RESEARCH ARTICLE OPEN ACCESS

Kernel Function for Malicious Node Detection in Social Internet of Things

Madhankumar Y
Government Arts College (Autonomus)
Kumbakonam-Thanjavur

ABSTRACT
Social Internet of Things (SIoT) is an interdisciplinary rising domain that enables self-governing connection among long range informal communication and the Internet of Things and the security of SIoT system is significant in present days. In this paper chiefly focus on the vindictive Node (MN) discovery in SIoT, by machine learning technique with Main Cluster Heads. Because of the conveyed nature, SIoT systems are defenseless against different dangers particularly insider attacks. The individual cluster key is given to every cluster in the system by the sink. The malignant hubs are identified by getting the affirmation from the goal hub. From the execution results the proposed framework execution assessed by Detection Ratio, throughput, loss level, and delivery ratio. In light of this current parameter's proposed MN recognition contrasted and other traditional methods.

Keywords: Malicious Node (MN) detection, Social Internet of Things (SIoT), Clustering, detection rate.

I. INTRODUCTION

Internet of Things (IoT) has turned into a prevalent framework to help numerous advanced applications and services, for example, brilliant homes, smart healthcare, open security, modern observing and condition assurance. [1-5]. to reinforce the unwavering quality and security in remote sensor systems. Hence, it is critical to structure a compelling security system for recognizing vindictive hubs in an IoT network [2]. IoT service enables certain capacities to be helped out through a predefined interface. A few researchers are especially keen on recognizing danger issues emerging during finding and coordinating information inside IoT[6-9]. The SIoT is a bigger social network, associating people and people and items, and articles and items. Numerous security issues in SIoT model, it experiences a similar security problem as customary Internet-based as well as remote frameworks, including sticking, spoofing and so forth [10-12]. SIoT model is an interdisciplinary developing space that empowers self-ruling association among informal communication and the Internet of Things. Thorough nature of SIoTs presents different difficulties in its plan, design, execution, and activity the executives [13-16]. In spite of the fact that SIoT is at its outset, yet its constituents are currently all around developed and different endeavors in introducing the arrangements from traditional and unconventional strategy's [17,18].

Also, with the scope of Social Network Service being extended from individual focused to a partnership focused on and being associated with Internet of Things empowers a business practical joint effort [19]. The attackers change the conduct of the hubs in the system to fall and debase the usefulness of the wireless sensor networks. The malicious hubs in the wireless sensor systems can be identified utilizing cross hybrid Acknowledge scheme (HAS). In this strategy, the hubs in the wireless sensor system are gathered into number of clusters. Each cluster ought to have just three hubs and have an individual cluster key in all hubs in the cluster [21]. On the off chance that malicious hubs effectively alter the information, it can make an impact on the IoT work, i.e., prompting an off- wrong decision [20].

II. REVIEW OF RECENT KINDS OF LITERATURE

In 2019 Ande, R et al [21]. Have proposed the Next Generation Internet; web systems which fuse human qualities. Following this transformative presentation, IoT designs are thought about and a portion of the advances that are a piece of every architectural layer are presented. Security dangers inside all design layer and some mitigation methodologies are talked about, at last, the paper finishes up with some future advancements. Given the potentially sensitive nature of IoT datasets, there is a need to build up a standard for the sharing of IoT datasets among the examination and professional networks and other important partners. At that point set the potential for blockchain technology in encouraging secure sharing of IoT datasets by Banerjee, M et al.2018 [22]. A methodology, deep learning, to cyber security to empower the discovery of assaults in social web of things by Diro, A. et al.2018 [23]. The exhibition of the deep model is thought

about against conventional machine learning approach, and appropriated assault discovery is assessed against the brought together detection system. The tests have demonstrated that our disseminated assault discovery system is better than brought together detection systems utilizing deep learning model.

III. NETWORK MODEL: SIOT

Internet of Things (IoT) is a developing worldview that aims to create the planet more astute in support of humankind. Brilliant structure, smart health keen industry, savvy grid, keen home, shrewd transportation and keen learning, are a few constituents of a smart city. Social IoT based strategy for better assistive living. SIoT condition encompassing an individual or association supports getting assortment and a lot of data and gathered data gets the opportunity to be a clever service through the procedure of advanced obstruction. For IoT conditions, the traffic elements and baselines are altogether different from heritage computer networks and consequently should be estimated and considered for IoT assault detection [24-26]. The SIoT network structure can be shaped as expected to guarantee efficient safety among the parts dependent on a few social perspectives with the goal that the discovery of administrations and article is done successfully that guide in arrangement synthesis for complex errands. Second, versatility is guaranteed as in informal communities through coordinated effort. This isn't constantly substantial in certain conditions, which may influence the detection accuracy and even reason amassing faults.

