# Integrating DOTS With Blockchain Can Secure Massive IoT Sensors

Syed Badruddoja
*Department of Computer Science and Engineering*
*University of North Texas*
Denton, TX, 76207, USA
syedbadruddoja@my.unt.edu

Ram Dantu
*Department of Computer Science and Engineering*
*University of North Texas*
Denton, TX, 76207, USA
ram.dantu@unt.edu

Logan Widick
*Department of Computer Science and Engineering*
*University of North Texas*
Denton, TX, 76207, USA
logan.widick@unt.edu

Zachary Zaccagni
*Department of Computer Science and Engineering*
*University of North Texas*
Denton, TX, 76207, USA
zacharyzaccagni@my.unt.edu

Kritagya Upadhyay
*Department of Computer Science and Engineering*
*University of North Texas*
Denton, TX, 76207, USA
kritagyaupadhyay@my.unt.edu

***Abstract*—This paper presents a novel approach to securing IoT devices by leveraging DDoS Open Threat Signaling (DOTS) architecture on a Blockchain framework. Like many areas of the information technology domain, IoT sensors are also prone to attacks but on a larger scale. There are millions of devices being connected to a central domain to provide different types of services. Since these low-powered IoT devices have constrained technical requirements with less computational capabilities, they lack the capacity to judge their behavior as benign or malignant. IoT relies heavily on the higher level of intelligent nodes to decide on their status. An IoT Controller/Edge server handles the registration and the limited management of devices. Since traditional security is unable to protect the IoT environment sufficiently, we present a Blockchain-based DDoS detection approach to secure and mitigate such attacks in the IoT environment. Our test setup includes dataset from four sensors over two months. These values were tested using a threshold calculation against the variation of temperature, humidity, pressure, and wind direction on that day to find out whether an IoT sensor is under a DDoS attack. Our results show how DOTS can help in detection of attack when mapped on IoT edge computing.**

***Index Terms*—Cybersecurity, Blockchain, IoT, Edge Computing, Distributed Ledger, DDOS Protection, Smart Contracts.**

## I. Introduction

Information Technology (IT) has transformed many people's lives in a short period of time. In the modern world, we have become more reliant on technology to run our lives sufficiently and to communicate with others. People are connected socially, economically, politically in many ways. These relationships have evolved with the technology into instantly sharing experiences, feelings, fund-raising and so much more in linking us in ways unfathomable for 50 years. The Internet of Things (IoT) is the latest transformation of IT into expanding what and how we interact with our immediate world. We've made them "smart" by connecting them to networks in a meaningful way. Some IoT devices are designed to be interacted directly like- adjusting room temperatures, turning lights on and starting your car while some are used to obtain information and communicate with other devices such as reading your blood pressure, relaying the status of your security system or even finding your smart keys. IoT aims to improve people's quality of life by allowing them to see and change things that require them to physically being there and manually doing them in the past.

With all the ways that information technology helps manage our lives in a better way, there comes certain challenges and risks that need to be dealt with. The acceptance and continued use of these inventions require

978-1-7281-7445-7/20/$31.00 ©2020 IEEE
DOI 10.1109/IPDPSW50202.2020.00156

that they don't regularly fail, especially in a disruptive manner. For example, how do you feel when you press the confirm payment button on a flight reservation website, and the link is unresponsive or when you are about to discuss something crucial about someone's health over phone and line drops or when you are buying a gift online for your loved one and the website link is unavailable. The failure in the technology disrupts your ability for results. The result of disruption may range from trivial to critical and life-changing. IT systems need to mitigate these technological disruptions, whether intentional or unintentional, to make better experience of users and businesses by ensuring key communication and information continue unobstructed.

## II. Motivation

The devices we use in our daily life to perform certain actions that require our input are vulnerable in many ways. The devices at home for instance, television, requires a valid input from a home user to direct itself to a particular output intended by the user. Services like Netflix, Amazon Prime, and other video streaming services are part of the home entertainment services. What happens when these services are not delivered on time? What if amazon prime is having its network up-time 99.99% and Netflix has an up-time of 80%? Customers will stop watching Netflix shows and move to Amazon Prime even if Netflix has more interesting shows than Amazon Prime. The mobile phones we own are installed with a lot of applications that are required for our daily use. Mail, chat-box, gaming, calendar, storage file and many other applications are used in smartphones by the user. These devices do have operating systems installed in them with a lot of possibilities for attacks and threats. A simple program can compromise the root and make the device unusable with delay in service response of the applications installed in the device. This program can be executed by one of the applications in the device or from the remote network. Since such devices are smart, they can also be relied upon for system-based protection software to evade or fight against any threat. Still, there is a risk of security vulnerability from the applications of anonymous publisher/source. Devices that are IP reachable can easily be made the victim of any security attacks. The big pool of IoT devices is a source of security attacks where things can go wrong in a massive way. The IoT devices are in an environment where there is low power and lossy network (LLN) and may or may not be IP enabled. The bandwidth that these devices consume is less compared to traditional IP devices. But if millions of IoT devices are compromised and combined together to perform a service disruption attack then, there can be a massive setback to the service industry irrespective of the compromise performed being internal or external. According to Symantec [1], many Distributed Denial of Services(DDoS) affect tens of thousands of weakly secured IoT devices and flood the IoT network with a high volume of traffic to disrupt targeted websites. IoT DDoS attack is a major cause of IoT traffic disruption due to a lot of reasons. The IoT devices are manufactured for a life span of over 5-10 years. These devices are very tiny and may contain a chip depending on their operation. The devices are hardly designed to sustain any update to their firmware. Since devices do not get the updates, they are susceptible to threats and as a result can be a victim of a hacker to perform DDoS attack.

