IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN'S APPLICABILITY FOR MITIGATING ATTACKS

Mr. P. Thiruselvan, S. Rajalakshmi

Computer Science and Engineering,

P.S.R. Engineering college, Sivakasi, India.

Abstract: The Internet of Things (IoT) makes smart cities feasible all around the world. Smart homes, smart farming, smart climate, smart wellness, smart governance, and many more types of smart communities are all possible in today's world. The Internet of Things is also utilized in the petroleum, gas mining, and industrial industries. In the human world, IOT increases efficiency, optimizes pricing, optimizes human capital, retains forecasts, and addsa great deal of convenience to daily activities. With the participation of a huge number of different devices and the processing of enormous amounts of data, security concerns are becoming more prevalent. The lack of success of the Internet of Things is mostly due to security and privacy concerns. One of the most serious dangers is the possibility of a distributed denial of service (DDOS) assault. This study discusses the application of blockchain-based techniques to prevent distributed denial of service (DDOS) attacks in the internet of things. It gives a thorough examination of the existing blockchain-based architectures for dealing with distributed denial of service (DDOS) assaults.

Index terms - IoT, Blockchain, Smart Contract, DDOS, Threat, Attack, Mitigation

1. INTRODUCTION

Kevin Ashton [1] is the creator of the Internet of Things. The Internet of Things has, however, become a haven for nearly all applications in the previous decade, including home automation, intelligent healthcare, utility facilities, and smart transportation [2]. RFID technology (WLAN), Wi-Fi, Bluetooth, Internet technology, and intelligent computing (Artificial Intelligence), among other things, are key Internet of Things enabling technologies. WIC (Wise Intelligence Computing) technology is also featured. The Internet of Things (IoT) is a rapidly expanding network of internet sensors embedded in a variety of physical objects, or "things," that communicate with one another. Stuff may, of course, be any physical object on the planet thatcan be interacted with or on which a sensor can be embedded. This includes both living and nonliving things. Sensors are capable of performing a wide variety of computations. Things can be accessed over the Internet via wired or wireless connections. Objects may be anything, both living and inanimate, that needs physical existence to exist.

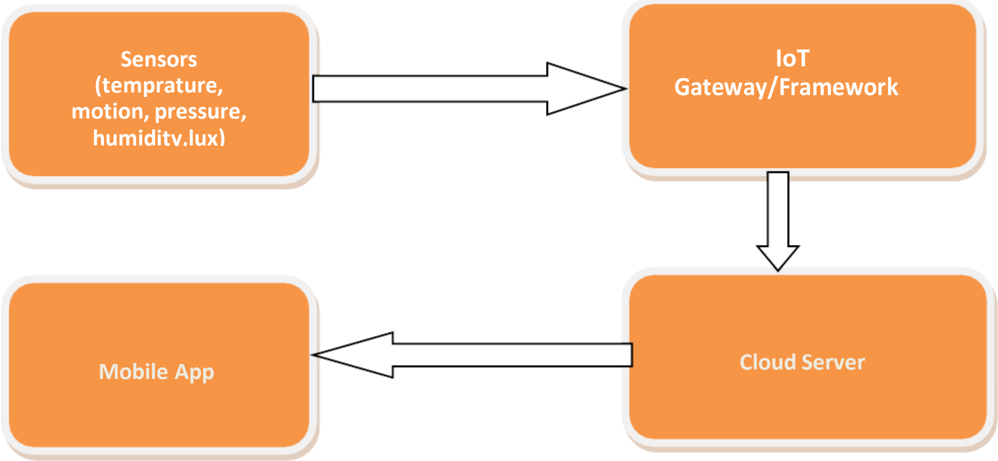

Fig. 1. IoT's Basic Building Blocks

As shown in the preceding figure 1, sensors are a large number of diodes that are equipped to detect natural physical boundaries such as temperature and pressure. Sensors are in charge of acquiring data from the environment. They have the capability of collecting data continually. Sensors are capable of recording a variety of data such as humidity, temperature, motion, and others. The Internet of Things platform is a middleware. There are several high-quality Internet of Things platforms available today, including Microsoft Azure IoT and AWA IoT. The actual data is kept on a cloud-based storage server. When data analytics apps are used in the cloud, theyare shared with stakeholders using mobile applications that are accessible from anywhere.

