International Journal of Management (IJM)
Volume 13, Issue 12, December 2022, pp. 11-25, Article ID: IJM_13_12_003
Available online at https://iaeme.com/Home/issue/IJM?Volume=13&Issue=12
ISSN Print: 0976-6502 and ISSN Online: 0976-6510
DOI: https://doi.org/10.17605/OSF.IO/T56J7

A SURVEY ON BLOCKCHAIN BASED DDOS ATTACK FOR IOT DEPEND ON SOFTWARE DEFINED NETWORKING

Shraddha Joshi
Ph.D. Scholar, Gujarat Technological University, Gujarat, India

Dr. Vikram Agrawal
Assistant Professor, Bhailalbhai & Bhikhabhai Institute of Technology,
Gujarat Technological University, Gujarat, India

ABSTRACT

Internet of Things (IoT) is based on the integration of several processes, like networking, sensing, identification, and computation. Billions of Internet-of-Things (IoT) devices are connected to make available creative ubiquitous services and simplify our everyday tasks (e.g., smart healthcare, smart homes). The effect of Distributed Denial-of-Service (DDoS) attacks is expanding as the number of vulnerable IoT devices. It continues to increase New technologies, such as Blockchain and SDN, creates new possibilities for reliable, cost-effective, scalable, and efficient DDoS attacks to work together in the IoT world. In this paper software-defined DDoS attack affects the online transaction in the Blockchain. Decentralized payments, wealth management, healthcare, and cloud computing, among other applications, have all benefited from blockchain technology. The various types of DDOS attacks in the IoT are identified and defined in this survey. For the first time, we present an extensive and systematic study on the use of blockchain technology in the Internet of Things and explore the advantages of SDN in this paper. Finally, some critical concerns and research problems were addressed in this paper.

Keywords: IoT, DDoS attack, Blockchain, Software Defined Networking (SDN)

Cite this Article: Shraddha Joshi and Dr. Vikram Agrawal, A Survey on Blockchain Based DDOS Attack for IOT Depend on Software Defined Networking, International Journal of Management (IJM), 13(12), 2022, pp. 11-25.
https://iaeme.com/Home/issue/IJM?Volume=13&Issue=12

1. INTRODUCTION

Internet of Things (IoT) is a network of interconnected smart devices, mechanical and digital, things, animals, and people with unique identification and the right to share without data needing human-to-human or human-to-computer interaction are shown in fig 1.

Smart city technologies based on the Internet of Things include smart security, completely automated transportation, smart energy management, water distribution, urban protection, and environmental management. Low-control radios are used to connect to the internet to decrease the impact of such devices based on the environment and energy consumption. Low-control radios do not use WiFi or existing cell arrangement technologies. IoT needs higher-request figuring devices to perform at higher level-duty tasks; it isn't simply made up of plugged-in devices and sensors. Sensors need a small gadget structure factor, which limits their preparation, memory, and communication capabilities. These are the characteristicsofIoT.

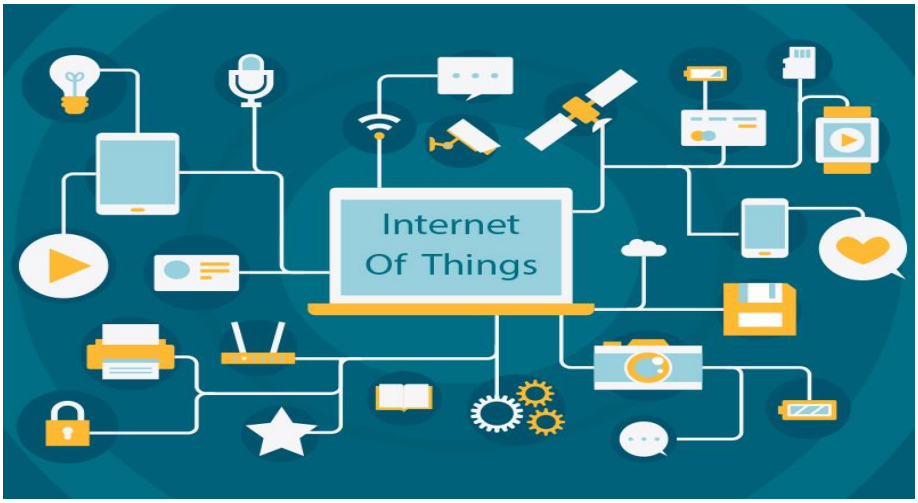

Figure 1: Internet of Things (IoT)

Different security services are required for the Internet of Things [1].

1) **Confidentiality**: An attacker could easily intercept a response as it travels from source to destination, and the information could be compromised. As a result, the response should be hidden from all relay nodes, implying that response security is needed in IoT. The same can be said for device storage. An encryption/decryption process is an easy solution to this issue.
2) **Integrity:** The message should not change as it travels from source to destination; it should be obtained exactly as it was sent. While the message is being passed or stored on the device, no intermediary can alter the content of the message.
3) **Availability:** It is also critical that the devices' services are still accessible and in working mode for IoT to continue working and access to data as required. To ensure availability, it is therefore critical to detect and prevent intrusion.
4) **Authenticity:** End-users can verify each other's identities to ensure that they're dealing with the same organizations.

2. ARCHITECTURE OF IOT

Initially, IoT Architecture was three- layers. Due to IoT improvement, the design of three-layers cannot fulfill the whole structure of applications, so some researchers support the four-layer design. IoT is divided into the main three layers: Application Layer, the Network Layer, and the Perception Layer.

