RESEARCH ARTICLE OPEN ACCESS

Enhance the Security for Internet of Things Information Using Block Chain

Elayaraja P
Software Engineer-Chennai.

ABSTRACT
In recent decades, the Internet of Things (IoT) is transforming into an attractive system to drive a substantive hop on stock and enterprises through physical, computerized, and social spaces. For enhancing the security level of IoT multimedia data, a block-based security model is proposed. After forming the clusters, a hash function with blockchain technique is utilized to the secure the IoT information. Initially, the data is changed over into a number of blocks then applies a hash function to each block for an end to end blockchain model. Based on this function the information's are encrypted and decrypted stored in the cloud by an authenticated person. From the implementation results of data security, the execution time and security levels are analyzed.

Keywords: Internet of things, security, optimization, clustering and blockchain

I. INTRODUCTION

Internet of Things (IoT) is a type of network that is being utilized by wireless sensor associations and radio frequency identification (RFID) via network topology [1] to accomplish high reliability in transmission as well as intelligent processing [2-10]. IOT comprises three layers: the sensing layer, transport layer, and application layer. IOT has made a tremendous change in different areas such as business, agriculture, pharmacy, also in nuclear reactors [11-16]. To receive the IoT innovation it is important to assemble the certainty among the clients about its security and privacy that it won't make any risk to their data integrity and authority [17-20]. In secure systems, the secrecy of the information is kept up and it is ensured that at the processing of message exchange the information holds its inventiveness and no modification by the system [21-23]. In spite of the fact that, the IoT can encourage the digitization of the data itself, the dependability of such data is as yet a key challenge by Bitcoin [6]. It's upheld by a protocol that points of interest the infrastructure responsible for guaranteeing that the data remains unchanging after some time [24-26]. Benefiting from blockchains power and versatility, in this work, propose an effective decentralized verification system [27-30]. The principle motivation behind network security data insurance is to accomplish secrecy as well as integrity. Security issues are of extraordinary significance in amplifying the size of network and gadgets [31-35]. Different cryptographic algorithms have been produced that tends to the said issue, however, their use in IoT is questionable as the equipment we deal in the IoT is not appropriate for the execution of computationally costly encryption algorithms [36-38].

II. LITERATURE REVIEW

A blockchain is a database that stores every processed transaction – or information – in the sequential request, in an arrangement of PC recollections that are carefully designed to foes. These exchanges are then shared by all users by DanielMinoli et al in 2018 [39], More significantly, we talk about, how blockchain, which is the basic innovation for bitcoin, can be a key empowering agent to tackle numerous IoT security issues by Minhaj Ahmad Khan and Khaled Salah in 2018 [40]. It's additionally distinguished open research issues and difficulties for IoT security. One of the real issues of a clustering protocol is choosing an optimal group of sensor nodes as the group heads to isolate the network by Khalil Bennani et al. 2012 [41-42]. In any case, optimum clustering is an NP-Hard issue and solving it includes searches through tremendous spaces of conceivable solutions. Two fundamental periods of optimization, exploration, and exploitation,, are structured by the social interaction of dragonflies in exploring, hunting foods, and keeping away from foes while swarming powerfully or factually by Seyedali Mirjalili in 2015[43-45]. In Emanuel Ferreira Jesus et al in 2018 [46] the ideas about the structure and task of Blockchain and, mostly, investigate how the utilization of this innovation can be utilized to give security and privacy in IoT.

III. SECURITY ISSUES IN IOT MULTIMEDIA INFORMATION

Security approaches that depend greatly on encryption are not a solid match for these constrained gadgets since they are not equipped for performing complex encryption and decryption rapidly enough to have the capacity to transmit information safely in a progressive manner. Some security challenges in IoT security are tag attack, Sybil attack, wormhole attack and, etc. Regardless, with traditional encryption procedures, before dealing with some sensitive data from customers, the third party administration (cloud) would decrypt this information and after that find that data [47]. Data that is very sensitive to bank account details, usernames, passwords need to encrypt with at least two-factor authentication procedures to guarantee security. For enhancing the security in IoT data, BC is utilized. Now, the header turns out to be a piece of a cryptographic riddle which must be comprehended by the block chain's network of clients via a trial and error procedure, from trillions of opportunities – before it is included to the block chain [48--52].

