International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

RAFT to Improve Failure Recovery in Wireless Sensor Networks

B. Harish Goud[1,2], Raju Anitha[3]

Submitted: 27/06/2023 **Revised**: 07/08/2023 **Accepted**: 27/08/2023

Abstract: Networks of wireless sensors are an essential method to preserve dispersed remote situations. Failure is a major issue in the majority of applications. Numerous strategies are available for failure detection and recovery. Yet, the majority of these could result in poor accuracy or decreased network lifetime. This paper suggests a failure recovery strategy based on RAFT, a blockchain consensus mechanism that employs in a unique node path arbitrator. Path arbitrator with RAFT Mechanism will control byzantine fault in Wireless sensor networks and recover from malicious activates. Utilization of energy and the precision of defect detection, packet delivery ratio, number of dead nodes, and time number of neighbor nodes are used in the simulation to evaluate the proposed algorithm.

Keywords: *WSNs; fault detection; failure recovery technique; Blockchain techniques RAFT*

1. Introduction

Wireless Sensor Networks have advanced during the last few years. WSNs have been the focus of both military and civilian uses. A large number of inexpensive and low-powered sensor devices are present in the WSN, an individually structured network. The world of communications has been transformed by wireless technologies. Early wireless telegraphy used radio receivers or transceivers, and today the term wireless is used to represent technologies like mobile networks and wireless broadband Access [1]

Node is the name of the sensor, which can be used under challenging conditions. As a result, sensor nodes are designed to eliminate errors. To assure the quality of service in sensor networks, it is therefore advantageous to identify and fix malfunctioning sensor nodes. The energy issue with sensors arises because they are unable to handle long-distance communications to reach a remote command station. Yet, there are problems with the WSNs, particularly with the ineffective information transfer today [2]

There are two sorts of node failures that can affect a WSN. The first category is the failure of a single node at random due to a node internal issue or battery drain. The second type is an area failure, where all of the nodes in a specific area fail due to a fire, detonation of a bomb, natural disaster (such an earthquake), or successful Denial of Service attacks. Both times, problematic nodes must be separated from the rest of the sensor network and stopped from being used by applications once they are discovered. So, other nodes must make up for it. The most crucial factor in designing an algorithm for data gathering, processing, and communication right now is energy awareness and efficiency [3]. Furthermore, the fact that WSN routing protocols are currently in the "Growing" stage.

Resources for wireless sensor networks are constrained (battery, memory size and bandwidth). Due to the additional send and receive messages caused by multi-hop data access, energy consumption rises, potentially causing network failures and shortening network lifetime. Routing techniques are an effective method for boosting wireless networks' data communication performance since they enable quicker data access, use less power, find and repair defective nodes, and extend the lifespan of WSNs. The Directed Diffusion (DD) algorithm, Ladder Diffusion (LD), and Grade Diffusion (GD) algorithms are a few examples of distinct routing techniques used in wireless sensor networks [4].

The survey includes a justification of the advantages of blockchain for WSN data management. In addition to auditing, event logging, and storage for information analysis and offline query processing, this comprises online information aggregation. In this survey, the traditional WSN data management solutions are described first, and then the blockchain-based WSN data management options. This survey also covers the contributions of blockchain to WSN security management. It starts by examining centralized WSN models for security concerns, then moves on to a discussion of blockchain-based WSN security management solutions, such as those that offer access control, safeguard data integrity, guarantee anonymity, and extend the life of WSN nodes.[6]

The transaction data is displayed as sensing information from a wireless network. In essence, the system uses the

[1]*Research Scholar in Dept of CSE,Koneru Lakshmaiah Education Foundation,Vaddeswaram,AndhraPradesh 522502,India*
[2]*Assistant professor Dept of I.T,Chaitanya bharathi institute of technology,Gandipet,Hyderabad,Telangana,500075,india*
e-mail: bhg120109@gmail.com
[3]*Dept.CSE. Koneru Lakshmaiah Education Foundation,Vaddeswaram,Guntur,Andhra Pradesh 522502,India*
Corresponding Author Email e-mail: bhg120109@gmail.com
e-mail: anitharaju@kluniversity.in
** Corresponding Author Email: bhg120109@gmail.com*

Merkel-tree algorithm and the hash function for calculation. With such programming, it is challenging to alter the content of the block using blockchain technology [5].