## III. Literature Survey

There have been several mitigating solutions proposed by the IoT researchers, and yet the research is progressing towards finding a robust, secure and stable mechanism to address the security issues in IoT. Solutions can be simple or complex depending on the problem statement of the existing challenges. Many works are done in the field of securing IoT with various technologies. Number of IoT security issues are discussed by Salah, et al. [7]related to IoT device constraints like low-power and low-security levels that are similar to traditional IP enabled networks. They have mentioned solutions that Blockchain can provide by solving most of the issues starting from addressing identity registration, secure communication (eliminate Trusted Third Party), data authentication, integrity, and privacy. Still, they are working more on how to address the problems in a better way. Reyna, et al. [8] speaks about integrating Blockchain with IoT by discussing several challenges and opportunities that may arise from the integration. Blockchain has a possibility in many ways that can provide features like decentralization, scalability, identity, autonomy, reliability, and security. Blockchain is discussed to solve the problem of central dependency for IoT devices where trust can be compromised by Singh, et al. [9]. There is also a possibility of a single point of failure for a central architecture. In a decentralized Blockchain-based environment there will not be a dependency on a single server to decide upon any action to a particular device or a policy. Participants in the IoT network will come

to a consensus about whether a particular action is to be taken or not. Later in the document, the main reasons for proposing Blockchain as a solution to IoT is presented. A case study is presented with Blockchain for IoT security and privacy for a smart home environment. In the setup by Dorri, et al. [10], where each smart home will be equipped and made available with always-online status, which will be a high resource device and will behave as a miner. This miner will be handling communication within and external to the home. The miner will be a part of a secure and private Blockchain that will be used for controlling and auditing communications. Pietro, et al. [11] mentions the trust system of the Internet of things with Blockchain. Problems such as relating to the traditional PKI model that relies on the root of the trust and is not compatible with heterogeneous IoT ecosystems where the constrained devices are under different administrative domains are mentioned. The solution provided by these group speaks about a distributed trust model that does not rely on any single authority for trust management but rather create an end-to-end trust that bridges existing domains. Falco, et al. [12] discusses a friendly Botnet vaccine to protect IoT against the threats and attacks using Bitcoin Blockchain technology. Singh, et al [13] discusses putting transactions of IoT devices on the Blockchain network to avoid forgery of transactions.

## IV. Problem Statement

Internet Engineering Task Force(IETF) has formed a working group called DDOS Open Threat Signalling (DOTS) [6], which is working towards a robust, scalable solution for DDOS protection in the IP enabled network. DOTS has defined an architecture where the DDOS attack mitigation is addressed using a client, server, and mitigator architecture. DOTS architecture works only to define client and server connectivity details in the face of a DDOS attack. The devices under attack send performance statistics to DOTS clients with their health information. The client on the reception of any abnormal activity requests attack mitigation through a signal to the DOTS server. The DOTS server is connected to many mitigators and sends the requests to a specific mitigator for taking further action. The mitigation is done by the mitigator and the report is sent to the DOTS server. The DOTS server defines the policy to be pushed to clients and then from the clients to the devices to mitigate the attack at the source. IoT environments require a robust, reliable, scalable, and efficient mechanism to shield against the ever-growing DDOS attacks. With billions of devices connected, it is difficult to control the management and security plane for any unusual activity. DOTS can play a major role in such a situation. But how can DOTS help IoT to make the security solution trustable and reliable so that at any point in time IoT sensors are given protection against DDoS attacks?

## V. System Architecture

### A. Core Idea

IoT environments can use DOTS architecture to identify unobserved attacks in the IoT sensors for better security enhancements. The IoT environment can be thought of as an edge computing environment where a group of IoT sensors are managed by a single edge compute node and the edge compute nodes can provide information to cloud nodes for better visibility and control. Converting the IoT design into a DOTS architecture may add some benefits but not in a qualitative way. Most of the IoT networks are hierarchical and require collaboration between different regions to detect any malicious behavior. Blockchain is the perfect technology that provides such a distributed architecture in a collaborative fashion to process any computation.