IV. METHODOLOGY FOR IOT INFORMATION SECURITY

The IoT visualizes a completely associated world, where things can convey estimated information and connect with one another. For enhancing the security dimension of the multimedia data's in IoT, optimal Block Chain (BC) security model is utilized, Its behinds the bit coin concept a permanent open record of data secured by a network of distributed members, its strategy that to enables exchanges to be confirmed by a gathering of untrustworthy on-screen characters. The fundamental of this proposed strategy is, enhance the secrecy as well as the reliability of the IoT data, Moreover, this BC, every block contains the number of transactions. CH has coordinate proof about CH in the event that it confirmed a block created by different squares of data [53-56]

4.1 Security and privacy Analysis in IoT

Security in IoT is difficult because of low asset abilities of the vast majority of devices, huge scale, heterogeneity among the gadgets, and absence of standardization. Besides, a considerable lot of these IoT gadgets gather and offer a lot of information from our own spaces, in this way opening up noteworthy privacy concerns. Security and privacy risk analysis for a commonplace shrewd home engineering that depends on existing and promptly accessible market IoT gadgets and stages. As opposed to existing security and threat investigation of IoT situations, we focus on a genuine IoT smart home condition sent in our tested concentrating on the interactions among the diverse IoT parts.

4.2 IoT information Generation

The new invention of IoT and multimedia data applications is necessary to address explicit business solutions which require needs, for example, predictive maintenance, loss prevention, asset utilization, inventory tracking, disaster planning, and recovery, downtime minimization, energy usage optimization, device performance effectiveness. These datasets are particular in information structures, volume, get to procedures, and some extraordinary perspectives; they can scarcely be stored and gotten as well, its shows in figure 1. IoT applications have quite certain qualities; they produce extensive volumes of data and require network and power for significant time periods [57].

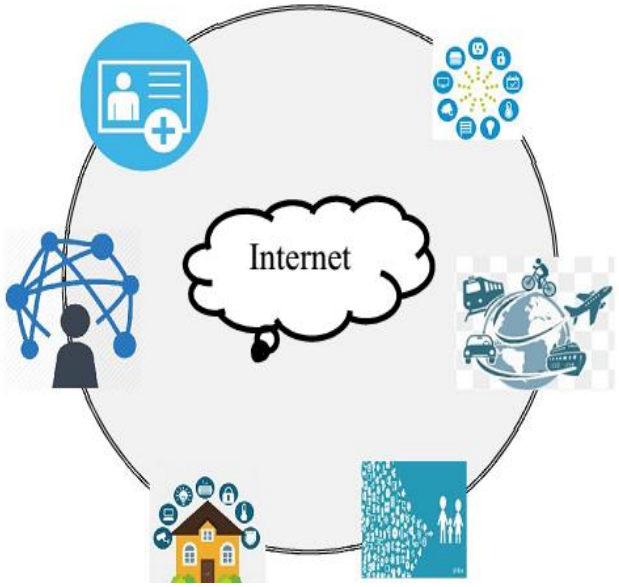

Fig 1: IoT Components

Pre-processing

This underlying preprocessing IoT data are separated to choose the sensitive or quality information for security, the purpose behind preprocessing is diminishing the computational time. Moreover, the goal is to ensure successful security and improve the performance of the model, we secure sensitive data only. IoT data clustering using optimization Information is clustered by utilizing irregular clustering model with optimization. Each data is assessed by the weights of its cluster associations. Finally, among various nodes and as indicated by their weights a node is elected as the cluster head, for optimal cluster head selection dragonfly optimization is proposed. Finally, among

various nodes and as shown by their information a node is elected as the cluster head.
individuals to that of different individuals in the area and $a_1, a_2, a_3, a_4 and\ a_5$ coefficient parameters. After the alignment procedure of individuals among the dragonflies, cohesion process is performed which implies the inclination of individuals towards the focal point of the mass of the area. The new position refreshed by utilizing the following condition

$$C_{t+1} = C_t + Levy(dis\tan ce) * C_t \quad (1)$$

Food source and the enemy is selected over best and the most exceedingly terrible solutions obtained in the whole swarm at any minute. In light of above process select optimal cluster head for IoT data clustering model. After that, the clustered data are secured by utilizing the BC technique.