The validation group necessary for proofreading is selected using a deep learning procedure that emphasizes each node's properties. The appropriate next hop is then chosen using MDPs as a forwarding node capable of sending messages fast and securely. When compared to current routing algorithms [7]

Localization in WSNs is plagued by a number of concerns, including location estimate issues that impair localization accuracy, energy conservation issues that shorten the lifespan of WSNs, and malicious behavior or attacks that may result in erroneous location estimation [8]

2. Related Works

The system is limited by node and connection capacity, and a new traffic metric termed "directional edge betweenness" determines the network load.," in this article's more realistic cascade model for WSNs by X. Fu *et al.* [1].

N. Berjab *et al.* [2] introduces FuzHD++, a novel technique that combines the detection of aberrant nodes with the recovery of lost sensor data. To successfully accomplish accurate recovery estimation and detection performance, Data recovery and aberrant node detection both rely on the temporal and geographical correlation of the sensor data that has been observed.

B. S. Awoyemi *et al.* [3]. In order to develop the best p-cycle restoration models that can effectively protect the network from both link and node failures, we take use of the ring-like recovery rates and mesh-like capacity efficiencies that p-cycle-based restoration solutions may provide.

P. Sun *et al.* [4] introduces energy-efficient and reliable data collection in cluster-based CDG in WSNs, we offer a sparsest random sampling technique (SRS-CCDG). Sensor nodes are specifically arranged into clusters. Each time data is collected, a random selection of sensor nodes detects the field being watched and sends measurements to the respective cluster heads (CHs). The information obtained within each CH's cluster is then sent to the sink. Each sensor reading is treated as one CS in SRS-CCDG.

S. -J. Hsiao *et al.* [5] This block includes the hash value from the preceding block as well as the sensor data that was independently obtained. The mining calculation programme then determined the value of the hash of its own block, which is used to determine how to hash the next block. Each block contains the suggested combination of the current timestamp, the transaction details, and the encrypted hash value of the preceding block.

L. K. Ramasamy *et al.* [6] This study covers a thorough investigation of the integration of blockchain technology with WSNs (BWSN), in-depth analysis of a blockchain-based approach for malicious node detection, and insights into this novel concept. BWSN in two parts: 1) the BWSN architecture for identifying dangerous nodes, and 2) the application of smart contracts for identifying harmful nodes.

I. A. A. E. -M. *et al.* [7] The reliability and efficiency of WSN routing are increased by the trusted routing technique of deep blockchain and Markov Decision Processes (MDPs). To authenticate the transmission of the node, the suggested method employs a Proof of Authority (PoA) method inside the blockchain network.

G. Li, B. *et al.* [8] sets up To ensure data transfer security of data transfer, a Merkle tree-based UAV identity recognition system is also planned. By fusing blockchain architecture with data aggregation, a disaster semantic blockchain (DSB) based on a consensus mechanism geared toward data reconstruction is presented.

T. -H. Kim *et al*. [10] suggests an Ethereum-based trust management architecture to improve beacon node relationships and remove errant nodes in wireless sensor networks (WSNs). Both behaviorally both data-based trust and based trust are evaluated as part of this composite level of trust. Beacon nodes' behavioral-based trust is determined by a variety of factors, including closeness, honesty, intimacy, and frequency of interaction.

K. Mrabet et al.[11]The new system is a fully decentralized general-purpose system that gathers and supplies global reputation data using blockchain technology. In order to establish privacy, this method makes use of a cryptographic fundamental called "safe multiparty computation" only needs O(n) messages and maintains criticism privacy even when n2 malicious parties gain a dishonest majority.

Aluvalu, Rajanikanth et al [13,15,16] This wireless technology uses sensors to manage the information obtained from various areas. The wearable sensor used in this study has information from the system's many departments. To locate the position and persuade individuals, The hybrid microwave transmission method and the gradient boosting methodology have both been presented[17]. The decision on the patient's health has been sent over using a hybrid microwave and gradient boosting[19]. Bayesian network-based intrusion detection system with feature selection[18].

K. K. Chennam et al [19]The most effective approach is to encrypt the data before storing it in a third-party cloud database and then encrypt the data before storing it in a third-party cloud database and then to decrypt it once more after getting it from the cloud.

B. HarishGoud et al[20]By keeping an intelligent agent acting as a bridge between the cloud and the sensors, direct communication with the target router is made feasible. By

maintaining an intelligent agent in place to operate as a conduit between the cloud and the sensors .