### B. Blockchain Technology

Blockchain Technology: Blockchain is a cutting edge technology that solves many real-world problems today with it's decentralized solution that is ruling over centralized operations. Many businesses are now shifting towards Blockchain-based applications due to its resilience, stability, features and robustness. Blockchain works in a decentralized fashion where every participant has some contribution towards making a decision as a whole group. With a decentralized solution, every participant needs to compute results or vote towards a decision so that a minimum of 51% of votes will mean that a decision can be taken. Along with this, Blockchain provides features like immutability where any data that is already mined cannot be changed by any intruder or attacker.

Another feature that praises Blockchain is the ability to be fault-tolerant in it's defined architecture. Every participant in the Blockchain maintains a copy of the transactions by all other nodes in the network. At any point of time, if any participant is experiencing failure, other nodes can still participate in performing the operations required in Blockchain. Last but not the least, incentivization is another feature that represents Blockchain benefits to every participant in the network.

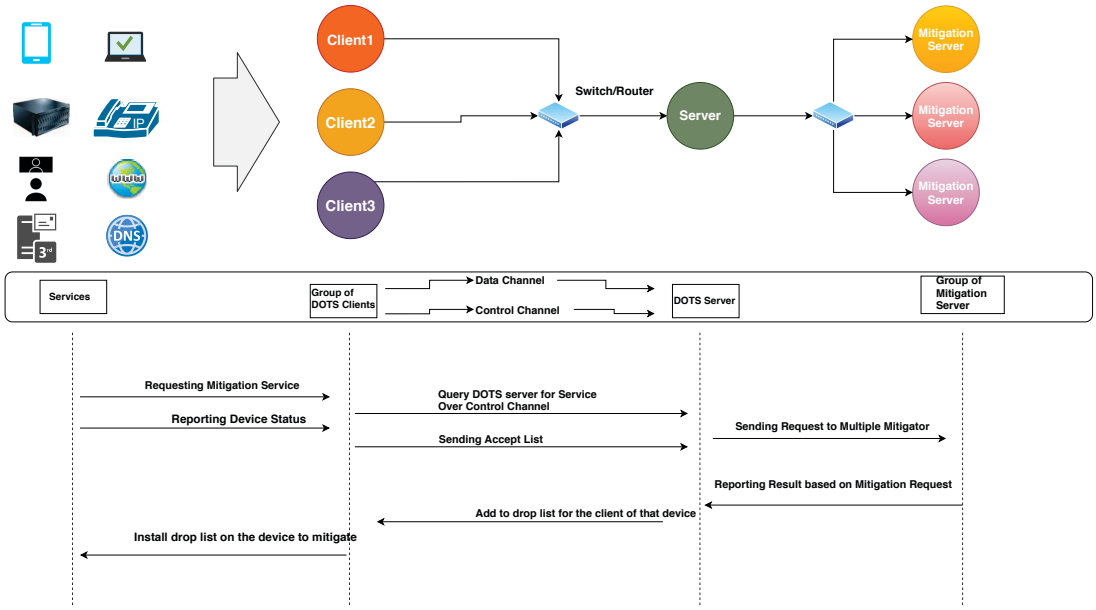


Fig. 1. DOTS Architecture Detailed

| Features | Benefits |
|---|---|
| Trust | Trust can be shared among several participants in a network to decide upon a legitimate action. Trust would increase from one device to many devices getting a better control over the policies and automation |
| Consensus | Central trust dependency is removed to achieve a distributed consensus based decision to come determine an outcome. |
| Immutability | Any change in the DDOS policy modification of data is restricted as the data is immutable based on which decision can be taken. History of data can be used over time to build heuristics problems that are based on legitimate signed data. |
| Collaboration | Collaboration is closely related to a consensus but can be considered as one of the engineered feature of Blockchain |
| Fault Tolerance | Decentralized correlation will ensure that the central server even if compromised, other participants in the network will continue the operation |

TABLE I
Advantages of Decentralized Blockchain Architecture For DDOS detection in IOT Sensors. [27]

Every element in the Blockchain are rewarded with certain credits or incentives that attract them towards solving a complex problem like mining. In a central server architecture, a single authority enjoys the benefit since it is only doing the necessary operations. Now in decentralized architecture, every participant in the Blockchain network gets a share of the incentive after solving the problem.

### C. Blockchain To Address IoT DDOS

Blockchain can help map DOTS architecture to IOT DDOS protection mechanism. Blockchain provides the tamper-proof, consensus based, fault-tolerant,decentralized architecture that can detect a malicious sensor by voting mechanism.

