RESEARCH ARTICLE OPEN ACCESS

Survey: Mutual Authentication Mechanism for Smart City Healthcare (SHC2) Applications

Mr. Muhib Anwar Lambay

Assistant Professor & Project Coordinator, Department of Computer Engineering
at Theem College of Engineering, Boisar - Mumbai

ABSTRACT
Smart City healthcare (SHC2) is a system used to monitor the patient in the home by expecting and reacting to their needs and conceding their freedom. Thus, IoT is a path for thought. It is trusted that IoT-based healthcare devices will almost certainly give the early recognition of potential intensifications and advise patients and medical experts to such an extent that they can be dealt with instantly. From the implementation results, our proposed SHC2 analyzed by encryption time, decryption time, access time and response time in minimum range.

***Keywords*:** Light Weight Cipher, Smart City Healthcare (SHC2), encryption time and decryption time.

I. INTRODUCTION

As a result of the significance of shrewd metropolitan regions to various accomplices and the focal points and troubles related with its utilization, the thought has been attracting basic thought from experts inside different kind assessments, including Internet of Things (IoT), Information Systems (IS) and more standard programming designing and planning controls [1-5]. Different metropolitan networks have now begun advancing toward grasping this thought. There are four zones around the possibility of reasonability that were directed by Amsterdam and these join versatility, working, open space, and living [6-10]. Medical services (HC) IoT can in like manner uphold quiet duty and satisfaction by empowering them to contribute more energy partner with their primary care physicians [11-15].

The blend of the recognizing gadgets and the customer equipment development which is an important application will help in observing the patient's wellbeing consistently in the medical care an area [16-20]. These including assistive conditions don't need any correspondence or wearables concerning the customer yet need to vanquish the expected challenges of observing different people at once [21-25].

Utilizing far off sensor networks in medical services frameworks involves a creating field for legitimate assessment especially. In all honesty, present-day medical services will require pervasive observing of wellbeing with less correspondence among experts and patients [26-30]. Ground-breaking just as solid cryptography limits are basic for working up a secured application as distant sensor frameworks for Smart Cities Heath care (SC-HC) change sensitive physiological and individual data [30-35]. To overhaul the security of the Infrastructure needed for distant medical services is picked up from various traders. Medical care data is Reliable and secure trade over the nearby organization and through the quite a while in the past framework like the Internet to the medical services worker [36-40].

Each security system must supply some security process that guarantees the secrecy of the system. Some of the goals that can be achieved by cryptography are as follows [40-50]:

Authentication: It is the process of verifying the identity of the users before they communicate between them. It assures that communicating party is the one that can claim.

Confidentiality: It means that only the authenticated people are able to interpret the message (data) content and no one else. It ensures that nobody can understand the received message except the one who has the decipher key. It means that system is secure.

Access Control: In order to prevent the unauthorized use of resources. The system will verify the user has adequate permission to use the service. Further, it verifies the conditions and restrictions for access.

Integrity: It assures that the data is not tampered or it is free from any modification in-between the end points.

Non-Repudiation: This implies that neither the sender nor the receiver can erroneously deny that they have sent a certain message.

Availability: Cryptographic model must be designed for work, in any case of failure.

Accountability: All user activities are monitored so that if any user attempts some illegal activities, then it stops and gives punishment.

1. Related works:

Keen metropolitan zones use data and correspondence advancements to improve: the individual fulfillment for its locals, the close by economy, transport, traffic the chiefs, condition, and participation with the legislature [51-60]. In light of the congruity of shrewd metropolitan as data and correspondence advancements are changing standard metropolitan networks into shrewd metropolitan regions, the IoT makes brilliant metropolitan regions powerful and responsive. Taking everything into account, for clinical technologists to enter and develop themselves in the new medical care industry, it is essential that we look past regular kinds of mechanical advancements [61-65].

As to keen medical services inside savvy metropolitan zones, this part presents an examination where an optoelectronic regulator chip was proposed to control the miniature light-radiating diode (LED) structure used in the retinal prosthesis. An independently addressable low force more modest miniature LED group is arranged and the results are represented. In all honesty, a remote sensor framework is used to assemble clinical data, for instance, major signs and individual data to send it to the parental figure. Consequently, the ensuring security and assurance of this fragile data are outstandingly fundamental. Data security is a relating movement between controlling admittance to information while allowing free and basic admittance to people who need that information. Given the sensitive thought of therapeutic administrations data, it is irreplaceable for human administrations providers to have a solid and reliable information security organization set up. The techniques to react and make sure about the social protection data, yet additionally predict and hinder any assaults pushed by computerized gangsters [66-73].

