International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 6, Issue 6, ISSN No. 2455-2143, Pages 106-112
Published Online October 2021 in IJEAST (http://www.ijeast.com)

OPTIMIZING THE SECURITY OF IOT SYSTEMS VIA AI BASED BLOCKCHAIN ARCHITECTURE

Mrs. Munazza Zarin R. Shaikh
M.E Digital Electronics (Student)
Department of Electronics and Telecommunication Engineering
Babasaheb Naik college of Engineering, Pusad
Maharashtra, India

Dr. N. A. Charniya
Professor(Guide)
Department of Electronics and Telecommunication Engineering
Babasaheb Naik college of Engineering, Pusad
Maharashtra, India

Abstract— **Security in Internet of things (IoT) networks is a diverse test. It includes planning security calculations that should work adequately on a battery fuelled gadget. This adequacy should be as far as low defer prerequisite, low energy necessity, high throughput necessity and high parcel conveyance proportion necessity. This load of necessities is hard to accomplish because of the way that the quantity of assaults common to any IoT network are extremely huge in number, and each assault has its own particular kind. For example, DDoS assaults focus on a specific hub from various assault focuses, while sybil assaults adjust the information bundles to such an extent that the real beneficiary doesn't get the parcel; there are numerous such assaults pervasive to IoT organizations. This paper proposes a blockchain controlled calculation that utilizations evidence of work (PoW) agreement (on the switch side), to distinguish and safeguard against an assortment of IoT assaults. The primary benefit of utilizing a PoW fuelled blockchain is the adaptability of square plan, which can be changed according to the IoT application. This content likewise covers validation and approval utilizing a blend of blockchain and trust-assessment between partaking hubs. This content looks at the proposed block-chain fuelled organization results with a non-blockchain execution and the organization proficiency showed over 20% improvement as far as postponement, and bundle conveyance proportion. Our concern definition is, to at first plan a blockchain based framework, then, at that point test the security of the application. Whenever that is done then assess the security openings in the framework, and join confirmation with blockchain. Post this plan of an AI and ML based encryption layer for information security, and if necessary, adjust the AI layer to incorporate information approval for further developed security. At long last, coordination of validation and information security to shape a security structure, then, at that point testing the framework on the given application, and assessment of execution of this new framework. If necessary, we can go for enhancement of the planned framework.**

Keywords— **IoT, DDoS (Distributed Denial of Service), Sybil assaults, blockchain, AI (Artificial Intelligence), ML (Machine Learning).**

I. INTRODUCTION

Security is a critical worry for a wide scope of IoT frameworks. For high security applications like banking, the need to ensure that safe data outflanks the need to propel the limit cost, computational cost and surprisingly the running cost of the structures. As needs be, in any occasion 60% of everything research done in the field of data planning is associated with security in one way or the other. Ensuring about data is secure in the framework makes the structure have a huge computational breaking point, from that point forward the system can perform complex encryption activities like handling elliptic bends or evaluating complex cross segment organizations. Regardless, for low energy IoT contraptions, having such complex mathematical computations is both monotonous and requires enormous energy. Generally, all IoT structures rely upon peer frameworks and need to recognize, gauge and perform undertakings inside a predetermined time span. Thusly, there is a prerequisite for low defer systems which can fulfil the accompanying measures,

- Must be low force
- Must be fast in scrambling the data
- Should have high security

In order to design an IoT based security system that fulfils all the above imperatives, researchers have made powerful methodology like blockchains and friend registering. Blockchains work using a direct P2P standard, which relies upon understanding based check. The most broadly perceived instance of a blockchain based IoT organize is the Ethereum blockchain. Ethereum stores its worth put together data with respect to low controlled and computationally light weighted IoT network hubs by means of agreements. These IoT network hubs basically pass on copies of the worth-based data which are affirmed by other honourably believed IoT network hubs called as verifiers or diggers. Blockchain excavators are other amazing IoT network hubs that make new agreements for the blockchain. Thusly, by using a mix of a wide scope of IoT and non-IoT network hubs, the Ethereum framework can give a raised degree of safety for contingent data. An instance of how blockchain can be used in IoT frameworks is given in figure 1. It highlights various spots where blockchain can be used to ensure about the IoT frameworks like enrolment, verification, agendas, etc.