### D. Architectural Flow

In DOTS architecture, clients can be thought of edge compute nodes in an IoT environment that handles small jobs for devices. This scenario can be compared to a gateway based IoT environment where the IoT server is decentralized with edge gateways. The edge gateways maintain information about the devices that are controlled under this edge controller, and the high-level servers detect any anomaly through the Blockchain network. The edge controller and servers will be part of

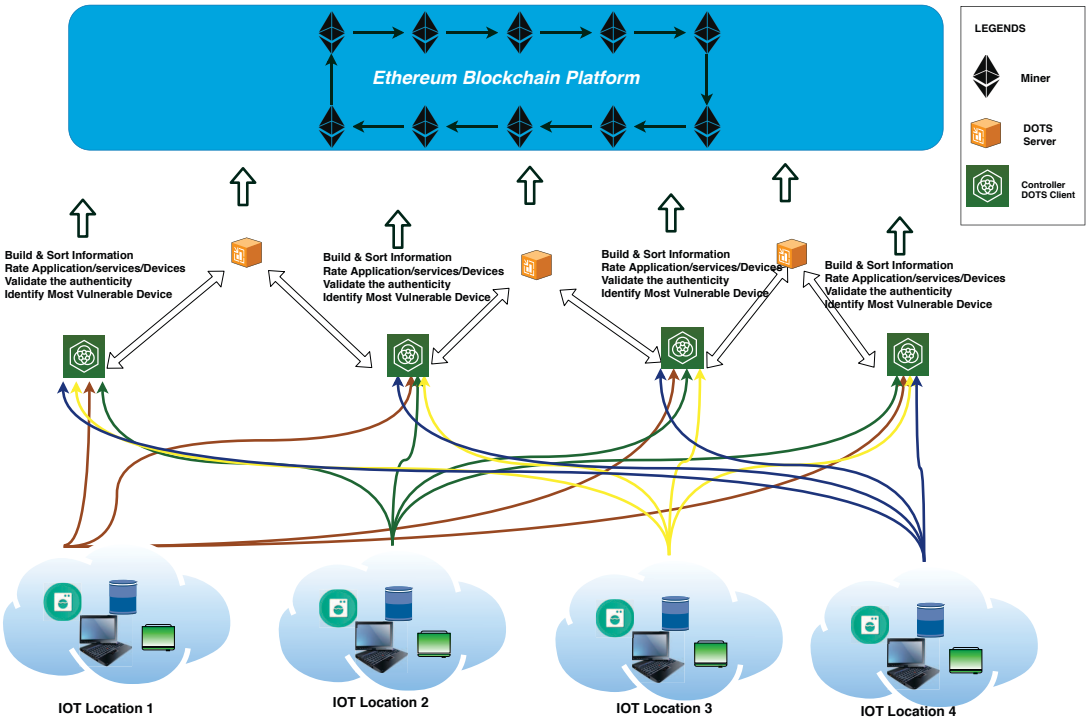


Fig. 2. Design Logic For IoT Edge Compute Collaboration

Blockchain transactions where each transaction is mined on the public or private Blockchain environment.

### *E. Design Diagram and Logic*

This architecture is to achieve the performance similar to DOTS Architecture to detect DDOS attacks on the sensors of IoT devices. The individual controller will send information about their sensors and the controllers will define a threshold level based on learned data on which the anomaly can be detected. Based on the threshold, the attacks will be detected and sensors can be blacklisted. The flow chart depicting the smart contract operational flow is very simple to give ease of operation for the operations manager or automation to perform the anomaly detection of a sensor device. The sensor information is stored in different files in the server for humidity, temperature, pressure and wind direction. Prepossessing of data is performed as per the date and values of individual sensors. The minimum and maximum of the temperature are calculated based on the variance of the input file. Then individual data is sent to the smart contract functions and loaded on Blockchain ledger. After that, detection of anomaly is performed with the votes and the sensor is blacklisted or not is determined. The data structure contains the values given

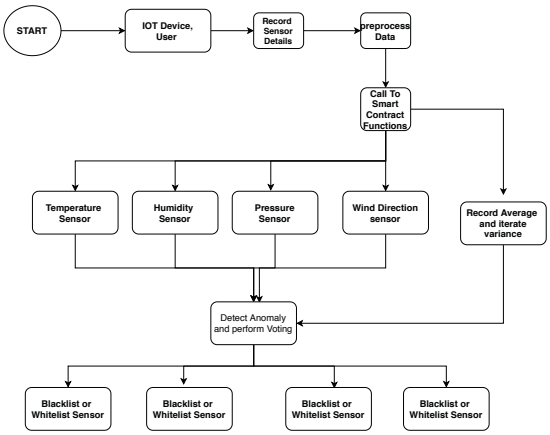


Fig. 3. Flow chart for the Anomaly Detection Mechanism

by the sensors in terms of ID, date and sensor value. These data structures are fed to the smart contract. The minimum and maximum value of the sensors on the same day is recorded and processed for threshold value that can be used to detect an attack in a day.

