RESEARCH ARTICLE OPEN ACCESS

Secure Data Transmission on Internet of Healthcare Things

Dr. S. Rama Sree
Professor In Cse Aditya Engineering College-Surampalem

ABSTRACT

The ever-growing advancement in communication innovation of modern smart objects carries with it a new era of improvement for IoT (Internet of Things) based networks. The health care system is the best approach to store the patient's personal health data in online with high privacy. Ensuring the privacy and confidentiality of patient information in the cloud is of utmost importance; here, enhanced security model of healthcare data gives rise to trust. Then, we presented healthcare service providers for giving the full scope of medical services to people enrolled in IoHT. The performance of Secure Data is approved through simulations in terms of energy cost, computation time, etc. of the proposed algorithms and the results show that Secure Data can be efficient while applying for ensuring security chances in IoT-based healthcare systems.

Keywords: Internet of things (IoT), Security, Optimization, Sensor Network, share creation and block ciphers.

I. INTRODUCTION

The Internet of Things (IoT) is gathered of an extraordinary number of things (devices) that are linked through the Internet [1-10]. In everyday things the framework can be equipped with distinguishing, measuring, network and processing capabilities; for such a way that this device can interact with different devices and it can give service to accomplish a specific objective through the internet [2]. In attractive virtual and physical world, this system related to an integrated communication environment of interconnected devices and platforms [11-20]. Therefore, it is important to build up an effective model to guarantee the security and integrity of the patient's diagnostic information transmitted and received from IoT environment [21-26]. The sophisticated chips and sensors are surrounded in the physical things that envelop us, for each transmitting valuable data [5].The way toward sharing such substantial measure of information starts with the devices themselves which should safely communicate with the IoT stage [27-35]. In most countries, the healthcare data offer real sensitive information that should be confined by law via Health Information and Portability Accountability Association (HIPAA) [36].

A need of serial to parallel converter and parallel to serial converter is avoided by choosing lightweight figure (simeck, simon, katan) family which is having adaptability [37-40] in choosing variable information and key sizes [15]. In the secret cipher sharing, a whole cipher is analyzed into a number of shares at the computing layer [41].

II. LITERATURE REVIEW

In 2018 Sanaz Rahimi Moosavi et al. [42] proposed the scheme is demonstrated by simulation and a full hardware/software prototype. The result showed that the energy-performance evaluation compared to existing approaches. The proposed model reduces the communication by 26% communication latency between smart gateways and end users by 16%. Investigation of our usage uncovered that the handover idleness caused by versatility is low and the handover procedure does not bring about any preparing or correspondence overhead on the sensors.

The security system authenticates a user based on the Open ID standard by Mahmud Hossain et al in 2018 [43]. In security the system that ensures user authentication and protected access to resources and services by IoT. Once the authentication is successful, the user is issued an authorization ticket, called Security Access Token (SAT). The SAT contains a set of privileges that grants the user access to medical IoT devices and their services and/or resources. The SAT is cryptographically protected to guard against forgery. A medical IoT device verifies the SAT prior to serving a request, and thus, ensures protected access.

A secure data collection scheme for IoT based healthcare system named SecureData by Hai Tao et al. [44]. We use the idea of secret cipher sharing technique to protect patients' data privacy and it is implemented and optimized in the FPGA hardware platform using KATAN algorithm. In the cloud computing layer, apply a distributed database technique that includes a number of cloud data servers to guarantee patients' personal data privacy at the cloud computing layer. The result showed that secure data can be effective when applying for securing risks in IoT based healthcare.

The patient data are stored as a cloud server in the hospital due to which the security is vital by Mohamed Elhoseny et al. [46]. Thus, the framework is required for the secure transmission and effective storage of medical images interleaved with patient information. For increasing the security level of encryption and decryption process, the optimal key will be selected utilizing hybrid swarm optimization, i.e., grasshopper optimization and particle swarm optimization in elliptic curve cryptography. In view of this method, the medical images are secured in IoT framework.