3. The Proposed System

3.1 ISSUE STATEMENT

When a sensor node in a cluster wants to connect with another sensor node in another cluster, they pass through numerous intermediary nodes before eventually reaching the destination sensor node, which causes a delay and lower packet delivery ratio and throughput. Network eavesdropping and man-in-the-middle attacks are possible because of the extremely low security on intermediary nodes. Moreover, data packets are buffered at nodes due to the sluggish transmission speed.

3.2 ALGORITHM FOR LDTR

The objective of LDTR (LEAST DISRUPTIVE TOPOLOGY REPAIR) is to reestablish links while maintaining the pre-failure topology's shortest path length between nodes. Making use of the Shortest-path Routing Table (SRT), which is only partially filled the LDTR method first locates the problematic node and determines if it has a cut vertex before moving on to the recovery procedure. The neighboring node from the failing node's smallest block is then used to replace the defective node. Then, in order to restore connectivity, The parent node's directly related children's nodes are also moved.

3.3 ALGORITHM FOR FAILURE NODE RESTORATION TECHNIQUE

FAILURE NODE RESTORATION TECHNIQUE ALGORITHM is a WSN-based genetic algorithms and grade diffusion algorithms. For each sensor node, the FNR algorithm generates the grade value, routing table, neighbour nodes, and payload value using the grade diffusion technique. The FNR algorithm is used to count the number of sensor nodes that aren't operating properly while the wireless sensor network is in use.

3.4 ALGORITHM FOR GRADE DIFFUSION

In addition to creating the path taken by each sensor node, the GD algorithm also finds a group to reduce transmission loading of neighbor nodes. When a relay-capable node is not present in its grade table, A single sensor node may select one sensor node from its neighbors. The Grade diffusion method can additionally keep a record of some data relay-related information. The extra relay operation can then be carried out by a sensor node choosing a node that has less loading or more energy available than the other nodes. In other words, Since the GD algorithm modifies the routing path in real-time, the event data is sent to the sink node promptly and accurately.

3.4 NODE/LINK RECOVERY MODEL BY RAFT

The behavior of failed nodes needs to be addressed if multimedia distribution in wireless sensor networks (WSN) is to perform better. The recovery from failure method is based on RAFT, a node path arbitrator-based blockchain consensus process. The Byzantine failure in wireless sensor networks will be controlled by a path arbitrator with RAFT Mechanism, and it will recuperate from fraudulent actions. Path arbiter with RAFT framework, which has been presented as a solution to this problem, tries to restore normal behavior to failed nodes. Implementing a reputation sensing framework and applying it to the network's failing nodes allows for this shift to take place.

PA-RAFT Algorithm

1. Start up

2. In proposed WSN's technique have path arbiter an intermediate device with RAFT Censuses mechanism.

3. Wireless sensor networks contains sensor followers' nodes, leader node RAFT path arbiter by that a byzantine faulty can be find in networks.

4. Two remote procedure calls (RPCs) are used by Raft to perform its basic tasks.

5. Raft separates time into periods of arbitrary length, each of which starts with a presidential election.

6. The leader is the candidate who receives the most support from the sensor nodes. Then, to establish dominance among the others in the cluster, it broadcasts a heartbeat message.

7. Other candidates will look for the term number if they receive the Append Entries RPC. They accept the PA-RAFT as the leader and revert to the follower role if the term number is higher than their own. In the event that the term number is less, they reject the RPC and continue to be a candidate.

7. End

4.Results

Network Simulation (NS) Version 2.35 is made use of., the path arbiter with RAFT (PAR) framework for wireless sensor networks (WSN) was implemented. The results of the simulation demonstrate how effectively the framework improves transfer of data performance. The comparison outcomes are covered in the following subsections.