The lack of success of the Internet of Things is mostly due to security and privacy concerns. Oneof the most serious dangers is the possibility of a distributed denial of service (DDOS) assault. An internet distributed denial of service (DDoS) assault includes a large number of impacted systems targeting a single target, which results in the denial of service for the devices that are being attacked and their users being affected. In response to the overwhelming volume of incoming messages, the targeted device was forced to shut down, thereby denying genuine users access to the computer.

An open automated record that is decentralized handed on, and opened is known as a blockchain [3] [4][5]. It is used to record trades transversely over multiple PCs and is designed to prevent any included record from being balanced retrospectively, without the difference in all resulting blocks. Individuals are given the ability to confirm and audit deals on their own while being financially self-sufficient and tolerable. A blockchain database is freely monitored using a common framework and a time-venturing worker who is appropriately suited for the task. They are backed up by widespread collaboration that is fueled by a wide range of individual concerns. Individuals' weaknesses in terms of data security are pushed to the margins by such a structure, allowing for a more dynamic work environment. Because of the utilization of a blockchain, a propelled asset no longer has the normal requirement for unfathomable reproducibility.

[5] Blockchains are used to enhance the accounting and sharing of budgetary exchange data. Benefits include increased speed, less procedural cost, fewer trade errors, more general security, and a decentralized way of accounting and sharing of budgetary exchange data. This decentralized method eliminates the primary issue of framework dissatisfaction as well as the vulnerability to cyber assaults that existed previously. In virtual budgetary exchanges, the key rationale for utilizing blockchain technology is to ensure that each client's wallet is not only partially protected, but that the wallet is completely protected by storing the record of all transactions between clients in a blockchain. When it comes to developing solutions to prevent distributed denial of service attacks, blockchain is essential.

I. RELATED WORK

According to Arsalon Mohsen Nia et al., 2016[6, possible attacks and flaws are thoroughly examined from the inside out. In 2014 [7], Mohamed Abomhara et al. discussed the security risks and problems associated with the Internet of Things. They also pointed out that there are four interrelated parts, namely persons, articles, equipment, and software, which communicate with one another through an untrustworthy private network. Cart Das et al., 2016 [8] provided anin-depth and inside-out examination of potential challenges in the Internet of Things.

Salim ELBOUANANI [9] has shown that, at present, no standard or solution addresses all security concerns in the context of the Internet of Things. They discovered that in the Internet of Things, confirmation is a legitimate test. According to Krishna Kanth Gupta et al., 2016 [10], there will be 25 billion Internet of Things (IoT) devices by 2020. They also acknowledged that there were issues with the Internet of Things. A study conducted by Gurpreet Singh Matharu et al. (2014 [11]) revealed that interoperability, standardization, and security are the three areas thatrequire further investigation for the network of things to develop.

Hui Suo et al., 2012 [12] developed an encryption-based technique to improve the security characteristics of Internet of Things systems.

When C. Flügel and colleagues [13] investigated some of the particular causes that need to be fought to create such a system, they found that L. Atzori and colleagues (2012) [14] advocated for the use of IoT in social media platforms.

IEEE range 2014 [15] recognized Java as a leading design tool for the Internet of Things (IoT) applications. The World Financial Gathering's Modern Web Overview, 2014 [16] helped participants get a better understanding of the remarkable opportunities and new risks that have emerged from the Industrial Internet. Air pockets of trust, as described by Hammi et al.,2018 [17], is a novel decentralized architecture that ensures that devices may be verified and verified with powerful recognized evidence of ownership. The authors of [18][19][20] presented a varietyof blockchain-based solutions for the Internet of Things environment.

For safe IoT circumstances, Javaid et al., 2018 [21] [22] presented a PUF and blockchain-based arrangement called BlockPro for information provenance and information respectability, whichis based on a PUF and blockchain.

In their paper, M. Anwer et al.,2020 [23] suggested a course of action for several masters' methods of the Blockchain to perform IoT checks, as well as a discussion about their limits.

Various security hazards in encryption algorithms used for different Internet of Things solutions were highlighted by the authors in [24][25][26]. Arbitrary number generators have always been seen as a significant source of vulnerability [27],[28],[29]. The new PRNG algorithm was developed by Stephen Checkoway and colleagues in 2014 [30] [31]. It was really quick.

Yu et al., 2015 [32] provided a variety of well-known weak devices to deal with DDOS attack scenarios. Zhang et al.,2015 [33] demonstrated a notable viewpoint in the IoT environment, which was supported by several authorities.

The authors of [37][35] carried out a comprehensive investigation of the underpowered Internet of Things devices, which included thousands of fascinating contraptions. A significant number ofthem were blatantly accessible using Internet-based approaches that did not necessitate the production of unmistakable evidence.