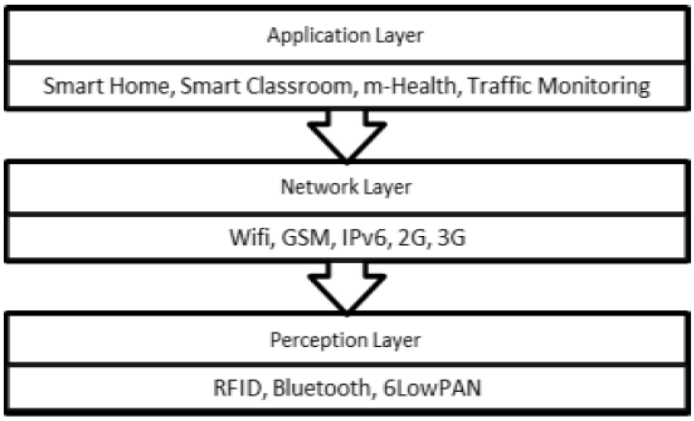

Figure 2 ARCHITECTURE OF IOT

2.1. IOT THREE LAYER ARCHITECTURE

1. PERCEPTION LAYER:

The perception layer gathers all data and information from the physical world, such as temperature, speed, time, humidity, etc. It is nothing more than a set of sensors and actuators that make up a Wireless Sensor Network (WSN).

2. NETWORK LAYER:

The Network Layer is a middle layer that handles data/information transmission, data broadcasting, data aggregates, etc.

3. APPLICATION LAYER:

The topmost layer is the application layer that contains user-facing logic in industry, algorithms, and UI. It isn't easy to supply specific solutions for all attainable applications.

(i) An application must give a state of operation indication.
(ii) The system ought to be automatic, which will be close up or replace harm nodes.

2.2. FOUR LAYER ARCHITECTURE IN IOT (SUPPORT LAYER)

Three-Layer design cannot fulfill all the needs. Thus, an advanced design called a four-layer design was developed with an added layer called the Support Layer. As compared to a three-layer design, it's safer.

Three-layer architecture: Information has been directly sent to the network layer. There's a chance of attacks increase, attempt to avoid the possibility of threat new layer called support layer developed with two approaches.

(i) It checks and verifies whether the knowledge has been sent from demonstrating user or not.
(ii) It will send information to the next layer, i.e., network layer by victimization wired or wireless network.

3. APPLICATION OF IOT

IoT does not have any values without applications. Emerging the IoT application is possible through the efficient interaction of device to device or human to device communication. An autonomous device to device application has performed monitor the environment; indicate the problem, deciding without human interaction with dynamic interaction.

There are many types of application has been used in IoT. They are smart cities, cloud computing, machine learning, embedded systems are the application of IoT.

3.1. SMART CITIES

The right one will combine, process, and interpret the data that smart devices generate and ensure that the infrastructure is to take these cities into the new epoch of connectivity [36]. The concept of the smart city poses service management (e.g., waste management, transport, lighting, energy), control of pollution and CO2 emissions, urban planning, traffic management, and so on [2], [3]. Cars, traffic flow, seeking better roads, and smart parking are also part of the transportation applications. The building field focuses on technologies that automate building-related services such as safety and home automation, public building security, and infrastructure monitoring [4]. Moreover, the environmental-based application has attention on monitoring of air pollution, climate and noise.

3.2. CLOUD COMPUTING

Cloud computing is the use of the internet to provide computing, storage, utilities, and applications. In general, primary software and hardware levels are needed to make smartphones that are both energy-efficient and capable of processing data. This necessitates collaboration between designers and manufacturers [5]. Mobile cloud computing is characterized as combining cloud services and mobile devices to increase the computational capacity, memory, storage, energy, and context awareness of mobile devices. Interdisciplinary research has resulted in mobile cloud computing technology that combines mobile computing and cloud computing. As a result, this multidisciplinary area is also known as mobile cloud computing [33].

4. SECURITY IN IOT

When any computer is linked to the system, the protection of the IoT system is considered insecure, and there is a chance that many attackers can gain access. This phenomenon can be observed even with a single small unit. Indeed, there are significant risks in IoT systems, which arise primarily during data transfer, device access, and device connectivity. As a result, it is critical to secure IoT devices and services from unauthorized access to external devices to ensure protection. Furthermore, the numerous facilities, physical hardware, and information present in the transition and storage must be secured. As mentioned below, there are three significant concerns about the protection of IoT services and devices.

- Data security
- Privacy
- Trust.

Data security is also a major concern when it comes to IoT devices and services. It is stated that the primary goal of the IoT framework is to determine safe data and approved objects for the user. When dealing with security problems in IoT systems, there are probably two things to keep in mind. These are the methods for (1) access control and authorization, (2) authentication, and identity management (IdM). Besides, the IoT device verifies an individual to ensure that the person is allowed to access a service. The authorization mechanism aims to determine whether an individual or computer is eligible to receive a service. The access control process determines whether the requested service is granted or refused based on a broad range of parameters. Indeed, it is critical to developing authorization and access control within these systems to provide a safe connection between the various devices and services. Different access control rules can be used to generate, recognize, and manipulate scenarios.

Furthermore, as authentication and identity management are combined, a new feature is introduced since multiple users, objects, and devices must be authenticated using trusted services. Without confusion, a safe process is needed for this reason, as it is a significant problem that must have addressed.

Moreover, privacy is a big concern to remember when it comes to IoT devices and services. The objects in the IoT system are explicitly related, and data is transmitted over the internet. As a result, due care must be taken to protect the privacy of users. Perhaps this is why information sharing and management and data protection within the collected data are relevant to research domains. Unpredictable Behavior, System Similarity, Unstable Long Device Life, Deployment and Discontinued Support, No Update Support, Weak or No Visibility, Vulnerability Disclosure, Risks are some of the other security issues that occur in the IoT.