### *F. Distributed Ledger*

The Blockchain ledger contains the information about the function output in the distributed ledger and every

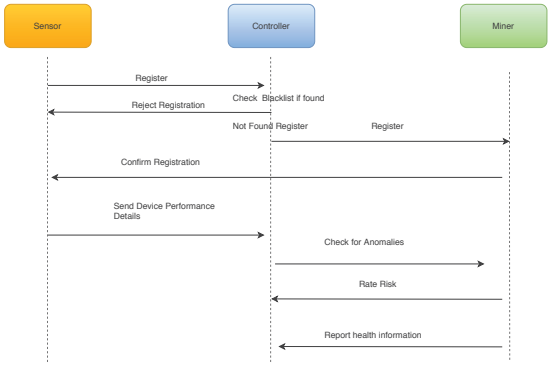


Fig. 4. Event Flow in the Design

transaction is recorded in a block. When a smart contract function is recorded, specific data information is recorded on Blockchain that is immutable and fault-tolerant due to the nature of Blockchain. The ledger will record information on sensor ID, date the input value of the sensor, and the status of the sensor[Blacklisted/Whitelisted].

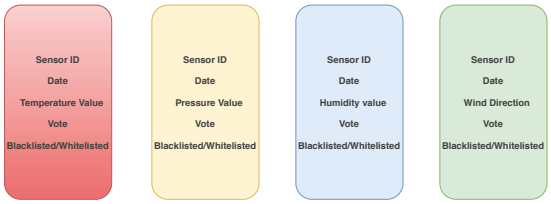


Fig. 5. Blockchain Ledger Data Structure

## VI. Test Setup

The test setup will include a file generated by sensor devices and DDOS Mitigation Engine on the Blockchain framework for all the anomaly detection procedures. A smart contract is coded and deployed based on the logic diagram mentioned earlier in this document. The server and mitigator will be part of the Blockchain network, where they will store and transact each of the device performances and their anomalous behavior. The function method calls will be sent through a node.js platform to mine transaction on the Blockchain network.

### A. Blockchain Terminologies

Some of the basic terms of Blockchain technology are required to be explained prior to going ahead with the test setup of the proposed idea.

- Gas - A unit of measurement for computational work performed. [28]
- Gas Limit - Amount of gas offered for a transaction. [28]
- Gas Price - Amount of ethers to be spent per gas unit and usually measured in GWei. [28]
- Ethereum - A connected network of large number of computers performing heavy computational work called as Ethereum Virtual Network(EVN). [28]
- Ropsten -A public testnet with EVN to perform transactions. [29]
- Ether - Currency used in Ethereum network for transaction. [28]
- Smart Contract - A set of rules and regulations coded to perform transactions. [28]

### B. Dataset

The dataset [26] is collected from City Pulse Dataset from the category of weather information from the City of Aarhus in Denmark. The dataset used contains information of sensor for two months for each sensor on temperature, humidity, pressure, and wind direction. Every sensor values will be tested against the variation of temperature on that day to find out whether an IoT is under any DDOS attack.70 readings are collected per day for 60 days.

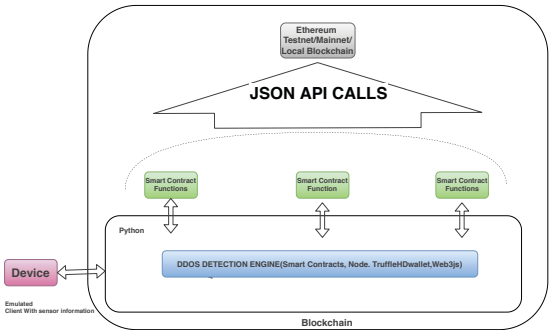


Fig. 6. Test Setup Diagram

### C. DAPP Automation

The automation of the Blockchain framework is the hardest part as a lot of technologies are undergoing release updates, maintenances, and bugs. DAPP automation requires many software and packages with javascript support such as truffle, node.js, trufflehdwalletprovider, web3js, solidity, Metamask and a Ropsten provider or local Blockchain framework. Apart from these, we also need fake ethers to run a transaction on public testnet. The main dependencies are between web3x developer and truffleHDwallet compatibility that has to be negotiated well.

### D. Smart Contracts

Since there are four sensors, the smart contract is coded with 4 functions to read in data. One function would check the variance and other would detect anomaly based on variance and the last one display blacklisted ID of the sensor.