This document [36] provides a high-level overview of the guts and bolts of Machine Learning, aswell as the standards and computations that are used. Submissions. After a more in-depthmachine definition study, we will consolidate different forms of learning, including controlled and uncontrolled methods of instruction, as well as profound learning Perfect standards of instruction. In the remainder of the article, we'll look at the use of machine learning algorithms ina variety of fields, such as design recognition, sensor systems, anomaly detection, the Internet of Things (IoT), and health monitoring and assessment.

[37] describes a method that integrates the Internet of Things (IoT) with certain commonly used artificial intelligence computations to create a predictive model that may be used to assess the inside temperature of intelligent constructions. This predictive model was created to increase the usefulness of a completely new

dataset by employing an online learning system. To validate the technique, the article conducts a Machine Learning-based test using real-world sensor data that has been captured. The article after that proposes that the accompanying process be included inan Internet of Things architecture that is based on Edge Computing to enable the structure to operate in an energy-efficient manner.

II. RESEARCH DIFFICULTIES IN THE IOT

During the literature review, the following gaps were discovered:

- It was discovered that authentication is a significant problem in the Internet of Things. The reason for this is that there is no adequate authentication infrastructure available in the Internet of Things [9].
- The distribution of keys presents additional difficulty [9].
- The most common source of concern for most industries is security [16].
- Because of the design of the building, men in the middle assaults are a significant concern [20].
- Distributed denial-of-service (DDOS) attacks are also a significant issue with IoT networks. However, there is no such thing as a universal mitigation plan [21].
- Vulnerability in the Internet of Things devices is a serious problem. It is necessary to classify and forecast [32] the situation. A vulnerable device poses a danger to the Internetof Things network. Identification of such devices is necessary [35].

III. MITIGATION OF DDoS ATTACKS WITH THE USE OF BLOCKCHAIN

Part of this section's content is a critical examination of the blockchain-based designs that are now available for mitigating distributed denial of service attacks.

CloudFlare's services have benefited from Wikipedia's assistance in defending themselves against attacks. This strategy is effective since Cloudflare has a wealth of experience in dealing with these types of assaults. This is an exciting moment to be involved with online encyclopedias. Spamhaus, for example, was protected in March 2013 with the use of CloudFlare's services. Furthermore, in August 2015, a distributed denial of service (DDoS) attack using the hijacking of insufficient web browsers was launched against CloudFlare Client GitHub (an online coding site).

On the 28th of February, 2018, the most devastating of these was made public. This threat was neutralized thanks to the prolific DDoS service from Akamai. Akamai has made significant investments in DDoS protection. It comprises seven scrubbing centers and 150 personnel who are all dedicated to the battle against distributed denial of service (DDoS) assaults. Accordingly,it will require a significant amount of cash, work, and time to be successful. Even though there are a large number of Memcached servers (about 50 000), such attacks are still possible [39].

In October 2016, a distributed denial of service (DDoS) attack was launched via Botnets, affecting a large number of Internet of Things (IoT) devices [40].

A small number of typical DDoS assaults are directed at the railways' transportation networks. During an assault by a distributed denial-of-service (DDoS) network in Sweden in October 2017, the service was delayed, the IT system that records the position of trains was crashed, andthe corresponding email networks, websites, and traffic maps were all dismantled.

Rodrigues and colleagues [41] proposed a shared distributed denial-of-service mitigation blockchain architecture for smart contracts. This is exactly what we're doing. DDoS mitigationis provided by the architecture through the use of several independent machine-managed network domains (ASes). A distributed Ethereum-based blockchain is what this architecture is referred to as. In blockchain technology, intelligent contracts are used to report IP addresses thathave been defined in white or black across a variety of categories. As a result, a transaction is created by inserting an IP address into a block on a blockchain.

According to network rules, the IP address with a black list flow halted or an IP address with a white list relocated would be the one to be used. This design makes it feasible to link IP addresses to the shared blockchain in groups, which is useful for scalability. Instead of exchanging attack information via message, attachments between different sections of theinfrastructure, such as between ASes and consumers, are transferred using blockchain technology. Each block in Ethereum is generated every 14 seconds, which is a very fast rate. Asa result, the block/allow addresses will be sent to the relevant ASes throughout this period.