5. ATTACK ON DISTRIBUTED DENIAL OF SERVICE (DDOS)

The Internet of Things (IoT) world is made up of sensitive and interconnected devices, sensors, software, infrastructure, and much more. Many IoT modules are made up of low-cost generic hardware components. They're also planned and implemented with a lower level of protection. As a result, attackers can easily access and attack a single target using compromised IoT devices by hacking those devices or IoT servers, as shown in Figure 3.

Most of the Hub's firmware is publicly available. An attacker can easily download the firmware to analyze and revise the firmware. [6] Therefore they can use exploitation to get the root password. Most often, root password uses encryption. But nowadays, decrypting the hash is so accessible from available online hash crackers or brute force attacks. For hub control, the attacker needs to get remote control access. The attacker can trick and get the device identifier or device number using HTTP SYN from the config.jar file. Similarly, downloading an archive can also be done using that device identifier in the same manner. [7] There are many other ways to hack IoT servers or devices, such as malware attacks, hijacking a server, social engineering, using Metasploit payloads, spoofing, cloning, middle man attack, and many more attacks.

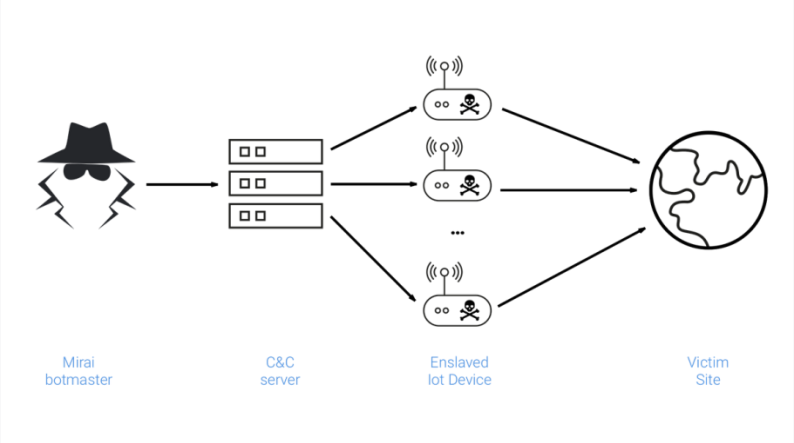

Figure: 3 Attack on Distributed Denial Of Service (DDoS)

Hackers got their communication channel known as the Dark web. There they can get a wide range of illegal scripts and source code, and software. For example, a white hat malware research gap named MalwareMustDie openly released the Mirai in August 2016. The Mirai malware searches for vulnerable IoT devices in general. Vulnerabilities such as whether they are either using their factory-issued or default password. From that, the malware can rope them into a zombie's network, and that can also be used to launch a DDoS attack, just like fig. A wide range of IoT devices got infected, and till now, it has taken down many internet giants like Twitter, Amazon, PayPal, and many more.

6. CLASSIFICATION OF DDOS ATTACK

Different forms of DDoS attacks work in a networked world to disrupt a website's operations in today's world. They are SYN flooding, ICMP flooding, UDP flooding, and domain name server amplification attacks.

A) SYN Flooding

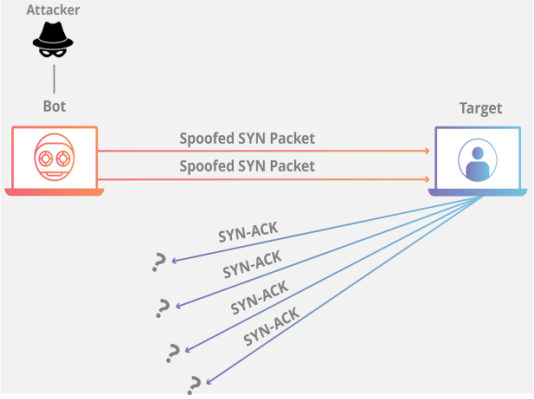

Figure: 4 SYN Flooding Attack

SYN Flooding is a form of DDoS attack that exploits TCP vulnerabilities. The attacker sends SYN packets to the target host's ports-state of 'Listening. [8] It usually includes the real host's source address, but it does not depict the real host's source address during the attack. When the host sends SYN packets to the target, it responds by sending SYN/ACK packets and then waits for the host to respond with an ACK to complete the communication phase. Since the attacker's source address in the SYN packet is invalid, the goal will never be to receive an ACK, and the attack ports will have to hold off until the link times out.

B) ICMP Flooding

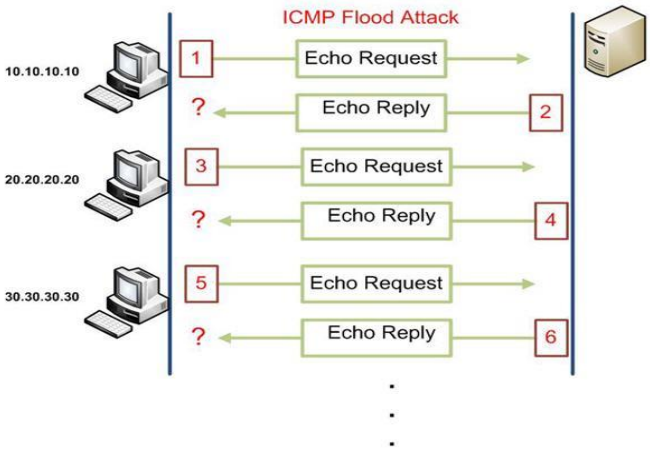

Figure: 5 ICMP Flooding Attack

ICMP flooding causes network interface configuration errors. The attacker consigns an immense number of ICMP packets with a bogus return address to the server not to have the time to retort to other servers. The data is not exchanged between the systems. The attacker installs on the master machine a controller program (Trojan horse) and then instructs the slave machine on how to propagate the attack to the victim.

