European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 10 ,2020

Applicability of Blockchain towards Mitigation of Distributed Denial of Service Attack in IoT

Manoj Kumar Beuria[1],Pradeep Kumar Sharma[2], Jitendra Dangra[3], Chetan Bulla[4], Kishori Abadar[5]

[1]KIIT Deemed to be University, [2]MIT, Ujjain ,[3] PITS, Ujjain,[4] KLE College of Engineering and Technology, Chikodi ,[5] Sadguru Gadage Maharaj College, karad, Maharashtra, India.

Abstract:

IoT makes the smart cities worldwide possible. Smart home, smart farming, smart climate, smart wellness, smart government, and more are all kinds of smart towns. IoT is also used in the petroleum, gas mines and manufacturing sectors. IOT improves efficiency, optimizes prices, optimizes human capital, retains predictions and provides a lot of convenience to human life. Security issues are growing with involvement of large number of different devices and voluminous processing of data. Protection and privacy problems are the key reasons why IoT does not thrive. One of the main threats is vulnerability to DDOS attack. This paper presents use of block chain based methodologies to mitigate DDOS attack in internet of things. It provides a critical analysis of available block chain based architectures to encounter DDOS attacks.

Keyword: IoT, Blockchain, Smart Contract, DDOS, Threat, Attack, Mitigation,

I. INTRODUCTION:

Kevin Ashton [1] built an internet of things. Since the last decade, however, IoT has sheltered almost all applications, including home automation, intelligent healthcare, utility facilities, intelligent transport [2]. Key IoT enabling technologies include RFID technology (WLAN), Wi-Fi, Bluetooth, Internet technology and intelligent computing (Artificial Intelligence), etc. Smart computing (WIC) technology is also included. Internet of Things (IoT) is a fast-moving array of internet sensors installed in different physical items, i.e. stuff. Stuff may, of course, be any (animate or inanimate) physical entity on the earth you can interact with or embed a sensor on. A huge range of calculations can be done by sensors. Wired or wireless Internet access to stuff. Objects can be something, i.e. animate and inanimate, that needs physically to exist.

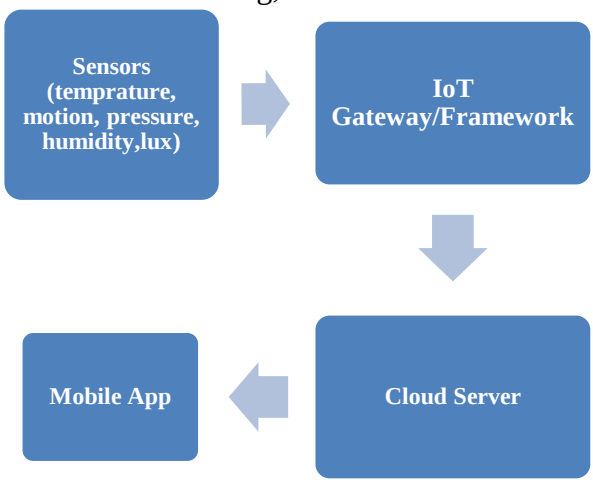

Fig. 1. Basic building Blocks of IoT

In above figure 1, Sensors are a lot of diodes equipped for detecting natural physical boundaries, for example, temperature, pressure .Sensors are responsible for acquisition of data. They can be configured to collect data continuously. Sensors are capable of capturing humidity, temperature, motion and many more. IoT platform is a middleware. Many quality IoT platforms are available now a day's such as- Microsoft Azure IoT and AWA IoT. Actual data is stored in cloud server. In cloud, data analytics applications are applied and relevant data is shared with stakeholders using mobile applications.

Protection and privacy problems are the key reasons why IoT does not thrive. One of the main threats is vulnerability to DDOS attack. On the internet, a distributed denial of service (DDoS) attack involves a large number of affected systems attacking a single target which contributes to the denial of service for targeted device users. The influx of incoming messages forced the targeting device to stop, thereby denying legitimate users the operation of the machine.