Flow rules are configured and applied by the individual ASes using Software Specified Networking (SDN) to prevent DDoS assaults from taking place. Different ASes (domains) differ from one another in terms of their security policy and DDoS threat countermeasures against DDoS attacks (domains). The target server is protected while the DDoS assault is being carried out by filtering the attack traffic on its ASN while the attack is being carried out. Attack traffic is likewise filtered in other ASes following the flow regulations that have been established. As a result, a DDoS assault from a nearby source is mitigated. The combination of SDN and blockchain technology provides a scalable and robust DDoS mitigation solution.

The primary advantage of this design, on the other hand, is that it may be utilized in conjunctionwith existing defensive mechanisms as an external security tool. The proposed architecture is rudimentary and provides only the bare minimum in terms of DDoS mitigation. The developers have not provided details on implementation and evaluation, and a significant amount of work has to be completed.

A decentralized blockchain is employed, which can result in increased data flow (transactions)

being an issue for scalability, and the authors propose to reduce the space-spread bloom filter, although this is not a serious worry. What method will be used to authenticate a node that records an attack? How can I be confident that other components of the transaction will not attempt to steal information? It is not adequately developed; (c) IP blocking is only possible for static IP addresses; and (d) cooperative domain justice is an issue, since a single domain may beable to employ a higher number of other domain services than those provided by DDoS assaults.

The authors of Javaid et al [21] suggest an IoT built-in blockchain architecture to reduce the number of IoT device-based attacks. The Ethereum blockchain of intelligent contracts is being employed in the construction of the building. The Internet of Things devices must first be registered with the registry to be able to transmit and receive messages. An Internet of Things system can only operate up to the gas threshold above the gas threshold and no further. A servercan deregister or remove any Internet of Things system that has a network failure or a gas cap that has expired at any moment. The server is also responsible for the development and recording of the smart contract.

When a contract address is registered, the server extends that address to all network IoT devices.An Internet of Things machine connected to a server is on the trusted list for the transaction. It is determined at the initialization of smart contracts [21] how much gas will be allocated for each contract transaction to guard against DDoS assaults.

The intelligent contract (a software component) serves as the primary regulator for all Internet of Things devices participating in the transaction. It not only allows the usage of Internet of Things devices, but it also limits their use to a certain quantity of gasoline. In this design, gateways are used to link the Internet of Things devices.

A smart contract makes contact with an IoT computer to transmit a message. An Internet of Things system will only operate up to the amount of gas that has been allotted to it when the server is registered. This limit is set following the bandwidth and resource specifications of the IoT device. In this design, every transaction and procedure has a gas cap associated with it.

Probably the most significant advantage of this approach is that the decentralized blockchain with a PoW consensus system possesses the strength and confidence of the Ethereus cryptocurrency. The failure of a single node has little impact on the overall operation of the system. The use of distributed estimating decreases the load on servers in an effective manner. To provide DDoS defense, each system's architecture is limited to the amount of gas it can hold.Another advantage is that no hardware update is required on an IoT device, (b) an overlay network over the present conventional network may be integrated into the design, and (c) both the solution identified and the solution functions for prevention can be implemented in the architecture. This design, on the other hand, feeds a trustworthy contract list that is evaluated whenever a new message is issued by a system or whenever communication between devices occurs. As a result, there are still issues with scalability using this technique.

During the registration process, there is no discussion of how to trust an IoT device that has been registered with the registry. The method through which a server will determine the current gas/resource need for the IoT node stays unambiguous. If an attacker can identify distinct Internet of Things addresses, the trusted smart deal list may include those addresses.

For reducing DDoS assaults carried out by IoT devices utilizing trust list traffic management architecture, Kataoka et al [42] propose this design, which makes use of blockchain technologies integrated into SDN technology.

There are three major components to it: Internet of Things/device applications; Internet of Things/edge networks; and Internet of Things/gateway/-validators. Contact is only possible in this architecture if the communication devices/servers are confident in their ability to communicate. Using the trust list principle, it is possible to distinguish between trustworthy and untrustworthy devices. In its most basic form, Trust List is a data structure via which the network distributes "application profiles" and "application profiles."

DDoS assaults on the edge network might result in malicious traffic being stopped and filtered by the SDN switch on the network. The SDN controller guarantees that the blockchain environment is synergistic and that the blockchain provides access to information about trustworthy resources and computers. IoT servers, gateways, and validators keep track of the information about "trusted services and devices." The SDN controller also offers flow rules for screening or approving Internet of Things traffic on the SDN switches, which are controlled by the SDN controller.