In cryptography, the party that only exchange the secret messages know the private or secret key i.e., encryption/decryption key. In earlier secret key cryptography methods, each of the encrypted and decrypted message keys could be shared by the communicators. The main disadvantage of this system is, if anyone loses the key or if it is stolen, the system is broken. Later this system was changed as a combination of both public and private keys. For example, Alice wants to send a message to Bob where both Alice and Bob shared the same key for an encrypted message. If Alice shared XORs her message with the secret key, then Bob also need XORs message with her (the same) secret key for decrypt the message. Before long, the usage of this development is for all intents and purposes unexplored in medical care circumstances, where potential applications consolidate understanding observing, asset perceptibility, and drug association frameworks, to allude to a couple. The medical services data identified by the IoT sensor framework is encoded by Lightweight SIMON block figure. The decision of the customers in IoHT is made by the metaheuristic calculation called Hybrid Teaching and Learning Based Optimization (HTLBO). By then, we present medical care specialist organizations for giving the full degree of clinical administrations to people got together with IoT.

II. CONCLUSION

This proposed Cipher plays out the key booking two unmistakable assessed key was picked and planned the 80bit and 128bit keys. By then, it tends to be considered with other cryptography calculations to improve the security of a half and half calculation for more data. The fate of security in distant medical care frameworks, which demands dynamically quiet determined and customizable security arrangements, is taken a gander at with different challenges. In addition, consolidate the more than block codes to expanding the security level of the medical services data.

REFERENCES

[1] Feng, Y., Yi, J. H., & Wang, G. G. (2019). Enhanced Moth Search Algorithm for the Set-Union Knapsack Problems. IEEE Access, 7, 173774-173785.

[2] Sivaram, M., Batri, K., Amin Salih, M., &Porkodi, V. (2019). Exploiting the Local Optima in Genetic Algorithm using Tabu Search. Indian Journal of Science and Technology, 12(1), 1-13.

[3] Venkatraman, S., &Surendiran, B. (2020). Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems. Multimedia Tools and Applications, 79(5), 3993-4010.

[4] 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.

[5] Ezhilarasu, P., Krishnaraj, N., &Dhiyanesh, B. (2015). Arithmetic Coding for Lossless Data Compression–A Review. International Journal of Computer Science Trends and Technology, 3(3).

[6] Porkodi, V., Singh, A. R., Sait, A. R. W., Shankar, K., Yang, E., Seo, C., & Joshi, G. P. (2020). Resource Provisioning for Cyber–Physical–Social System in Cloud-Fog-Edge Computing Using Optimal Flower Pollination Algorithm. IEEE Access, 8, 105311-105319.

[7] Gao, D., Wang, G. G., &Pedrycz, W. (2020). Solving fuzzy job-shop scheduling problem using DE algorithm improved by a selection mechanism. IEEE Transactions on Fuzzy Systems.

[8] Sivaram, M., Mohammed, A. S., Yuvaraj, D., Porkodi, V., Manikandan, V., &Yuvaraj, N. (2019, February). Advanced expert system using particle swarm optimization based adaptive network based fuzzy inference system to diagnose the physical

constitution of human body. In International Conference on Emerging Technologies in Computer Engineering (pp. 349-362). Springer, Singapore.

[9] Jiménez, A. C., García-Díaz, V., González-Crespo, R., &Bolaños, S. (2018). Decentralized Online Simultaneous Localization and Mapping for Multi-Agent Systems. Sensors, 18(8), 2612.

[10] Venkatraman, S., Surendiran, B., & Kumar, P. A. R. (2020). Spam e-mail classification for the Internet of Things environment using semantic similarity approach. The Journal of Supercomputing, 76(2), 756-776.

[11] Lydia, E. L., Raj, J. S., PandiSelvam, R., Elhoseny, M., & Shankar, K. (2019). Application of discrete transforms with selective coefficients for blind image watermarking. Transactions on Emerging Telecommunications Technologies, e3771.

[12] Ezhilarasu, P., Prakash, J., Krishnaraj, N., Kumar, D. S., Babu, K. S., &Parthasarathy, C. (2015). A Novel Approach to Design the Finite Automata to Accept the Palindrome with the Three Input Characters. Indian Journal of Science and Technology, 8(28).

[13] Devaraj, A. F. S., Elhoseny, M., Dhanasekaran, S., Lydia, E. L., & Shankar, K. (2020). Hybridization of firefly and Improved Multi-Objective Particle Swarm Optimization algorithm for energy efficient load balancing in Cloud Computing environments. Journal of Parallel and Distributed Computing.