## VII. Results

Different statistical data are collected to check the performance of the Blockchain-based DDOS detection with a voting mechanism so that the confidence on the technology can lead to the next level of revolution for security enhancement in cybersecurity space. Different metrics such as time complexity, cost and prediction accuracy are measured.

### A. Time and Gas Cost

The transaction time varies from 5 seconds to 42 seconds on the Ropsten network and from 150ms to 520 ms in the local Blockchain Ganache platform. We may need to add up the transaction times of 6 functions that will give us the result of prediction time for a DDOS attack. On the Ropsten network, the average function transaction time is 20.06 seconds and the average prediction time is 120 seconds. So time will be a major factor when there is a demand for online DDOS detection.

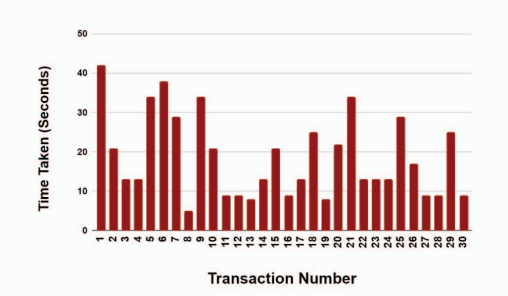


Fig. 7. Time(seconds) taken per transaction on Ropsten

Two platforms are tested with the same datasets. Local Blockchain shows that gas-use is constant with respect to the function execution. Ropsten network is showing little different variance than the local Blockchain. One thing to note that local Blockchain gas-use, ranging from 38000 to 62000 GWei for reading the sensor values but Ropsten ranges from 25000 to 85000 GWei with the rate of ethers fluctuating. In Ropsten, there are certain spikes that speak about greedy miners that can use up gas for the computation of the function or the processor load of that particular miner. Another reason for the gas-use to be higher is when the computations performed has more lines of codes in the function.

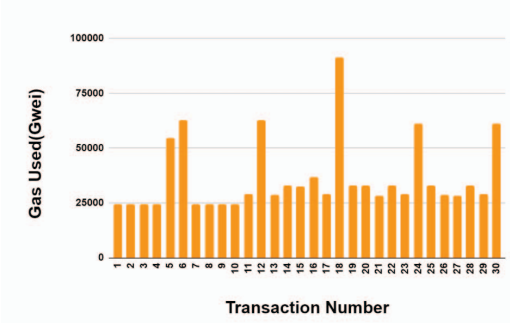


Fig. 8. Gas used per Transaction on Ropsten

### B. Threshold Decision

The mean of the data points(sensor information) is calculated for all sensor data readings of the same day and tested for the accuracy of detection based on the fact that the sensor value falls under the minimum and maximum range around the mean. The threshold technique is used to detect anomaly in IoT sensor behavior. The dataset consists of 70 readings of 60 days, where each day will reflect a certain variation of sensor information. The mean of the sensor data is calculated and variance is applied to consider a threshold. A new data of the same day is taken and checked for the detection of an abnormal behavior based on the threshold.

### C. Detection Accuracy

It was found that the accuracy is increasing rapidly between the variance of Humidity range between 12 to 20 percentage in figure 9. The graph shows a stable line between 18 to 28 percentage of humidity, reflecting no change in accuracy for these many data points variation citing the fact that we can arbitrarily fix a variance of 18 percentage for benign behavior of an IoT sensor.

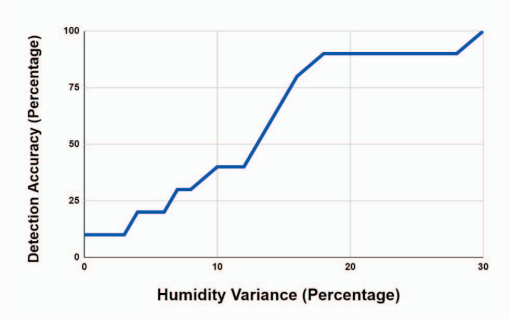


Fig. 9. Detection accuracy for varying Humidity

Figure 10 shows detection accuracy with varying temperature measurements. The detection accuracy for temperature variance is seen to be linear, which means as the number of variance increase number of IoT sensor outputs fall under the variation. The data points and the variance is just between -4 to +4 degree Celsius, which is very less compared to the humidity variance in figure 9. The miners will be calculating the mean and adding variance to the mean to detect anomaly.