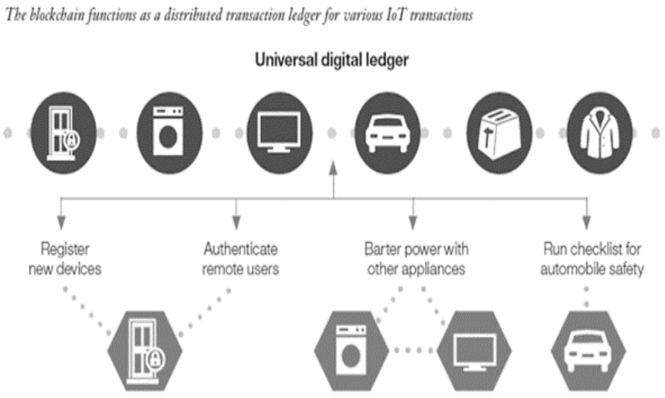
The blockchain functions as a distributed transaction ledger for various IoT transactions
Universal digital ledger
Register new devices
Authenticate remote users
Barter power with other appliances
Run checklist for automobile safety

Figure 1. Application of blockchain to secure IoT

Like Ethereum other contingent structures like banking, land, immense extension undertaking resource overseeing systems, etc are similarly embracing blockchain as their security framework. Blockchain security can be completed by choosing an arrangement computation like Proof of Work, Proof of Stake, etc, then, at that point finishing the construction of brilliant agreements or different squares in the chain, then, at that point choosing the mining unpredictability lastly fixing a hashing and encryption procedure.

Considering these limits, a blockchain structure's multifaceted nature can be tuned. For IoT security, a lower diverse understanding computation, close by lower multifaceted nature mining and cryptographic estimations can be picked. The grandness of blockchain is that its security isn't dependent upon the eccentricism of the computations, yet the amount of IoT network hubs in the framework can increment. Henceforth, a distorted blockchain execution is adequate for a tremendous IoT association. As the size of the IoT association increment there can be a further abatement in the eccentricism of the computations which can moreover smooth out the Quality of Service (QoS) limits of the framework. Blockchain has become an exemplification of safety calculations since its initiation. This is because of the way that blockchain fuelled organizations utilize hashing, encryption, agreement, design coordinating, and other profoundly better calculation all together than work on the security. Any blockchain controlled organization plays out the accompanying tasks while imparting bundles from sender to collector [1],

- The bundle begins from the sender side, and another square is made
- The block is loaded up with the accompanying data prior to being sent over the organization,

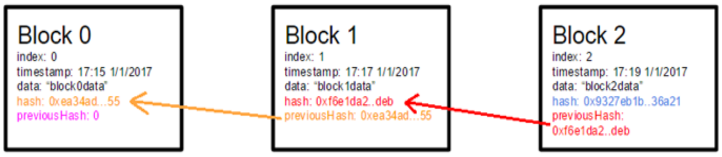

Figure 2. A sample blockchain (with sample blocks)

- The source and objective locations
- The time stamp of correspondence
- A nonce number that is utilized to produce rule-based hashes
- The CRC of the information, or potentially the actual information
- A hash from the past block (given by the switch)
- Any other correspondence related data, similar to the parcel number, the maximum number of jumps, and different fields

- The block is encoded utilizing elliptic bend cryptography (ECC), Advanced Encryption System (AES), or some other cryptographic calculation
- This scrambled square is sent through the organization by means of any of the IoT controlled designs like LoRA, SigFox or NBIoT
- During the steering of these squares, every one of the hub on the course communicates this parcel to the adjoining hubs, to such an extent that every bundle is available with numerous hubs in the organization
- The hubs that take an interest in this communicating cycle are called as verifiers
- Each of the verifier hub has an obligation to keep the square put away inside it for a specific time frame span 't'
- In case a verifier needs to quit the organization, or requirements to drop obstructs if there should arise an occurrence of limit or energy issues, then, at that point the verifier illuminates the adjoining hubs about this occasion with a specific key, that is pre-divided among the verifier and the organization switch

