Journal of Research in Engineering and Computer Sciences
October 2023, Vol. 1, No. 4, pp. 85-92

Mitigation of IoT Device Based DDoS Attacks (Using Blockchain)

Isonkobong Christopher Udousoro

1. Department of Information Technology, School of Computing and Information Technology, Federal University of Technology, Owerri

Abstract:
Internet of Things (IoT) refers to the connection or interconnection of smart objects or devices sharing data and/or information. In the world of today, devices are being made smart which makes internet of things to emerge as an area of incredible impact, potential and growth. Therefore, the rapid development of internet of things also brings about threat of insecurity. There is difficulty in the securing of private data and information as the internet of things (IoT) is being vulnerable to various attacks. In this review article, we focus on the Distributed Denial of Service (DDoS). This is an attack initiated by the attacker to disrupt the authentic user from using the required services and also make network resources unavailable thereby consuming bandwidth. This paper aims at reviewing different methods and articles used to mitigate these attacks with great focus on blockchain variant used with smart contracts. This blockchain variant known as Ethereum is integrated with the Internet of Things devices and prevents the rogue devices and DDoS attacks from gaining access to the server. The research methodology is based on qualitative analysis where various literatures is being reviewed based on IoT devices and DDoS attack mitigation. This paper will be of benefit to individual in the cyber security field.

Keywords: Internet of Things (IoT), Distributed Denial of Service (DDoS), Blockchain, Ethereum, Smart Contracts.

INTRODUCTION

Technology is fast becoming an integral part of the human race where every device is moving towards the "always connected" model. The trending revolution of technology has made all devices to be interconnected with each other thereby introducing a new concept known as Internet of Things (IoT) [4]. Internet of Things (IoT) can be defined as the integration of physical devices which are capable of communicating, sharing, operating and disseminating, thereby enabling new services in a wide range of areas [9]. Figure 1 below shows a high-level overview of the Internet of Things (IoT) based systems and their interaction where a centralized server communicates with the IoT devices like sensors through a communication network.

A lot of security platforms that are required for IoT; Confidentiality is one of them where message that is sent from one source to the other can be easily intercepted by an attacker and the content can easily be compromised. It is necessary to secure the message by hiding it from the relay nodes. The solution to this is a method known as encryption/decryption mechanism [1]. Integrity is also a security service which means message that is sent should not be altered, it should get to the receiver the same way it was sent. Altering the message breaks the security measures [2]. For the internet of Things to continue working, the services must always be available for use and accessibility must be granted so that it will be easy to detect when the service is being intruded then intrusion can be prevented to ensure availability always [7]. Users of the services from end to

end should be able to identify those they are interacting with so that an attacker will not be introduced into the system [3].

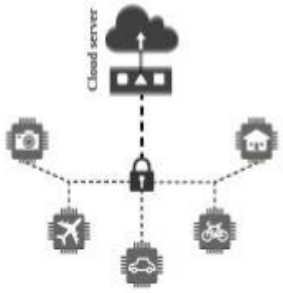

Figure. 1: IoT Architecture [9].

Security has been a major concern for to these IoT applications and devices. This is due to the high volume of data and large size of network being used and produced. Distributed Denial of Service (DDOS) attack should be focused on and tackled as it is a security threat to Internet of Things systems [3]. DDoS attack is when an attacker that is malicious attempts to consume bandwidth of legitimate users and make network resources unavailable. In terms of IoT devices, DDoS attack overloads the network resources or targeted computing device using any IoT application [9]. A DDoS attack flow diagram is shown below in figure 2 where the attacker uses various units as handlers to fill the host with packets which ends up taking up resources and bandwidth [23]. Some of the most common DoS attacks are SYN flood, DNS flood, Ping flood, UDP flood, ICMP broadcast etc.

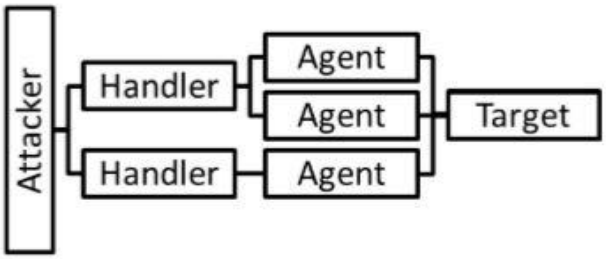

Figure. 2: DDoS Attack Flow [23].