- A general IoT architecture is conveyed to assume control over open IoT applications with open working capacity.
- The Service Layer moderates approaching information solicitations and activation endeavours, permitting only approved associations through to the private cloud in SIoT.
- To locate the malicious nodes in the system model, picking an edge falsely to recognize malicious hubs from all hubs may lessen the detection accuracy.
- Since sensor hubs cannot know their neighbor's hubs before arrangement, there ought to be a neighbours revelation period after the initial deployment and after any redeployment, empowering every sensor node to discover its neighbors.
- A little gathering of mobile malicious hubs can disturb these tasks in a single region at once as they move around in the system, making steering dark gaps in SIoT model

3.1 Malicious Attacker Model in SIoT

A general attacker model characterizes attacker activities and potential targets. In any case, past works accept that the attacker consistently arrives at its objective legitimately which is false. To stronger malicious hubs that can dispatch a few assaults at the same time, for example, alter assault, drop assault and replay assault. The attacker in one significant, that is accepting that portable malicious hubs are equipped with similar remote equipment as the original hubs. An attacker can utilize radios with high signal solidarity to accomplish a comparable impact on moving hubs. The attacker benefits significantly from utilizing portable malicious hub assaults, because of expanded way decent variety and the trouble of neighborhood identification and the attack model shows in figure 1.

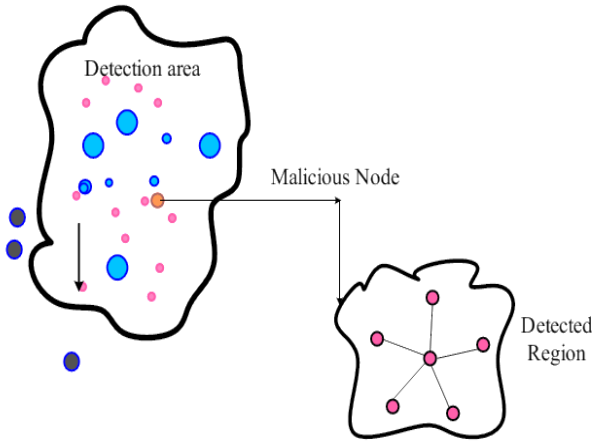

Figure 1: Detection of Malicious Node

All the more explicitly, he can dispatch a DDoS attack against the base station by having a lot of malicious hubs move to however many various areas as could reasonably be expected and flood the base station from every area turn. The attacker can likewise utilize a lot of mobile malicious hubs to disturb the different self-sorted out conventions, for example, directing, cluster development, time synchronization, and limitation. For example, mobile malicious hubs could produce and dispose of control bundles utilized in these conventions and in this manner make these protocols malfunction [27-30].

IV. PROPOSED SYSTEM

Our proposed SIoT systems' malicious Node recognition is significant, so here Exponential Layer based methodology used for detection process. Considered information data's to the Exponential kernel work, to improve its learning procedure and acquire the last yield to the trust estimations of a node. To analyze the MN, at first main cluster Head (MCH) chose from the SIoT arranges by imaginative clustering procedures. The non-MCH individuals in perspective on lingering energy, the MCH transmit the

accumulated video or sound bundles to the MCH in light of need line. For securable directing, we have displayed trust-based QoS routing estimation. This computation removes the pernicious centres a long way from the gathering. This is on the grounds that picking a limit falsely to recognize malicious hubs from all hubs may decrease the detection accuracy. They at that point identified that the provenance may grow excessively quick with the expansion of bundled transmission jumps of system suspend [31-35]. Choice EK for MN detection assumes a critical role since it helps with mapping dataset to a higher dimensional space to acquire a superior understanding of the characterization model, this Detection procedure numerically represented in streaming equation.

$$\{Node_i\} \rightarrow \begin{cases} (node(node_i^{'} \neq MN_i) \text{ with proabaility factor MCH} \\ (node^{'}(node_i^{'} = MN_i) \text{ with proabality } (1-MCH)^{'} \end{cases} \quad (1)$$

Focusing on this issue, formalize the connection between the reputation of directing ways and hubs, by seeing that a hub's notoriety can be formalized as a multiple linear regression issue [36-40]. To discover the MD according to proposed technique the heaviness of every sensor hub some procedure that is a sensor hub is undermined and as often as possible sends its report conflicting with an official choice, its weight is probably going to be diminished. Along these lines have the option to call the part hub which is dispensed by the MCH as a general cluster. In this way, the MCH will put broadcasting live the assemble information from extra cluster individuals to the picked chosen vice cluster head [41-43].