- This key is utilized just a single time by the verifier, and just if there should arise an occurrence of inconsistencies with the verifier hub
- Upon gathering of this key at the switch, the verifier hub is set apart as 'non-reliable' and its information is disposed of from any confirmation cycle
- Once the bundle is gotten at any beneficiary hub, a confirmation interaction is performed
- This confirmation measure assembles blocks from arbitrary hubs, and checks if the sent square is really the right one
- The checking measure looks at the hash of the current square, with the hash upsides of the got blocks
- Under typical organization activity conditions, these hash esteems should be same
- But, in the event of assaults, the hash esteems change, and consequently the recipient hub needs to perform block approval
- In request to perform block approval, the recipient checks whether the hash of the got block is coordinating with the hash of over half squares got from the verifiers
- If it matches, then, at that point the coordinating with blocks are set apart as protected squares, while different squares are disposed of from the blockchain of the beneficiary

This whole stream can be portrayed with the assistance of figure 3 as follows [2],

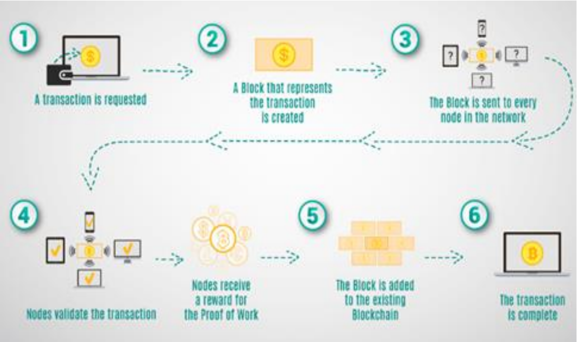
1
A transaction is requested
2
A Block that represents the transaction is created
3
The Block is sent to every node in the network
4
Nodes validate the transaction
Nodes receive a reward for the Proof of Work
5
The Block is added to the existing Blockchain
6
The transaction is complete

Figure 3. Example of blockchain working

Utilizing the standard referenced in the means, any organization planner can install blockchain into their organization. To recognize and eliminate assaults from a blockchain controlled organization, the idea of square confirmation must be demonstrated cautiously. In this progression, the squares should be confirmed with the assistance of a chose agreement convention. For example, this content uses Proof of Work (PoW) agreement, while specialists have proposed other agreement strategies like Proof of Stake (PoS), Proof of Energy (PoE), Delegated Proof of Stake (DPos), and others [10,11]. The following area depicts an examination about various blockchain-fuelled organizations for assault location and evacuation. In this paper, PoW is utilized to safeguard the organization against an assortment of assaults. Insights concerning the proposed calculation are introduced in the later area, trailed by execution assessment of the framework. This content finishes up for certain fascinating perceptions about the proposed work, and furthermore suggests techniques through which the framework execution can additionally be upgraded.

II. PROPOSED MODEL

The architecture can be observed from the following figure 4. The proposed framework will initially perform security investigation of the framework. Then, at that point the framework will choose an IoT application and any agreement based blockchain calculation alongside it. The calculation will run and the ML layer will guarantee that all the blockchain related boundaries like, blockchain type, encryption and unscrambling, rules and other standard boundaries are available inside every one of the squares. This will build the square length imperceptibly at the same time, it would help the calculation to give better security. Private data identified with encryption and unscrambling, for example, keys and code length would be pre-designed in the organization, so that there are no spillages on this part. When the ML layer is in activity, numerous chain types, and side chains will be underlying request to impart the information between different hubs of the organization.