File size	Encryption size	Decryption size	Memory (byte)	Execution Time (ms)
10	23	10	1242488	94523
20	34	20	374528	105481
30	44	30	312458	98450
40	49	40	412141	112345
50	56	50	423412	112482

4.2 Security model: A Block chain Model

In a BC, each transaction in the set that contains a block is hashed to produce a hash value. Hashes are combined into a Merkle Tree. Generally, the BC indicates a consistently maintained and controlled database considering developing variables and gathered information test sets. The key components of BC are a member made transactions and the recorder blocks of such exchanges. Here, the block checks whether transaction details were sustained in the correct grouping or not. This does not permit any altering of the data accessible.

Bitcoin

Bitcoin is cryptographic money and a digital payment system, in view of a public BC, each block of the Bitcoin blockchain. In Bitcoin, transactions are processed to check their integrity, authenticity, and accuracy by a gathering of creative network nodes called "Miners". Specifically, rather than mining a single transaction, the miners package various transactions that are waiting for the network to get processed in a single unit called “block".

Encryption

Encryption system function as given a message and a key, it creates a ciphered message to be transmitted over unprotected channels, without any risk being comprehended by other people who don't have the decryption key. For the security purpose, the key generation dependent on the two sets, one public and one private. The first to encrypt and the second to decrypt and the vice versa; this is conceivable because of the utilization of some numerical functions that have the property of being irreversible.
For encrypted and decrypted information

$$Enc = hash(\inf\ o\ group, hash, publickey, IP) \quad (2)$$

Each block of data encrypted by

$$E \Rightarrow m^k \mid \mathrm{mod}\inf\ o \mid \quad (3)$$

V. RESULTS AND ANALYSIS

Our proposed IoT information security model is executed in the Java programming language with the JDK 1.7.0 in a windows machine enclosing the configurations such as the Intel (R) Core i3 processor, 1.6 GHz, 4 GB RAM, and the operating system platform is Microsoft Window7 Professional. This proposed security analysis is compared with other techniques.

Table 1: Proposed (blockchain) Security analysis results

Table 1 shows the result of proposed parameters which obtains in the study. Depends on file size, we find encryption size, decryption size, memory and execution time. The result depicts that encryption size and decryption increases if the file size increased, the execution time also increased. But compared to other techniques proposed model secure the IoT data in a high manner.