This design included the implementation of a new computer known as a validator. It is the responsibility of an authentication protocol to verify the legitimacy of an IoT device. The trusted user profile is also transferred to the IoT device through the use of blockchain technology and reliable service information. As a result, the first Internet of Things system is reliable for communication. Following this, the registry's contact information is provided in casethere is any additional interaction. This design may be utilized in conjunction with a variety of additional criteria, including system location, ownership, user license, and other factors, among others. In terms of application and device profiles, the architecture is adaptable.

In this study, a practical implementation model for an open-source technology blockchain and confidence list is shown.

(a) A significant amount of time has elapsed before the monitoring is performed. It aids in thedetection of anomalies.

(b) Measurements of avoidance and response; et cetera

(c) The traffic generated by DDoS attacks are restricted to edge networks. There are just a fewdownsides to this type of architecture:

1. The confidence list for the architecture is not encrypted/in plain text, and as a result, it willraise security concerns on a public blockchain.

2. The increase in the size of the secret list translates into greater processing expenses forblockchain technology.

3. There is just an indication of a definition in this case. It is necessary to conduct an additional study into its practical use.

4. In the case of public blockchains, there is a privacy problem.

5. In such cases, the attacker must constantly examine and update the confidence list while alsogaining access to the network by circumventing the restrictions.

6. As a result of the use of intermediary blockchains, SDNs, and validators, there are variousdelays required before a system can interact successfully.

IV. CONCLUSION:

A distributed denial-of-service (DDOS) assault is catastrophic. It stops legitimate users from accessing web-based services. When this type of event occurs, the Internet of Things system has a communication breakdown. Although there are blockchain-based techniques available toprevent DDOS attacks, they are not widely used. Blockchain technology ensures the authenticity, integrity, and dependability of transactions. This article has shed light on all of the contemporary blockchain-based methods for mitigating distributed denial of service attacks. It isthe purpose of this article to give a critical examination of a blockchain-based mitigation approach. Following this thorough examination, it is discovered that there is still more work to be done in the area of blockchain-based approaches. The concerns of scalability and cost are two of the most pressing ones that must be addressed.

REFERECES:

[1] Raghuvanshi, A., & Singh, U. (2020). Internet of Things for smart cities- security issues andchallenges. Materials Today: Proceedings. DOI: 10.1016/j.matpr.2020.10.849

[2] Birje M.N, Bulla C.M, "Cloud Monitoring System: Basics, Phases and Challenges," IJRTE, vol. 8, no. 3, pp. 4732–4746, Sep. 2019, DOI: 10.35940/ijrte.C6857.098319,

[3] Chetan M. Bulla & Mahantesh N. Birje, 2021. "A Multi-Agent-Based Data Collection and Aggregation Model for Fog-Enabled Cloud Monitoring," International Journal of Cloud Applications and Computing (IJCAC), IGI Global, vol. 11(1), pages 73-92, January

[4]Siddiqui S.T., Ahmad R., Shuaib M., Alam S. (2020) Blockchain Security Threats, Attacks and Countermeasures. In: Hu YC., Tiwari S., Trivedi M., Mishra K. (eds) Ambient Communications and Computer Systems. Advances in Intelligent Systems and Computing, vol 1097. Springer, Singapore. https://doi.org/10.1007/978-981-15-1518-7_5

[5] Shuaib, M., Daud, S., Alam, S. and Khan, W., 2020. Blockchain-based framework for the secure and reliable land registry system. TELKOMNIKA (Telecommunication Computing Electronics and Control), 18(5), p.2560.

[6] Arsalan Mohsen Nia, Niraj K. Jha, Fellow, "A Comprehensive Study of Security of Internet of Things", IEEE Transactions on Emerging Topics in Computing, 2016.

[7] Mohamed Abomhara, Geir M. Køien, "Security and Privacy in the Internet of Things: Current Status and Open Issues", IEEE Conference on Privacy and Security in Mobile Systems (PRISMS), 2014.

[8] Dolly Das, Bobby Sharma, “General Survey on Security Issues on Internet of Things”, International Journal of Computer Applications”, vol 139, pp. 23-29, 2016.

[9] Salim ELBOUANANI, My Ahmed EL KIRAM, “Introduction To The Internet Of Things Security Standardization and research challenges”, 11th International Conference on InformationAssurance and Security, IEEE, pp 32-37, 2015.

[10] Krishna Kanth Gupta, Sapna Shukla, “Internet of Things: Security Challenges for Next Generation Networks”, 1st International Conference on Innovation and Challenges in Cyber Security, IEEE, pp. 315-318, 2016.