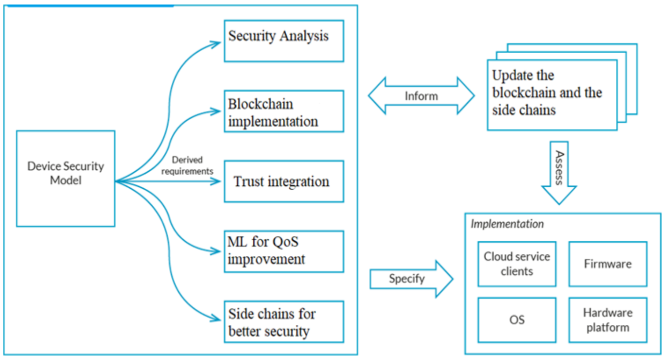

Figure 4. The proposed architecture

These side chains and principal chains will be re-arranged utilizing the profound nets and other ML and AI based strategies to additionally reinforce the security of the organization. It ought to be seen here that only one ML layer will be functional, which will deal with both the calculation type, and control the generally speaking blockchain design of the organization. This load of modules will be conveyed on the switch, where administration customers, working framework programming, firmware and equipment stages will be incorporated. Layers like data, evaluation, and particulars will be utilized to shape an input circle between the sent layers and the carried-out module. The gadget model determination will be given to the sent layer, wherein dependent on the input, the sidechains will be changed, lastly dependent on the sidechain execution the data will be given to the IoT equipment. This shut circle layer will be useful in ID of any sort of assaults, or QoS decreases, and will at long last assistance in further developing the framework execution.

A. Data flow diagram

The stream outline of the proposed framework can be portrayed in figure 5 as follows:

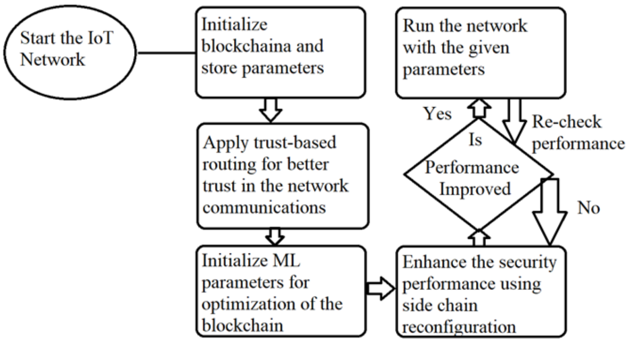
Start the IoT Network
Initialize blockchaina and store parameters
Apply trust-based routing for better trust in the network communications
Initialize ML parameters for optimization of the blockchain
Run the network with the given parameters
Yes
Re-check performance
Is Performance Improved
No
Enhance the security performance using side chain reconfiguration

Figure 5. Flow diagram for the system

The proposed framework will begin by choosing an IoT application and conveying blockchain into it. Trust-based steering will be applied to further develop the correspondence trust in the organization. Then, at that point Machine Learning boundaries will be introduced to upgrade both security and QoS execution of the blockchain utilizing side fastening. In the event that the exhibition isn't improved, these boundaries will be re-tuned and the last boundaries will be utilized to convey the organization. At last, nonstop checking of these boundaries will be done to upgrade the framework execution utilizing AI.

B. System Design

The proposed PoW controlled IoT network utilizes 2 primary segments for coordinating blockchain into the organization,

- A light-weight trust assessment structure
- A PoW controlled blockchain structure for joining with the organization

The light weight trust assessment structure further develops the directing presentation of the framework, by choosing hubs that have high trust levels. The hub determination cycle can be clarified with the assistance of the accompanying advances.

- Identify the hubs that require information directing, let the source hub be 'src' and the objective hub be 'dest'
- For every hub close 'src' assess the sending proportions 'frab' and 'frba' as follows,

$$frab = \frac{fpi}{fpi - fpsrc} \ldots (1)$$

$$frba = \frac{fpsrc}{fpsrc - fpi} \ldots (2)$$

Where, frab is the forwarding ratio from node 'i' to node source node, while frba is the counterpart, and fpi is the number of packets forwarded from node 'i'

- Now evaluate the value of 'tau' using the following formula,

$$tau = tau + alpha * abs(frba - frab) \ldots (3)$$

Where, alpha is the trust constant, and tau is initially set to 0

- Using the value of 'tau', the error value is evaluated,

$$error = \frac{tau^2}{di_{src} * di_{dest}} \ldots (4)$$

Where, 'disrc' is the distance between the current node and the source, while 'didest' is the distance between current node and the destination

