ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue IX September 2024

Blockchain Mechanism Approach to Smothering of Denial of Service (DoS) Spikes: A Focus on Internet of Things (IoT) Technologies

***Gbeminiyi Falowo., Adenike Adegoke-Elijah., Mba Obasi Odim., Sunday John Agbolade**

Computer Science Department, Redeemers University, Ede

***Correspondent Author**

DOI: https://doi.org/10.51244/IJRSI.2024.1109014

Received: 05 August 2024; Accepted: 02 September 2024; Published: 28 September 2024

ABSTRACT

Denial of Service (DoS) is a cybercrime that attempts to impede electronic consumers from accessing websites and online services by saturating a server with internet traffic. Cyber-spikers use a network of infected computers, tools like bots, and other machines they can access remotely. A decade ago, businesses and financial institutions lost approximately half a trillion dollars due to DOS spikes. DoS savages would triple in number before the closure of the year 2023 from about eight million less than five years ago. This study uses a blockchain-based decentralized authentication technique to guard against DoS attacks on the application layer of Internet of Things (IoT) technologies. This secured mechanism involves starting the communication process, developing the system, and suggesting an intelligent contract. Performance evaluation of the developed model was carried out by comparing the approaches' temporal complexity. The recommended method was also used on two processors operating at two distinct speeds while utilizing the SolarWinds application, an online CPU stress test, and usage with a deduction that the second is preferred. An Intelligent contract for IoT machine usage is established to authorize the blockchain level.

Keywords: Denial of Service, Blockchain, Cyber security, Intelligent contract, Internet of Things.

INTRODUCTION

With the numerous pros cyberspace has brought to our world, this revolutionary age, through the innovative sprout of the internet elephant called the Internet of Things (IoT), also came the setback of constant Denial of Service, a spike on the top layer of IoT network. [13] submit that the Internet of Things provides Internet connectivity to day–to–day electronic objects and that a large number of connected machines has to be adequately managed, taking into account communication constraints viz-a-viz the Internet and all other network resources. Communication constraints include designed protocol for remote management, internet service enablement, and end-to-end latency caused by constant denial of service (DoS). IoT networks are accessed typically through IoT gateways or proxies that route application requests and device responses and implement several extra functionalities to improve system performance [3].

Cyber-spikers target IoT gateways to the end that application requests, proxies, and device resources are rerouted to cause DoS. These perpetrators of customer denial of service are fast becoming a menace, knowing fully well that the intelligent community is the next and present big deal because IoT devices construct large-scale botnets that possess significant high-tech ability and network bandwidth. If nothing is done to curb these spikers, DoS may triple from approximately eight million spikes by 2024.

Notably, the rapid increase of IoT with the vulnerabilities identified in IoT devices has attracted cyber-spikers' interest to subvert those devices [1]. The botnet is one of the grounds these malicious agents explore. It is a type of malware that alternates electronic consumer devices into bots or dummies to execute DoS Spikes. This type of spike may also focus its attacks on servers or network equipment [10], and due to botnet open source code, spikers managed to originate different imbalances. [2, 12]. The bot can do activities such as raking IoT devices for loopholes and risks, sending spam emails, and infecting weak devices and systems, among many others.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue IX September 2024

However, cyber security saddles itself with fixing IoT devices identified as assailable by monitoring and evaluating the network system. Cryptography applications have previously provided classic security measures for embedded IoT devices. Still, this study offers a simple but intelligent approach to smothering these loopholes using blockchain mechanisms. Blockchain mechanisms proffer new ways to securely exchange digital assets using solid cryptography technology in innovative computing protocols. Even though the blockchain mechanism is the fundamental building block of the highly hyped cryptocurrency, blockchain engineering has found its way across other paths. These paths include mitigating security cons and risks, an area far from its initial conception [4].

Again, this study proposes a mechanism that allows robust and scalable interactions between service providers, electronic business owners, and their consumers with blockchain through Intelligent Contract application techniques on the application layer of the network to secure end-to-end network functionality from the Internet Service Providers (ISP) to the user network.