C) UDP Flooding

The User Datagram Protocol (UDP) is a network protocol that does not require a link or a session, is used in this form of DDoS attack. It doesn't connect a three-way handshake like TCP, and it has lower over the head, so it can be gotten rid of with just a few resources. In this attack, the attacker floods the targeted host's arbitrary ports with IP packets that carry the UDP datagram. The receiving host examines these datagrams for applications; if none are found, it receives an ICMP destination unreachable packet as a response. DNS amplification attacks can be combined with UDP flooding attacks. Botnet clusters of different sizes can emit both amplified and non-amplified UDP. There are no commercially available software packages to carry out a UDP Flood attack (ex. UDP Unicorn).

D) DOMAIN NAME SERVER (DNS) AMPLIFICATION ATTACK

Attackers use free DNS resolvers in DNS amplification attacks. They submit these resolvers requests for DNS lookups with a spoof source address. When the DNS resolver receives these packets, it sends a DNS record answer to the target device rather than the attacker's device. The domain is the only part of the answer, usually much larger than the query [9]. For a domain, there are several different records of knowledge that may be included in a response.

7. CHALLENGES

Business feuds: – Businesses can use DDoS attacks to strategically bring down rival websites, such as to prevent them from performing in a significant occurrence like Cyber Monday.

Boredom:– Boredom Cyber vandals, also referred to as "script-kiddies," initiate DDoS attacks using short written scripts. These attacks are usually carried out by bored would-be attackers searching for a blast of adrenaline.

Extortion: Perpetrators extort money from their targets by using DDoS attacks or the threat of DDoS attacks.

Cyberwarfare: – DDoS attacks sanctioned by the government may be used to cripple opposition websites as well as an enemy country's infrastructure.

The DDoS attack has been divided into two methods.

(i) Reflection: In this method, the attacker tries to send packets to different target addresses, so the actual target address has not received data.

(ii) Amplification: There are a lot of packets are sent to the victim's machine.

Both attacks occurred due to the weakness in TCP/IP protocol using different types of attacks, likewise TCP Syn Flood, UDP Flood, IMP flood, and others.

8. DDOS ATTACKS IN ONLINE TRANSACTION

The major issues addressed by blockchain technology are discussed in this segment. The SDN architecture was created to reduce the significant effect of Distributed Denial-of-Service (DDoS) attacks. The Blockchain is structured following several transactions. Any invalid transactions that join the blockchain network are discarded by the peers connected to it. For security provisioning, IoT using Blockchain is guaranteed. Our research is focused on DDoS attack affects the online transaction in a blockchain-based software-defined network (SDN).

8.1. SOFTWARE DEFINED DDOS ATTACK

The majority of existing DDoS attacks, avoidance and mitigation techniques in an IoT network are implemented directly on the Internet of Things [10]. Such IoT DDoS defense techniques are resource-intensive and can disable the Internet of Things (IoT) network in the event of large-scale DDoS attacks, such as those that have surfaced lately.

In the IoT, it is possible to use centralized control to improve the DDoS process. The amount of traffic originating from and departing from the Internet of Things was analyzed using an SDN-based method. The traffic is routed via a switch that supports SDN. To begin with, the majority of packets sent as a result of a DDoS attack are created using a computer program process. As a result, in milliseconds script, the speed at which an attacker sends a DDoS packet is currently constant and relatively smooth.

An attack script generates the Attack packet. If a match is found, then there is no probability of attack, but if there isn't a suitable match found in the SD-IoT table, then the SD-IoT switch will compress the packet SD-IoT, there is a controller pool.

Table 1: Comparison of DDoS Attacks Defense Mechanisms Using SDN

References	Contribution	Merits	Demerits
Azka Wani et al. [11]	the effect of DDoS attacks in IoT is discussed, as well as an SDN-based approach for detecting and mitigating DDoS	Robust and flexible security	security and privacy issues
Jianjun et al. [12]	an SDN setting, a fast and lightweight protection strategy against DDoS attacks on IoT devices.	Discount factor and weight factor	Less realistic states
Jalal Bhayo et al. [13]	For the SD-IoT network, a DDoS attack detection solution is available that is dynamic and programmable.	Network throughput and memory utilization	Different attacks and irregularities, which are crucial issues for IoT.
Suman et.al [14]	machine learning to achieve dynamic detection methods of IoT traffic for early detection of IoT attacks.	High precision	IoT security problem
Zhuo Chen et.al [15]	XGBoost Classifier detection tool in an SDN-based cloud.	Higher precision, a lower false-positive rate, and is faster and more scalable.	Evaluation of security techniques is complex.
Yi-Wen Chen et al. [16]	prevent DDoS attacks in IoT gateways, a multi-layer DDoS detection system based on machine learning	high accuracy DDoSattack detection in the natural IoT environment.	a severe problem in network security
Marcos et.al [17]	An online protection scheme protects DDoS and Port Scans attacks.	restoring the SDN to average service	impact over legitimate users
Shi et.al [18]	detect DDoS attacks in SDN	achieved higher detection rates	improving the algorithm so that it can be used in a real-world SDN environment.
Nagarathna et.al [19]	Learning-driven detection mitigation (LEDEM) is a DDoS detection system.	High accuracy rate, increase the throughput	Detection accuracy should be improved.
Da et.al [20]	DDoS attacks are detected and minimized using an SDx algorithm.	SDx algorithm is fast and effective at handling and mitigating DDoS attacks.	Improve the efficient algorithm
Yang et.al [21]	the SDN architecture, which uses machine learning to identify and protect against DDOS attacks.	KDD99 dataset shows the effectiveness.	improve the flow table delivery model
Yao Yu et al. [22]	DDOS attack based on open source fuzzy logic controller in SDN.	Reduce time delay	Improve the network

Azka et al. [11] obtained the effect of DDoS attacks in IoT is discussed, as well as a novel SDN-based approach for DDoS attack detecting and mitigating. Software-defined network (SDN) is a modular approach to network operation and supervision that separates control and data planes. The major drawback is security and privacy issue.