- Using the error value, the value of trust is evaluated using the following formula,

$$t_i = \frac{E_i * error + E_{src} * error}{2} \ldots (5)$$

Where, 'Ei' and 'Esrc' are the energy of 'ith' and source nodes respectively

- This introduces the energy, distance and packet forwarding ratios in a single trust equation

The conditions are assessed for every one of the hubs, and the hubs with most extreme trust levels are found. The cycle ends when a hub is discovered, that can send information to the objective in most extreme one bounce. Guaranteeing that the information is sent with least bounces from source to objective with most noteworthy trust level. When these trust levels are set up, then, at that point the light weight PoW blockchain is introduced. This blockchain stores the accompanying data about every correspondence,

prev_hash [256]	Source	destination
data	None	hash [256]

Table 1: Structure of the block

This structure is used at each communication stage, and at each hop during data transmission. The data from source is given to the destination via trust-based hopping. Thus, during each hop the source and destination in the block will vary. A combination of these blocks is stored on each of the neighbouring nodes of the network. The neighbouring nodes are defined as the nodes that can be covered via one-hop of the network. In case of any attack, the following verification process is performed to check whether a given block is valid or not.

This data is given to the jumping hub, and in the event that the inward hub's blockchain doesn't follow condition 7, the chain is disposed of, and is supplanted by the right chain. The right chain is assessed from the most comparative right chains of the bouncing hubs. This load of activities takes precisely one correspondence cycle, and consequently are light weight as far as calculation intricacy, and correspondence delay. Because of this reality, the general organization gets secure, and is decentralized as far as organization correspondence. Besides, because of the immediate trust and confirmation estimations, the organization is shielded from any sort of steering and parcel alteration assaults. The framework was tried under various organization conditions, and the outcomes are classified.

C. TOOLS AND TECHNIQUES

Simulation has been done on large scale compatible tools NS2(Version 2.34)
Some of these utilities used for the experiments are further described below-
(i) cbrgen.tcl: The ns –package comes with a traffic generator utility which can be found in the folder ~ns/indep-utils/cmu-scen-gen/ (where ~ns denotes the ns-directory, for example, /home/administrator/ns-allinone2/ns-2.27/ for the ns-2.27 version) . This utility is used to generate trace files for specifying the type, duration and the rate of traffic flow in the network. The utility can be invoked by calling the Tcl script cbrgen.tcl as follows-

```
$ ns cbrgen.tcl  [list of parameters]
```

List of Parameters:

- Type of traffic: CBR or TCP
- Seed: starting number for random number generator
- Nr: number of node
- Nc: maximum number of connection
- Rate: number of packet per second (bit rate)

III. RESULT

The proposed convention is successful in eliminating Sybil, Masquerading and Flooding assaults from the organization. This is because of the way that after utilization of the light-weight blockchain based trust convention into the IoT organization, the bundles are being sent and gotten with diminished postponement and energy necessities. The normal of these postponement and energy esteems is assessed, and can be seen from figure 6 and 7 separately.

