposed System

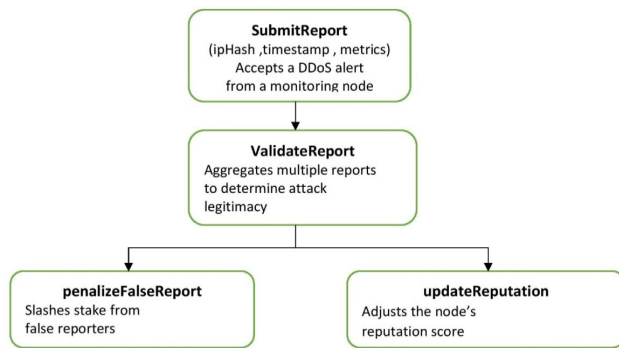


Figure 2: Key Functions of the Proposed System

When the node detects a suspicious behavior of DDoS, it dispatches a signed message to the blockchain. On-chain implementation of Ethereum smart contracts which takes care of report validation, reputation management, reward and punishment distribution as well as attack event tracking. These contracts are immutable once deployed and come with a fixed set of rules. The reporting mechanism allows nodes to announce structured attack reports, including reporter's identity, the time of attack detection, detection metrics, and a hashed source IP through blockchain transactions. Reports are gathered and verified by multiple nodes for authenticity. This is done by blacklisting malicious IP addresses or node identities against a set of acceptable ones after being validated, but it can also take steps in the real world such as signalling gateways or firewalls through the use of oracles or API's. Figure 2 illustrates the Key functions of the Proposed System.

The incentive mechanism encourages honest and active participation by requiring nodes to stake a small amount of tokens. The existing network of reporters is compensated once their reports are validated, and malicious or simply incorrect reporters can have portion of their stake slashed or reputation degraded. Finally, each of the participating nodes has a dynamic reputation score regulated by both the stake and reputation registry. This score gets updated depending on how truthful previous reports are, and directly affects the weight and validity of this node's future submissions. Figure 3 illustrates the sample data structure.

Data Structures

Sample Data Structure shown in Figure 3.

Detection Algorithm

To detect possible DDoS attacks, the off-chain detection node combines the probabilistic classifiers and simple threshold models. The packet rate threshold is one such technique that identifies spikes in traffic that surpass a predetermined threshold. In order to detect amplification attempts, entropy-based filtering also computes the

```

solidity
CopyEdit
struct Report {
    address reporter;
    bytes32 ipHash;
    uint256 timestamp;
    string metrics;
    bool isValid;
}

struct Node {
    unit reputation;
    unit stake;
}
  
```

Figure 3: Sample Data Structure

entropy of source IP addresses or destination ports. To categorize traffic according to characteristics like packet size, transmission rate, and protocol type, Bayesian classification can be used. Anomalies are only reported on-chain when they above a certain threshold in order to maximize blockchain utilization and lower gas expenses.

Each participating node must stake tokens in order to dissuade harmful activity and stop Sybil attacks and widespread false reporting. The Ethereum blockchain records every action and log, making them unchangeable, publicly verifiable, and impervious to tampering. Because of its decentralized architecture, the system is more resilient because there is no single point of failure. Additionally, the system may send off-chain signals to routers and firewalls, such as alerts or instructions, thanks to optional Oracle integration, expanding the mitigation capabilities beyond the blockchain.

Implementation of DDoS mitigation system for Ethereum smart contracts based on decentralization describes the smart contract logic, development environment and tools used & simulation setup for evaluating the system. By incorporating crypto-economic incentives to encourage node collaboration, the prototype demonstrates how decentralized detection (off-chain), reporting (on-chain), cross-referencing and consensus verification, and smart contract logic can be integrated to mitigate DDoS attacks effectively.