Jianjun et al. [12] obtained an SDN setting, a fast and lightweight protecting IoT devices from DDoS attacks. The discounted factor and incentive weighing scale can also be modified, according to the simulation results. Less realistic states are a major drawback.

Jalal et al. presented [13] the SD-IoT network, a DDoS attack detection solution is available that is dynamic and programmable. The outperform demonstrates that the SD-IoT system detects the attack quickly and effectively, reducing attack detection time—different attacks and irregularities, crucial issues for IoT.

Suman et al. [14] used machine learning to achieve dynamic detection methods of IoT traffic to detect IoT attacks. The answer indicates that the MiniNet-based emulation high precision to detect the attack IoT security issue.

Extreme gradient boosting (XGBoost) was introduced by Zhuo et al. [15] as a detection tool in an SDN-based cloud. The detection results show that XGBoost has higher precision, a lower false-positive rate, and is faster and more scalable. The main problem is that evaluating security strategies is difficult.

Yi-Wen [16] et al. to protect IoT devices from DDoS attacks gateways, a machine learning-based multi-layer DDoS detection system has been developed. The experimental results show that DDoS attack detection with high accuracy in a real-world IoT environment. The major drawback is the service problem in the network.

Marcos et al. [17] developed an online security device that protects against DDoS and port scans for SDN network environments. The outcome suggests that the mitigation strategies were successful in restoring the SDN to normal service. The disadvantage is that it affects legal users.

Shi Dong et al. [18] found two ways to detect DDoS attacks in SDN. The experiments show that the KNN algorithm has a higher detection rate. Future work will focus on improving the algorithm to be used in a real-world SDN environment.

Nagarathna et al. [19] developed a DDoS detection mechanism called learning-driven detection mitigation (LEDEM). The solution shows that the accuracy is high in detecting DDoS attacks. Detection accuracy should be improved.

Da et al. [20] presented a detection algorithm based on SDx and minimizing DDoS attacks with the SD-IoT system. The simulation results show that the SDx algorithm is fast and effective at handling and mitigating DDoS attacks. Improve the algorithm's performance.

Yang et al. [21] introduced the SDN architecture, which uses machine learning to identify and protect against DDOS attacks. The experiment results dataset shows the effectiveness. Improve the distribution model for the flow table.

Yao et al. [22] designed the DDOS detection system based on the open-source fuzzy logic controller in SDN. The solution demonstrates that the detection reduces the time delay and has a lower false alarm rate. Improve the network in future research.

8.2. BLOCKCHAIN TECHNOLOGY

Blockchain is a novel and exciting idea that makes use of public digital encryption and public-key cryptography certificates. It's commonly utilized as a method in various fields, including bitcoin, health records, etc. It satisfies the most critical security requirements, such as transaction authenticity, non-forgery, efficient encryption, flexibility, and reliability. It also offers a decentralized distribution infrastructure that eliminates the possibility of a single point of failure.

The Blockchain was created to allow users to conduct simple peer-to-peer transactions without a middleman such as banks or other Institutions of finance. As a result, a block is a file format that usually stores several transactions. The blocks are chained together in a Blockchain. The size of the block and the time it takes to generate it differ depending on the type of Blockchain.

The ledger and the freshly created and validated block are attached and chained to this current copy of the Blockchain by all participating nodes. As a result, the Blockchain continues to expand in size. Both people or a group of people (peers) can share any asset or value in a blockchain network. [23] Banks, users, payment gateways, and other entities are examples of peers. Financial transactions were initially registered in the blockchain ledger in chronological order. Supply chain operations, logistic processes, data processing functions, management of identification and access, protection methods, policy and economics, and other things that can be done online are all bolstered by the blockchain network nowadays.

Table 2: Comparison of Blockchain Technology

Publication	Contribution	Disadvantages	Benefits
Haotong et al. [24]	blockchain technology to embed a virtual network for secure SDN.	single node failure in SDN	Improve the algorithm
Manikumar et.al [25]	DDoS Mitigation Using Machine Learning Techniques on the Blockchain	improve the algorithms to find the malicious IP address	Random forest provide high accuracy
Lo-Yao et al. [26]	SOChain DDoS data exchange network has blockchain technology to address the issues of confidence and justice.	trust and fairness issue	Sochain has good performance
Arnab Bose et.al [27]	blockchain onto the data and control planes' interaction channels	unauthorized access, data leakage	blockchain to secure switches from an attacker in SDN is a reliable and efficient method
Zakaria et.al [28]	a blockchain-based solution that incorporates two types of DDoS mitigation	Low versatility, a lack of capital, and a high cost	versatility, performance, security, cost-effectiveness, and high accuracy
Maninderpal et.al [29]	All switches are registered, verified, and validated in the Blockchain using a blockchain mechanism.	single point of failure	communication cost and computation time
Mathieu et.al [30]	a confidence evaluation system focused on SDN and Blockchain	end-user has a difficult time judging and lacks the necessary skills	SDN reduces the surface attack within the home network
Durbadal et.al [31]	The SDN architecture lacks adequate access control. The access control is built on the Blockchain o solve this issue.	Improve the robust accounting.	BACC-SDN protects against potential threats, which is crucial for the security of an SDN network.
Abou et.al [32]	scalable and constructive approach for securing blockchain applications	Improve the precision Entropy calculation scheme	high accuracy
Abou et.al [33]	Co-IoT is a blockchain-based framework for preventing DDoS attacks collaboratively.	To ensure two degrees of mitigation, improve the CO-IoT.	flexibility, efficiency, security, cost-effectiveness
Safi et.al [34]	a blockchain-based platform with insufficient SDN support	Improve the working with distributed cloud computing	High efficiency
Ying et.al [35]	created a safe data sharing model for SDN-enabled smart communities.	data leakage	blockchain has a good output and high throughput of smart contracts