REVIEW OF LITERATURE

In [8], the authors reasoned that Machine Learning and Artificial Intelligence caused an orbital turn in the qualitative change of IoT research by introducing new advanced possibilities and features by giving existing and new applications the intrinsic ability to develop from heterogeneous processed data and datasets. Picone [9] elucidated that Intelligent IoT research took an upward trend as a result of multiple technologies integration and skills to support and create cognitive systems able to automatically understand the operational context, adapt, reason, and act in real-time according to changes, and external inputs or to reach defined goals. For instance [7], it proposes the merger of technologies, such as IoT, big data, high-performance computing (HPC), open data, and artificial intelligence, to apply High-Performance Data Analytics (HPDA) to the cultivation of agricultural data and improve the efficiency and effectiveness of farms, the substantive research result. The referenced authors of [5 and 6] examined intensely different IoT firmware on the Internet for basic security and DoS investigation; they discovered over half a million exposed devices, with many using the default login details inputted by the electronic customers. These devices had backdoor access, such as telnet, and the security effect had multiplied exponentially over the decade. Notably, the large quantity of information created by the IoT can service new IoT cognitive systems (both in the cloud and Edge) and augment their functionalities to understand the context, discover new behaviors, and operate more efficiently and profitably [14]. These trends and growing research fields illustrate how interdisciplinary approaches may easily lead to further knowledge, such as high-tech DoS spikes, and alternatively provide an innovative way to combat such attacks [9, 14]. Mendez [11] proposed a decentralized actionable cyber threat intelligence for networks and IoT, which motivated this work. Mendez's work uses blockchain to decentralize network protocol functionalities to secure end-to-end edge variations in IoT machines.

Five Layer Architecture of IoTs

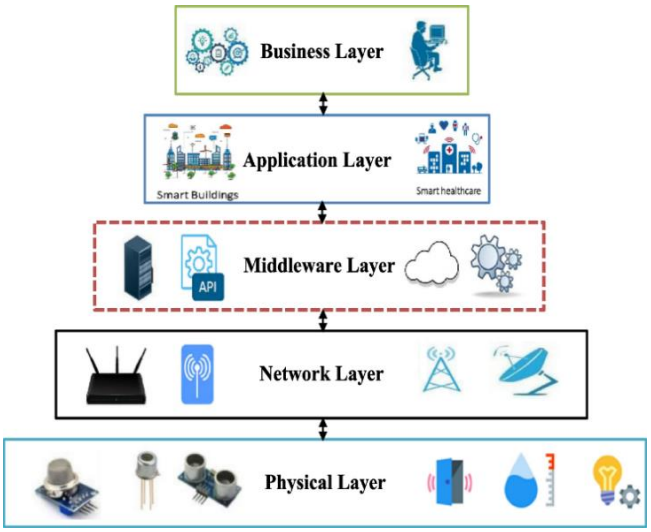

Figure 1: The IoTs' Architecture Layer [Alaghbari; Saad; Hussain and Alam (2022)]

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue IX September 2024

LEVERAGING ON THE DISTINCT FEATURES OF BLOCKCHAIN METHODOLOGY

The blockchain mechanism's intrinsic and intuitive ability to decentralize a network's trust entity allowed it to share critical information changelessly. In this study, the HPC process obviates human intervention to reduce human errors during incident handling. Using flexible governing intelligent contracts helped streamline incident responses in the network. The main idea of DoS spikes on IoT machines is to attack the Open System Interconnection (OSI) seventh layer by exhausting the target's resources**.** These spikers understand that on the application layer, otherwise known as the seventh layer of the OSI model, web pages are created on the server and transmitted in response to Hypertext Transfer Protocol (HTTP) queries. Thus, they cause malicious and valid traffic on this layer because it is unavoidable. Consider the following models;

A. Algorithm 1:

Intelligent Contract Start-Up

{

Input object id;

if (ObjIdinExistence (obj.id, bc) == true) **return** Error ();

ifAddrinIdExistence (obj.grpId, bc), **return** Error ();

if (obj.type == manager) **then**

{**if**GrpIdExists(obj.grpId, bc) == true **then return** Error ();

}**else if** (obj.type == follower) **then**

{**if**GrpIdExists (obj.grpId, bc) == true **then**

return Error ();} **if** (bc.CertificateAdmit (obj.certificate) == false), **then return** Error ();

else return Error ();

}

In this study, we propose an authenticator system using blockchain with the feature of an intelligent contract, otherwise called a smart contract, that recognizes clusters and produces the address of IoT management devices with multiple unique identifiers for all systems reactors. The blockchain authenticator ensures that all IoT machines, including the ones on the white trusted list, are first disallowed from accessing the targeted server.