Smart Contract Functionality

To achieve a decentralized mechanism for DDoS detection and mitigation, a smart contract was implemented using Solidity. These contracts consist of several essential functions. The functions validateReports() serves as the core decision-making component, executing logic to check whether a predefined number of nodes have reported

the same IP address within a stipulated time interval, `submitReport` (bytes32 IPHash, string memory metrics) enables nodes to submit the attack-related data in form of hashed IP address and associated detection metrics. `applyMitigation` (bytes32 IPHash) logs the reported IP address and add it the blacklists once malicious attack has been confirmed. `penaltyAndSlashForFalseReports()` function penalize nodes that submit false reports by slashing their staked tokens. `distributeRewards()` function rewards nodes that accurately identify attacks. In addition, events such as `ReportSubmitted`, `MitigationApplied` and `RewardDistributed` are logged on the blockchain to ensure transparency and traceability. A Sample Solidity snippet for report submission is presented in Figure 4.

```
solidity
CopyEdit
function submitReport(bytes32 ipHash,string memory metrics)public{
    require(stakes[msg.sender]>=minStake, "Insufficient stake");
    reports[ipHash].push(Report(msg.sender, metrics , block.timestamp));
    emitReportSubmitted(msg.sender, ipHash);
}
```

Figure 4: Sample Solidity snippet for report submission

It is a staking-based crypto-economic model that ensures reliability across the network and encourages honest reporting. Before they submit reports, the detection nodes that take part in this process must stake some tokens. If the report gets accepted by consensus, the reporter receives the tokens. If the report is identified as a fraud or malicious attempt, then either all of the node's staked tokens are slashed, or just part of them. These operations rewards and penalties that depend on these predetermined thresholds and whether the consensus norms are satisfied or not, so you can think about it as a contract between all parties where the smart contract guarantees their adherence to it.

The off-chain DDoS detection system is constructed as Python scripts imitating real-time traffic monitoring and attack detection. Entropic analysis of source IPs is used to detect amplification attacks, and packet rate thresholding (greater than 100 packets/second for a single unicast target) are used. Network data aggregation and Processing with tools such as Scapy& Wireshark. The IP address is hashed, and the on-chain reporting uses Web3. js or Ethers. js so as to invoke the `submitReport()` method in the smart contract. The reporting process is initiated when a detection node executes the off-chain detection logic and identifies the suspicious traffic pattern. The suspected IP address is hacked, and a Python script sends a transaction to the smart contract by invoking `submitReport()`. The smart contract collects reports from multiple nodes concerning the same IP address and monitors the reported activity. When sufficient

number of matching reports received, the `validateReports()` function verifies whether the reported activity constitutes an anomaly. Upon confirmation, the offending IP address is added to the blocked list through the `applyMitigation()` function. The function `DistributeRewards()` rewards nodes that submitted legitimate reports. This implementation enables a simplified, decentralized and autonomous framework for DDoS detection, validation and mitigation without relying on centralized management.

Result and Discussion

To assess functionality and performance, the system was set up in both local and testnet settings. The Truffle framework was used in conjunction with Ganache, a personal Ethereum blockchain for testing, to create and deploy the smart contract locally. The following figure illustrates the command used in the Truffle framework in combination with Ganache, personal Ethereum blockchain.

```
bash
CopyEdit
truffle compile
truffle migrate -- network development
For testnet deployment , the Goerli testnet was used , with deployment facilitated through
infura and a MetaMask wallet. The command for deployment was :
bash
CopyEdit
truffle migrate -- network goerli
```

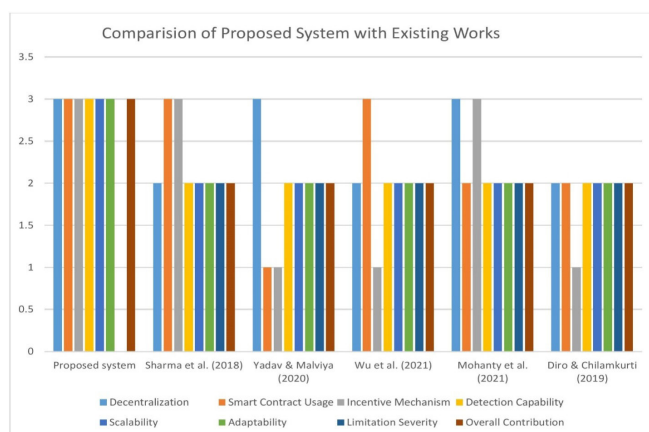
Figure 5: Truffle framework in combination with Ganache, a personal Ethereum blockchain

Scapy was used to mimic UDP flood attacks from several virtual nodes, generating both malicious and lawful traffic streams in order to evaluate the proposed system. Detection nodes were set up to keep an eye on this traffic and notify any unusual activity to the smart contract. Five reporter nodes made up the test environment, and three nodes were designated as the consensus threshold. On-chain costs were assessed by measuring Ethereum gas fees per transaction. A reputation score of 100 was initially assigned to each detection node and it was later modified in accordance with the accuracy of the reports that were submitted.