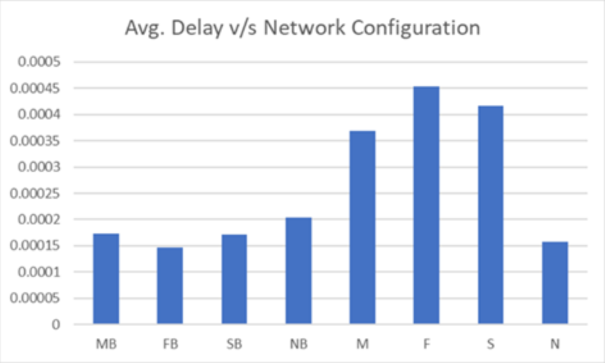

Figure 6. Average delay v/s Network Configuration

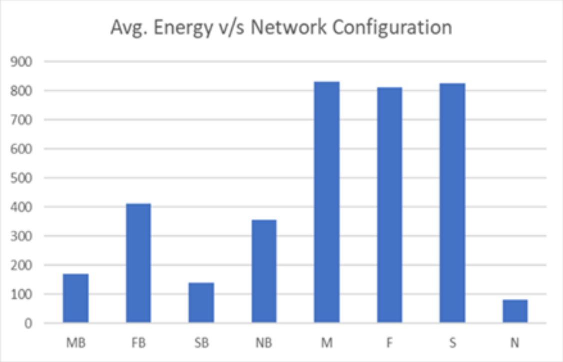

Figure 7. Avg. Energy v/s Network Configuration

The carried out network design guarantees that the lifetime and speed of the organization are expanded, in this manner working on the QoS of the organization. Because of incorporation of QoS-mindful fix at radio-level, the QoS execution of the proposed portion is predominant when contrasted.

IV. CONCLUSION

more noteworthy number of sensors, and handling units for better execution considerably under various types of assaults. The framework execution can be assessed under more perplexing IoT network conditions, with a more noteworthy number of hubs and cloud combination. Likewise, the presentation can be improved by utilizing light-weighted AI arrangements that further upgrade the QoS of the organization. Alteration of an IoT piece requires proficient plan of patches, that should further develop execution at both organization level, and hub level. The basic piece fix can decrease energy utilization, and start to finish postpone when contrasted and existing cutting-edge models. This presentation improvement is additionally going with further developed bundle conveyance proportion, and further developed organization throughput. Because of fuse of patches for QoS improvement, the deferral is decreased by 5%, while energy effectiveness is improved by 15% on a normal. This improvement in QoS execution shows that the fundamental part modules can be carried out for a wide assortment of IoT applications that require low energy utilization and fast of activity. In addition, because of joining of adaptation to non-critical failure fix, the bit execution is additionally worked on as far as throughput and bundle conveyance proportion. It is seen that the hidden portion has 15% better throughput, and 23% better parcel conveyance proportion under broken hub conditions when contrasted and existing part models. This exhibition is additionally improved through option of a security fix, wherein light weight confirmation is going with accumulation security and high velocity encryption. Determination of these security modules helps with decreasing likelihood of assaults, because of which start to finish delay is diminished by more than 10%, and parcel conveyance proportion is improved by more than 20% when contrasted with different pieces. This 3-

overlay improvement in execution makes the fundamental portion model pertinent for high velocity, low force, and high consistency applications like mechanical IoT, home IoT, and military IoT situations. This presentation can be additionally upgraded by utilization of profound learning models, alongside mathematical position models that help with further developing hub revelation and steering stages. Besides, expansion of blockchain to the framework can additionally help with further developing its security execution, and cause the calculation to perform better for a more extensive scope of assaults like blackhole, wormhole, and other infusion assaults.

V. REFERENCE

[1] X. Sun, Y. Li, N. Wang, Z. Li, M. Liu and G. Gui, "Toward Self-Adaptive Selection of Kernel Functions for Support Vector Regression in IoT-Based Marine Data Prediction," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9943-9952, Oct. 2020, doi: 10.1109/JIOT.2020.2988050. program (NCEP) expert panel on detection, evaluation, and treatment of highblood cholesterol in adults (adult treatment panel III) finalreport. Circulation. 2002;106(25, article 3143).

[2] D. Li, Z. Zhang, W. Liao and Z. Xu, "KLRA: A Kernel Level Resource Auditing Tool For IoT Operating System Security," 2018 IEEE/ACM Symposium on Edge Computing (SEC), 2018, pp. 427-432, doi: 10.1109/SEC.2018.00058.

[3] Sigwart, M., Borkowski, M., Peise, M. et al. A protected and extensible blockchain-based information provenance system for the Internet of Things. Pers Ubiquit Comput (2020). https://doi.org/10.1007/s00779-020-01417-z

[4] Mbarek, B., Jabeur, N., Pitner, T. et al. MBS: Multilevel Blockchain System for IoT. Pers Ubiquit Comput 25, 247–254 (2021). https://doi.org/10.1007/s00779-019-01339-5

[5] Jabbar, S., Lloyd, H., Hammoudeh, M. et al. Blockchain-empowered inventory network: investigation, difficulties, and future bearings. Interactive media Systems (2020). https://doi.org/10.1007/s00530-020-00687-0 H. Haddadpajouh, A. Mohtadi, A. Dehghantanaha, H. Karimipour, X. Lin and K. - K. R. Choo, "A Multikernel and Metaheuristic Feature Selection Approach for IoT Malware Threat Hunting in the Edge Layer," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4540-4547, 15 March15, 2021, doi: 10.1109/JIOT.2020.3026660.