III. SECURITY ISSUE AND CHALLENGES IN IOHCT

- For getting to IoT administrations, the interfaces utilized through web, mobile, and cloud are powerless against various attacks which may seriously influence the information privacy.
- The physical layer communication of IoHT should be secured so as to make it difficult to reach to unapproved recipients [24,19].
- Privacy Violation on cloud based IoHT: Different attacks which may disregard personality and area privacy might be propelled on cloud or defer tolerant network based IoHT [26].
- With the heterogeneous networks, structures, and conventions, the IoT pattern turns out to be more powerless against single points of failure than some other pattern.
- Within the worldwide system, an efficient combination of security benchmarks at each layer would then be able to be characterized through IoHT structural requirements.

IV. PROPOSED MODEL

Enhance the security model of Heath care medical information from body sensor Network in IoT condition is proposed in this manuscript. To give the extra security, Lightweight SIMON block cipher based implementation is presented for cipher information creation process. By choosing SIMON cipher family which is having adaptability in choosing variable information and key sizes, after this model imaginative Share creation model is used to produce the copy of cipher information in the cloud server, besides, Selection of Number of the user in IoHT security process optimization is used. In this way, security is a fundamental prerequisite of healthcare applications. The shares are sent through secure communication independently towards the cloud. The achievement of healthcare application depends mostly on patient security and privacy, for an ethical and legitimate reason.

5.1 IoT Sensor Network Model

IoT architecture is essentially made out of a lot of low processing detecting units called nodes and a cloud-based layer that empowers the user to screen those nodes remotely and progressively. The work introduces an IoT approach for deploying a Wireless Sensor Network (WSN) connected to the natural observing of temperature and relative stickiness inside doctor's facilities or center labs.

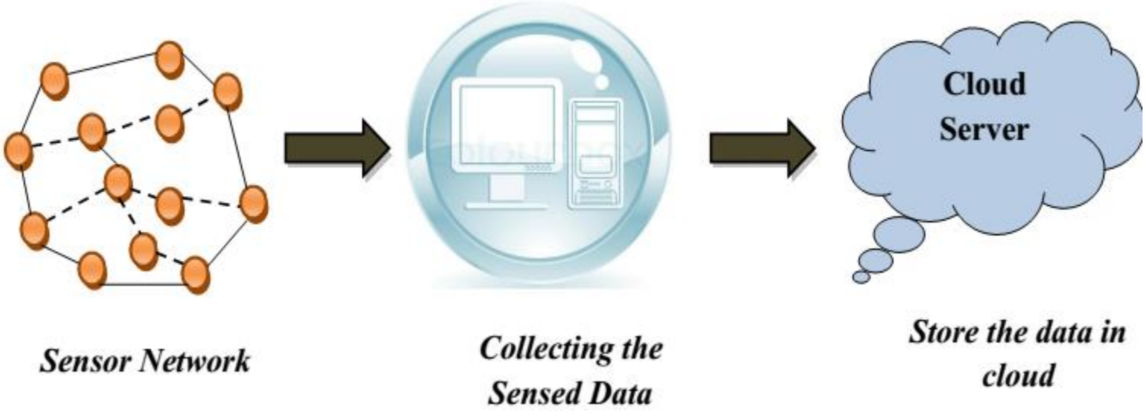

Fig 1: IoT Sensor Network

The design of the IoT sensor network appears in figure 1. The proposed design is made out of three layers to be specific, node layer (sensor network) where the healthcare related data are sensed, local administration layer (computer) and cloud-based layer. The second layer gathers the detected information from the network and after that transfers the information to the cloud [47].

5.2 Cipher Information Generation Model

For secure transmission, cipher text is generated for the considered healthcare information. In the proposed study, SIMON block cipher is used to encrypt the input data. The structure of SIMON [50-60] square cipher comprises parallelism of encryptions which includes round functions and key generation blocks. The essential capacity of block ciphers is to give secure on stored information or information from the outsider utilizing symmetric encryption strategies. They perform an activity on fixed-size blocks of plain content and resulting in about a block of cipher content for each. The most generally utilized block sizes in presently block ciphers are 64 bits and 128 bits [61-65].