Table 2 signifies decentralization, smart contract usage, incentive mechanism, detection capability, scalability, and flexibility, the comparison analysis demonstrates that the suggested Ethereum-based decentralized DDoS mitigation system outperforms current methods. The suggested system completely integrates Ethereum smart contracts with crypto-economic incentives to automate attack mitigation and promote secure node participation, in contrast to previous works. Due to a lack of automation, inadequate incentive systems, conceptual implementations, or scalability problems, current systems only offer mediocre performance. As a result, the suggested framework provides

Table 2: Comparison of Existing Vs Proposed System

Paper	Technology	Platform Score	Decentralization	Smart Contract Usage	Incentive Mechanism	Detection Capability	Scalability	Adaptability	Limitation Severity	Overall Contribution
Proposed system	Ethereum	3 (Ethereum)	3	3	3	3	3	3	1	3
Sharma et al. (2018)	Blockchain and IoT	3 (Ethereum)	2	3	3	2	2	2	2	2
Yadav & Malviya (2020)	Ethereum	2 (General BC)	3	1	1	2	2	2	2	2
Wu et al. (2021)	Game Theory and Blockchain	3 (Ethereum)	2	3	1	2	2	2	2	2
Mohanty et al. (2021)	Ethereum	2 (Conceptual)	3	2	3	2	2	2	2	2
Diro & Chilamkurti (2019)	Hyper ledger	2 (Hyperledger)	2	2	1	2	2	2	2	2

**Figure 6:** Comparison of proposed system with Existing Works

a more effective, flexible, and scalable way to counteract contemporary DDoS attacks with less severe limitations and a greater total contribution.

The following Figure illustrates how well the suggested decentralized DDoS mitigation system performs in comparison to current blockchain-based methods. The suggested solution maintains the least severity of limitations while achieving the greatest marks in decentralization, smart contract usage, incentive mechanism, detection capabilities, scalability, flexibility, and overall contribution. However, due to limited automation, weaker incentive models, lesser scalability, or conceptual implementations, previous studies offer modest performance. Overall, the comparison shows that the suggested Ethereum-based framework provides a more effective, scalable, and flexible way to mitigate contemporary DDoS attacks.

Conclusion

In this study, we present a decentralized architecture consisting of Ethereum smart contracts and crypto-economic incentives for DDoS threats identification and mitigation. The entire approach, using offchain detection

and consensus-based on-chain validation ensures that decisions to identify and mitigate malicious traffic are made in a trustless, transparent and tamper-resistant manner. Smart contracts eliminate centralized control by automating the processes of reporting, validating, mitigating, and allocating incentives.

The implementation includes a staking system that deters cheating and ensures nodes are held accountable for their reports. Experimental evaluations demonstrated the detection algorithms, said mitigation, and effectiveness of economic gas usage against simulated DDoS attacks. While the modular architecture provided this foundation, realtime detection, user-friendly monitoring via a frontend dashboard & other intuitiveness were made possible only due to integration with tools such as Scapy, Web3 etc. js, and React. js. Designed to eliminate key pitfalls often found in centralized mitigation methods including single points of failure, censorship, and a lack of transparency, this decentralized system enables an innovative community-driven strategy for defending networks from volumetric assaults.

Acknowledgement

The authors, Dr.S.Malathi and Ms.R.Akilandeswari, sincerely thank and acknowledge the management of A. Veeriya Vandayar Memorial Sri Pushpam College (Autonomous), Poondi, Thanjavur(dt), 613503, India and Swami Dayananda College of Arts & Science, Manjakkudi, Tiruvarur(dt), Tamil Nadu, India, for their valuable support in successfully carrying out this research work.