Publication	Contribution	Disadvantages	Benefits
Kotaro et.al [36]	blockchains and Software-Defined Networking, regulation of edge network traffic control for IoT (SDN).	reducing transaction costs	trustworthy, scalable
Liu et.al [37]	a trust block method, which calculates the SDN network node's trust value based on Blockchain	Difficult to detect	blockchain increase the accuracy rate and detection rate
Mehran et.al [38]	a new technical framework that was built in the form of an IoT network based on SDN	In a large-scale network, improve the architecture	more effective and stable
Muhammad et al. [39]	In PoW-based Blockchain Systems, Mempool Optimization for Defending Against DDoS Attacks	less efficient	high level of precision
Pradip et.al [40]	deal with the present and future challenges and meet the needs of potential customers requirement by using blockchain techniques	Stable fog nodes should be used to construct the architecture.	DistBlockNet approach has a high performance and effectiveness.
Abbas et.al [41]	Techniques such as Blockchain and software based networking (SDN) to eliminate the need for re-authentication during frequent handover between diverse cells.	User privacy and security issues	low latency, better scalability, and optimized energy consumption.

8.3. BLOCKCHAIN

Haotong et al. [24] presented blockchain-based virtual network requests (VNR) embedding algorithm (BloC-VNE), aiming at solving the single node failure in SDN-enabled networks. SDN has network programmability. The results of our experiments demonstrate the effectiveness of our blockchain-based algorithm outperforms in terms of fault tolerance, and it is comparable to its equivalent without blockchain technology.

Manikumar et al. [25] discussed machine learning techniques to handle various DDoS attacks and Blockchain technology to achieve transparency and immutability. A hacker cannot alter the IP Addresses stored in Blockchain. The solution shows the algorithm of random forest achieves high accuracy.

Lo-Yao et al. [26] investigated the SOChain DDoS data exchange network, which used blockchain technology to address issues of confidence and justice. The outperformance demonstrated that the Sochain has good performance. The major drawback is the trust and fairness issue.

By embedding encryption using Blockchain onto the data and control planes' interaction channels, Arnab Bose et al. [27] can prevent DDoS attacks at the switch stage. The simulation shows that using Blockchain to secure switches from an attacker in SDN is reliable and efficient. The disadvantages are unauthorized access and data leakage.

Zakaria et al. [28] presented Cochain-SC, a blockchain-based solution that incorporates two types of DDoS mitigation. Cochain-SC accomplishes versatility, performance, high accuracy, protection, and cost-effectiveness according to the experimental results. Low versatility, a lack of capital, and a high cost are major issues with DDOS attacks.

Maninderpal et al. [29] developed all registered, verified, and validated switches in the Blockchain using a blockchain mechanism. The outcome was calculated in terms of contact costs and computation time.

Mathieu et al. [30] presented a confidence evaluation system focused on SDN and Blockchain. The solution shows that the SDN reduces the surface attack within the home network. The end-user has a difficult time judging and lacks the necessary skills.

The SDN architecture lacks a proper access control system for various organizations, including SDN controllers and switches to overcome this difficulties, blockchain-based access control is introduced by Durbadal et al. [31]. The result shows that the BACC-SDN secures the potential threats, which is crucial for the security of an SDN network. Improve the robust accounting.

Using SDN, Abou et al. [32] created a scalable and constructive approach for securing blockchain applications. The results of the experiments show that ChainSecure defends Blockchain with high accuracy in detecting unauthorized transactions. Improve the precision Entropy calculation scheme (ECS) by using machine learning methods.

Co-IoT is a blockchain-based platform for preventing DDoS attacks collaboratively was presented by Abou et al. [33]. The results of the experiments show that Co-IoT provides versatility, performance, security, and cost-effectiveness. To ensure two degrees of mitigation, improve the CO-IoT.

To service millions of IoT computers, Safi et al. [34] provided a solution based on the Blockchain supported in redundant SDN. The experimental results show the accuracy, upgrade operation, and bandwidth utilization gains and performance. Improve the working with distributed cloud computing.

Using Blockchain and IBPRE, Ying et al. [35] created a safe data sharing model for smart communities with SDN capabilities. The encrypted device's data is sent to a third-party remote server, and the IBPRE protocol is used to securely share encrypted file keys between authorized users and many others. Crypto keys can be uploaded to the Blockchain by users and use smart contracts to communicate with it, such as updating and looking for documents. The results show the Blockchain has a good output and a high throughput of smart contracts. The main drawback is data leakage.

By combining blockchains and Software-Defined Networking, Kotaro et al. [36] presented regulation of edge network traffic control for IoT (SDN). The outperform demonstrates that Blockchain is well-practised, and it suggests research for practical implementation. Reducing the transaction cost is the major problem.