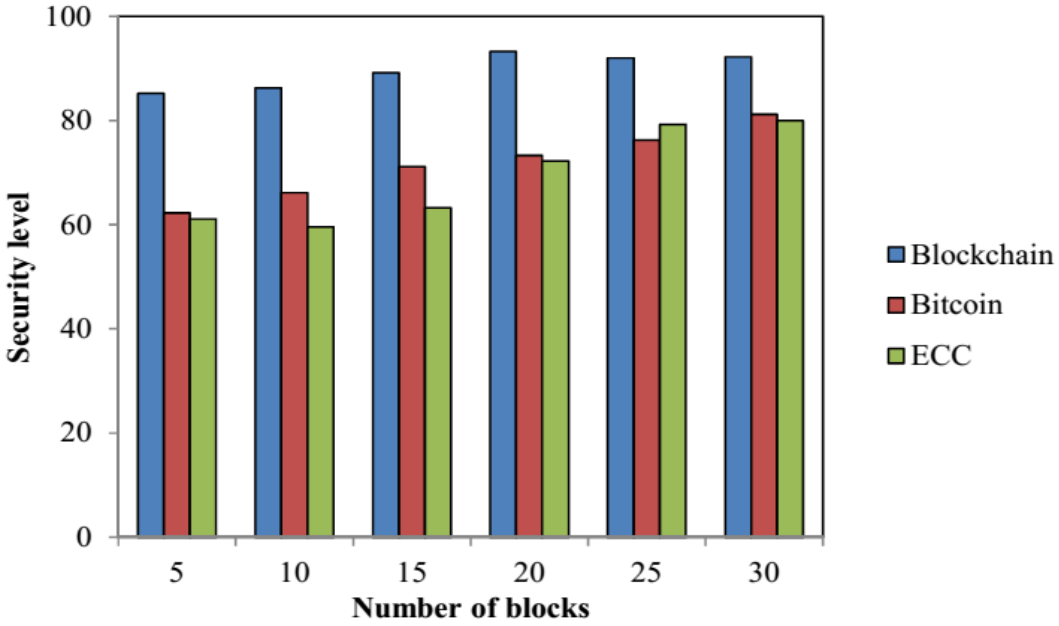

Fig 4: Number of blocks Vs hash value

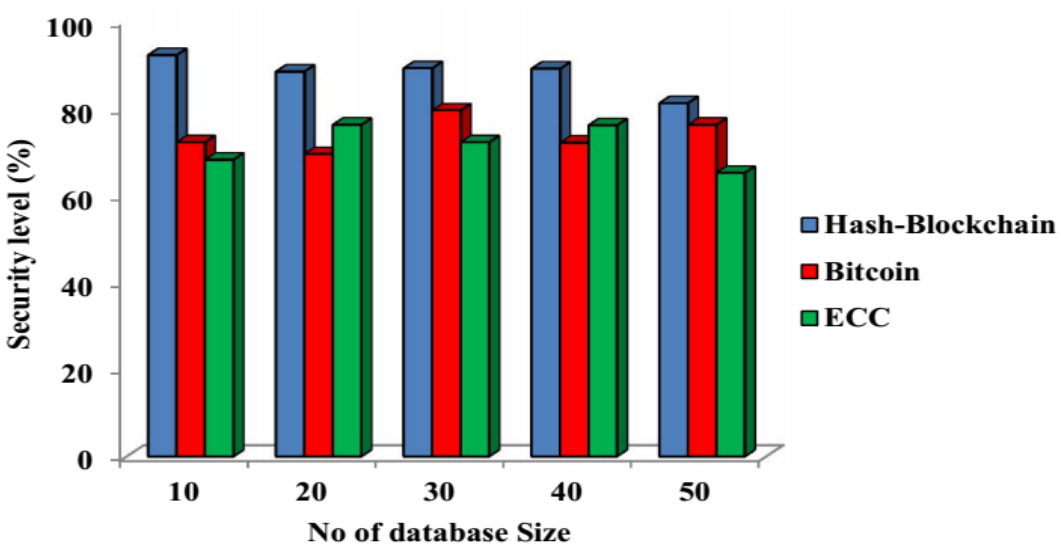

Fig 5: Security Level comparative analysis

Figure 4 shows the graph of security level based on a number of blocks. Here, we compare the security result with the proposed method to existing techniques such as bitcoin and ECC. The graph depicts that block chain reaches optimal security in the range of 82 to 91.23% compared to the other two. Figure 5 shows the security level based on the database size. The hash blockchain performs an optimal security level for every database size. The security level reaches a maximum at 90% in hash block chain function.

VI. CONCLUSION

In this chapter, the IoT multimedia information's security model with help hash function based blockchain was discussed. Thusly, the advantages of applying BC to the IoT ought to be examined precisely and taken with caution. Also, this chapter provided an analysis of the main difficulties that blockchain and IoT must address in order for them to effectively cooperate. This blockchain technology can help to improve IoT applications and also this

data clustering cluster head selection by DOA, its give better accuracy. However, it is still in the beginning periods of creating block chains, and these obstructions will be defeated, opening the best approach to numerous potential outcomes. One of the principle concerns about blockchain, and especially crypto currencies, resides in its volatility which has also been exploited by individuals to take unfair advantage of this situation. The incorporation of the IoT and blockchain will extraordinarily increase the security level.

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] Jesus, E.F., Chicarino, V.R., de Albuquerque, C.V. and Rocha, A.A.D.A., 2018. A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. Security and Communication Networks, 2018.