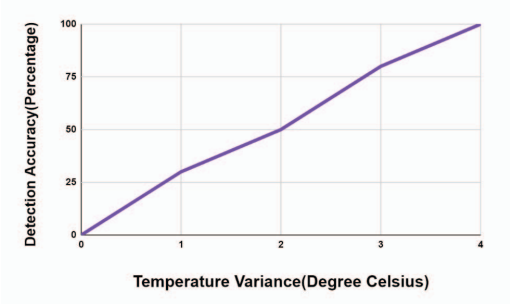


Fig. 10. Detection accuracy for varying temperature

### D. Parameter vs Cost

Related to smart contract behavior, interesting facts have been explored with the smart contract functions being exploited with the number of input data points. As observed, if the number of input parameters increases, the gas used increases linearly. The gas-use ranges from 170000 - 580000 GWei for 0-30 data point inputs. It is important to keep in mind that, with the Blockchain framework, IoT edge nodes and servers will have to spend a good amount of ethers to come to a consensus of detecting the state of an IoT sensor. We are expecting to solve the high cost issues in our future work with a better design criteria.

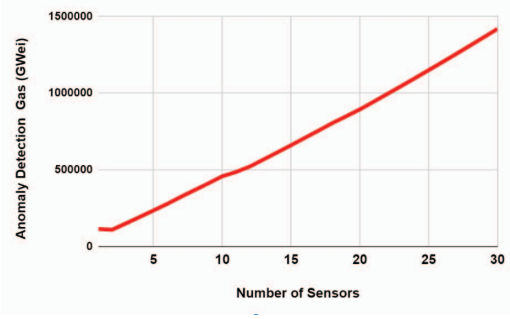


Fig. 11. Gas Consumed For an increasing number of data points on Smart Contract

### E. Function Computations vs Gas Used

Another interesting graph that illustrates the behavior of Blockchain is the amount of computation performed inside a function versus the gas used. It is seen from figure 11 that the gas-use increase with more number of sensors inputs to detect anomaly in the IoT environment. Therefore, while designing an application with Blockchain for the IoT environment for security enhancement, the cost is a major factor as the cost of the protection should not exceed the cost of the property to be protected.

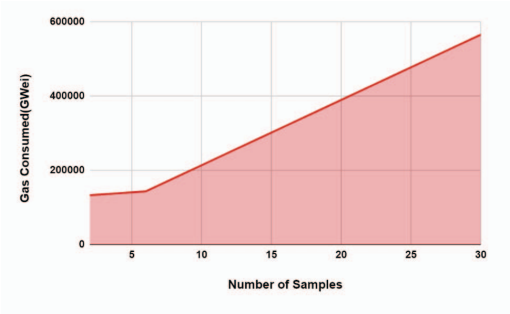


Fig. 12. Gas consumed for Anomaly Detection Process On Smart Contract Functions

The gas consumed for more parallel sensor DDOS detection is shown in Figure 11. the gas use varies between 100000 to 15000000 GWei, showing a massive increase in gas use for 0-30 sensors. So this means that if we execute a function with more sensors, it will cost the miner more to detect the anomaly.

## VIII. Conclusion

DOTS architecture provides a scalable and robust solution for mitigating the DDOS problems in the current information technology arena. DOTS architecture is designed for every possible design platform including IoT edge computing. Why Blockchain? To map DOTS with IoT requires a major security trust which can be supported by Blockchain technology. Blockchain provides the best possible solution to eliminate any third-party involvement and secure the transactions of DOTS architecture in IoT environments. It does this by securing IoT sensors, preventing them from being the victim of any malicious devices through the voting mechanism of a Blockchain (consensus). This collaborative voting mechanism could go a long way to secure billions of IoT devices and eventually protect any network from being choked or compromised.

## IX. Future Work

With more sampling inputs and more parallel sensor DDOS detection, there is possibility of high gas use eventually leading to a high cost. We would like to address this part to reduce the cost to make the proposal more feasible in terms of cost. The technique used in this paper is threshold-based and is very simple to detect and give outputs of the sensor status. The behavior would be more interesting if some kind of predictions can be performed by learning the data points for predicting an attack in the IoT environment. Next, the focus would be on prediction based on learned data of the sensors. We will be exploring some of the machine learning techniques that can help us in predicting a DDOS attack. architecture.

## References


[1] Dwight B. Davis, "Symantec IoT Cyber attack growth",April 2019,https://symantec-blogs.broadcom.com/blogs/expert-perspectives/ istr-2019-internet-things-cyber-attacks-grow-more-diverse

[2] Christina Quast,"Common Attacks on IoT device",October 2018, Europe, Open IoT Summit,https://elinux.org/images/f/f8/Common-Attacks-on-IoT-Devices-Christina-Quast.pdf

[3] Ziv Chang and Shin Li,"Trendmicro discussion on IoT security threats",May 2019,https://www.trendmicro.com/vinfo/us/security/news/ internet-of-things/the-IoT-attack-surface-threats-and-security-solutions

[4] Josh Fruhlinger,"Mirai botnet discussion", March 2018 https://www.csoonline.com/article/3258748/ the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