Example of Proposed Detection System

- ✓ To analyze the probability of these assaults dependent on solely their harm or impact, in light of the fact that these assaults may influence one another.
- ✓ A malicious node could spread the false data that a standard node is suspicious and, with this single vote, viably dispose of from the system, possibly causing a huge forswearing of- service in huge pieces of the system.
- ✓ If there are in excess of two malicious nodes in a similar way, which perform two various assaults [44-55].
- ✓ The condition, it is difficult to analyze the probability of these assaults dependent on exclusively their harm or impact, in light of the fact that these assaults may influence one another.
- ✓ The passes a malicious node, accept that the malicious hub can perform a SIoT organize [56-58].

4.3 Detection Model

It is characterized as the proportion between quantities of nodes effectively-identified to all outnumber of hubs. detection stage is sorted into malicious hub detection ratio and non-malicious hub identification proportion. It is estimated in rate and it changes somewhere in the range of 0 and 100. The transmission is comprised of an assault and the data to locate the malicious node data.

$$\text{Detection} = \pm MAX_{(\text{Fixed value})}\{\beta + 10\log(\beta^2)\} \quad (6)$$

The value relying upon the estimation of its multiplier, a malicious transmission may or may not be detected as malicious.

V. RESULTS AND ANALYSIS

This proposed SIoT MN recognition executed in NS2 with 300 nodes for recreation model, these nodes are performing in the district 1000m×1000m with the transmission range 250m. Reproduction parameters for recreation model depicted in table 1, in light of the leftover vitality of non-MCH and the execution results are investigated by confusion grid and some recognition rate to the comparison process.

Technique	Throughput (kb/bit)	Delivery Ratio (%)	Loss Ratio	Detection Ratio (%)
Proposed Model	1.88	93.22	10.08	96.58
ANFIS	1.48	86.22	9.08	92.55
Bayesian approach	0.95	79.88	10.11	88.59
Trust model with a Defence scheme	0.79	81.11	15.68	90.45
Epidemic Routing	1.15	79.56	12.44	90.22

Table 1: Detection Level analysis

In the assessment, the detection perplexity lattice appears in table 2, here two arrangements of data are referenced like the genuine and anticipated class of SIoT network system and the detection execution can be estimated utilizing both the accuracy rate and the error rate. This is on the grounds that the two models erroneously distinguished the low-positioning ordinary nodes as the malicious ones. At that point table, 3 demonstrates the proposed consequences of MN detection in SIoT system, the measurements like Throughput, delivery ratio, loss level and proposed detection pace of the framework. For instance, the proposed throughput is 1.88kb/sec thought about o existing that is ANFIS, Bayesian methodology the thing that matters is 5.52 to 10.12%, correspondingly other relative regular strategies. Among the metrics the significant factor is detection rate and data loss, so were discussed the graphical portrayal examined up and coming area. Abuse detection by identifying assaults by their realized marks doesn't require numerous assets; however has the disadvantage of unrecognizing unpublished assaults. So as to guarantee a high evaluation of effectiveness for our malicious hub detection procedure a topology of SIoT arranges. Likewise, But this happens just when the objective hub and the one that is additionally tricked have nearly a similar separation to the made-up position of the malicious node just as to its genuine position. Toward the end over every one of the four methods correlation, our proposed framework is better for MN detection SIoT networks.

VI. CONCLUSION

One of the significant issues that are identified with the utilization of SIoT in cruel conditions is the hole in their security. Most existing algorithms ascertain the notoriety of all nodes dependent on the directing way or data transmission in SIoT organize. The recreation results demonstrate that the proposed model get the greatest detection level SIoT network systems. The malicious nodes are recognized by getting the acknowledgments from the goal nodes and the exhibition of the proposed framework is analyzed utilizing parcel conveyance ratio and dormancy is significant. As the size of malicious nodes is little because of which the lifetime of sensor node is additionally extremely less and the battery life is likewise less. The reproduction results showed that our model could successfully distinguish malicious conduct, for example, arrangement, Sybil and record polluter. In Future deep learning and some roused optimization mode utilized to distinguish the MN in SIoT network.