A block chain [3] [4][5] is a decentralized, passed on and opens mechanized record that is used to record trades transversely over various PCs so any included record can't be balanced retroactively, without the difference in all resulting blocks. This empowers the individuals to affirm and audit trades self-sufficiently and tolerably monetarily. A block chain database is supervised freely using a common framework and an appropriated time-venturing worker. They are confirmed by mass collaboration powered by total individual issues. Such an arrangement empowers vivacious work process where individuals' weakness regarding data security is fringe. The use of a block chain empties the typical for unfathomable reproducibility from a propelled asset.

Block chains are utilized to improve the account and sharing of budgetary exchange data, which can be found as far as sped up, diminished procedural cost, less exchange blunders, expanded general security, and a decentralized methodology [5]. This decentralized technique expels a main issue of framework disappointment and weakness to cyber attacks. The primary thought behind block chain utilization in virtual budgetary exchanges is that the wallet of every client isn't halfway spared; rather, it is made sure about by putting away the record of exchanges between clients in a block chain. Block chain is instrumental is designing solutions to mitigate ddos attacks.

II. RELATED WORK

Arsalon Mohsen Nia et al., 2016[6] gives an inside and out examination of potential assaults and weaknesses. Mohamed Abomhara et al., 2014 [7] gave security dangers and difficulties in Internet of Things. They likewise tended to that there are four interconnected segments, in particular individuals, article, equipment and programming, which speaks with one another over untrusted private system. Cart Das et al., 2016 [8] gave an insightful and inside and out investigation of future problems in IoT.

Salim ELBOUANANI [9] demonstrated that there is at present no norm or system which covers all security perspectives in the Internet of Things. They found that confirmation is a genuine test in IoT. Krishna Kanth Gupta et al., 2016 [10] anticipated that there will be 25 billion IoT gadgets

by 2020. They likewise recognized difficulties in Internet of Things. Gurpreet Singh Matharu et al., 2014 [11] explained that interoperability; normalization and security are the regions which require a ton of examination so web of things can flourish.

Hui Suo et al.,2012 [12] introduced encryption based methodology to enhance security features in IoT solutions.C. Flügel et al.,2009 [13] introduced a review over a portion of the specialized provokes that should be defeated to assemble such system. L. Atzori et al.,2012 [14] promoted the idea of using IoT in social platforms.

IEEE range 2014 [15] established java as the prominent design tool for IoT solutions. World financial gathering modern web overview, 2014 [16] set up a more clear comprehension of the extraordinary chances and new dangers emerging from the Industrial Internet. Hammi et al.,2018 [17] proposed a unique decentralized framework called air pockets of trust, which guarantees a powerful recognizable proof and verification of gadgets. Authors in [18][19][20] proposed different block chain based solutions for IoT ecosystem.

Javaid et al., 2018 [21] [22] introduced a PUF and blockchain based arrangement called BlockPro for information provenance and information respectability for secure IoT conditions. M. Anwer et al.,2020 [23] proposed course of action of different masters' procedures of Block chain to make IoT check and discussion about their limitations.

Authors in [24][25][26] discussed various security pitfalls in encryption techniques used for different IoT solutions. Arbitrary number generators have generally been a critical wellspring of weakness [27],[28],[29]. Stephen Checkoway et al.,2014 [30] [31]introduced the new PRNG algorithm. it was speedy.

Yu et al., 2015 [32] introduced distinctive known feeble gadgets to encounter DDOS attack. Zhang et al.,2015 [33] showed by various authorities a noteworthy perspective in IoT landscape.

Authors in [37][35] played out a wide examination on the powerless IoT devices, including thousands of interesting contraptions. A large portion of them were transparently accessible by methods for the Internet requiring no unmistakable evidence.