This paper uses blockchain technology for providing security solution to the DDoS attacks on IoT devices. Blockchain is being described as an online distributed ledger which consists of a list of blocks, each block is an ordered record of a timestamp and hash of the previous record [11]. Blockchains are mostly used in cryptocurrencies such as bitcoin and smart contracts such as ethereum [9]. This paper will review other methods of mitigating DDoS attacks on IoT devices but more attention will be given to blockchain being used as a defense mechanism against DDoS attacks using the ethereum blockchain. This paper is organized as follows: Section 2 describes the various models and methods being reviewed based on DDoS attacks on IoT devices and also highlights the number of journals and their sources being used for this paper. Section 3 introduces and highlights the proposed Ethereum blockchain model being used to prevent DDoS attack on IoT devices while section 4 presents the conclusion of the paper.

RELATED WORKS

Various methods and models have been developed by scholars in other to mitigate DDoS attacks on IoT devices. This section of the paper highlights some of the models and methods adopted and reviewed accordingly.

Learning Automata (LA) concept is being deployed as a strategy in mitigating DDoS attacks as Service Oriented Architecture (SOA) is presented as a system model for IoT [14]. Here the Service Oriented Architecture gives room to various developers to develop applications for IoT thereby acting as a middleware. With this, the prevention of DDoS attacks on IoT devices has proven effective.

Software Defined Networking (SDN) provides a better solution to the mitigation of DDoS attacks compared to sampling-based approaches. Traffic flow statistics are being checked and also normalized at each SDN-enabled switch [3].

The application of correlation and regression analysis is also being deployed to detect security incidents which could also include DDoS attacks on Internet of Things devices [13]. These correlation and regression analysis is also capable of detecting other various security threats that are eminent on the IoT devices.

A framework known as Multi Level DDoS Mitigation Framework (MLDMF) is proposed to defend against DDoS attacks on Internet of Things devices [19]. This framework includes edge computing level, fog computing level and cloud computing level. SDN is also being deployed to manage and mitigate DDoS attacks on IoT devices.

Kuusijarvi J., Savola R., Savolainien P., & Evesti A. in 2016 proposed as a solution a system known as trusted Network Edge Device (NED). Here, the trusted network elements download the security counter-measures of individual devices. The advantage of this system is the protection of the IoT devices with defined policies which are also initiated on other devices. Managing the countermeasures of the multiple Internet of Things devices all at once is also an added advantage of the model.

A DNS query-based distributed denial of service attack mitigation system using Software Defined Networking (SDN) is proposed to block and prevent the network traffic for DDoS attacks [3]. The network traffic traces obtained is distinguished from malicious traffic using a prototype system with Dirichlet process mixture model. Feng & Xu in 2018 designed and analysed a distributed and demand-based backscatter MAC protocol for Internet of Things. With this system and model, distributed denial of service attacks will be prevented and mitigated from IoT devices.

METHOD OF INVESTIGATION

This article took up a review of two hundred and fifteen journal papers that is published in reputable academic journals ranging from 2006 to 2018. To carry out the research properly, the keywords that were considered are "Internet of Things", Distributed Denial of Service" and "Blockchain". The search was carried out in databases which include IEEE, Elsevier, ProQuest, and Emerald publishing. Table 1 below shows a table detailing the distribution of the search, number of journals and its percentage distribution.

Table 1: Distribution of reviewed papers

S/no.	Database	Number of papers	Percentage
1	Google Scholar	80	37%
2	IEEE	31	15%
3	ProQuest	31	15%
4	Elsevier	40	18%
5	Emerald	16	15%

SYSTEM MODEL AND DESIGN

In this section, we will discuss the system model that comprises the devices and its peripherals and also discuss the proposed IoT-Blockchain model or design that will mitigate DDoS attacks on various IoT Devices.

NETWORK &THREAT MODEL

The figure below shows the network model and its entities which consists of Device, Gateway, Smart Contract and Server/Miner.