REFERENCE

[1] Chen, Y. T., Chen, C. H., Wu, S., & Lo, C. C. (2019). A two-step approach for classifying music genre on the strength of AHP weighted musical features. Mathematics, 7(1), 19.

[2] Elhoseny, M., Shankar, K., &Uthayakumar, J. (2019). Intelligent diagnostic prediction and classification system for chronic kidney disease. Scientific reports, 9(1), 1-14.

[3] Sivakumar, P., Velmurugan, S. P., & Sampson, J. (2020). Implementation of differential evolution algorithm to perform image fusion for identifying brain tumor.

[4] Khamparia, A., Gupta, D., Nguyen, N. G., Khanna, A., Pandey, B., & Tiwari, P. (2019). Sound classification using convolutional neural network and tensor deep stacking network. IEEE Access, 7, 7717-7727.

[5] Jansirani, A., Rajesh, R., Balasubramanian, R., & Eswaran, P. (2011). Hi-tech authentication for pslette images using digital signature and data hiding. Int. Arab J. Inf. Technol., 8(2), 117-123.

[6] Jain, R., Gupta, D., & Khanna, A. (2019). Usability feature optimization using MWOA. In International conference on innovative computing and communications (pp. 453-462). Springer, Singapore.

[7] Shankar, K., & Lakshmanaprabu, S. K. (2018). Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm. International Journal of Engineering & Technology, 7(9), 22-27.

[8] Lyu, L., & Chen, C. H. (2020, July). Differentially Private Knowledge Distillation for Mobile Analytics. In Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval (pp. 1809-1812).

[9] Poonkuntran, S., Rajesh, R. S., & Eswaran, P. (2011). Analysis of difference expanding method for medical image watermarking. In International Symposium on Computing, Communication, and Control (ISCCC 2009) (Vol. 1, pp. 31-34).

[10] Sampson, J., & Velmurugan, S. P. (2020, March). Analysis of GAA SNTFT with Different Dielectric Materials. In 2020 5th International Conference on Devices, Circuits and Systems (ICDCS) (pp. 283-285). IEEE.

[11] Elhoseny, M., Bian, G. B., Lakshmanaprabu, S. K., Shankar, K., Singh, A. K., & Wu, W. (2019). Effective features to classify ovarian cancer data in

internet of medical things. Computer Networks, 159, 147-156.

[12] Gochhayat, S. P., Kaliyar, P., Conti, M., Tiwari, P., Prasath, V. B. S., Gupta, D., & Khanna, A. (2019). LISA: Lightweight context-aware IoT service architecture. Journal of cleaner production, 212, 1345-1356.

[13] Dutta, A. K., Elhoseny, M., Dahiya, V., & Shankar, K. (2020). An efficient hierarchical clustering protocol for multihop Internet of vehicles communication. Transactions on Emerging Telecommunications Technologies, 31(5), e3690.

[14] Anand Nayyar, Vikram Puri, Nhu Gia Nguyen, BioSenHealth 1.0: A Novel Internet of Medical Things (IoMT) Based Patient Health Monitoring System, Lecture Notes in Networks and Systems. Springer, 2019

[15] Shankar, K., Lakshmanaprabu, S. K., Khanna, A., Tanwar, S., Rodrigues, J. J., & Roy, N. R. (2019). Alzheimer detection using Group Grey Wolf Optimization based features with convolutional classifier. Computers & Electrical Engineering, 77, 230-243.

[16] Paramathma, M. K., Pravin, A. C., Rajarajan, R., & Velmurugan, S. P. (2019, April). Development and Implementation of Efficient Water and Energy Management System for Indian Villages. In 2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS) (pp. 1-4). IEEE.

[17] Chen, C. H., Song, F., Hwang, F. J., & Wu, L. (2020). A probability density function generator based on neural networks. Physica A: Statistical Mechanics and its Applications, 541, 123344.

[18] Kathiresan, S., Sait, A. R. W., Gupta, D., Lakshmanaprabu, S. K., Khanna, A., & Pandey, H. M. (2020). Automated detection and classification of fundus diabetic retinopathy images using synergic deep learning model. Pattern Recognition Letters.

[19] Gupta, D., & Ahlawat, A. K. (2016). Usability determination using multistage fuzzy system. Procedia Comput Sci, 78, 263-270.