This paper [36] sets out a short outline of the nuts and bolts Machine Learning and its standards and calculations Submissions. We'll begin with a more extensive machine definition Study and afterward consolidating various types of getting the hang of including Methods administered and uncontrolled, and profound learning Perfect standards. We'll examine usage in the remainder of the paper Machine learning calculations in various territories including design Recognition, sensor systems, identification of irregularities and the Internet of Things (IoT), and checking of wellbeing.

This paper [37] features a system that incorporates the Internet of Things (IoT) and some generally utilized AI calculations to make a prescient model that can be utilized to gauge indoor temperature of shrewd structures. This prescient model was prepared to build up practicality to a totally new dataset utilizing on-line learning system. To approve the methodology, the paper leads a Machine Learning put together test with respect to recorded genuine sensor data. The paper at that point recommends that the accompanying procedure ought to be incorporated into

an IoT design dependent on Edge Computing to empower the structure to work in a vitality productive manner.

III. RESEARCH CHALLENGES IN IOT

Following gaps are identified during literature survey:

- It is found that authentication is a real challenge in IoT. The fact behind this is that appropriate authentication infrastructure is not available in IoT [9].
- Distribution of keys is another challenge [9].
- Security is the biggest worry for most industries [16].
- Man in Middle assault is a serious problem because of the architecture [20].
- DDOS attack is also a major problem with IoT network. But a universal mitigation plan is not available[21].
- Vulnerability in IoT device is a dangerous issue. It is needed to be classified and predicted [32]. Vulnerable device is a real threat to IoT network. Such Devices are required to be identified [35].

IV. MITIGATION OF DDOS ATTACK USING BLOCKCHAIN

This section mainly contains critical analysis of available block chain based architectures for mitigation of distributed denial of service attack.

Wikipedia has helped the CloudFlare's services to defend itself from attack. This approach is effective because CloudFlare has had ample expertise in managing such attacks. This is a very interesting time for online encyclopedias. Spamhous was, for example, secured in March 2013 by the services of CloudFlare. Furthermore, the DDoS assault by the hijacking of unsufficient web browsers was aimed at CloudFlare Client GitHub (an online coding site) in August 2015 [38].

On 28 February 2018, the most destructive was published. The prolexic DDoS service from Akamai mitigated this threat. High DDoS security was invested by Akamai. It consists of seven scrubbing centers and 150 employees working in the fight against the DDoS attacks. Therefore, it is apparent that it needs vast quantities of investment in capital, energy and time. Although a significant number of memcached servers (approx. 50 K), such attacks remain vulnerable [39].

The DDoS assault was perpetrated in Botnets in October 2016, it affected a larfe number of IoT based equipments [40].

Few standard attacks by the DDoS target the transport networks of the Railways. In October 2017, the attacks by the DDoS struck the transportation network in Sweden, which delayed the service, crashing the IT system that tracks the location of the trains, as well as disassembling the related email networks, websites and traffic maps.

Rodrigues et al [41] suggested a shared DoS mitigation blockchain framework for smart contracts. This is what we are doing. Architecture offers DDoS mitigation through multiple autonomous

machine managed network domains (ASes). This design calls a distributed Ethereum-based blockchain. Intelligent contracts are used in blockchain to report IP addresses specified in white or black across several fields. Therefore, an IP address in block in a blockchain is inserted as a transaction.

The IP will be the IP with a black list flow stopped or an IP with a white list moved according to the network policy. In this architecture, it is possible to connect IP addresses to the shared blockchain in classes. Instead, attachments between separate parts of the infrastructure, such as ASes/customers, are exchanged via blockchain instead of messaging attack information. Every 14 seconds, a new block is formed in Ethereum. Therefore, the corresponding ASes will receive during this time the block/allow addresses.

The person ASes use Software Specified Networking (SDN) to configure and apply the Flow rules to block DDoS attacks. Different ASes (domains) vary from other ASes in their own security policy and DDoS threat countermeasure (domains). The victim server is secured while the DDoS attack is carried out by filtering the attack traffic on its own AS. Attack traffic is also screened in other ASes in compliance with the installed flow laws. Thus, a near-source DDoS attack is attenuated. This SDN and blockchain architecture offers a scalable and powerful DDoS mitigation approach.