[5] Andrew Mortensen, Tirumaleswar Reddy ,Mortensen, et al, "DOTS Architecture for DDOS protection",,May 2019(Last revision), February 2020(Current), IETF Draft

[6] Tirumaleswar Reddy, Joshi Harsha "Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Call Home", September 2019, IETF Draft

[7] Khaled Salah, Minhaj Ahmad Khan"IoT security: Review, Blockchain solutions, and open challenges",November 2017,Volume 82, May 2018,

[8] Ana Reyna,Cristian Martin,Jaime Chen,Enrique Soler,Manuel Díaz *On Blockchain and its integration with IoT Challenges and opportunities*,Volume 88, November 2018, Pages 173-190

[9] M. Singh, A. Singh and S. Kim, "Blockchain: A game-changer for securing IoT data," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 51-55.

[10] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, 2017, pp. 618-623.

[11] Di Pietro, Roberto and Salleras, Xavier and Signorini, Matteo and Waisbard, Erez, "A Blockchain-based Trust System for the Internet of Things", Indianapolis, Indiana, USA, SACMAT '18

[12] Gregory Falco, Caleb Li, Pavel Fedorov, Carlos Caldera, Rahul Arora, KellyJackson, "NeuroMesh: IoT Security Enabled by a Blockchain-Powered Botnet Vaccine", BOOK, May 2019

[13] M. Singh, A. Singh and S. Kim, "Blockchain: A game-changer for securing IoT data," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 51-55.

[14] S. Chen et al., "A Novel Terminal Security Access Method Based on Edge Computing for IoT," 2018 International Conference on Networking and Network Applications (NaNA), Xi'an, China, 2018, pp. 394-398.

[15] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu and W. Lv, "Edge Computing Security: State of the Art and Challenges," in Proceedings of the IEEE, vol. 107, no. 8, pp. 1608-1631, Aug. 2019.

[16] O. B. Mora, R. Rivera, V. M. Larios, J. R. Beltrán-Ramírez, R. Maciel and A. Ochoa, "A Use Case in Cybersecurity based in Blockchain to deal with the security and privacy of citizens and Smart Cities Cyberinfrastructures," 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 2018, pp. 1-4.

[17] O. Abdulkader, A. M. Bamhdi, V. Thayananthan, F. Elbouraey and B. Al-Ghamdi, "A Lightweight Blockchain-Based Cybersecurity for IoT environments," 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Paris, France, 2019, pp. 139-144.

[18] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala and S. Elkhediri, "CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6.

[19] R. Neisse, J. L. Hernández-Ramos, S. N. Matheu, G. Baldini and A. Skarmeta, "Toward a Blockchain-based Platform to Manage Cybersecurity Certification of IoT devices," 2019 IEEE Conference on Standards for Communications and Networking (CSCN), GRANADA, Spain, 2019, pp. 1-6.

[20] T. Faika, T. Kim, J. Ochoa, M. Khan, S. Park and C. S. Leung, "A Blockchain-Based Internet of Things (IoT) Network for Security-Enhanced Wireless Battery Management Systems," 2019 IEEE Industry Applications Society Annual Meeting, Baltimore, MD, USA, 2019, pp. 1-6.

[21] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu and Y. Zhao, "EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4719-4732, June 2019.

[22] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019.

[23] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad and J. Wang, "Blockchain-enabled Distributed Security Framework for Next-Generation IoT: An Edge-Cloud and Software Defined Network Integrated Approach," in IEEE Internet of Things Journal.

[24] M. Alrowaily and Z. Lu, "Secure Edge Computing in IoT Systems: Review and Case Studies," 2018 IEEE/ACM Symposium on Edge Computing (SEC), Seattle, WA, 2018, pp. 440-444.

[25] A. S. Muttavarapu, R. Dantu and M. Thompson, "Distributed Ledger for Spammers' Resume," 2019 IEEE Conference on

Communications and Network Security (CNS), Washington DC, DC, USA, 2019, pp. 1-9.
[26] Muhammad Intizar Ali, Feng Gao and Alessandra Mileo, "CityBench: A Configurable Benchmark to Evaluate RSP Engines Using Smart City Datasets", The Semantic Web - ISWC 2015 - 14th International Semantic Web Conference, October 11-15, 2015, Bethlehem, PA, USA.
[27] J. Golosova and A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology," 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Vilnius, 2018, pp. 1-6.
[28] Aziz,"Guide to Ethereum: What is Gas, Gas Limit and Gas Price"[Online],Available: https://masterthecrypto.com/ethereum-what-is-gas-gas-limit-gas-price/ [Accessed: 15 March, 2020]
[29] Moritz Neto,"Get Ropsten Ethereum — The Easy Way."Available:https://medium.com/bitfwd/get-ropsten-ethereum-the-easy-way-f2d6ece21763,[Accessed: 15 March,2020]