B. Algorithm 2:

Communication Process

{

if *(ObjIdinExistence (sender.id, bc) == false || ObjIdinExistence (receiver.id, bc)== false)*

then return *Error ();*

if *(sender.grpId != receiver.grpId)* ***then return*** *Error ();*

if *(bc.SignAuthent (sender.msg) == false),* ***then return*** *Error ();*

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue IX September 2024

if *(bc.CurrentGaslimitValue>(AllowedGasLimitValue))* ***then return*** *Error ();*

LabelDeviceAsMalicious(); dropFromWhiteList();

}

The second phase of the Algorithm describes how the IoT machines and the target server communicate. The address of the IoT machine should appear on the trusted allowlist and must not exceed the gas limit required for the communication path to be established.

Outputs

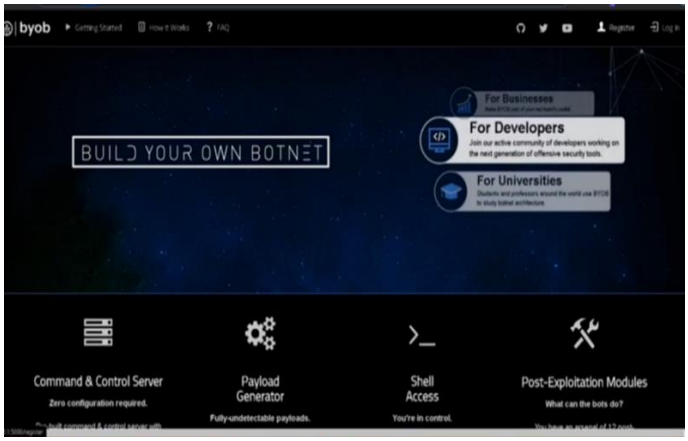

Figure 2: The Botnet interface

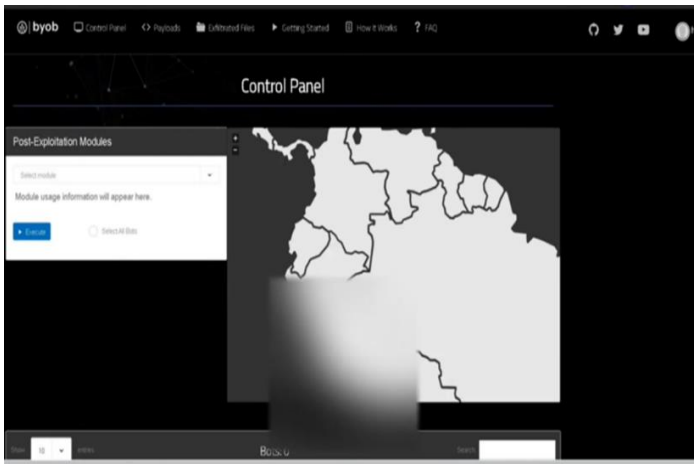

Figure 3: The Botnet Navigation Map

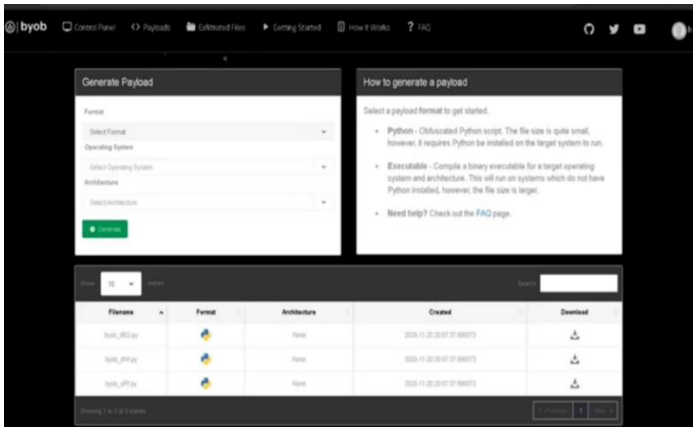

Figure 4: Firewall Selector

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue IX September 2024

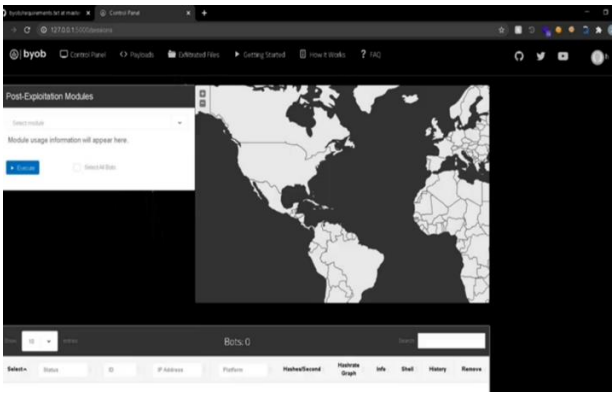

Figure 5: The Danger Area Indicator