Optimal Cloud Server Selection Model

Optimal cloud server is elected and secured by the implementation of meta-heuristic algorithm ie HTLBO. The TLBO method is based on the effect of the influence of a teacher on the output of learners in a class. The process of TLBO [30] is divided into three parts, namely the teaching phase, the learning phase and studying phase.

The procedure involved in the TLBO algorithm is explained as follows

Population Initialization: Generate a random population according to the population size (here, the number of users are considered) and a number of design variables.

Share generation using CRT: Using TLBO algorithm, an optimal cloud server is achieved and based on the available user, we can generate a number of shares, for that, an innovative share creation model is used, Chinese Remainder Theorem (CRT) [33]. CRT is issued to solve a set of simultaneous congruence equations which can be stated as follows.

V. RESULTS AND ANALYSIS

Our proposed IoHT security model implemented in Net beans with JAVA programming language JDK 1.7.0 windows machine containing the configurations such as the Intel (R) Core i5 processor, 1.6 GHz, 4 GB RAM. Moreover our proposed lightweight block cipher SIMON model compared with other cipher creation algorithm and optimization model, along with the Performance measure. Here considerable measures are energy consumption, Throughput, security level and execution time and some other Measures.

Analysis

The HealthCare data securities the implementation model, the collected information's are converted to packets ready to transmit from an IoT device/sensor. Then the SIMON cipher model in hardware implementation, it maintains the security model in healthcare provider (owner/ doctor) to body sensor network information. Encryption operations are activated by the confirmation of a start data. In the first cycle of encryption operations, plaintext is loaded in hardware properties.

Table 1: Our proposed Simon parameters

Data Size (Health info)	Key words	Key size	Number of Rounds	Energy (PJ/bit)	Cipher Secure Level (%)
16	4	64	32	3.22	85.45
24	3	72	36	5.22	92.12
32	4	128	36	2.14	89.45
48	3,4	144,192	42	3.12	94.15
64	3,4	192,256	42,44	3.45	88.4

96	2,3	192,288	52,54	3.88	82.2
128	2,3,4	256,384,512	68,69,72	3.85	81.2

Table 1 shows the proposed Simon parameters for IoHT. Here, the parameters are analyzed based on healthcare data sizes. In this table we take some data sizes like 16, 24, 32, 48, 64,96 and 128, for example, if the data size is 16, the keywords reaches 4, key size allotted as 64, the data performed in the Simon model for 32 rounds. The energy received as 3.22 PJ/bit and the cipher secure level is 85.45%. If the data sizes are increased, key size and number of rounds is increased, moreover, the cipher secure level reaches maximum in proposed Simon model.

VI. CONCLUSION

In this research paper, we have analyzed the difficulties with data collection in IoT-based healthcare applications and proposed another healthcare data secure scheme to provide high data security and ensure the privacy of the patients' personal data. The outcomes demonstrated that the proposed algorithm is able to optimize the number of users and enhance the data privacy accuracy in cloud. Furthermore, its execution time shows better performance than the other cipher algorithms and share generation model. For future investigations, we will study the detailed implementation of the algorithms with different measures by using innovative data encryption methods with hybrid optimization approach. This will be pertinent to various applications in cloud data security under threats/attacks condition.

REFERENCE

[1] 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

[2] Ezhilarasu, P., & Krishnaraj, N. (2015). Applications of Finite Automata in Lexical Analysis and as a Ticket Vending Machine–A Review. Int. J. Comput. Sci. Eng. Technol, 6(05), 267-270.

[3] Agrawal, U., Arora, J., Singh, R., Gupta, D., Khanna, A., & Khamparia, A. (2020). Hybrid Wolf-Bat Algorithm for Optimization of Connection Weights in Multi-layer Perceptron. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 16(1s), 1-20.