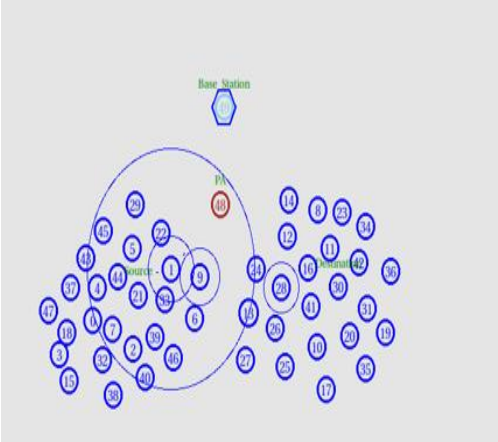

Fig 1 Path arbiter in WSN

Delay Performance

$$\text{Delay} = \text{PRT} - \text{PST} \quad \text{---------- Eq(1)}$$

Table1 Demonstrate the comparison results of delay performance

Simulation Time	Evaluation of Delay			
	PAR	GD	FNR	LDTR
0	0	0	0	0
10	0.101	0.311	0.444	0.577
20	0.0605	0.201	0.3321	0.484
30	0.0391	0.166	0.229	0.433
40	0.0321	0.111	0.199	0.368
50	0.0404	0.107	0.111	0.29

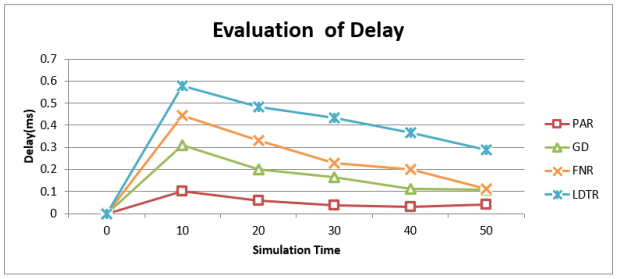

Fig 2 Delay Performance Comparison Results

Packet Delivery Ratio (PDR)

A measure of how many transmitted packets were compared to how many were received The equation displays at the target node (1).

$$PDR = \frac{\sum_{i=1}^{c} rpi}{\sum_{i=1}^{c} psi} \quad \ldots (1)$$

Table 2 Demonstrate the comparison results of PDR performance

Simulation Time	Evaluation of PDR			
	PAR	GD	FNR	LDTR
0	0	0	0	0
10	8	5	4	2
20	19	14	12	7
30	38	33	25	17
40	61	59	32	29
50	88	79	44	32

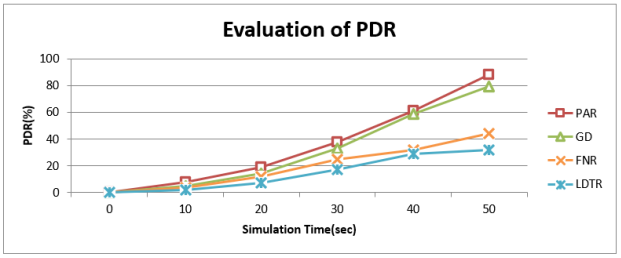

Fig 3 Performance evaluation of PDR

Throughput Performance

$$\text{Throughput} = \frac{TNBR}{SIT} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

TABLE 3 Demonstrate the performance throughput comparison results of PAR.

Simulation Time	Evaluation of Throughput			
	PAR	GD	FNR	LDTR
0	0	0	0	0
10	34546	32445	20546	17851
20	39210	37146	22876	19368
30	43236	41257	27467	22654
40	46701	44697	35036	32346
50	52559	50186	40035	37568

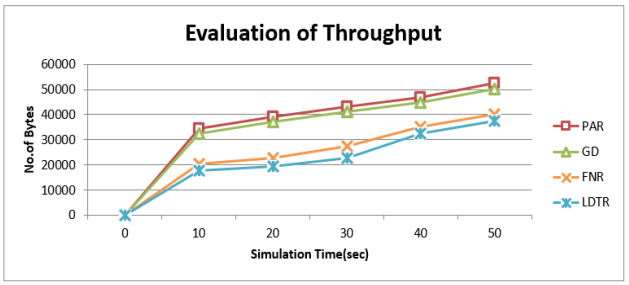

Fig 4 Comparison on Throughput performance

Energy Performance

$$EP = \sum (NIE - NCE) \quad \ldots\ldots\ldots\ldots\ldots (3)$$

TABLE 4 Demonstrate the performance Energy comparison results of PAR.