The output of the figures above display the outcomes of executing the proposed technique using SolarWinds software and an online processor stress test on two systems, as displayed in Tables 1 and 2 with varying specification

DISCUSSION

Table 1: Machine Specification

Machine Name	**Architecture**	**Processor Speed**	**RAM Capacity**
Laptop HP	Core i5	2.40 GHz	8 GB.
Personal Computer	Core i5	2.60 GHz	16 GB.

Table 2: Processor Association Time/Data Association Time

	Processor A	**Processor B**
Association Time per request (ms)	0.01	0.009
Association Time (SD in ms)	1.2×10^{-18}	6.0×10^{-19}
Association Time Average (ms)	0.0099	0.0091
Data Message Average Time (ms)	0.0070	0.0657
Data Message Time (ms)	0.0069	0.00657

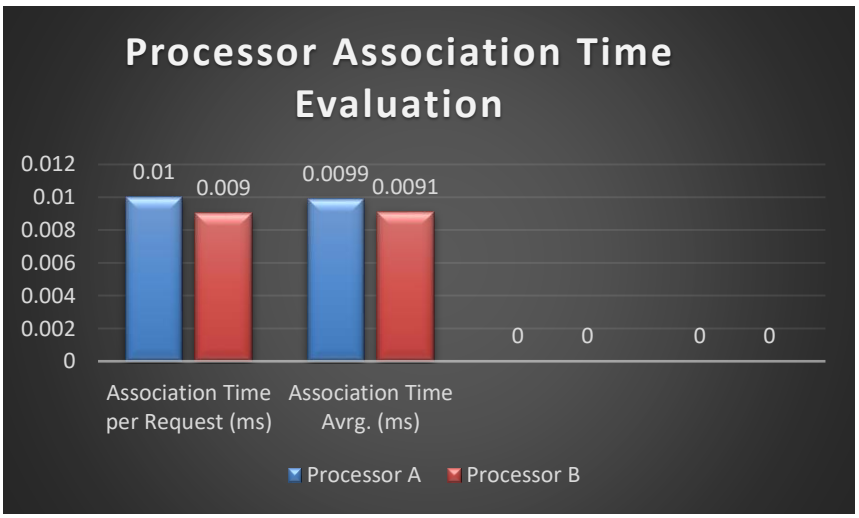

Figure 6: Processor Association Time

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue IX September 2024

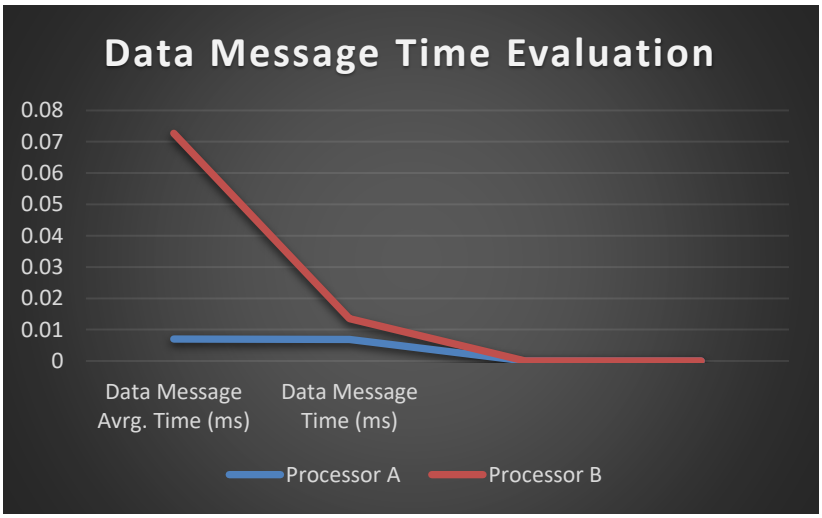

Figure 7: Data Message Time

The assessment depicted above shows that data were collated as data message average time (ms), data message time (ms), association time per request (ms), association time (SD in ms), association time average (ms), association time average (ms), as the evaluation's findings.