The key benefit of this architecture is, however, that it can be used along with current defense mechanisms as an external security tool. The suggested architecture is shallow and offers just the basis for DoS mitigation. The developers have not given implementation and evaluation and much of the work is still to be dealt with.

(a)The collective solution suggested by this architecture is just introductive, but there is no realistic implementation of SDN;
(b) a decentralized blockchain is used that can lead to enhanced data flow (transactions) becoming a problem for scalability, and the authors propose to minimize this space-spread bloom filter, but there is no real concern. How will a node that records an attack be authenticated? How do I trust other components of the transaction to attack information? not sufficiently developed;
(c) IP blocking only for static IP addresses is possible, and
(d) cooperative domain justice is a problem, and a single domain could be able to use a greater number of other domain services than those offered under DDoS attacks.

For the reduction of IoT device-based attacks, the Javaid et al [21] recommends an IoT built-in blocchain architecture. Ethereum blockchain of intelligent contracts is used in architecture. In order to send and receive messages, the IoT devices need first be registered on the registry. An IoT system can only run up to the gas threshold above the gas threshold. A server can at any time deregister or uninstall any IoT system that has network malfunctions or expired gas cap. The smart contract is developed and recorded by the server as well.

The server extends the registered contract address to all network IoT devices. An IoT computer with a server is on the trusted list of the deal. The gas cap for individual contract transactions

for the protection against DDoS attacks is fixed during the initialisation of smart contracts [21].
The intelligent contract (software component) is the major regulator for all IoT devices involved. It does not only permit IoT devices but also restricts their use to the amount of petrol. Gateways connect the IoT devices in this architecture.

Smart contract contacts to deliver a message to an IoT computer. An IoT system will run only up to its gas cap, which is allocated to it when the server is registered. This cap is based on the IoT device's bandwidth and resources specifications. Any transaction and method in this architecture has a gas cap.

The biggest benefit of this system is that the decentralized blockchain with PoW consensus system has the power and faith of Ethereus. A node malfunction has little effect on the operation of the whole system. Distributed estimation reduces demand on servers efficiently. For DDoS protection, each system's architecture is restricted to its own gas cap. Some other benefits include:
(a) no hardware update needed on an IoT device,
(b) as the overlay network over the current traditional network can be introduced in the architecture,
(c) both the solution found and the solution functions for prevention. On the other hand, this architecture feeds a reliable contract list that is reviewed when a new message is released by some system or when an interaction between devices takes place. In this method, thus, problems of scalability are still present.

Information on how to trust an IoT device at the registry during registration are not discussed. The way a server will find the current gas/resource necessity for the IoT node remains obvious. If an attacker can spot different IoT addresses, the trusted smart deal list can contain those addresses.

Kataoka et al [42] suggests this architecture, which uses blockchain technologies built into SDN technology, for minimizing DDoS attacks performed using IoT-devices based on trust list traffic management architecture.

There are three key components in it:: ioT/device applications; iote edge networks; ioT/gateway/- validators. Contact is only feasible within this architecture if the communication devices/servers are confident. The trust list principle is used to separate trustworthy devices from untrusted devices. Trust List is essentially a data system by which the network spreads 'application profiles' and 'application profiles.'

DDoS attacks can cause malicious traffic blocked and filtered by SDN switch on the edge network. SDN controller ensures synergy with the blockchain environment and access from the blockchain information about trustworthy resources and computers. IoT servers/gateways/validators preserve the details on "trusted services and devices." The SDN controller also provides flow rules for filtering or approval of IoT traffic on the SDN switches.

A new computer called a validator was implemented in this architecture. It is the job of

checking IoT device validity via a protocol of authentication. The trusted user profile is also transmitted to the IoT device by blockchain and trustworthy service info. Therefore the first IoT system is trustworthy for contact. Details of the registry are given for further correspondence after this. This architecture can be used with a number of other criteria, such as system location, ownership, user licence, and more. The architecture is versatile on application and device profiles.