Liu et al. [37] presented a trust block method, which calculates the SDN network node's trust value based on Blockchain. The outcome shows that the Blockchain increases the accuracy rate and detection rate. The disadvantage is that it is difficult to detect an external threat.

Mehran et al. [38] presented a new technical framework built in an IoT network based on SDN. The architecture of the SDN is more effective as well as stable as a consequence of findings. In a large-scale network, improve the architecture.

Muhammad et al. [39] described a new type of attack that can be used against blockchain-based cryptocurrencies' memory pools (Mempool). The fee-based architecture is more successful in Mempool size optimization when the attack is not serious. It accomplishes this, however, by influencing the attacker as well as legal users. The response demonstrates a high level of precision. One of the drawbacks is that spam detection is less efficient.

Pradip et al. [40] presented to deal with the present and future challenges and to meet the needs of potential customers requirement by using blockchain techniques.

The DistBlockNet focuses on shortening the attack window time by allowing IoT forwarding devices to search more frequently. The evaluation result shows the high performance and effectiveness of the DistBlockNet method. Stable fog nodes should be used to construct the architecture.

Abbas et al. [41] have developed a modern authentication method that employs software-defined networking (SDN) techniques and Blockchain to eliminate the need for re-authentication during the frequent transfer of ownership between diverse cells. The solution shows that the 5G obtained low latency, better scalability, and optimized energy consumption.

CONCLUSION

With the growing market of IoT, its security has become a significant concern. Hence, the IoT device with high computation power makes an attacker more interested in getting access and launching a DDOS attack at a low cost. The impact of a DDoS attack on online transactions in a blockchain-based SDN is discussed in this survey paper. Distributed Denial-of-Service (DDoS) attacks can be effectively mitigated with SDN architecture. For security provisioning, IoT using Blockchain is guaranteed. This paper's conclusion highlights the DDOS attack detection in IoT, which offers various benefits such as faster data rates, good accuracy, security issues, data recovery, and quicker application network response times.

REFERENCES

[1] Sonar, Krushang, and Hardik Upadhyay. "A survey: DDOS attack on Internet of Things." *International Journal of Engineering Research and Development* 10.11 (2014): 58-63.

[2] Chatterjee, Sheshadri, Arpan Kumar Kar, and M. P. Gupta. "Success of IoT in smart cities of India: An empirical analysis." Government Information Quarterly 35, no. 3 (2018): 349-361.

[3] Panda, Chandan Kumar, and Roheet Bhatnagar. "Social internet of things in agriculture: an overview and future scope." Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications (2020): 317-334.

[4] Vishwakarma, Satyendra K., Prashant Upadhyaya, Babita Kumari, and Arun Kumar Mishra. "Smart energy efficient home automation system using iot." In 2019 4th international conference on internet of things: Smart innovation and usages (IoT-SIU), pp. 1-4. IEEE, 2019.

[5] Stergiou, Christos, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. "Secure integration of IoT and cloud computing." Future Generation Computer Systems 78 (2018): 964-975.

[6] Rohit, Mehboob Hasan, Sakif Md Fahim, and Abu Hurayra Asif Khan. "Mitigating and Detecting DDoS attack on IoT Environment." In 2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON), pp. 5-8. IEEE.

[7] Ahmed, Abdul Wahab, Mian Muhammad Ahmed, Omair Ahmad Khan, and Munam Ali Shah. "A comprehensive analysis on the security threats and their countermeasures of IoT." Int J Adv Comput Sci Appl 8, no. 7 (2017): 489-501.

[8] Kamboj, Priyanka, Munesh Chandra Trivedi, Virendra Kumar Yadav, and Vikash Kumar Singh. "Detection techniques of DDoS attacks: A survey." In 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON), pp. 675-679. IEEE, 2017.

[9] Vishwakarma, Ruchi, and Ankit Kumar Jain. "A survey of DDoS attacking techniques and defence mechanisms in the IoT network." Telecommunication systems 73, no. 1 (2020): 3-25.

[10] Kasinathan, Prabhakaran, Claudio Pastrone, Maurizio A. Spirito, and Mark Vinkovits. "Denial-of-Service detection in 6LoWPAN based Internet of Things." In 2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob), pp. 600-607. IEEE, 2013.

[11] Wani, Azka, and S. Revathi. "DDoS detection and alleviation in IoT using SDN (SDIoT-DDoS-DA)." Journal of The Institution of Engineers (India): Series B 101, no. 2 (2020): 117-128.

[12] Zheng, Jianjun, and Akbar SiamiNamin. "Defending SDN-based IoT networks against DDoS attacks using markov decision process." In 2018 IEEE International Conference on Big Data (Big Data), pp. 4589-4592. IEEE, 2018.

[13] Bhayo, Jalal, Sufian Hameed, and Syed Attique Shah. "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)." IEEE Access 8 (2020): 221612-221631.

[14] Bhunia, Suman Sankar, and Mohan Gurusamy. "Dynamic attack detection and mitigation in IoT using SDN." In 2017 27th International telecommunication networks and applications conference (ITNAC), pp. 1-6. IEEE, 2017.

[15] Chen, Zhuo, Fu Jiang, Yijun Cheng, Xin Gu, Weirong Liu, and Jun Peng. "XGBoost classifier for DDoS attack detection and analysis in SDN-based cloud." In 2018 IEEE international conference on big data and smart computing (bigcomp), pp. 251-256. IEEE, 2018.

[16] Chen, Yi-Wen, Jang-Ping Sheu, Yung-Ching Kuo, and Nguyen Van Cuong. "Design and implementation of IoT DDoS attacks detection system based on machine learning." In 2020 European Conference on Networks and Communications (EuCNC), pp. 122-127. IEEE, 2020.