Simulation Time	Evaluation of Energy			
	PAR	GD	FNR	LDTR
0	100	100	100	100
10	82	79	70	64
20	69	63	59	53
30	59	52	49	43
40	50	44	35	32
50	41	33	29	22

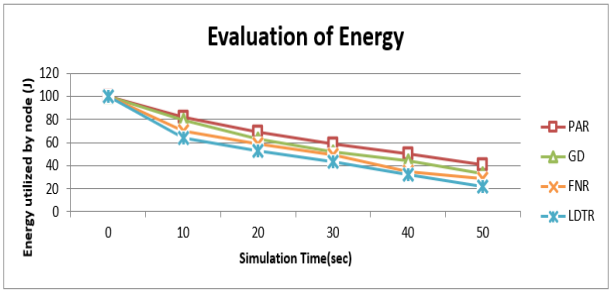

Fig 5 Energy Performance

5. Conclusions

The three failure node recovery methods used by WSN: LDTR, FNR, and GD algorithms are compared with the proposed system that is a path arbitrator with RAFT Blockchain Consensus technique. RAFT, a blockchain consensus technique that makes use of an independent node path arbitrator, is the foundation of a failure recovery strategy. In wireless sensor networks, a path arbitrator using the RAFT Mechanism will regulate byzantine faults and recover from malicious activities. We use the following parameters to compare the algorithms: Average delay, packet delivery percentage, and energy usage. Locating the failure nodes is made simple by using the output system provided Using x-graphs or NAM animator by NS2 , this system will provide us with certain recovery of failing nodes at a lower cost and with reduced energy consumption

Acknowledgements

Availability of data and material: The datasets used in this study are taken from public domain and the appropriate URLs have been cited in the text.

Author contributions

.Authors contribution statement: All authors are contributed equally. In particular,

B.Harish Goud– Conceptualization, Methodology, Formal analysis and investigation, Writing - original draft preparation.
Supervision:
Raju Anitha - Conceptualization, Methodology, Formal analysis and investigation, Writing - review and editing, Supervision.

Acknowledgments

A preliminary version of this work appears in this paper is extension research work of my previously published paper in expert systems journal title“**Energy optimization in path arbitrary wireless sensor network**.

Conflicts of interest

Conflict of interests: All the authors declare that they have no competing interests.

References

[1] X. Fu, H. Yao and Y. Yang, "Modeling Cascading Failures for Wireless Sensor Networks With Node and Link Capacity," in IEEE Transactions on Vehicular Technology, vol. 68, no. 8, pp. 7828-7840, Aug. 2019, doi: 10.1109/TVT.2019.2925013.

[2] N. Berjab, H. H. Le and H. Yokota, "Recovering Missing Data via Top-k Repeated Patterns for Fuzzy-Based Abnormal Node Detection in Sensor Networks," in IEEE Access, vol. 10, pp. 61046-61064, 2022, doi: 10.1109/ACCESS.2022.3181742.

[3] B. S. Awoyemi, A. S. Alfa and B. T. Maharaj, "Network Restoration in Wireless Sensor Networks for Next-Generation Applications," in *IEEE Sensors Journal*, vol. 19, no. 18, pp. 8352-8363, 15 Sept.15, 2019, doi: 10.1109/JSEN.2019.2917998.

[4] P. Sun, L. Wu, Z. Wang, M. Xiao and Z. Wang, "Sparsest Random Sampling for Cluster-Based Compressive Data Gathering in Wireless Sensor Networks," in *IEEE Access*, vol. 6, pp. 36383-36394, 2018, doi: 10.1109/ACCESS.2018.2846815.

[5] S. -J. Hsiao and W. -T. Sung, "Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks," in *IEEE Access*, vol. 9, pp. 72326-72341, 2021, doi: 10.1109/ACCESS.2021.3079708.

[6] L. K. Ramasamy, F. Khan K. P., A. L. Imoize, J. O. Ogbebor, S. Kadry and S. Rho, "Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey," in *IEEE Access*, vol. 9, pp. 128765-128785, 2021, doi: 10.1109/ACCESS.2021.3111923.

[7] S. -J. Hsiao and W. -T. Sung, "Enhancing Cybersecurity Using Blockchain Technology Based on IoT Data Fusion," in *IEEE Internet of Things Journal*, vol. 10, no. 1, pp. 486-498, 1 Jan.1, 2023, doi: 10.1109/JIOT.2022.3199735.

[8] I. A. A. E. -M. And and S. M. Darwish, "Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach," in *IEEE Access*, vol. 9, pp. 103822-103834, 2021, doi: 10.1109/ACCESS.2021.3098933.