This work offers a realistic implementation scenario for an open source tech blockchain and confidence list.

(a) considerable time is passed before monitoring . It helps in anomaly detection.
(b) avoidance and responding measures;
(c) DDoS attack traffic is limited to edge networks. The drawbacks to this architecture is few:

1. The architecture's confidence list are non-encrypted/plain text and will thus pose security questions in a public blockchain.
2. Rise in the size of the secret list means higher processing costs for blockchain.
3. There is just evidence of definition. It must be more researched in practical use.
4. There is privacy concern in public block chain.
5. In such instances, the attacker must continuously inspect and refresh the confidence list and access the Network by overruling the rules.
6. Methodology requires several delays until a system is enabled to communicate (as a function of intermediate blockchain/SDN/validators**).**

V. CONCLUSION:

DDOS attack is devastating. It prevents actual users to use the web services. Such kind of scenario results in communication break in IoT system. Although blockchain based methodologies are available to mitigate DDOS attack. Blockchain provides authentication, integrity, reliability in transactions. This paper has thrown a light on all the modern blockchain based solutions to mitigate DDOS attack. A critical analysis of blockchain based mitigation technique is provided in this paper. After this critical analysis, it is found that a lot of work is still to be done in these blockchain based methods. Scalability and cost are two major issues needed to be resolved.

References:

[1] Raghuvanshi, A., & Singh, U. (2020). Internet of Things for smart cities- security issues and challenges. 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 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 Information Assurance and Security, IEEE, pp 32-37, 2015.

[10] KrishnaKanth 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.

[11] Gurpreet Singh Matharu, Priyanka Upadhyay, Lalita Chaudhary, "The Internet of Things: Challenges & Security Issues", International Conference on Emerging Trends, IEEE, pp. 54-59, 2014.

[12] Hui Suo, Jiafu Wan, "Security in the Internet of Things: A Review", International Conference on Computer Science and Electronics Engineering, IEEE, pp. 648-651, 2012.

[13] C. Flügel, and V. Gehrmann, "Scientific workshop 4: intelligent objects for the Internet of Things: Internet of Things-application of sensor networks in logistics," Communications in Computer and Information Science, vol.32, pp.16-26, 2009.

[14] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social Internet of Things (SIoT) when social networks meet the Internet of Things: concept, architecture and network characterization," Computer Networks, vol.56, no.16, pp. 3594-3608, 2012.

[15] http://spectrum.ieee.org/computing/software/top-10-programming-languages

[16] www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

[2]17Hammi, Mohamed Tahar, et al. "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT." Computers & Security 78 (2018): 126-142
.
[18] Banerjee, Mandrita, Junghee Lee, and Kim-Kwang Raymond Choo. "A blockchain future for internet of things security: A position paper." Digital Communications and Networks 4.3 (2018): 149-160.

[19] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future Generation Computer Systems 82 (2018): 395-411.

[20] Agrawal, Rahul, Pratik Verma, Rahul Sonanis, Umang Goel, Aloknath De, Sai Anirudh Kondaveeti, and Suman Shekhar. "Continuous security in IoT using Blockchain." In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 6423-6427. IEEE, 2018.

[21] Javaid, Uzair, Ang Kiang Siang, Muhammad Naveed Aman, and Biplab Sikdar. "Mitigating loT Device based DDoS Attacks using Blockchain." In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, pp. 7176. ACM, 2018.

[22] Javaid, Uzair, Muhammad Naveed Aman, and Biplab Sikdar. "BlockPro: Blockchain based Data Provenance and Integrity for Secure IoT Environments." In Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, pp. 13-18. ACM, 2018.

[23] M. Anwer, A. saad and A. Ashfaque, "Security of IoT Using Block chain: A Review," 2020 International Conference on Information Science and Communication Technology (ICISCT), KARACHI, Pakistan, 2020, pp. 1-5, doi: 10.1109/ICISCT49550.2020.9079943.