[4] Prasanna, S., & Ezhilmaran, D. (2016). Association rule mining using enhanced apriori with modified GA for stock prediction. International Journal of Data Mining, Modelling and Management, 8(2), 195-207.

[5] Pustokhina, I. V., Pustokhin, D. A., Gupta, D., Khanna, A., Shankar, K., & Nguyen, G. N. (2020). An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems. IEEE Access, 8, 107112-107123.

[6] 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.

[7] Joshi, G. P., Perumal, E., Shankar, K., Tariq, U., Ahmad, T., & Ibrahim, A. (2020). Toward Blockchain-Enabled Privacy-Preserving Data Transmission in Cluster-Based Vehicular Networks. Electronics, 9(9), 1358.

[8] Saračević, M. H., Adamović, S. Z., Miškovic, V. A., Elhoseny, M., Maček, N. D., Selim, M. M., & Shankar, K. (2020). Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures. IEEE Transactions on Reliability.

[9] Namasudra, S., & Roy, P. (2017). Time saving protocol for data accessing in cloud computing. IET Communications, 11(10), 1558-1565.

[10] Elsir, A., Elsier, O., Abdurrahman, A., & Mubarakali, A. (2019). Privacy Preservation in Big Data with Data Scalability and Efficiency Using Efficient and Secure Data Balanced Scheduling Algorithm.

[11] Ezhilarasu, P., Krishnaraj, N., & Babu, S. V. (2015). Applications of finite automata in text search-a review. International Journal of Science, Engineering and Computer Technology, 5(5), 116.

[12] 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.

[13] Prasanna, S., & Maran, E. (2015). Stock Market Prediction Using Clustering with Meta-Heuristic Approaches. Gazi University Journal of Science, 28(3).

[14] Pustokhina, I. V., Pustokhin, D. A., Rodrigues, J. J., Gupta, D., Khanna, A., Shankar, K., ... & Joshi, G. P. (2020). Automatic Vehicle License Plate Recognition using Optimal K-Means with Convolutional Neural Network for Intelligent Transportation Systems. IEEE Access.

[15] Namasudra, S. (2018). Cloud computing: A new era. Journal of Fundamental and Applied Sciences, 10(2).

[16] 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.

[17] Deepalakshmi, P., & Shankar, K. (2020). Role and Impacts of Ant Colony Optimization in Job Shop Scheduling Problems: A Detailed Analysis. Evolutionary Computation in Scheduling, 11-35.

[18] Ashwin, M., Kamalraj, S., & Azath, M. (2019). Multi objective trust optimization for efficient communication in wireless M learning applications. Cluster Computing, 22(5), 10687-10695.

[19] Ezhilarasu, P., & Krishnaraj, N. (2015). Double Substring based Classification for Nondeterministic Finite Automata. Indian Journal Of Science And Technology, 8, 26.

[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.

[21] Prasanna, S., Govinda, K., & Kumaran, U. S. (2012). An Evaluation study of Oral Cancer Detection using Data Mining Classification Techniques. International Journal of Advanced Research in Computer Science, 3(1).

[22] Sankhwar, S., Gupta, D., Ramya, K. C., Rani, S. S., Shankar, K., & Lakshmanaprabu, S. K. (2020). Improved grey wolf optimization-based feature subset selection with fuzzy neural classifier for financial crisis prediction. Soft Computing, 24(1), 101-110.

[23] Namasudra, S., & Deka, G. C. (2018). Introduction of DNA computing in cryptography. In Advances of DNA computing in cryptography (pp. 1-18). Chapman and Hall/CRC.

[24] Mubarakali, A., Srinivasan, K., Mukhalid, R., Jaganathan, S. C., & Marina, N. (2020). Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems. Computational Intelligence.

[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.

[26] Ezhilarasu, P., Thirunavukkarasu, E., Karuppusami, G., & Krishnaraj, N. (2015). Single substring based classification for nondeterministic finite automata. International Journal on Applications in Information and Communication Engineering, 1(10), 29-31.

[27] 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.