References

- Akilandeswari, R., & Malathi, S. (2022). Design and implementation of controlling with preventing DDoS attacks using bitcoin by Ethereum blockchain technology. *Journal of Transportation Security*, 15(3), 281–297. doi: 10.1007/s12198-022-00245-x.
- Begum, S.R., & Malathi, S. (2026). Securing Smart IoT Networks from Cyber Threats Using Explainable Zero Channel Attention-aided Ghost Convolution Neural Network Framework. *The Scientific Temper*, 17(4):6103-6116. doi: 10.58414/

- SCIENTIFICTEMPER.2026.17.4.21.
- Chatterjee, P., Das, D & Rawat, D. (2023). Securing Financial Transactions: Exploring the Role of Federated Learning and Blockchain in Credit Card Fraud Detection. doi:10.36227/techrxiv.22683403.v1.
- Dheepika , S.P., & Umadevi, V. (2024). An optimized approach for detection and mitigation of DDoS attack cloud using an ensembled deep lerning approach. *The Scientific Temper*, 15(03),2579-2587. <https://doi.org/10.58414/SCIENTIFICTEMPER.2024.15.3.25>.
- Diro, A.A., & Chilamkurti, N. (2019). SecureChain: Blockchain-Based Distributed Firewall for Preventing DDoS Attacks in Cloud Networks. *Computers & Security*.
- Hema, V. (2022). An energy-efficient chaotic sparrow search algorithm based clustering protocol for wireless sensor network communications. *International Journal of Health Sciences*. <https://doi.org/10.53730/ijhs.v6nS5.9538>
- Javaid, M., Haleem, A., Singh, R.P., Suman, R. and Khan, S. (2022). A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, p.100073. doi:10.1016/j.tbench.2022.100073
- Kabla, A.H.H., Anbar, M., Manickam, S. & Karupayah, S. (2022). Eth-PSD: A machine learning-based phishing scam detection approach in ethereum. *IEEE Access*, 10, pp.118043-118057. doi:10.1109/ACCESS.2022.3220780
- Kim, J., Lee, S., Kim, Y., Ahn, S. & Cho, S. (2023). Graph Learning-Based Blockchain Phishing Account Detection with a Heterogeneous Transaction Graph. *Sensors*, 23(1), p.463. doi:10.3390/s23010463
- Kuppusamy, K., & Malathi, S. (2011). An effective prevention of attacks using gl time frequency algorithm under DDoS. *International Journal of Network Security and its Applications*, 3(6). doi: 10.5121/ijnsa.2011.3619.
- Kuppusamy, K., & Malathi, S. (2012). Prevention of attacks under DDoS using target customer behavior. *International Journal of Computer Science Issues*, 9(5).
- Malathi, S., & Razool Begum, S. (2024). Enhancing trustworthiness among IoT network nodes with ensemble deep learning-based cyber attack detection. *Expert System with Applications*. <https://doi.org/10.1016/j.eswa.2024.124528>.
- Mauri, L., Cimato, S & Damiani, E. (2018). A comparative analysis of current Cryptocurrencies. *Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP, Funchal, Madeira - Portugal*, pp. 127–138. doi.org/10.5220/0006648801270138.
- Mohanty, S., Choudhury, R., & Mahato, A. (2021). Blockchain-Based DDoS Attack Mitigation Using Ethereum Smart Contracts and Crypto-Economic. *Procedia Computer Science*.
- Rodrigues, B., Trendaflov, S., Scheid, E.J, & Stiller, B. (2026). SC-FLARE: cooperative DDoS Signaling based on smart contracts. In: *IEEE international conference on blockchain and cryptocurrency (ICBC 2020)*, pp. 1–3, IEEE, Toronto. doi:10.1109/ICBC48266.2020.9169750.
- Sakthiraman.R., & Arockiam, L. (2025). RRFSE: RNN based random forest and SVM ensemble for RPL DDoS in IoT-WSN environment. *The Scientific Temper*.16(02) , 3839-3847. <https://doi.org/10.58414.SCIENTIFICTEMPER.2025.16.2.16>.
- Sharma, P. K., Moon, S. Y., & Park, J. H. (2018). A Blockchain-Based Approach for Secure Data Storage and DDoS Mitigation in IoT Environment. *Journal of Information Processing Systems*.
- Wu, Y., Zhang, Z., & Lin, X. (2021). A Game-Theoretic Incentive Mechanism for Blockchain-Based DDoS Defense Systems. *Future Generation Computer Systems*.
- Xu, L., Chen, L., Gao, Z., Carranco, L., Fan, X., Shah, N., Diallo, N., & Shi, W. (2020). Supporting blockchain-based cryptocurrency mobile payment with smart devices. *IEEE Consumer Electronics Magazine*, 9(2), pp.26-33.
- Yadav, S., Malviya, M. (2020). Smart Contract-Based DDoS Detection and Mitigation for Resource-Constrained IoT Devices. *IEEE Access*.