[20] Amira S. Ashour, Samsad Beagum, Nilanjan Dey, Ahmed S. Ashour, Dimitra Sifaki Pistolla, Gia Nhu Nguyen, Dac-Nhuong Le, Fuqian Shi (2018), Light Microscopy Image De-noising using Optimized LPA-ICI Filter, Neural Computing and Applications, Vol.29(12), pp 1517–1533, Springer, ISSN: 0941-0643. (SCIE IF 4.664, Q1)

[21] Pan, M., Liu, Y., Cao, J., Li, Y., Li, C., & Chen, C. H. (2020). Visual Recognition Based on Deep Learning for Navigation Mark Classification. IEEE Access, 8, 32767-32775.

[22] Chen, C. H., Hwang, F. J., & Kung, H. Y. (2019). Travel time prediction system based on data clustering for waste collection vehicles. IEICE TRANSACTIONS on Information and Systems, 102(7), 1374-1383.

[23] Shankar, K., & Eswaran, P. (2015). ECC based image encryption scheme with aid of optimization technique using differential evolution algorithm. Int J Appl Eng Res, 10(55), 1841-5.

[24] Anand Nayyar, Vikram Puri, Nhu Gia Nguyen, Dac Nhuong Le, Smart Surveillance Robot for the Real Time Monitoring and Control System in Environment and Industrial Applications, Advances in Intelligent System and Computing, pp 229-243, Springer

[25] Le Nguyen Bao, Dac-Nhuong Le, Gia Nhu Nguyen, Vikrant Bhateja, Suresh Chandra Satapathy (2017), Optimizing Feature Selection in Video-based Recognition using Max-Min Ant System for the Online Video Contextual Advertisement User-Oriented System, Journal of Computational Science, Elsevier ISSN: 1877-7503. Vol.21, pp.361-370. (SCIE IF 2.502, Q1)

[26] Chakchai So-In, Tri Gia Nguyen, Gia Nhu Nguyen: Barrier Coverage Deployment Algorithms for Mobile Sensor Networks. Journal of Internet Technology 12/2017; 18(7):1689-1699.

[27] Le, D.-N.a, Kumar, R.b, Nguyen, G.N., Chatterjee, J.M.d, Cloud Computing and Virtualization, DOI: 10.1002/9781119488149, Wiley.

[28] Bhateja, V., Gautam, A., Tiwari, A., Nhu, N.G., Le, D.-N, Haralick features-based classification of mammograms using SVM, Advances in Intelligent Systems and Computing, Volume 672, 2018, Pages 787-795.

[29] Khamparia, A., Saini, G., Gupta, D., Khanna, A., Tiwari, S., & de Albuquerque, V. H. C. (2020). Seasonal crops disease prediction and classification using deep convolutional encoder network. Circuits, Systems, and Signal Processing, 39(2), 818-836.

[30] Uthayakumar, J., Elhoseny, M., & Shankar, K. (2020). Highly Reliable and Low-Complexity Image Compression Scheme Using Neighborhood Correlation Sequence Algorithm in WSN. IEEE Transactions on Reliability.

[31] Huyen, D.T.T., Binh, N.T., Tuan, T.M., Nguyen, G.N, Dey, N., Son, L.H, Analyzing trends in hospital-cost payments of patients using ARIMA and GIS: Case study at the Hanoi Medical University Hospital, Vietnam, Journal of Medical Imaging and Health Informatics, 7(2), pp. 421-429.

[32] Van, V.N., Chi, L.M., Long, N.Q., Nguyen, G.N., Le, D.-N, A performance analysis of openstack open-source solution for IaaS cloud computing, Advances in Intelligent Systems and Computing, 380, pp. 141-150.

[33] Shankar, K., & Eswaran, P. (2016, January). A new k out of n secret image sharing scheme in visual cryptography. In 2016 10th International Conference on Intelligent Systems and Control (ISCO) (pp. 1-6). IEEE.

[34] Dey, N., Ashour, A.S., Chakraborty, S., Le, D.-N., Nguyen, G.N, Healthy and unhealthy rat hippocampus cells classification: A neural based automated system for Alzheimer disease classification, Journal of Advanced Microscopy Research, 11(1), pp. 1-10

[35] Velmurugan, S. P., & Rajasekaran, P. S. M. P. (2017). CLASSIFICATION OF BRAIN TUMOR USING MULTIMODAL FUSED IMAGES AND PNN. International Journal of Pure and Applied Mathematics, 115(6), 447-457.

[36] Shankar, K., Elhoseny, M., Perumal, E., Ilayaraja, M., & Kumar, K. S. (2019). An Efficient Image Encryption Scheme Based on Signcryption Technique with Adaptive Elephant Herding Optimization. In Cybersecurity and Secure Information Systems (pp. 31-42). Springer, Cham.