[28] Latha, A., Prasanna, S., Hemalatha, S., & Sivakumar, B. (2019). A harmonized trust assisted energy efficient data aggregation scheme for distributed sensor networks. Cognitive Systems Research, 56, 14-22.

[29] Krishnaraj, N., Elhoseny, M., Lydia, E. L., Shankar, K., & ALDabbas, O. (2020). An efficient radix trie-based semantic visual indexing model for large-scale image retrieval in cloud environment. Software: Practice and Experience.

[30] Namasudra, S., Roy, P., Vijayakumar, P., Audithan, S., & Balusamy, B. (2017). Time efficient secure DNA based access control model for cloud computing environment. Future Generation Computer Systems, 73, 90-105.

[31] Lakshmanaprabu, S. K., Shankar, K., Rani, S. S., Abdulhay, E., Arunkumar, N., Ramirez, G., & Uthayakumar, J. (2019). An effect of big data technology with ant colony optimization based routing in vehicular ad hoc networks: Towards

smart cities. Journal of cleaner production, 217, 584-593.

[32] Namasudra, S., & Deka, G. C. (Eds.). (2018). Advances of DNA computing in cryptography. CRC Press.

[33] Mubarakali, A., Ashwin, M., Mavaluru, D., & Kumar, A. D. (2020). Design an attribute based health record protection algorithm for healthcare services in cloud environment. Multimedia Tools and Applications, 79(5), 3943-3956.

[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] Krishnaraj, N., Ezhilarasu, P., & Gao, X. Z. Hybrid Soft Computing Approach for Prediction of Cancer in Colon Using Microarray Gene Data. Current Signal Transduction Therapy, 11(2).

[36] Namasudra, S., Deka, G. C., Johri, P., Hosseinpour, M., & Gandomi, A. H. (2020). The revolution of blockchain: State-of-the-art and research challenges. Archives of Computational Methods in Engineering.

[37] Goel, N., Grover, B., Gupta, D., Khanna, A., & Sharma, M. (2020). Modified Grasshopper Optimization Algorithm for detection of Autism Spectrum Disorder. Physical Communication, 101115.

[38] Prasanna, S., Narayan, S., NallaKaruppan, M. K., Anilkumar, C., & Ramasubbareddy, S. (2019). Iterative Approach for Frequent Set Mining Using Hadoop Over Cloud Environment. In Smart Intelligent Computing and Applications (pp. 399-405). Springer, Singapore.

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

[40] Raj, R. J. S., Shobana, S. J., Pustokhina, I. V., Pustokhin, D. A., Gupta, D., & Shankar, K. (2020). Optimal Feature Selection-Based Medical Image Classification Using Deep Learning Model in Internet of Medical Things. IEEE Access, 8, 58006-58017.

[41] Namasudra, S., & Deka, G. C. (2018). Taxonomy of DNA-based security models. In Advances of DNA Computing in Cryptography (pp. 37-52). Chapman and Hall/CRC.

[42] Mubarakali, A., Ramakrishnan, J., Mavaluru, D., Elsir, A., Elsier, O., & Wakil, K. (2019). A new efficient design for random access memory based on quantum dot cellular automata nanotechnology. Nano Communication Networks, 21, 100252.

[43] Ramakrishnan, J., Mavaluru, D., Sakthivel, R. S., Alqahtani, A. S., Mubarakali, A., & Retnadhas, M. (2020). Brain–computer interface for amyotrophic lateral sclerosis patients using deep learning network. NEURAL COMPUTING & APPLICATIONS.

[44] 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.

[45] Sinha, A., Shrivastava, G., Kumar, P., & Gupta, D. (2020). A community-based hierarchical user authentication scheme for Industry 4.0. Software: Practice and Experience.

[46] Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., & Shanthini, A. (2020). Towards DNA based data security in the cloud computing environment. Computer Communications, 151, 539-547.