The outcomes of 100 trials are shown in Table 2 as follows: how long it takes a follower to join after applying. Each IoT follower device submits an association request to join the blockchain using two systems around 0.0099 milliseconds and 0.0091 milliseconds, respectively. The program calculates the standard deviation (SD) to analyze the data better.

The magnitude of the irregular behavior of the values and the system's low SD ratings in both machines indicate that it will probably work gradually and consistently going ahead. The overall transmission time for all messages transmitted by a PC device is 0.657 milliseconds, and each message takes 0.00657 milliseconds to send.

CONCLUSION

This study has canvased the demanding situation that Denial of Service (DoS) spikes has placed on our day-to-day electronic transaction with a significant focus on the advanced technology of the Internet of Things (IoT). A blockchain mechanism model was proposed for smothering DoS spikes on IoT machines through an intelligent contract, which proved positive from the stress evaluation test carried out with many trials on varying systems' specifications.

REFERENCES

1. Alaghbari, K.A.; Lim, H.-S.; Saad, M.H.M.; Yong, Y.S. (2023), "Deep Autoencoder-Based Integrated Model for Anomaly Detection and Efficient Feature Extraction in IoT Networks." IoT **2023**, 4, 345–365. https://doi.org/10.3390/iot4030016
2. Alaghbari, K.A.; Saad, M.H.; Hussain, A.; Alam, M.R. (2022), "Complex event processing for physical and cyber security in datacenters—Recent progress, challenges, and recommendations." J. Cloud Comp. **2022**, 11, 65. https://doi.org/10.1186/s13677-022-00338-x
3. Beniwal, G.; Singhrova, A. (2021) A systematic literature review on IoT gateways. J. King Saud Univ. Comput. Inf. Sci. 2021, in press. https://doi.org/10.1016/j.jksuci.2021.11.007
4. Conoscenti, M.; Vetro, A.; De Martin, J.C. (2016) "Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6. https://doi.org/10.1109/AICCSA.2016.7945805
5. Cui, A.; Stolfo, S.J. "A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan." (2010) In Proceedings of the 26th Annual Computer Security Applications Conference, Austin, TX, USA, 6–10 December 2010; pp. 97–106.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue IX September 2024

6. Karamanos, E. “Investigation of Home Router Security. Master’s Thesis, KTH Information and Communication Technology,” (2010) Stockholm, Sweden, 2010
7. Lemus-Prieto, F.; Martín, J.F.B.; Gónzalez-Sánchez, J.-L.; Sánchez, E.M. (2021) “Cultiv Data: Application of IoT to the Cultivation of Agricultural Data.” IoT **2021**, 2, 564–589. https://doi.org/10.3390/iot2040029
8. Li, H.; Ota, K.; Dong, M. Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing.” IEEE Netw. **2018**, 32, 96–101.dx.doi.org
9. Marco Picone (2020). “IoT: A New Open Journal Access for Internet of Things”, IoT **2020**, 1, 145–146; doi:10.3390/iot1010009
10. Marzano, A.; Alexander, D.; Fonseca, O.; Fazzion, E.; Hoepers, C.; Jessen, K.S.; Chaves, M.H.; Cunha, I.; Guedes, D.; Meira,W. (2018) “The evolution of Bashlite and Mirai IoT botnets.” In Proceedings of the 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 25–28 June 2018; pp. 00813–00818.
11. Mendez Mena, D.; Yang, B. (2021) Decentralized Actionable Cyber Threat Intelligence for Networks and the Internet of Things. IoT **2021**, 2, 1–16. https://doi.org/10.3390/iot2010001
12. Mira Botnet Source Code. Available online: https://github.com/jgamblin/Mirai-Source-Code (accessed on 1 October 2023).
13. Pappalardo, M., Virdis, A., & Mingozzi, E. (2022). “An Edge-Based LWM2M Proxy for Device Management to Efficiently Support QoS-Aware IoT Services.” *IoT*, *3*(1), 169-190. https://doi.org/10.3390/ iot3010011
14. Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A Survey on the Edge Computing for the Internet of Things. IEEE Access 2018, 6, 6900–6919. dx.doi.org