[37] Wu, L., Chen, C. H., & Zhang, Q. (2019). A mobile positioning method based on deep learning techniques. Electronics, 8(1), 59.

[38] Lydia, E. L., Kumar, P. K., Shankar, K., Lakshmanaprabu, S. K., Vidhyavathi, R. M., & Maseleno, A. (2020). Charismatic document clustering through novel K-Means non-negative matrix factorization (KNMF) algorithm using key phrase extraction. International Journal of Parallel Programming, 48(3), 496-514.

[39] Sujitha, B., Parvathy, V. S., Lydia, E. L., Rani, P., Polkowski, Z., & Shankar, K. (2020). Optimal deep learning based image compression technique for data transmission on industrial Internet of things applications. Transactions on Emerging Telecommunications Technologies, e3976.

[40] Lo, C. L., Chen, C. H., Hu, J. L., Lo, K. R., & Cho, H. J. (2019). A fuel-efficient route plan method based on game theory. Journal of Internet Technology, 20(3), 925-932.

[41] Kung, H. Y., Chen, C. H., Lin, M. H., & Wu, T. Y. (2019). Design of Seamless Handoff Control Based on Vehicular Streaming Communications. Journal of Internet Technology, 20(7), 2083-2097.

[42] Elhoseny, M., & Shankar, K. (2019). Reliable data transmission model for mobile ad hoc network using signcryption technique. IEEE Transactions on Reliability.

[43] Shanmugam, P., Rajesh, R. S., & Perumal, E. (2008, May). A reversible watermarking with low warping: an application to digital fundus image. In 2008 International Conference on Computer and Communication Engineering (pp. 472-477). IEEE.

[44] Shankar, K., & Elhoseny, M. (2019). Trust Based Cluster Head Election of Secure Message Transmission in MANET Using Multi Secure Protocol with TDES. J. UCS, 25(10), 1221-1239.

[45] Parvathy, V. S., Pothiraj, S., & Sampson, J. (2020). Optimal Deep Neural Network model based multimodality fused medical image classification. Physical Communication, 101119.

[46] Subbiah Parvathy, V., Pothiraj, S., & Sampson, J. (2020). A novel approach in multimodality medical image fusion using optimal shearlet and deep learning. International Journal of Imaging Systems and Technology.

[47] Parvathy, V. S., & Pothiraj, S. (2019). Multi-modality medical image fusion using hybridization of binary crow search optimization. Health Care Management Science, 1-9.

[48] Velmurugan, S. P., Sivakumar, P., & Rajasekaran, M. P. (2018). Multimodality image fusion using centre-based genetic algorithm and fuzzy logic. International Journal of Biomedical Engineering and Technology, 28(4), 322-348.

[49] Chen, C. H. (2018). An arrival time prediction method for bus system. IEEE Internet of Things Journal, 5(5), 4231-4232.

[50] Shankar, K., Perumal, E., & Vidhyavathi, R. M. (2020). Deep neural network with moth search optimization algorithm based detection and classification of diabetic retinopathy images. SN Applied Sciences, 2(4), 1-10.

[51] Mohanty, S. N., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., & Khanna, A. (2020). An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. Future Generation Computer Systems, 102, 1027-1037.

[52] Elhoseny, M., & Shankar, K. (2020). Energy efficient optimal routing for communication in VANETs via clustering model. In Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks (pp. 1-14). Springer, Cham.

[53] Chen, C. H. (2020). A cell probe-based method for vehicle speed estimation. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 103(1), 265-267.

[54] Khamparia, A., Singh, A., Anand, D., Gupta, D., Khanna, A., Kumar, N. A., & Tan, J. (2018). A novel deep learning-based multi-model ensemble method for the prediction of neuromuscular disorders. Neural computing and applications, 1-13.

[55] Shankar, K., Zhang, Y., Liu, Y., Wu, L., & Chen, C. H. (2020). Hyperparameter tuning deep learning for diabetic retinopathy fundus image classification. IEEE Access, 8, 118164-118173.

[56] Hajiheidari, S., Wakil, K., Badri, M. and Navimipour, N.J., 2019. Intrusion detection systems in the Internet of things: A comprehensive investigation. Computer Networks.

[57] Yong, B., Liu, X., Yu, Q., Huang, L. and Zhou, Q., 2019. Malicious Web traffic detection for Internet of Things environments. Computers & Electrical Engineering, 77, pp.260-272.