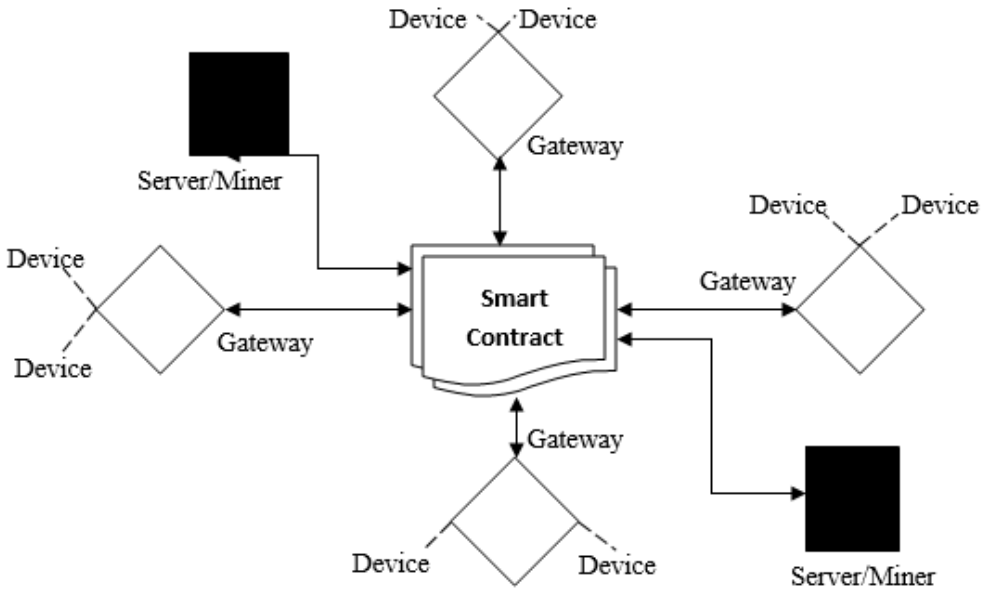

Figure 3: IoT-Blockchain System Model (Jayaid, Siang, Aman & Sikdar, 2018).

Device

This represents the Internet of Things (IoT) which are interconnected with each other, for transferring communicable data to the server through the gateway [9]. A gateway can be used to bring together multiple devices.

Gateway

This provides network connection to all the devices around itself. It also offers data aggregation and security features. In this case, it represents a gateway that group of devices can use for communication purposes.

Smart Contract

This is a system that serves as an authority and responsible for ensuring that the devices do not go further than what is required of the gas limit [9]. It is also considered as a regulatory body.

Server/Miner

This system is known for validating the transaction and data exchange through smart contracts using high computational processing capabilities.

The major objective of the distributed denial of service (DDoS) attack is to cause data traffic to the server which will cause outages [9]. With this flooding and overloading, it is assumed that the IoT devices are made to send a certain amount of data to the target of the DDoS attack. The IoT devices is used by the attacker to launch DDoS attacks on the servers.

IoT-BLOCKCHAIN MODEL

An online established software platform known as Ethereum which allows smart contracts and systems that are decentralized to be built on blockchains along with their states which are comprised of objects known as accounts that have fields like 20-byte address, a nonce, a balance of Ether, a contract code and storage [9] e. A state in Ethereum is known as data that is present in blockchain, therefore, when there is a transaction, a state transition occurs. There exists a gas limit when it comes to processing in Ethereum. Gas is known as resource. The model that is proposed is charged with allocating addresses for each node and also applying our coded smart contract with dependency on Ethereum. The contract determines which devices are trusted and those that are not trusted. Devices must be registered to the platform and given a specific gas limit. The enlistment will produce an account with special address for each device and a gas limit for a device to be related to their details. It depends on the transmission capacity and asset necessities of the device. Interactions between devices and servers are empowered by utilizing the smart contract represented by the server hub.

The smart contract in this system is charged with the task of checking invulnerable communication amongst the IoT units and the disbursed systems. It is developed with the usage of solidity, which is contract-oriented, high-level language for the ethereum digital computing device environment. Smart contract has two stages of operation which are

- **Initialization**: This phase of the smart contract describes how the system sends the smart contract which is regarded as server variable by using the contract to apprehend the trusted host. This paper takes into consideration that systems are the hosts that are trusted. The smart contract address will at that point be sent to all the Internet of Things device for them to lock in with the contract instance. The gas limit for each exchange within the contract is set in this stage to protect from the attacks.
- **Deployment:** In this stage, IoT devices will connect, communicate and log into the server hub which conveyed the smart contract thereby getting enrolled. It is only the server that can authorize devices to induce enlisted or erased. Upon accepting affirmation from the server, an IoT node address will be enlisted and kept in the smart contract list of trusted devices. Whenever the server suspects a node to be malicious or it is required to be removed, it can call the erase function which will remove that specific node.