[14] Zou, D., Wang, G. G., Sangaiah, A. K., & Kong, X. (2017). A memory-based simulated annealing algorithm and a new auxiliary function for the fixed-outline floorplanning with soft blocks. Journal of Ambient Intelligence a+nd Humanized Computing, 1-12.

[15] Kumar, A., Ahuja, H., Singh, N. K., Gupta, D., Khanna, A., & Rodrigues, J. J. (2018). Supported matrix factorization using distributed representations for personalised recommendations on twitter. Computers & Electrical Engineering, 71, 569-577.

[16] Sivaram, M., Porkodi, V., Mohammed, A. S., Manikandan, V., &Yuvaraj, N. (2019). Retransmission DBTMA protocol with fast retransmission strategy to improve the performance of MANETs. IEEE Access, 7, 85098-85109.

[17] Venkatraman, S., & Kumar, P. A. R. (2019). Improving Adhoc wireless sensor networks security using distributed automaton. Cluster Computing, 22(6), 14551-14557.

[18] Lydia, E. L., Govindaswamy, P., Lakshmanaprabu, S., &Ramya, D. (2018). Document clustering based on text mining K-means algorithm using euclidean distance similarity. J. Adv. Res. Dyn. Control Syst.(JARDCS), 10(2), 208-214.

[19] Ortin, F., Mendez, S., García-Díaz, V., & Garcia, M. (2014). On the suitability of dynamic languages for hot-reprogramming a robotics framework: a Python case study. Software: Practice and Experience, 44(1), 77-104.

[20] 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).

[21] Le Nguyen, B., Lydia, E. L., Elhoseny, M., Pustokhina, I., Pustokhin, D. A., Selim, M. M., ... & Shankar, K. (2020). Privacy Preserving Blockchain Technique to Achieve Secure and Reliable Sharing of IoT Data. CMC-COMPUTERS MATERIALS & CONTINUA, 65(1), 87-107.

[22] Chavhan, S., Gupta, D., Chandana, B. N., Khanna, A., & Rodrigues, J. J. (2019). IoT-based Context-Aware Intelligent Public Transport System in a metropolitan area. IEEE Internet of Things Journal.

[23] Gu, Z. M., & Wang, G. G. (2020). Improving NSGA-III algorithms with information feedback models for large-scale many-objective optimization. Future Generation Computer Systems, 107, 49-69.

[24] Porkodi, V., Khan, J., Mohammed, A. S., Bhuvana, J., & Sivaram, M. OPTIMIZED COOPERATIVE QOS ENHANCED DISTRIBUTED MULTIPATH ROUTING PROTOCOL.

[25] Geerthik, S., Venkatraman, S., & Gandhi, R. (2016). AnswerRank: Identifying Right Answers in QA system. International Journal of Electrical and Computer Engineering, 6(4), 1889.

[26] Samad, A., Salima, R., Lydia, E. L., & Shankar, K. (2020). Definition and Features of Rural Marketing Strategies for Encourage Development in Rural Areas. TEST Engineering & Management, 82, 4983-4988.

[27] Palani, E., Nagappan, K., &Alhadidi, B. (2016). Segmentation and Texture Analysis for Efficient Classification of Breast Tumors from Sonograms. Current Signal Transduction Therapy, 11(2), 84-90.

[28] Dhenakaran, S. S., & Naganathan, E. R. (2007). A new approach to multiple symmetric keys. IJCSNS, 7(6), 254-259.

[29] Rajagopal, A., Ramachandran, A., Shankar, K., Khari, M., Jha, S., Lee, Y., & Joshi, G. P. (2020). Fine-tuned residual network-based features with latent variable support vector machine-based optimal scene classification model for unmanned aerial vehicles. IEEE Access, 8, 118396-118404.

[30] Mondragon, V. M., García-Díaz, V., Porcel, C., & Crespo, R. G. (2018). Adaptive contents for

interactive TV guided by machine learning based on predictive sentiment analysis of data. Soft Computing, 22(8), 2731-2752.

[31] Feng, Y., Yu, X., & Wang, G. G. (2019). A Novel Monarch Butterfly Optimization with Global Position Updating Operator for Large-Scale 0-1 Knapsack Problems. Mathematics, 7(11), 1056.

[32] Mohammed, A. S., & Sivaram, P. (2018). Securing the Sensor Networks Along With Secured Routing Protocols for Data Transfer in Wireless Sensor Networks.

[33] Geerthik, S., Venkatraman, S., & Gandhi, K. R. (2016, February). Reward rank: A novel approach for positioning user answers in community question answering system. In 2016 International Conference on Information Communication and Embedded Systems (ICICES) (pp. 1-6). IEEE.