[9] G. Li, B. He, Z. Wang, X. Cheng and J. Chen, "Blockchain-Enhanced Spatiotemporal Data Aggregation for UAV-Assisted Wireless Sensor Networks," in *IEEE Transactions on Industrial*

Informatics, vol. 18, no. 7, pp. 4520-4530, July 2022, doi: 10.1109/TII.2021.3120973.

[10] T. -H. Kim et al., "A Novel Trust Evaluation Process for Secure Localization Using a Decentralized Blockchain in Wireless Sensor Networks," in IEEE Access, vol. 7, pp. 184133-184144, 2019, doi: 10.1109/ACCESS.2019.2960609.

[11] K. Mrabet, F. E. Bouanani and H. Ben-Azza, "Generalized Secure and Dynamic Decentralized Reputation System With a Dishonest Majority," in IEEE Access, vol. 11, pp. 9368-9388, 2023, doi: 10.1109/ACCESS.2023.3239394.

[12] B.Harish Goud,T.N.Shankar., Basant Sah. ,Rajanikanth Aluvalu., 2023. Energy Optimization in Path Arbitrary Wireless Sensor Network. Expert Systems, DOI: 10.1111/exsy.13282.

[13] Aluvalu, Rajanikanth & N., Senthil & Thirumalaisamy, Manikandan & Basheer, Shajahan & aldhahri, Eman & Shitharth,. (2023). Efficient data transmission on wireless communication through a privacy-enhanced blockchain process. PeerJ Computer Science. 9. e1308. 10.7717/peerj-cs.1308.

[14] Goud, B. ., & Anitha, R. . (2023). Emerging Routing Method Using Path Arbitrator in Web Sensor Networks. International Journal on Recent and Innovation Trends in Computing and Communication, 11(4),232–237. https://doi.org/10.17762/ijritcc.v11i4.6444

[15] Aluvalu Rajanikanth., Chennam K.K., Uma Maheswari V., Jabbar M.A. (2021),” A Novel and Secure Approach for Quantum Key Distribution in a Cloud Computing Environment”, Intelligent Computing and Networking. Lecture Notes in Networks and Systems, vol 146. Springer, Singapore.

[16] Aluvalu, Rajanikanth, Nitin Birari, and Supriya Byreddy. "Efficient real-time video transmission in wireless mesh network." *International Journal of Research in Computer Science* 2, no. 1 (2011): 11.

[17] Aluvalu, rajani kanth, and lakshmi muddana. "Access control model with enhanced flexibility and scalability for cloud." green computing and internet of things (icgciot), 2015 international conference on. ieee, 2015.

[18] M. A. Jabbar, R. Aluvalu and S. S. Satyanarayana Reddy, "Intrusion Detection System Using Bayesian Network and Feature Subset Selection," *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Coimbatore, India, 2017, pp. 1-5, doi: 10.1109/ICCIC.2017.8524381.

[19] K. K. Chennam, L. Muddana and R. K. Aluvalu, "Performance analysis of various encryption algorithms for usage in multistage encryption for securing data in cloud," *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, 2017, pp. 2030-2033, doi: 10.1109/RTEICT.2017.8256955.

[20] B. HarishGoud, T. N. Shankar, P. K. Sahoo and W. H. Cheng, "A Novel Method for Routing Packet between Patient and Doctor using Sensor and Cloud," *2021 6th International Conference for Convergence in Technology (I2CT)*, Maharashtra, India, 2021, pp. 1-5, doi: 10.1109/I2CT51068.2021.9418092.

[21] Shanmugam, S. P. ., Vadivu, M. S. ., Anitha, D., Varun, M., & Saranya, N. N. . (2023). A Internet of Things Improvng Deep Neural Network Based Particle Swarm Optimization Computation Prediction Approach for Healthcare System. International Journal on Recent and Innovation Trends in Computing and Communication, 11(4s), 92–99. https://doi.org/10.17762/ijritcc.v11i4s.6311

[22] Ghazaly, N. M. . (2020). Secure Internet of Things Environment Based Blockchain Analysis. Research Journal of Computer Systems and Engineering, 1(2), 26:30. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/8

[23] Kathole, A. B., Katti, J., Dhabliya, D., Deshpande, V., Rajawat, A. S., Goyal, S. B., . . .Suciu, G. (2022). Energy-aware UAV based on blockchain model using IoE application in 6G network-driven cybertwin. Energies, 15(21) doi:10.3390/en15218304