All Internet of Things devices within the IoT-Ethereum framework are able to be communicated with the smart contract to deploy a message. This message will be deployed and put away within the blockchain for recovery only if the Internet of Things device is granted access. The Internet of Things node is checked with the list of authorized addresses by the smart contract and is passed as a trusted device as expressed so within the contract [9]. If the node does not gain access, the

messages will be dropped and rendered void. The figure below shows the flow diagram of the IoT-Blockchain model.

The DDoS issue here is that a device is sending amazingly huge amount of data to over-burden a server and consume its assets. In the system framework, any of the devices may begin persistently sending data to the system and impact a DDoS attack.

Such attacks can be avoided with the gas limit trait of Ethereum because it guarantees no advanced assets can be devoured once the limit is surpassed [9]. Within the smart contract, there is a gas limit which acts as a component to anticipate the framework from over-burdening.

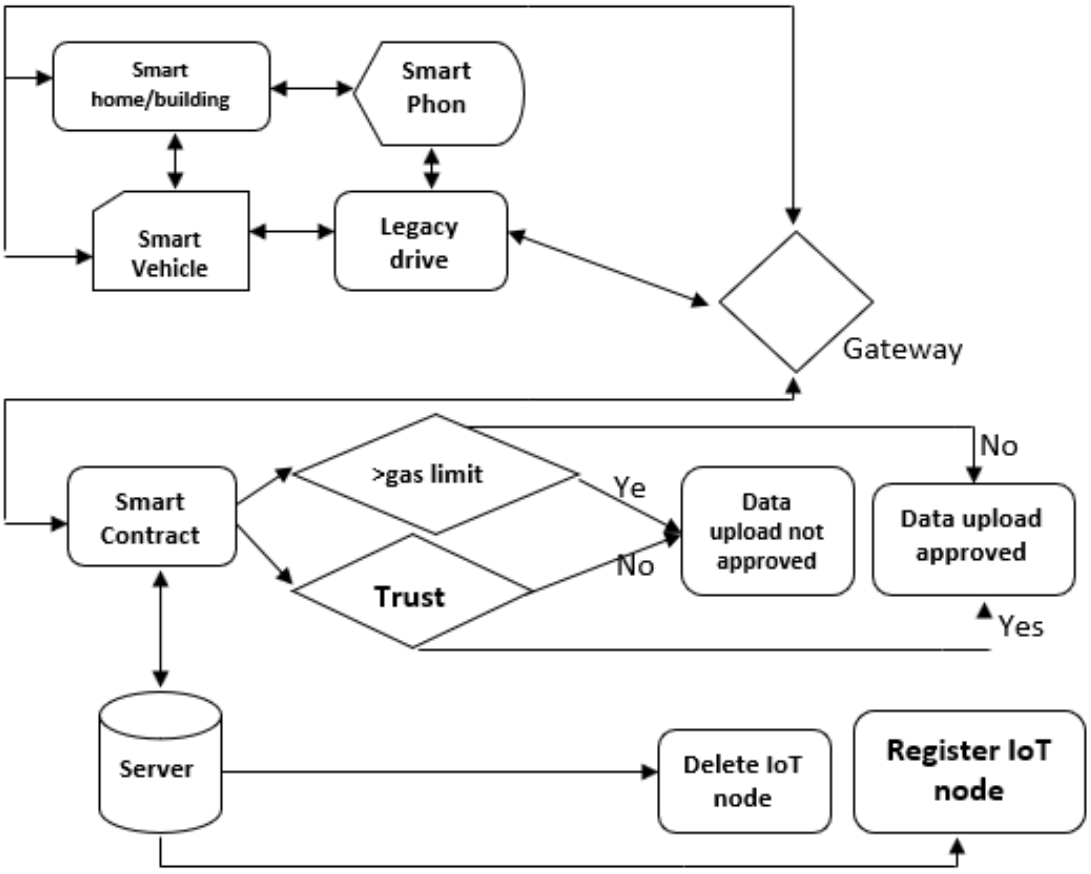

Figure 4: Flow Diagram of IoT-Blockchain Network [9].

CONCLUSION

This review presented Internet of Things (IoT) devices and how its security challenges which is mostly Distributed denial of service (DDoS) attacks to flood and overload the system and deny legitimate users access to their resources. The paper reviews literatures of other models and methods being applied to mitigate the security challenges of Internet of things (IoT) devices.

It takes a comprehensive review on blockchain being used as a mitigating tool where a platform known as Ethereum introduces smart contracts into the system and sets a gas limit for each IoT device so that whenever the attacker seeks to overload the server, the IoT device being used will reach its limit and then it drops.