[34] Sivaram, M., Lydia, E. L., Pustokhina, I. V., Pustokhin, D. A., Elhoseny, M., Joshi, G. P., & Shankar, K. (2020). An optimal least square support vector machine based earnings prediction of blockchain financial products. IEEE Access, 8, 120321-120330.

[35] Ghantasala, G. P., &KrishnaRaj, N. Support Vector Machine Based Automatic Mammogram Classification Using Hybrid Optimization Algorithm.

[36] Rajalakshmi, K., & Dhenakaran, S. S. (2015). Analysis of Datamining Prediction Techniques in Healthcare Management System. International Journal of Advanced Research in Computer Science and Software Engineering, 5(4), 1343-1347.

[37] Sikkandar, M. Y., Alrasheadi, B. A., Prakash, N. B., Hemalakshmi, G. R., Mohanarathinam, A., & Shankar, K. (2020). Deep learning based an automated skin lesion segmentation and intelligent classification model. Journal of Ambient Intelligence and Humanized Computing, 1-11.

[38] Zhang, Z., Wang, G. G., Zou, K., & Zhang, J. (2014). A solution quality assessment method for swarm intelligence optimization algorithms. The Scientific World Journal, 2014.

[39] Sivaram, Murugan et al. ‘Data Fusion Using Tabu Crossover Genetic Algorithm in Information Retrieval’. 1 Jan. 2020 : 1 – 10.

[40] Khamparia, A., Pandey, B., Tiwari, S., Gupta, D., Khanna, A., & Rodrigues, J. J. (2020). An integrated hybrid CNN–RNN model for visual description and generation of captions. Circuits, Systems, and Signal Processing, 39(2), 776-788.

[41] Geerthik, S., Gandhi, K. R., &Venkatraman, S. (2016, December). Domain expert ranking for finding domain authoritative users on community question answering sites. In 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-5). IEEE.

[42] Muruganantham, A., Nguyen, P. T., Lydia, E. L., Shankar, K., Hashim, W., &Maseleno, A. (2019). Big data analytics and intelligence: A perspective for health care.

[43] Ramkumar, V., &Krishnaraj, N. Weight Based LSA to Retrieve Information from Web Pages Based On Document Score.

[44] Balakiruthiga, B., Deepalakshmi, P., Mohanty, S. N., Gupta, D., Kumar, P. P., & Shankar, K. (2020). Segment routing based energy aware routing for software defined data center. Cognitive Systems Research.

[45] Chu, H. C., Wang, G. G., & Deng, D. J. (2016). The social networking investigation of metadata of forensic artifacts of a typical WeChat session under Windows. Security and Communication Networks, 9(18), 5698-5709.

[46] Sivaram, M., Yuvaraj, D., Mohammed, A. S., Manikandan, V., Porkodi, V., &Yuvaraj, N. (2019). Improved Enhanced Dbtma with Contention-Aware Admission Control to Improve the Network Performance in Manets. CMC-COMPUTERS MATERIALS & CONTINUA, 60(2), 435-454.

[47] Yasodha, S., & Dhenakaran, S. S. (2014, January). An ontology-based framework for semantic web content mining. In 2014 International Conference on Computer Communication and Informatics (pp. 1-6). IEEE.

[48] Gochhayat, S. P., Lal, C., Sharma, L., Sharma, D. P., Gupta, D., Saucedo, J. A. M., &Kose, U. (2019). Reliable and secure data transfer in IoT networks. Wireless Networks, 1-14.

[49] Subbarayalu, V., Surendiran, B., &Arun Raj Kumar, P. (2019). Hybrid Network Intrusion Detection System for Smart Environments Based on Internet of Things. The Computer Journal, 62(12), 1822-1839.

[50] Rosa, A. T. R., Pustokhina, I. V., Lydia, E. L., Shankar, K., & Huda, M. (2019). Concept of electronic document management system (EDMS) as an efficient tool for storing document. Journal of Critical Reviews, 6(5), 85-90.

[51] Espada, J. P., Diaz, V. G., Crespo, R. G., Bustelo, B. C. P. G., &Lovelle, J. M. C. (2015). An intelligent Mobile Web Browser to adapt the mobile web as a function of the physical environment. IEEE Latin America Transactions, 13(2), 503-509.

[52] Kumar, R. S., Krishnaraj, N., &Keerthana, G. (2017). Assessment of Quality of Service in Communication Network and Evaluating Connectivity Among IP Networks. Asian Journal of

Applied Science and Technology (AJAST), 1(3), 319-322.