[6] Firoozjaei, MD, Lu, R, Ghorbani, AA. An assessment system for privacy-preserving arrangements relevant for blockchain-based internet-of-things stages. Security and Privacy. 2020; 3:e131. https://doi.org/10.1002/spy2.131.

[7] Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo, and Antonino Nocera. 2017. Conquering Limits of Blockchain for IoT Applications. In Proceedings of the twelfth International Conference on Availability, Reliability and Security ARES. Relationship for Computing Machinery, New York, NY, USA, Article 26, 1–6. DOI: https://doi.org/10.1145/3098954.3098983 M. Yaker et al., "Guaranteeing IoT Security with an Architecture Based on a Separation Kernel," 2018 IEEE sixth International Conference on Future Internet of Things and Cloud (FiCloud), 2018, pp. 120-127, doi: 10.1109/FiCloud.2018.00025.

[8] Xudong Jia, Ning Hu, Shi Yin, Yan Zhao, Chi Zhang, Xinda Cheng, "A2 Chain: A Blockchain-Based Decentralized Authentication Scheme for 5G-Enabled IoT", Mobile Information Systems, vol. 2020, Article ID 8889192, 19 pages, 2020. https://doi.org/10.1155/2020/8889192

[9] Y. Zheng, Z. Melody, Y. Sun, K. Cheng, H. Zhu and L. Sun, "An Efficient Greybox Fuzzing Scheme for Linux-based IoT Programs Through Binary Static Analysis," 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC), 2019, pp. 1-8, doi: 10.1109/IPCCC47392.2019.8958740.

[10] S. Dami and M. Yahaghizadeh, "Productive occasion expectation in an IOT climate dependent on LDA model and backing vector machine," 2018 sixth Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), 2018, pp. 135-138, doi: 10.1109/CFIS.2018.8336655.

[11] N. Suga, K. Yano, J. Webber, Y. Hou, T. Higashimori and Y. Suzuki, "Assessment of Probability Density Function Using Multi-data transfer capacity Kernel Density Estimation for Throughput," 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2020, pp. 171-176, doi: 10.1109/ICAIIC48513.2020.9065033.

[12] Li, H., Pei, L., Liao, D. et al. BDDT: use blockchain to work with IoT information exchanges. Bunch Comput 24, 459–473 (2021). https://doi.org/10.1007/s10586-020-03119-w

[13] F. Peng, W. Peng, C. Zhang and D. Zhong, "IoT Assisted Kernel Linear Discriminant Analysis Based Gait Phase Detection Algorithm for Walking With Cognitive Tasks," in IEEE Access, vol. 7, pp. 68240-68249, 2019, doi: 10.1109/ACCESS.2019.2915290.

[14] Y. Zhao et al., "Protection Preserving Blockchain-Based Federated Learning for IoT Devices," in IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1817-1829, 1 Feb.1, 2021, doi: 10.1109/JIOT.2020.3017377.

[15] C. H. Liu, Q. Lin and S. Wen, "Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3516-3526, June 2019, doi: 10.1109/TII.2018.2890203.

[16] Uriarte, RB, Zhou, H, Kritikos, K, Shi, Z, Zhao, Z, De Nicola, R. Conveyed service-level understanding administration with keen agreements and blockchain. Simultaneousness Computat Pract Exper. 2020;e5800. https://doi.org/10.1002/cpe.5800

[17] Shi, P, Wang, H, Yang, S, Chen, C, Yang, W. Blockchain-based believed information dividing between confided in partners in IoT. Softw: Pract Exper. 2019; 1–14. https://doi.org/10.1002/spe.2739