[17] De Assis, Marcos VO, Matheus P. Novaes, Cinara B. Zerbini, Luiz F. Carvalho, TaufikAbrãao, and Mario L. Proença. "Fast defense system against attacks in software defined networks." IEEE Access 6 (2018): 69620-69639.

[18] Dong, Shi, and Mudar Sarem. "DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks." IEEE Access 8 (2019): 5039-5048.

[19] Ravi, Nagarathna, and S. Mercy Shalinie. "Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture." IEEE Internet of Things Journal 7.4 (2020): 3559-3570.

[20] Yin, Da, Lianming Zhang, and Kun Yang. "A DDoS attack detection and mitigation with software-defined Internet of Things framework." IEEE Access 6 (2018): 24694-24705.

[21] Yang, Lingfeng, and Hui Zhao. "DDoS attack identification and defense using SDN based on machine learning method." In 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN), pp. 174-178. IEEE, 2018.

[22] Yu, Yao, Lei Guo, Ye Liu, Jian Zheng, and Yue Zong. "An efficient SDN-based DDoS attack detection and rapid response platform in vehicular networks." IEEE access 6 (2018): 44570-44579.

[23] Singh, Rajeev, Sudeep Tanwar, and TeekParval Sharma. "Utilization of blockchain for mitigating the distributed denial of service attacks." Security and Privacy 3, no. 3 (2020): e96.

[24] Cao, Haotong, Yue Hu, Qin Wang, Shengchen Wu, and Longxiang Yang. "A blockchain-based virtual network embedding algorithm for secure software defined networking." In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1057-1062. IEEE, 2020.

[25] Manikumar, D. V. V. S., and B. Uma Maheswari. "Blockchain Based DDoS Mitigation Using Machine Learning Techniques." In 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 794-800. IEEE, 2020.

[26] Yeh, Lo-Yao, Peggy Joy Lu, Szu-Hao Huang, and Jiun-Long Huang. "SOChain: A privacy-preserving DDoS data exchange service over soc consortium blockchain." IEEE Transactions on Engineering Management 67, no. 4 (2020): 1487-1500.

[27] Bose, Arnab, Gagangeet Singh Aujla, Maninderpal Singh, Neeraj Kumar, and Haotong Cao. "Blockchain as a service for software defined networks: A denial of service attack perspective." In 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pp. 901-906. IEEE, 2019.

[28] Abou El Houda, Zakaria, AbdelhakimSenhajiHafid, and LyesKhoukhi. “Cochain-SC: An intra- and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract.” IEEE Access 7 (2019): 98893-98907.

[29] Singh, Maninderpal, Gagangeet Singh Aujla, Amritpal Singh, Neeraj Kumar, and Sahil Garg. "Deep-learning-based blockchain framework for secure software-defined industrial networks." IEEE Transactions on Industrial Informatics 17, no. 1 (2020): 606-616.

[30] Boussard, Mathieu, Serge Papillon, Pierre Peloso, Matteo Signorini, and ErezWaisbard. "STewARD: SDN and blockchain-based Trust evaluation for Automated Risk management on IoT Devices." In IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 841-846. IEEE, 2019.

[31] Chattaraj, Durbadal, Sourav Saha, BasudebBera, and Ashok Kumar Das. "On the Design of Blockchain-Based Access Control Scheme for Software Defined Networks." In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 237-242. IEEE, 2020.

[32] Abou El Houda, Zakaria, LyesKhoukhi, and AbdelhakimHafid. "Chainsecure-a scalable and proactive solution for protecting blockchain applications using sdn." In 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1-6. IEEE, 2018.

[33] Abou El Houda, Zakaria, AbdelhakimHafid, and LyesKhoukhi. "Co-IoT: A collaborative DDoS mitigation scheme in IoT environment based on blockchain using SDN." In 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1-6. IEEE, 2019..

[34] Faizullah, Safi, M. Asad Khan, Ali Alzahrani, and Imdadullah Khan. "Permissioned blockchain-based security for SDN in IoT cloud networks." In 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), pp. 1-6. IEEE, 2020.

[35] Gao, Ying, Yijian Chen, Hongliang Lin, and Joel JPC Rodrigues. "Blockchain based secure IoT data sharing framework for SDN-enabled smart communities." In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 514-519. IEEE, 2020.

[36] Kataoka, Kotaro, Saurabh Gangwar, and Prashanth Podili. "Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN." In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), pp. 296-301. IEEE, 2018.

[37] Liu, Yifan, Bo Zhao, Xiaofei Li, Shuo Wang, Bin Zhang, and Zhenpeng Liu. "A trust chain assessment method based on blockchain for sdn network nodes." In 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), pp. 240-245. IEEE, 2019.

[38] Pourvahab, Mehran, and Gholamhossein Ekbatanifard. “An efficient forensics architecture in software-defined networking-IoT using blockchain technology.” IEEE Access 7 (2019): 99573-99588.

[39] Saad, Muhammad, Laurent Njilla, Charles Kamhoua, Joongheon Kim, DaeHunNyang, and Aziz Mohaisen. "Mempool optimization for defending against ddos attacks in pow-based blockchain systems." In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 285-292. IEEE, 2019.

[40] Sharma, Pradip Kumar, Saurabh Singh, Young-SikJeong, and Jong Hyuk Park. "Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks." IEEE Communications Magazine 55, no. 9 (2017): 78-85.41

[41] Yazdinejad, Abbas, Reza M. Parizi, Ali Dehghantanha, and Kim-Kwang Raymond Choo. "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks." IEEE Transactions on Network Science and Engineering (2019).