REFERENCES

[1] Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In *2015 IEEE Symposium on Computers and Communication (ISCC)* (pp. 180-187). IEEE.

[2] Angrishi, K. (2017). Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. *arXiv preprint arXiv:1702.03681*

[3] Ahmed, M. E., Kim, H., & Park, M. (2017, October). Mitigating dns query-based ddos attacks with machine learning on software-defined networking. In *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)* (pp. 11-16). IEEE.

[4] Alsaadi, E., & Tubaishat, A. (2015). Internet of things: features, challenges, and vulnerabilities. *International Journal of Advanced Computer Science and Information Technology*, *4*(1), 1-13.

[5] Bhunia, S. S., & Gurusamy, M. (2017, November). Dynamic attack detection and mitigation in IoT using SDN. In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)* (pp. 1-6). IEEE

[6] Bertino, & Islam, N. (2017). Botnets and Internet of Things Security. *Computer*, *50*(2), 76-79. doi: 10.1109/mc.2017.62 (Bertino & Islam, 2017)

[7] Chahid, Y., Benabdellah, M., & Azizi, A. (2017, April). Internet of things security. In *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)* (pp. 1-6). IEEE.

[8] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*, *6*, 32979-33001.

[9] Javaid, U., Siang, A. K., Aman, M. N., & Sikdar, B. (2018, June). Mitigating IoT Device based DDoS Attacks using Blockchain. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems* (pp. 71-76). ACM.

[10] Kshetri, N. (2017). Can Blockchain Strengthen the Internet of Things? *IT Professional*, *19*(4), 68-72. doi: 10.1109/mitp.2017.3051335 (Kshetri, 2017)

[11] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

[12] Kuusijärvi, J., Savola, R., Savolainen, P., & Evesti, A. (2016, December). Mitigating IoT security threats with a trusted Network element. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 260-265). IEEE

[13] Lavrova, D., & Pechenkin, A. (2015). Applying correlation and regression analysis to detect security incidents in the internet of things. *International Journal of Communication Networks and Information Security*, *7*(3), 131.

[14] Misra, S., Krishna, P. V., Agarwal, H., Saxena, A., & Obaidat, M. S. (2011, October). A learning automata-based solution for preventing distributed denial of service in Internet of things. In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing* (pp. 114-122). IEEE.)

[15] Ma, Z., Feng, L., & Xu, F. (2018). Design and Analysis of a Distributed and Demand-based Backscatter MAC Protocol for Internet of Things Networks. *IEEE Internet Of Things Journal*, 1-1. doi: 10.1109/jiot.2018.2869015 (Ma, Feng & Xu, 2018)

[16] Mahlyanov, D. (2018). Internet of Things – A New Attack Vector for Hybrid Threats. *Information & Security: An International Journal*, *39*(2), 175-182. doi: 10.11610/isij.3915 (Mahlyanov, 2018)

[17] Oliveira, L. M., Rodrigues, J. J., de Sousa, A. F., & Lloret, J. (2013). Denial of service mitigation approach for IPv6-enabled smart object networks. *Concurrency and Computation: Practice and Experience*, *25*(1), 129-142.

[18] Rodrigues, B., Bocek, T., Lareida, A., Hausheer, D., Rafati, S., & Stiller, B. (2017, July). A blockchain-based architecture for collaborative DDoS mitigation with smart contracts. In *IFIP International Conference on Autonomous Infrastructure, Management and Security* (pp. 16-29). Springer, Cham.

[19] Razzaq, M. A., Qureshi, M. A., Gill, S. H., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): a comprehensive study. *International Journal of Advanced Computer Science and Applications*, *8*(6).

[20] SathishKumar, J., & R. Patel, D. (2014). A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computer Applications*, *90*(11), 20-26. doi: 10.5120/15764-4454 (SathishKumar & R. Patel, 2014)

[21] SIMPLE SERVICE DISCOVERY PROTOCOL BASED DISTRIBUTED REFLECTIVE DENIAL OF SERVICE ATTACK. (2017). *International Journal of Recent Trends in Engineering and Research*, *3*(12), 143-150. doi: 10.23883/ijrter.2017. 3549.zaf08 ("SIMPLE SERVICE DISCOVERY PROTOCOL BASED DISTRIBUTED REFLECTIVE DENIAL OF SERVICE ATTACK", 2017)

[23] Zlomislić, V., Fertalj, K., & Sruk, V. (2017). Denial of service attacks, defences and research challenges. *Cluster Computing*, *20*(1), 661-671.