[53] Elhoseny, M., Rajan, R. S., Hammoudeh, M., Shankar, K., &Aldabbas, O. (2020). Swarm intelligence–based energy efficient clustering with multihop routing protocol for sustainable wireless sensor networks. International Journal of Distributed Sensor Networks, 16(9), 1550147720949133.

[54] Kumar, P. R., & Dhenakaran, S. S. (2012, December). Pixel based feature extraction for ear biometrics. In 2012 International Conference on Machine Vision and Image Processing (MVIP) (pp. 40-43). IEEE.

[55] Chu, H. C., Wang, G. G., & Park, J. H. (2015). The digital fingerprinting analysis concerning google calendar under ubiquitous mobile computing era. Symmetry, 7(2), 383-394.

[56] Manikandan, V., Sivaram, M., Mohammed, A. S., &Porkodi, V. (2020). Nature Inspired Improved Firefly Algorithm for Node Clustering in WSNs. CMC-COMPUTERS MATERIALS & CONTINUA, 64(2), 753-776.

[57] Kuppusamy, P., Venkatraman, S., Rishikeshan, C. A., & Reddy, Y. P. (2020). Deep learning based energy efficient optimal timetable rescheduling model for intelligent metro transportation systems. Physical Communication, 101131.

[58] Asih, E. S., Nguyen, P. T., Lydia, E. L., Shankar, K., Hashim, W., &Maseleno, A. (2019). Mobile E-commerce website for technology-based buying selling services. International Journal of Engineering and Advanced Technology, 8(6), 884-888.

[59] Lydia, E. L., &Swarup, M. B. (2015). Big data analysis using hadoop components like flume, mapreduce, pig and hive. International Journal of Science, Engineering and Computer Technology, 5(11), 390.

[60] Sengar, S. S., Hariharan, U., &Rajkumar, K. (2020, March). Multimodal Biometric Authentication System using Deep Learning Method. In 2020 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 309-312). IEEE.

[61] Maseleno, A., Hashim, W., Perumal, E., Ilayaraja, M., & Shankar, K. (2020). Access control and classifier-based blockchain technology in e-healthcare applications. In Intelligent Data Security Solutions for e-Health Applications (pp. 151-167). Academic Press.

[62] Li, J., Lei, H., Alavi, A. H., & Wang, G. G. (2020). Elephant Herding Optimization: Variants, Hybrids, and Applications. Mathematics, 8(9), 1415.

[63] Mohammed, A. S., Kareem, S. W., Al Azzawi, A. K., & Sivaram, M. (2018). Time series prediction using SRE-NAR and SRE-ADALINE. Journal of Advanced Research in Dynamical and Control Systems, Pages, 1716-1726.

[64] Shankar, K., Elhoseny, M., Chelvi, E. D., Lakshmanaprabu, S. K., & Wu, W. (2018). An efficient optimal key based chaos function for medical image security. IEEE Access, 6, 77145-77154.

[65] Geerthik, S., Gandhi, R., &Venkatraman, S. (2006). CATEGORY BASED EXPERT RANKING: A NOVEL APPROACH FOR EXPERT IDENTIFICATION IN COMMUNITY QUESTION ANSWERING.

[66] Laxmi, C. V., &Somasundaram, K. (2014). Application Level Scheduling (AppLeS) in Grid with Quality of Service (QoS). International Journal of Grid Computing & Applications, 5(2), 1.

[67] Kumar, R. S., Krishnaraj, N., &Keerthana, G. Highly Energy Efficient and Scalable Distributed Clustering Procedure for Dense Wireless Sensor Networks.

[68] Krishnaraj, N., Kumar, K. A., & Kumar, P. K. (2018). DESIGN OF ADAPTIVE SCHEDULER TO IMPROVE PERFORMANCE OF COMPUTATIONAL GRIDS. International Journal of Pure and Applied Mathematics, 119(18), 1741-1751.

[69] 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.

[70] Kumar, P. R., Sailaja, K. L., Dhenakaran, S. S., & SaiKishore, P. (2012). Chakra: A new approach for symmetric key encryption. In 2012 World Congress on Information and Communication Technologies (pp. 727-732). IEEE.

[71] Wei, C. L., & Wang, G. G. (2020). Hybrid Annealing Krill Herd and Quantum-Behaved Particle Swarm Optimization. Mathematics, 8(9), 1403.

[72] Sivaram, M., Yuvaraj, D., Mohammed, A. S., &Porkodi, V. Estimating the Secret Message in the Digital Image. International Journal of Computer Applications, 975, 8887.

[73] Nieto, Y., Gacía-Díaz, V., Montenegro, C., González, C. C., & Crespo, R. G. (2019). Usage of machine learning for strategic decision making at higher educational institutions. IEEE Access, 7, 75007-75017.