[47] Mubarakali, A., Durai, A. D., Alshehri, M., AlFarraj, O., Ramakrishnan, J., & Mavaluru, D. (2020). Fog-Based Delay-Sensitive Data Transmission Algorithm for Data Forwarding and Storage in Cloud Environment for Multimedia Applications. Big Data.

[48] Reshmi, T. R., & Azath, M. (2020). Improved self-healing technique for 5G networks using predictive analysis. Peer-to-Peer Networking and Applications, 1-17.

[49] Namasudra, S., Chakraborty, R., Majumder, A., & Moparthi, N. R. (2020). Securing multimedia by using DNA based encryption in the cloud computing environment. ACM Transactions on Multimedia Computing Communications and Applications.

[50] Patro, K. K., Reddi, S. P. R., Khalelulla, S. E., Kumar, P. R., & Shankar, K. (2020). ECG data optimization for biometric human recognition using statistical distributed machine learning algorithm. The Journal of Supercomputing, 76(2), 858-875.

[51] Rajagopal, A., Joshi, G. P., Ramachandran, A., Subhalakshmi, R. T., Khari, M., Jha, S., ... & You, J. (2020). A Deep Learning Model Based

on Multi-Objective Particle Swarm Optimization for Scene Classification in Unmanned Aerial Vehicles. IEEE Access, 8, 135383-135393.

[52] 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.

[53] Mubarakali, A., Bose, S. C., Srinivasan, K., Elsir, A., & Elsier, O. (2019). Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. Journal of Ambient Intelligence and Humanized Computing, 1-9.

[54] Devaraj, A. F. S., Murugaboopathi, G., Elhoseny, M., Shankar, K., Min, K., Moon, H., & Joshi, G. P. (2020). An Efficient Framework for Secure Image Archival and Retrieval System Using Multiple Secret Share Creation Scheme. IEEE Access, 8, 144310-144320.

[55] Mubarakali, A. (2020). Healthcare Services Monitoring in Cloud Using Secure and Robust Healthcare-Based BLOCKCHAIN (SRHB) Approach. MOBILE NETWORKS & APPLICATIONS.

[56] Namasudra, S. (2019). An improved attribute-based encryption technique towards the data security in cloud computing. Concurrency and Computation: Practice and Experience, 31(3), e4364.

[57] 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.

[58] Govinda, K., & Prasanna, S. (2015, February). Medical dialysis prediction using fuzzy rules. In 2015 International Conference on Soft-Computing and Networks Security (ICSNS) (pp. 1-5). IEEE.

[59] Sujatha, R., Navaneethan, C., Kaluri, R., & Prasanna, S. (2020). Optimized Digital Transformation in Government Services with Blockchain. In Blockchain Technology and Applications (pp. 79-100). Auerbach Publications.

[60] Govinda, K., & Prasanna, S. (2015, February). A generic image cryptography based on Rubik's cube. In 2015 International Conference on Soft-Computing and Networks Security (ICSNS) (pp. 1-4). IEEE.

[61] 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

[62] Prasanna, S., & Narayanan, V. (2017). A Novel Approach for Generation of All-Optical OFDM Using Discrete Cosine Transform Based on Optical Couplers in a Radio-Over-Fiber Link. International Journal of Advanced Research in Engineering and Technology, 8(3).

[63] Sanjeevi, P., Prasanna, S., Siva Kumar, B., Gunasekaran, G., Alagiri, I., & Vijay Anand, R. (2020). Precision agriculture and farming using Internet of Things based on wireless sensor network. Transactions on Emerging Telecommunications Technologies, e3978.

[64] Rathi, V. K., Chaudhary, V., Rajput, N. K., Ahuja, B., Jaiswal, A. K., Gupta, D., ... & Hammoudeh, M. (2020). A Blockchain-Enabled Multi Domain Edge Computing Orchestrator. IEEE Internet of Things Magazine, 3(2), 30-36.

[65] Khanna, A., Rodrigues, J. J., Gupta, N., Swaroop, A., & Gupta, D. (2020). Local mutual exclusion algorithm using fuzzy logic for Flying Ad hoc Networks. Computer Communications.