[24] David Lazar, Haogang Chen, Xi Wang, and Nickolai Zeldovich. Why does cryptographic software fail?: a case study and open problems. In APSys 2014, pages 7:1–7:7, 2014.

[25] Gregory V. Bard. The Vulnerability of SSL to Chosen Plaintext Attack. IACR Cryptology ePrint Archive, 2004:111, 2004.

[26] BEAST. https://vnhacker.blogspot.co.uk/2011/09/beast.html, 2011. [Online; accessed 3-May-2017].

[27] Ian Goldberg and David Wagner. Randomness and the Netscape browser. Dr Dobb's Journal-Software Tools for the Professional Programmer, 21(1):66–71, 1996.

[28] Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, and Nicko van Someren. Factoring RSA Keys from Certified Smart Cards: Coppersmith in the wild. In ASIACRYPT 2013, pages 341–360, 2013.

[29] Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Mining your Ps and Qs: Detection of Widespread Weak Keys in Network Devices. In USENIX Security 2012, pages 205– 220, 2012.

[30] Stephen Checkoway, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, Hovav Shacham, and Matthew Fredrikson. On the practical exploitability of dual EC in TLS implementations. In USENIX Security 2014, pages 319–335, 2014.

[31] Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, RalfPhilipp Weinmann, Eric Rescorla, and Hovav Shacham. A systematic analysis of the Juniper Dual EC incident. In ACM CCS 2016, pages 468–479, 2016.

[32] Yu, T., Sekar, V., Seshan, S., Agarwal, Y., and Xu, C. Handling a trillion (unfixable) flaws on a billion devices. Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV, ACM Press (2015), 1–7.

[33] Zhang, Z.-K., Cho, M.C.Y., and Shieh, S. Emerging Security Threats and Countermeasures in IoT. Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security - ASIA CCS ’15, ACM Press (2015), 1–6

[34] Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., and Chen, H. Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT). IEEE Joint Intelligence and Security Informatics Conference, IEEE (2014), 232–235.

[35] Airehrour, D., Gutierrez, J., and Ray, S.K. Secure routing for internet of things: A survey. JNCA66, (2016), 198–213.

[36] U. S. Shanthamallu, A. Spanias, C. Tepedelenlioglu and M. Stanley, "A brief survey of machine learning methods and their sensor and IoT applications," 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA), Larnaca, 2017, pp. 1-8, doi: 10.1109/IISA.2017.8316459.

[37] D. Paul, T. Chakraborty, S. K. Datta and D. Paul, "IoT and Machine Learning Based Prediction of Smart Building Indoor Temperature," 2018 4th International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, 2018, pp. 1-6, doi: 10.1109/ICCOINS.2018.8510597.

[38] Dunn JE. Wikipedia fights off huge DDoS attack; Sep 11, 2019. https://nakedsecurity.sophos.com/2019/09/11/wikipedia-fights-off-huge-ddos- attack/. Accessed September 18, 2019.

[39] World's largest DDoS attack: US firm suffers 1.7 Tbps of DDoS attack; March 6, 2018. https://www.hackread.com/worlds-largest-ddos-attack- us-firm-suffers-1-7-tbps-of-ddos-attack/. Accessed January 8, 2019.

[40] Osborne C. GitHub suffers “largest DDoS” attack in site's history; March 30, 2015. https://www.zdnet.com/article/github-suffers-largest-ddos- attack-in-sites-history/. Accessed January 8, 2019.

[41] Rodrigues B, Bocek T, Lareida A, Hausheer D, Rafati S, Stiller B. A blockchain-based architecture for collaborative DDoS mitigation with smart contracts. IFIP Int Conf Auton Infrastruct Manag Secur. 2017;10356:16-29.

[42] Kataoka K, Gangwar S, Podili P. Trust list: internet-wide and distributed IoT traffic management using blockchain and SDN. Paper presented at: Proceedings of IEEE 4th World Forum on Internet of Things (WF-IoT); February 2018: 296–301.